

XIA Configuration Administrator's Guide

Version: 17.0

Table of contents

XIA Configuration Server	10
Installation	11
Server Requirements.....	24
Client and Server Advanced Settings	26
Configure SSL (HTTPS)	28
Server Installation Log Files.....	37
Database Requirements.....	38
Installed Roles and Features	39
Performing your first scan.....	40
Server Installation Troubleshooting.....	44
Server Migration	56
Server Upgrade	76
Technician License Installation Best Practice.....	80
Uninstallation.....	89
Web Server Account.....	100
Compare Items	101
Item Comparison Dialog.....	102
Viewing Results in Excel	106
Compliance Benchmarks	108
Result Types	109
Configuration Settings	110
Automatic Update Settings	111
Cache.....	112
Check Out.....	113
Client Installations.....	115
Custom Sections and Attributes.....	119
Database Settings.....	133
Diagnostics	134
Event Log Settings	135
General Settings	136
Hardware Definitions	137
HTML Editor Settings.....	142
Import Engine Settings.....	144
Item Comparer Settings	145
Item Creation Rules.....	146
Integration.....	151
Item Naming.....	161
Licensing Configuration.....	162

Manual Item Creation	176
Manufacturer Definitions.....	177
Password List.....	180
PDF Output Settings	186
Relationship Settings.....	190
Reporting Settings.....	197
Scheduler.....	198
Security Settings.....	217
SMTP	220
Usage and Diagnostics Data	222
Version Control Settings.....	224
Web Proxy Settings	226
Web Service Settings.....	227
Decommissioned Items	228
Decommissioning Items	229
Recommissioning Items	230
Deleting Items.....	231
Deleted Items.....	232
Diagnostics.....	234
Diagnostics Logs	235
Diagnostics Test Page.....	237
Event Log	238
Filter	239
Entry Types.....	241
Entry Codes	242
Entry Details	244
Toolbar	246
Files	247
Data Files	248
Web.Config.....	251
Generating PDF Documents	252
Generate Documents Dialog	254
Globalization.....	258
Globalization: Date Formats	259
Item Identifiers	260
Item Names	261
Item Types	262
Active Directory Domains.....	263
Azure Tenants	264
Backup Exec Servers.....	265
Citrix XenApp Farms (Classic).....	266
Citrix XenDesktop Sites	267

Containers	268
Customers	270
Disk Shelves.....	271
Entra Directories	272
External Links	273
Generic Network Devices	274
Hyper-V Servers.....	275
IIS Servers	276
Knowledge Base Articles	277
Locations	278
Microsoft DHCP Servers	279
Microsoft DNS Servers	280
Microsoft Exchange Organizations	281
Microsoft Failover Clusters	282
Network Storage Devices	283
Network Switches	285
Password Lists	288
Racks	302
Resources	303
Rooms	305
Software Packages	306
SQL Instances	313
Support Provision.....	314
Tape Libraries.....	315
Terminal Servers	316
Unix Systems	318
VMware Physical ESX Hosts	322
VMware Systems.....	323
Windows Machines.....	324
Location Hierarchy.....	341
Assigning Locations	342
Main Page	344
Managed Service Providers	345
MSP Deployment Topology.....	346
MSP Configuration Guidelines	347
Manual Data Upload.....	349
Manually Creating Items.....	352
Mobile Support.....	355
Organization Hierarchy.....	356
Assigning Parent Containers	357
Reporting	359
Reports	360
Report Binders	403

Report Folders	418
Scheduler Service	427
Configuring Client Certificates	428
Importing Data	431
Scheduler Configuration Tool.....	432
Scheduler Registry Keys	434
Scheduler Service Details	435
SDK.....	436
Web Services SDK.....	437
Search	573
Default Search Fields.....	574
Advanced Search Menu	575
Search by Container	576
Search by Type	577
Search by Location	578
Security	579
Authentication	580
Granting Access.....	586
System Administrators	589
User Access Control (UAC)	590
Server Troubleshooting	592
A blank page is displayed	593
Access to this XIA Configuration System has been denied by ACL	594
Could not execute the report with ID 'XXXX'. Timeout expired.....	596
Error decrypting string value.....	597
HTTP Error 401.1 - Unauthorized	598
HTTP Error 401.1 - Unauthorized (locally only).....	600
HTTP Error 401.2 - You are not authorized to view this page due to invalid authentication headers ..	602
HTTP Error 500.0 - Internal Server Error	604
HTTP Error 500.19 - This configuration section cannot be used at this path	607
The 'PRIMARY' filegroup is full	609
This page can't be displayed	610
Uploading of data to the server fails.....	611
You are prompted for a password when you attempt to access the web interface	612
ServiceNow Integration	613
Supported Item Types	614
Technical Reference	616
Credentials and Security Contexts Overview	617
GUID	618
Viewing and Editing Items	619
Checking Out Items	620
Custom Sections.....	621

General Information.....	622
Client Information	624
Editing Items	626
Effective Permissions	627
Location.....	628
Manually Updating Environment Identifiers.....	629
Relationships.....	630
Renaming Items	638
Save as XML.....	639
Security Descriptor	640
ServiceNow Synchronization.....	645
Support Provisions	648
Version History.....	649
Web Controls.....	654
Advanced Upload Control	655
Date Picker	657
HTML Editor	659
Schedule	678
XIA Configuration Client.....	683
Installation	684
Automatic Updates	691
Client Migration	692
Client Requirements.....	694
Client Advanced Settings.....	696
Client Installation Troubleshooting.....	698
Configuring Client Certificates	700
Client Installation Log Files.....	704
Installed Roles and Features	705
Unattended Installation	706
Uninstallation.....	709
Service Account	715
Changing the Service Account.....	716
Changing the Service Account Password	720
Managed Service Accounts	721
Administration Tools	722
Connecting to a Service.....	723
Diagnostics Log Viewer	725
Menu	726
Opening Data Files	732
Scan Monitor.....	734
Service Information.....	735
Service Settings	736

Scan Results Files	753
Compliance Benchmarks	765
Custom Titles.....	766
PowerShell Connection Settings.....	767
Scan Profiles	769
General.....	771
Credentials	772
Default Agent Settings	774
Server Upload.....	776
File Output	777
Exclusions.....	780
Email Notifications	783
Performance.....	789
Scan Schedules	790
Context Menu	791
Scan Schedule Settings.....	792
Scan Tasks.....	799
Active Directory Domain	800
Active Directory Search.....	831
Azure Tenants	840
Backup Exec Server	873
Citrix XenApp Farm (Classic)	889
Citrix XenDesktop Site.....	910
CSV File Search	934
Entra Directory	940
Generic Network Device	962
Hyper-V Server	971
IIS Server	982
Microsoft 365 Organization	999
Microsoft DHCP Server.....	1011
Microsoft DNS Server	1024
Microsoft Exchange Organization	1039
Microsoft Failover Cluster	1088
Microsoft Network Load Balancing Cluster.....	1099
Network Device Search Scan Task.....	1111
Network Range Search (WMI).....	1117
Network Storage Device.....	1122
Network Switch	1130
SQL Database Search.....	1144
SQL Instance.....	1152
Terminal (RDP Session Host) Server.....	1182
Unix System.....	1189
VMware System	1209

Windows Machine	1228
WINS Service	1336
General Settings	1345
Context Menu	1346
SDK.....	1348
Dynamic Agent Plugins.....	1349
SSH Settings	1391
Advanced Settings.....	1393
SNMP Settings	1395
SNMP v3 Security Settings	1397
Tools	1399
Microsoft Online Agent UI	1400
Microsoft Service Principal Creation Tool.....	1417
SNMP Data Collector.....	1419
Troubleshooting	1426
Diagnostics Trace	1427
Windows Management Instrumentation (WMI)	1428
Common Issues	1437
PowerShell Remoting	1458
Server Connections	1474
XIA Configuration Local Service	1479
Group Policy	1480
Local Service Settings	1484
Requirements.....	1485
Troubleshooting.....	1486
XIA Configuration Express.....	1488
Installation	1489
System Requirements	1493
Uninstallation.....	1494
Active Directory Computer Browser.....	1499
Advanced Settings	1500
Credentials Form	1501
Default Agent Settings.....	1502
Compare Items	1503
Default PDF Options	1505
PDF Branding Settings	1506
PDF Colors	1508
Quick Start	1509
Scanning.....	1510
Active Directory Domain	1511
Azure Tenant	1512

BackupExec Server	1513
Citrix XenApp (Classic) Farm	1514
Citrix XenDesktop Site	1515
Entra Directory	1516
Generic Network Device	1517
Hyper-V Server	1518
IIS Server	1519
Microsoft DHCP Server	1520
Microsoft DNS Server	1521
Microsoft Exchange On-Premises	1522
Microsoft Exchange Online	1524
Microsoft Failover Cluster	1525
Microsoft Network Load Balancing Cluster	1526
Network Storage Device	1527
Network Switch	1528
SQL Instance	1529
Terminal (RDP) Server	1530
Unix System	1531
Windows Machine	1532
WINS Service	1533
VMware System	1534
Scan Data	1535
Item Data Viewer	1536
Scan Data Context Menu	1537
Scan Data Actions Context Menu	1539
Scan Result Logs	1540
Scan Result Details	1542
Scan Result Log Context Menu	1543
End User License Agreement (EULA)	1544

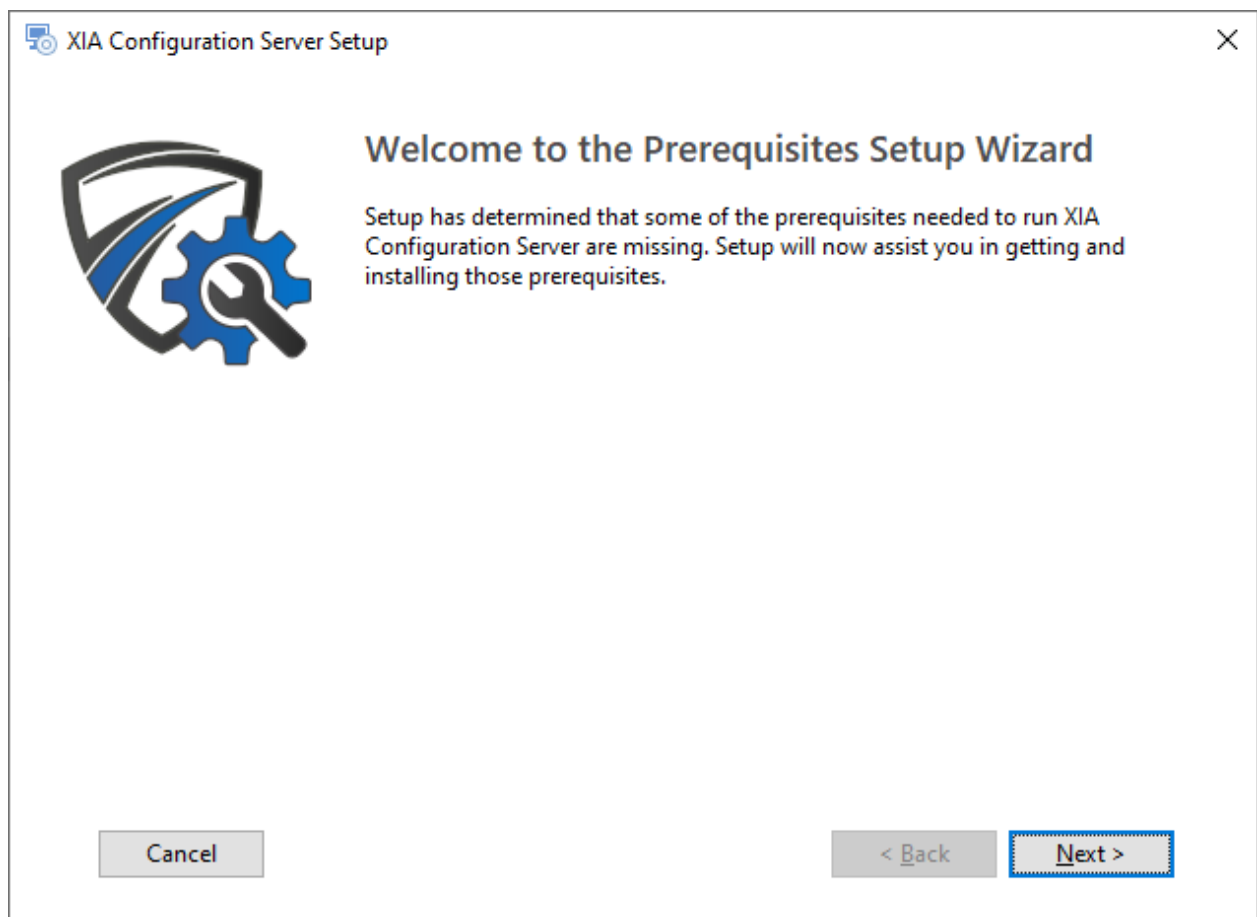
XIA Configuration Server

XIA Configuration Server is a network documentation tool which automates the audit, inventory and documentation of your IT infrastructure including [reporting](#), analysis and [change tracking](#).

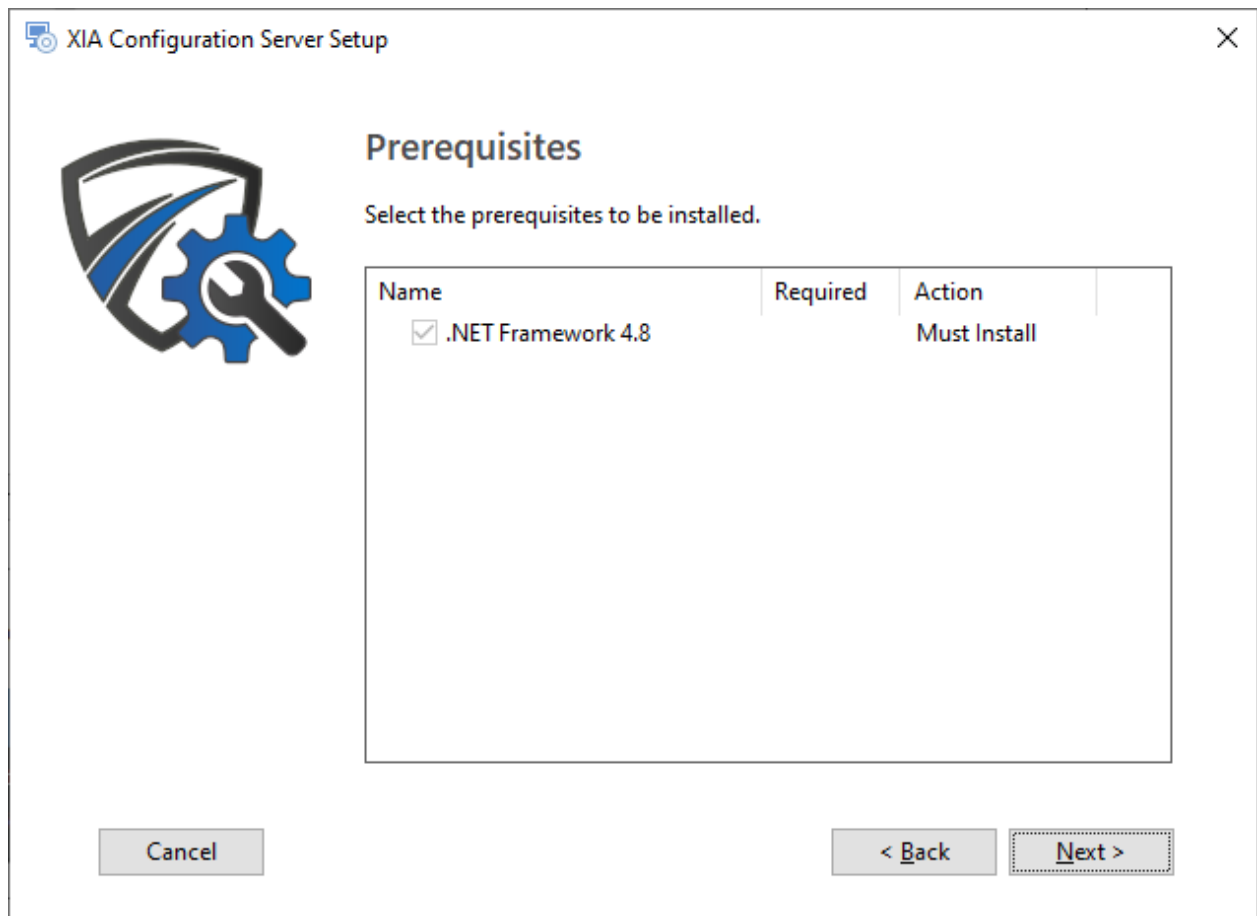
Installation

This section describes the installation process of [XIA Configuration Server](#). For information about the removal of the product see the [uninstallation](#) section.

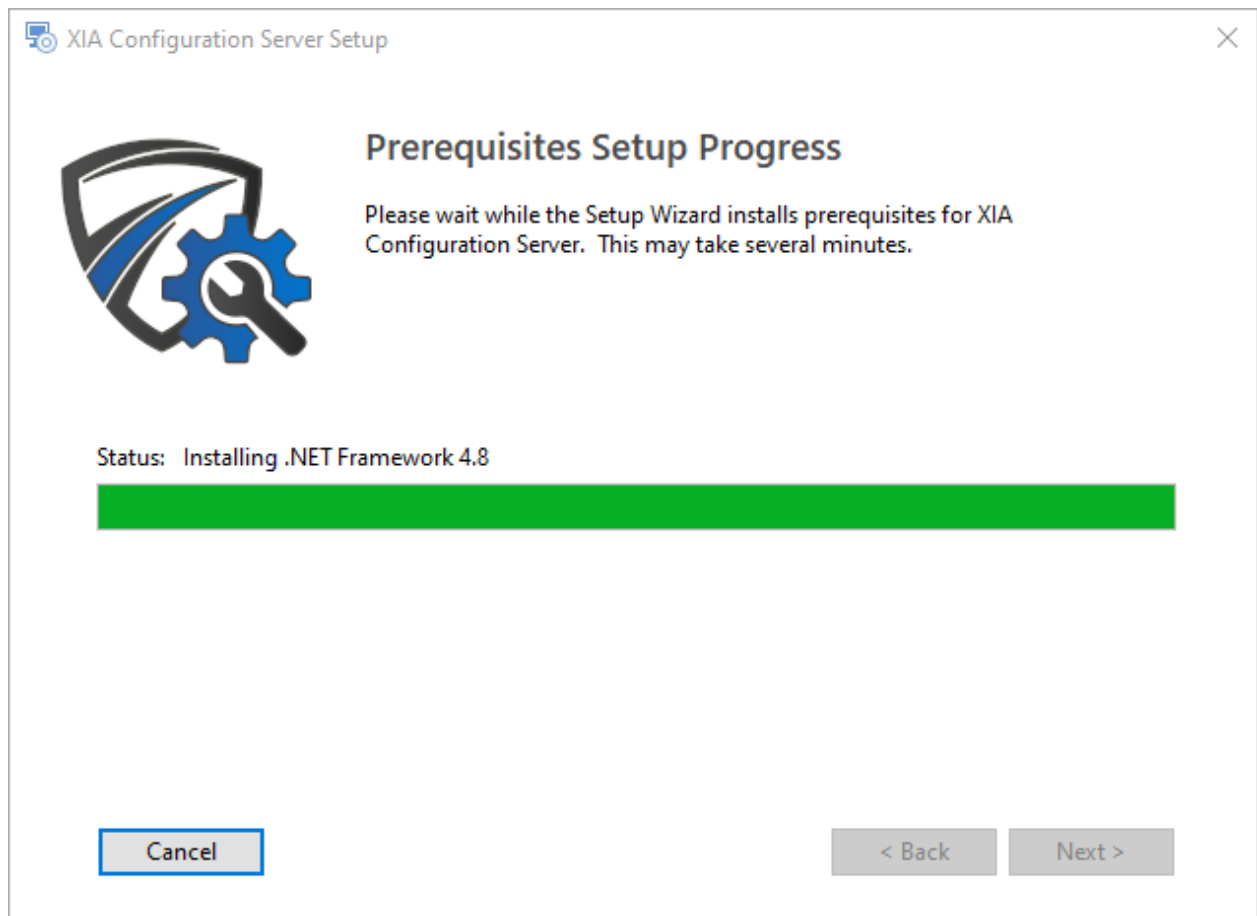
- Download the latest [installation package](#).
- Ensure you have an appropriate license file, or [request a trial license](#).
- Review the [roles and features](#) that will be automatically installed.
- Check that the system you are installing on meets the [server requirements](#).
- Check that you have a database server that meets the [database requirements](#).
- Start the installer.
- If the [.NET Framework 4.8](#) is not installed the *Prerequisites Setup Wizard* will be displayed.



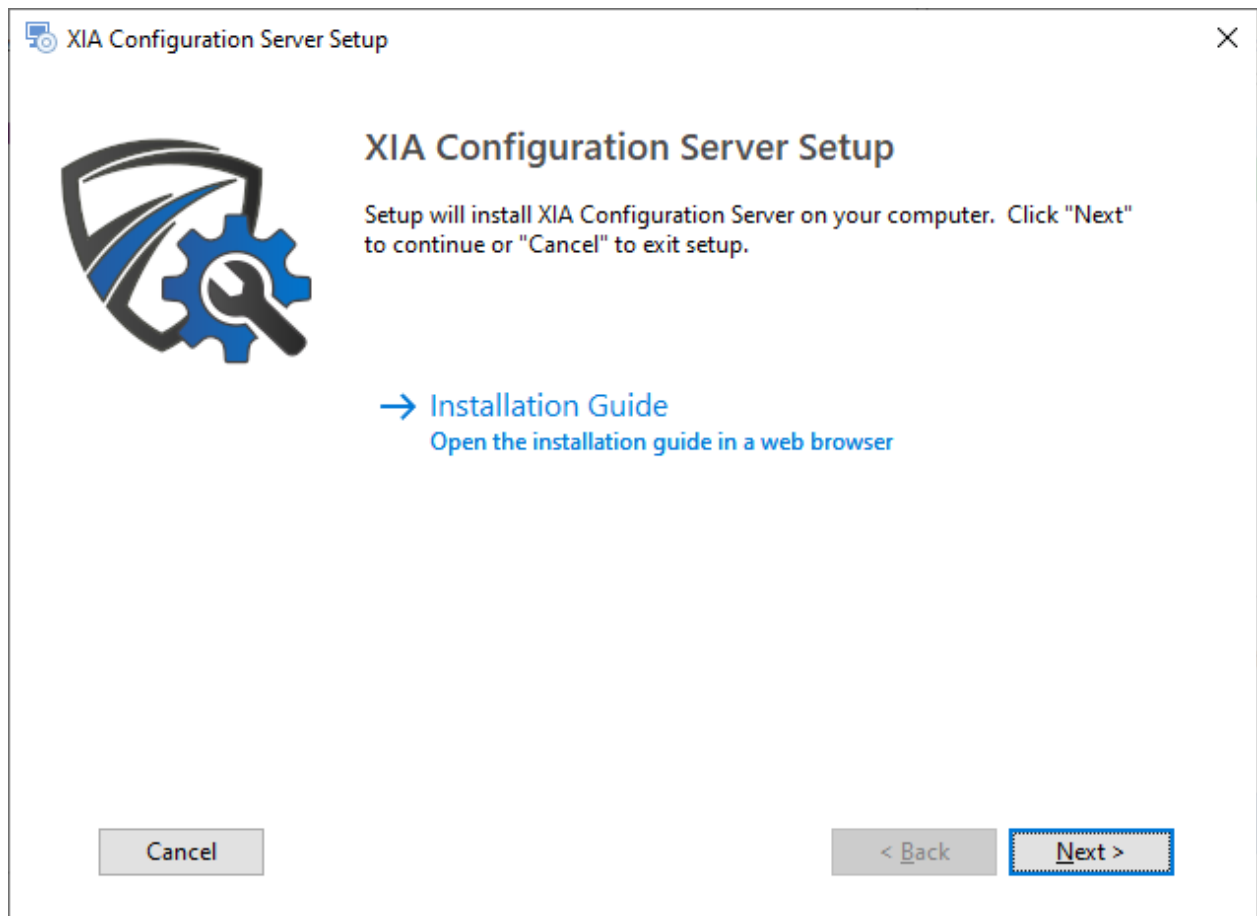
- You will be prompted to install the [.NET Framework 4.8](#) as required.



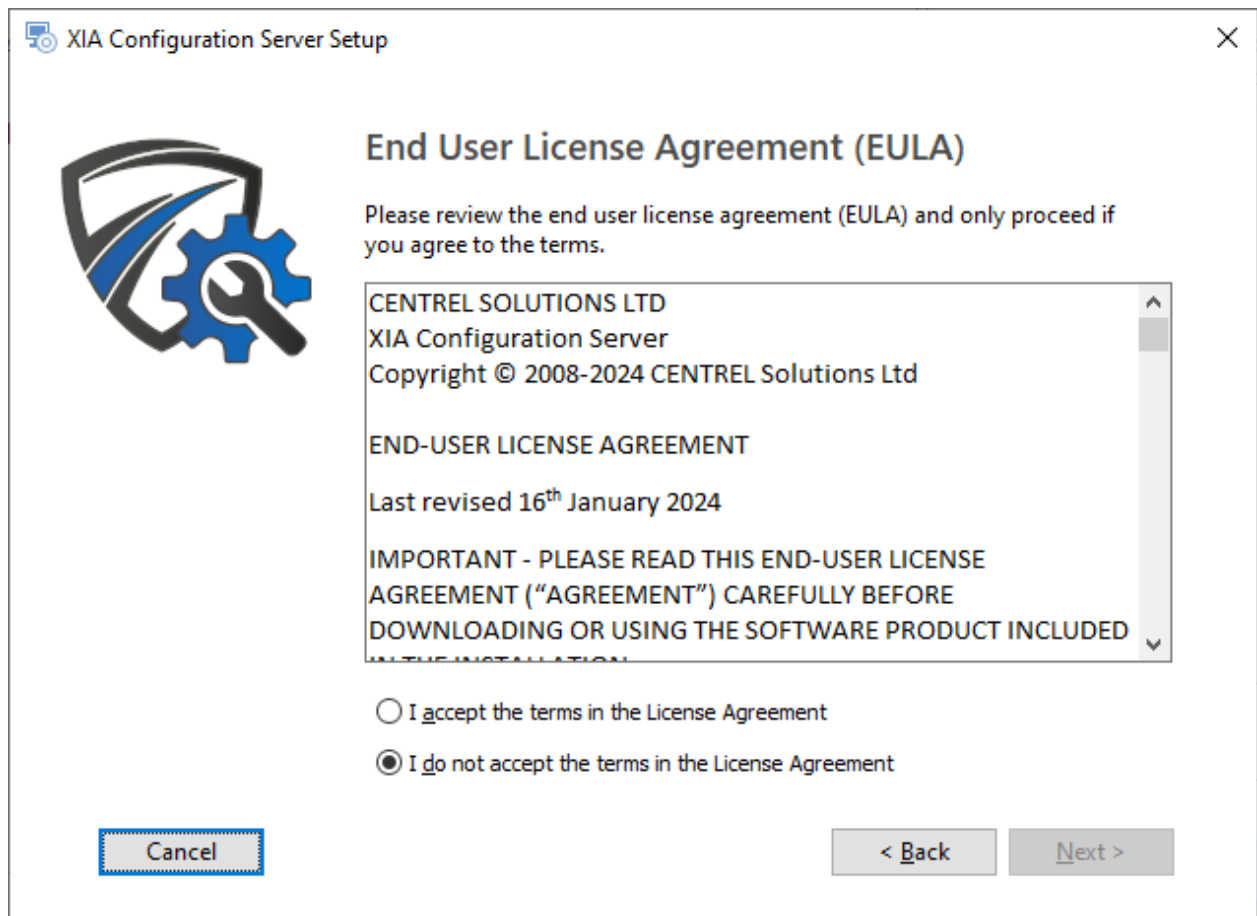
- The [.NET Framework 4.8](#) will be installed and a [log file](#) created for the installation.



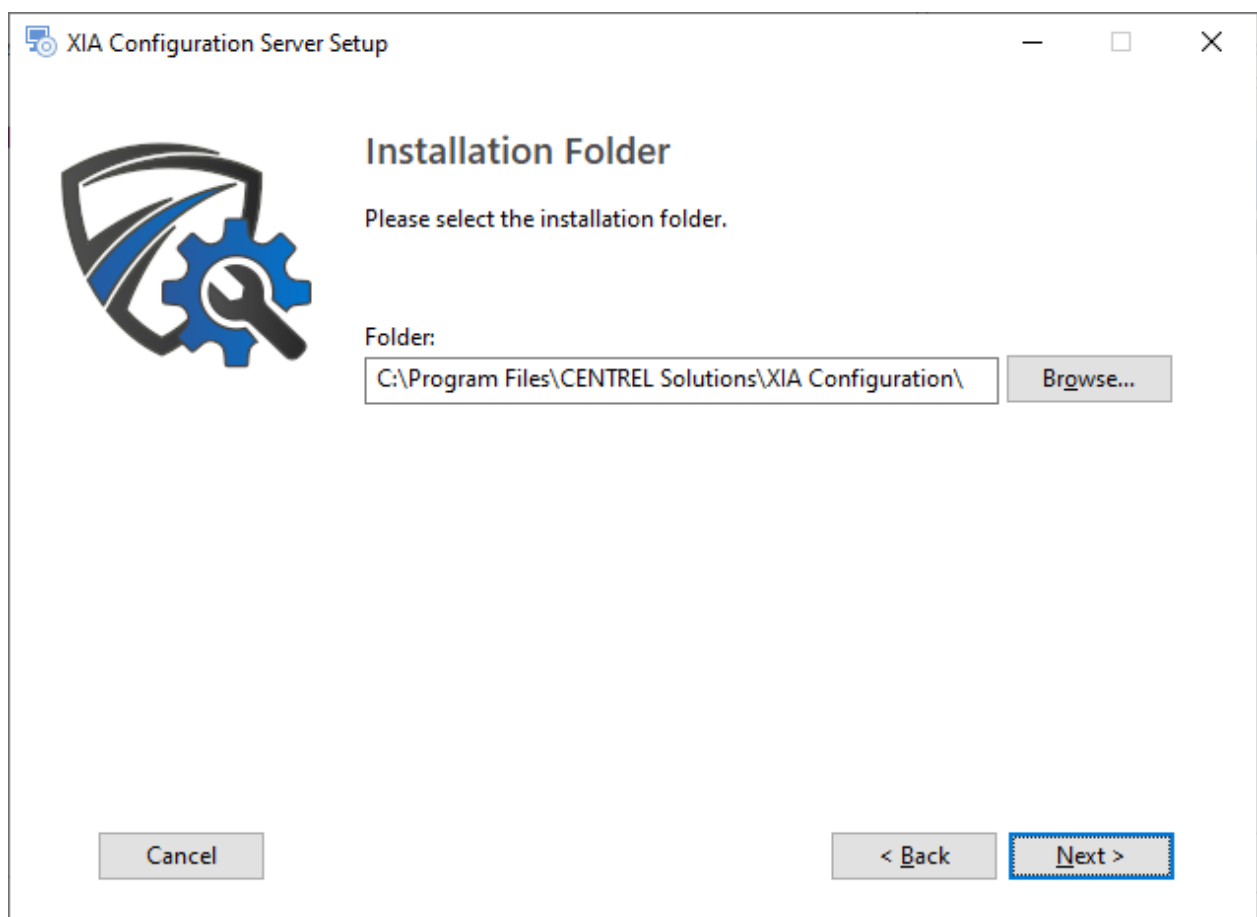
- You may be required to reboot to continue the installation. The installation will resume automatically after logging in following the reboot.
- The main installation screen will then be displayed.



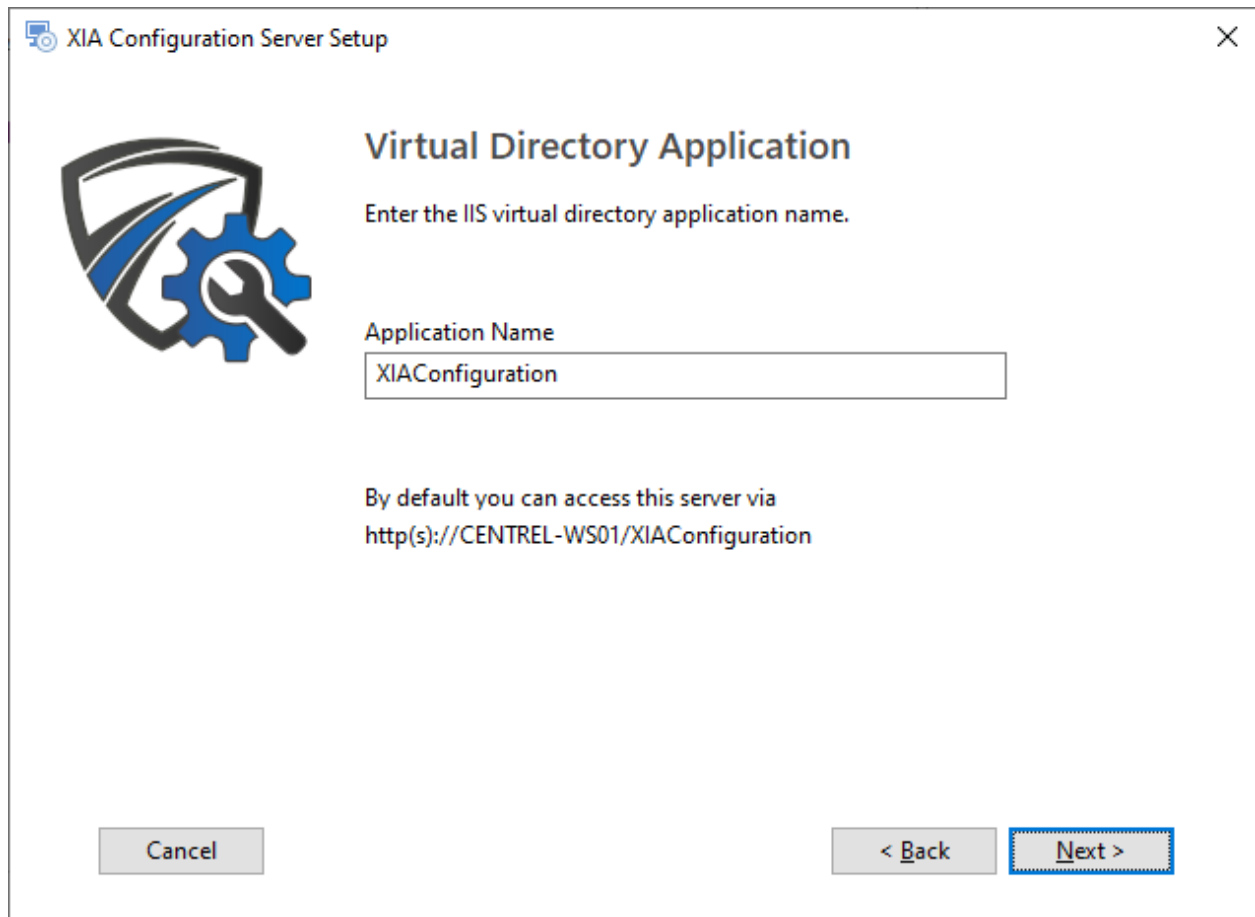
- Review the [End User License Agreement \(EULA\)](#) and only accept if you agree to the terms. If you do not accept the terms of the agreement please cancel the installation.



- Select the directory into which [XIA Configuration Server](#) should be installed and click *Next*.



- Enter the application name, this is used to form the URL at which [XIA Configuration Server](#) can be accessed and click *Next*.



The image shows a Windows-style dialog box titled "XIA Configuration Server Setup". On the left is a logo featuring a shield and a gear. The main heading is "Virtual Directory Application". Below this, it says "Enter the IIS virtual directory application name." There is a text input field labeled "Application Name" containing the text "XIAConfiguration". Below the input field, it says "By default you can access this server via" followed by the URL "http(s)://CENTREL-WS01/XIAConfiguration". At the bottom, there are three buttons: "Cancel", "< Back", and "Next >". The "Next >" button is highlighted with a blue dashed border.

XIA Configuration Server Setup

Virtual Directory Application

Enter the IIS virtual directory application name.

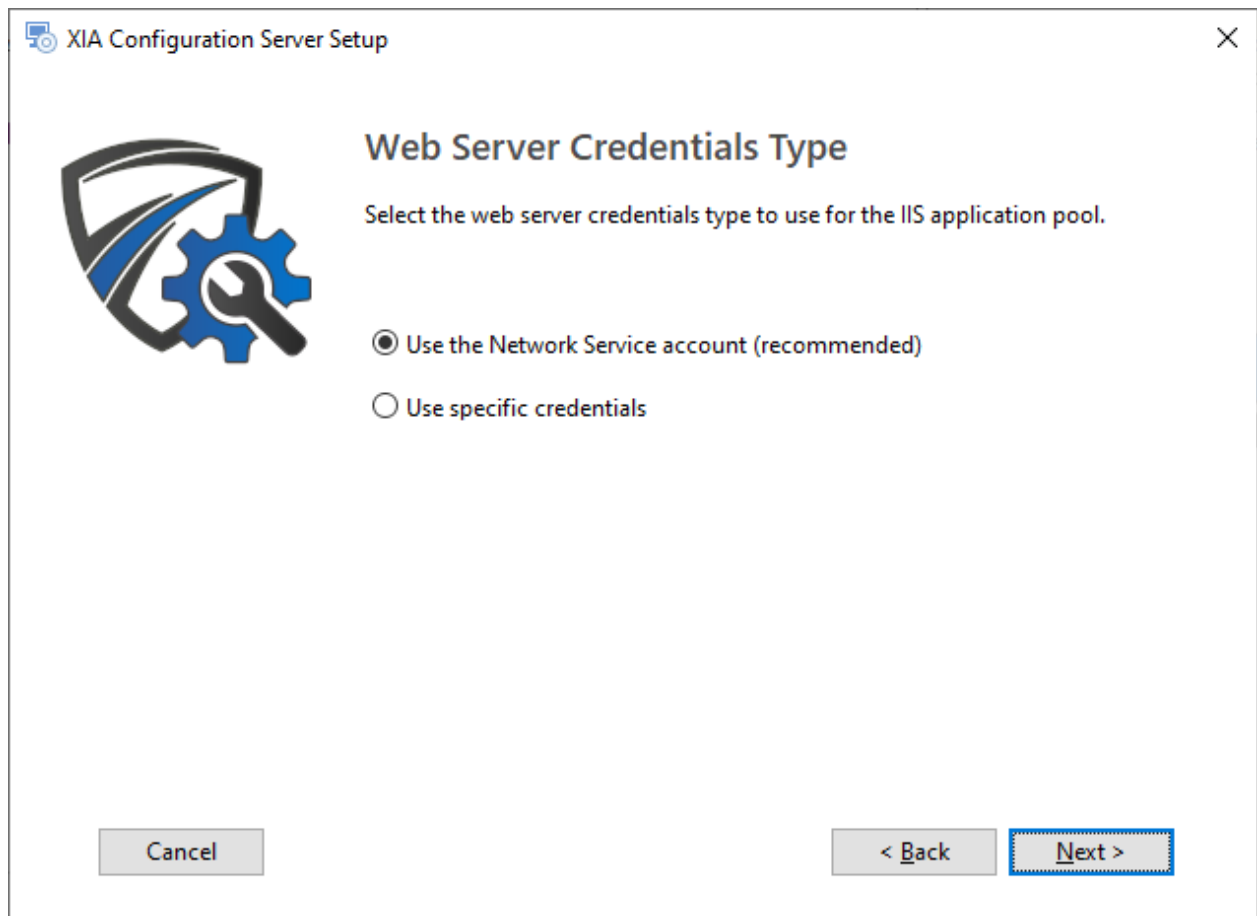
Application Name

XIAConfiguration

By default you can access this server via
http(s)://CENTREL-WS01/XIAConfiguration

Cancel < Back Next >

- Determine whether to use the [Network Service](#) account as the [web server account](#) (recommended) or whether to use a specific account.



- If *Use specific credentials* was selected then enter the credentials for the [web server account](#) and click *Validate Credentials* to validate the account, and then click *Next*.

XIA Configuration Server Setup

Web Server Credentials

These credentials are used for web server and access to the SQL Server database. They are not used for scanning items and require only minimal privileges.

Username
XiaConfigurationServer

Domain
DEMONSTRATION

Password
●●●●●●●●●●

Validate Credentials

Cancel < Back Next >

- Select or enter the instance name of a local or remote [Microsoft SQL Server](#) that meets the [database requirements](#).
- Enter the database name and click *Validate*, and then click *Next*.

XIA Configuration Server Setup

Database Settings

Enter the database settings used by XIA Configuration Server.

SQL Instance Name
(local)SQLEXPRESS

Database Name
XIAConfiguration

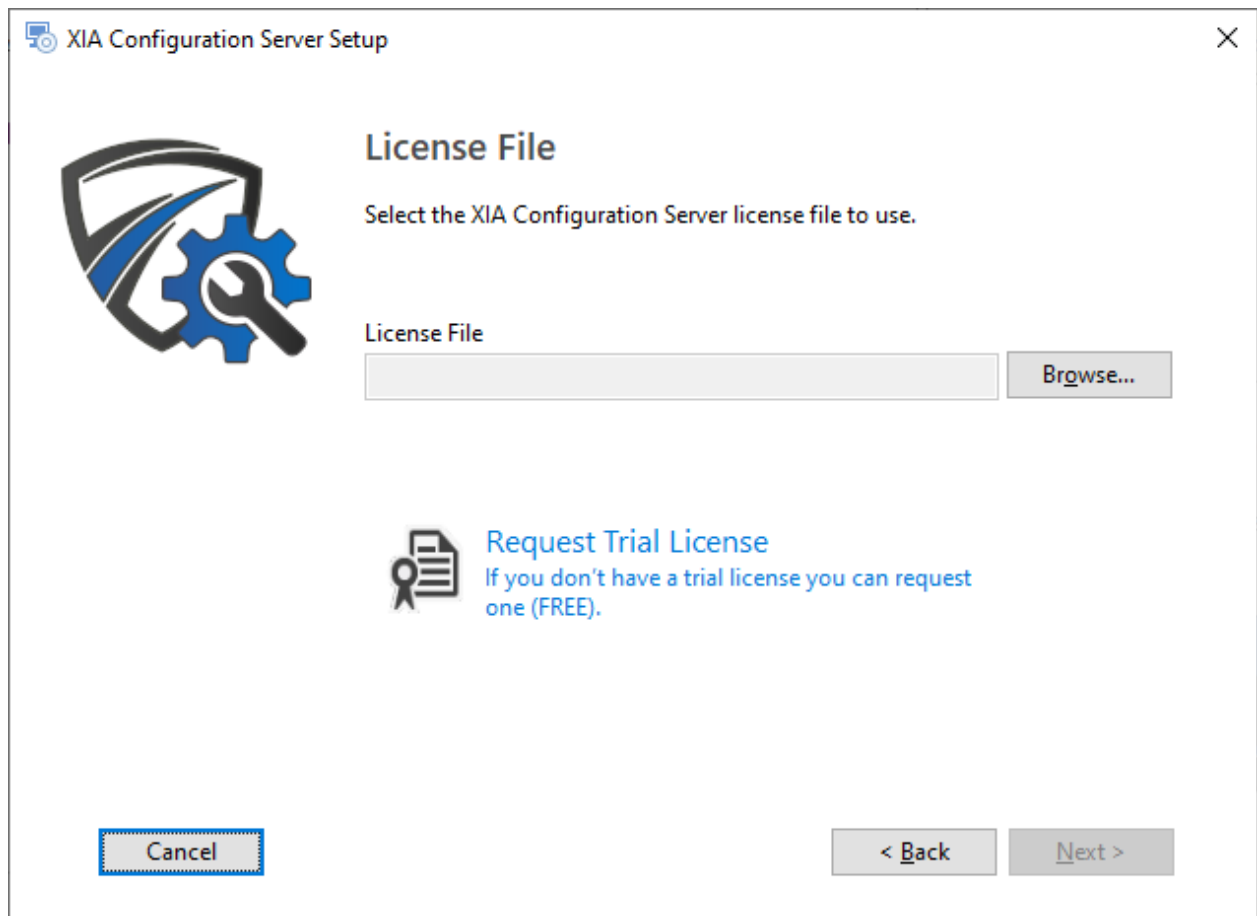
☐ Use existing database, preserving the schema

Validate

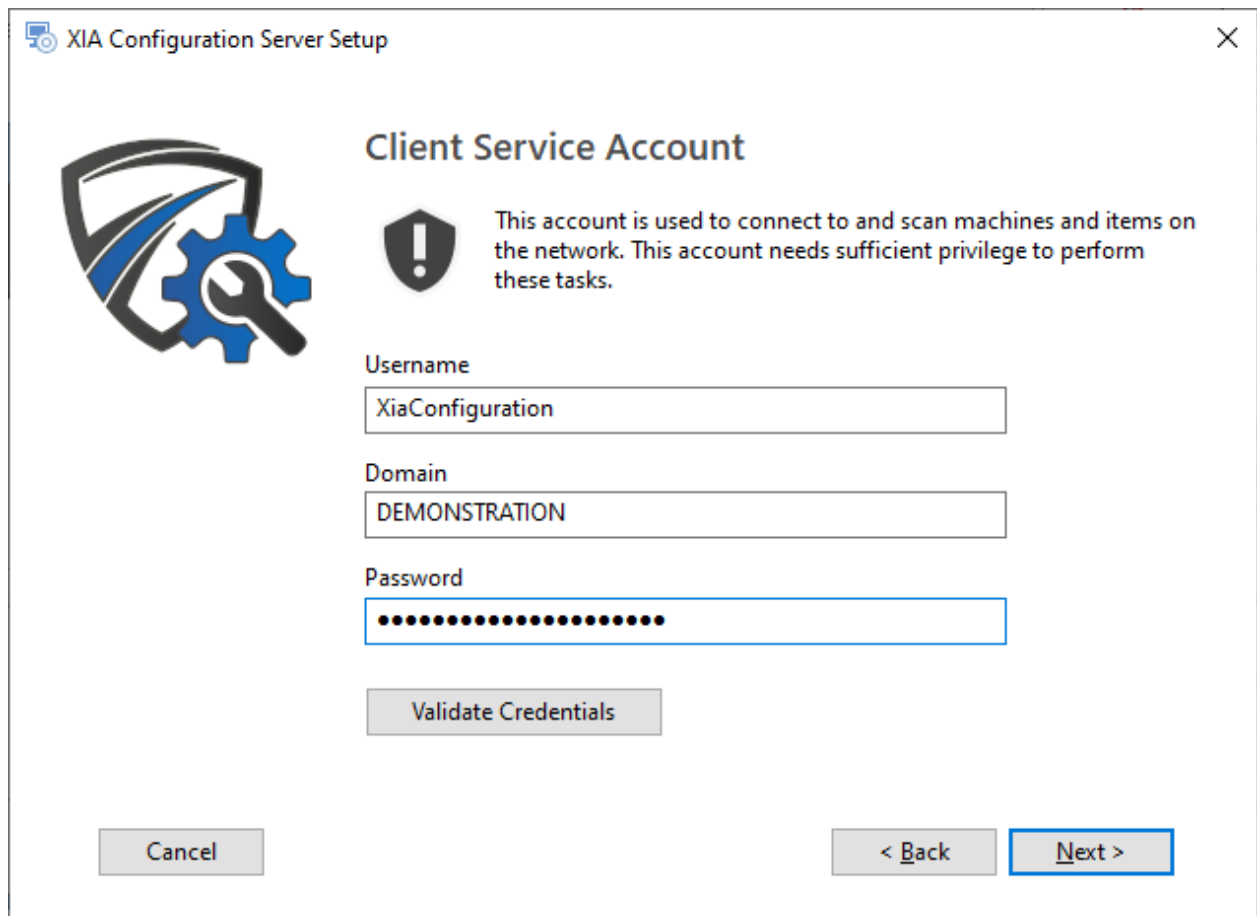
 **SQL Express**
If you don't have SQL Server you can download SQL Express (FREE).

Cancel < Back Next >

- If you do not have [Microsoft SQL Server](#) installed you can [download Microsoft SQL Express](#) for free.
- Click *Browse* to browse for the [trial](#) or [production license](#) file you have been provided. If you do not have a [license](#) you can [request a trial license](#).



- Select the [trial](#) or [production license](#) file you have been provided (this must have a .licx extension) and click *Open* and then click *Next*.
- Enter the credentials to use for the [service account](#), this is the account that will by default be performing the scans of devices and click *Validate*.



XIA Configuration Server Setup

Client Service Account

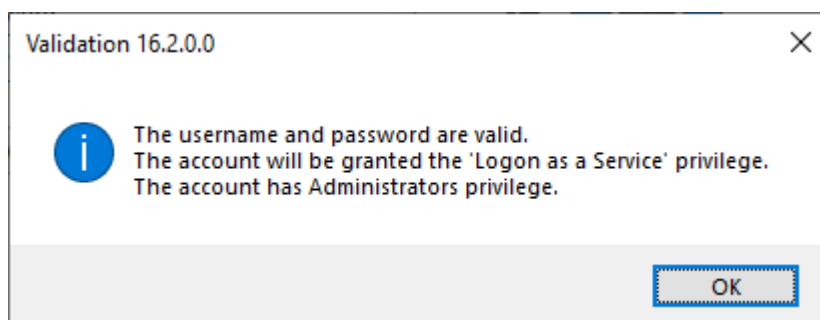
This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks.

Username:

Domain:

Password:

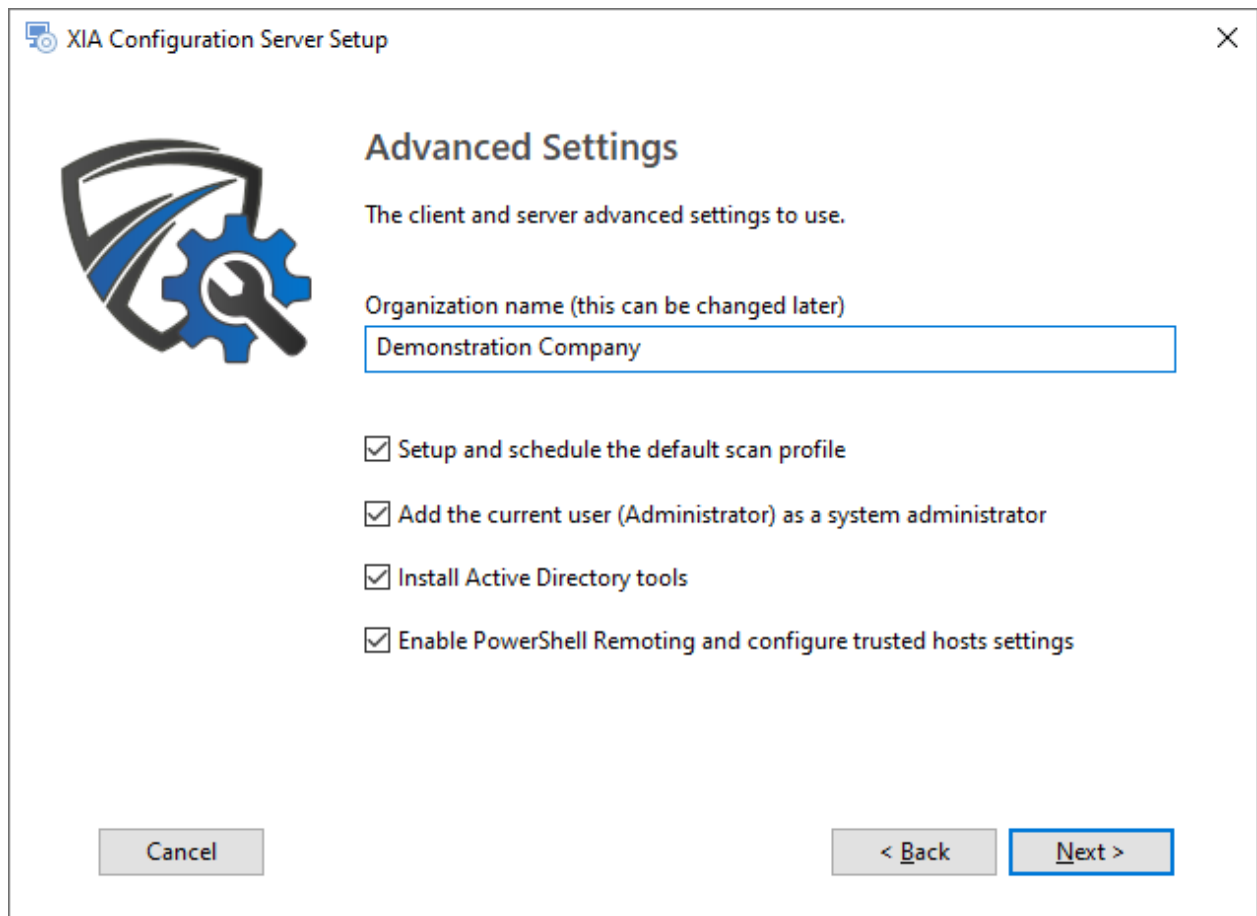
- **NOTE:** When using a computer on a WORKGROUP enter the computer name in the *Domain* field.
- Confirm that the account has the appropriate permissions and click *OK*, then click *Next*.



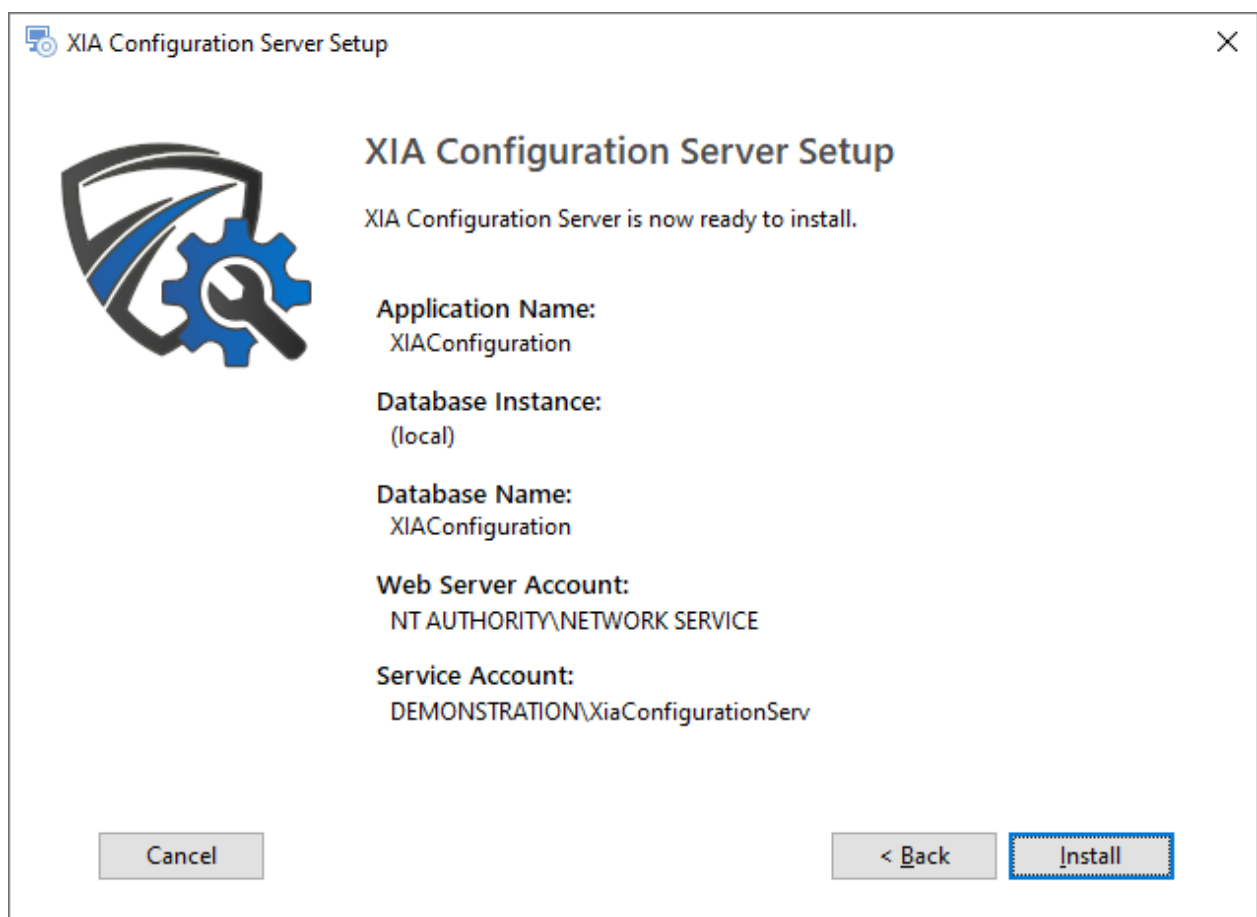
Validation 16.2.0.0

The username and password are valid.
The account will be granted the 'Logon as a Service' privilege.
The account has Administrators privilege.

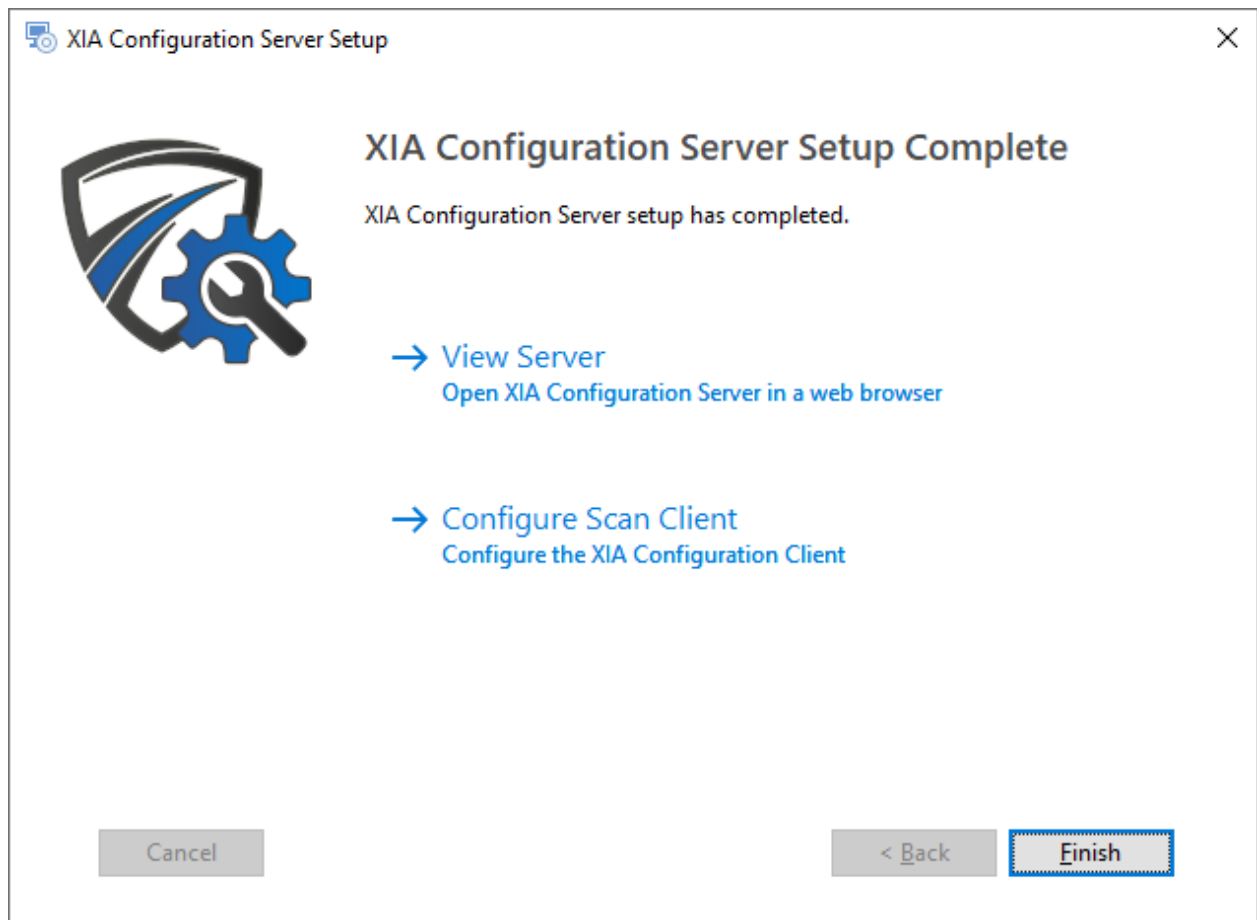
- Determine the appropriate [advanced settings](#) and click *Next*.



- Click *Install* to begin the installation.



- When the installation is complete you will be prompted to [View Server](#) or [Configure Scan Client](#).



- If you experience any issues please see the [server installation issues](#) section.
- For more information, view the [performing your first scan](#) section.

Server Requirements

This section describes the requirements for the [installation](#) of [XIA Configuration Server](#).

Operating Systems (Server)

The following operating systems are supported for installation of a production version of [XIA Configuration Server](#):

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Desktop Operating Systems

The following desktop operating systems are supported for testing purposes and single user technician license installations:

- Windows 11 Pro (64-bit)
- Windows 10 Pro Anniversary Edition (64-bit)

.NET Framework

- [.NET Framework 4.8](#) * (*installed automatically*) **

ODBC Driver

- [Microsoft® ODBC Driver 18 for SQL Server®](#) (installed automatically) *

Windows Management Framework

- [Window Management Framework 5.1](#) (pre-installed on Windows 10, Windows Server 2016 and above).

Internet Information Server

- Internet Information Server * (installed automatically)

Acrobat Reader

- It is recommended that [Acrobat Reader](#) is installed on the machine running [XIA Configuration Server](#) to allow the viewing of generated documentation.

SQL Server

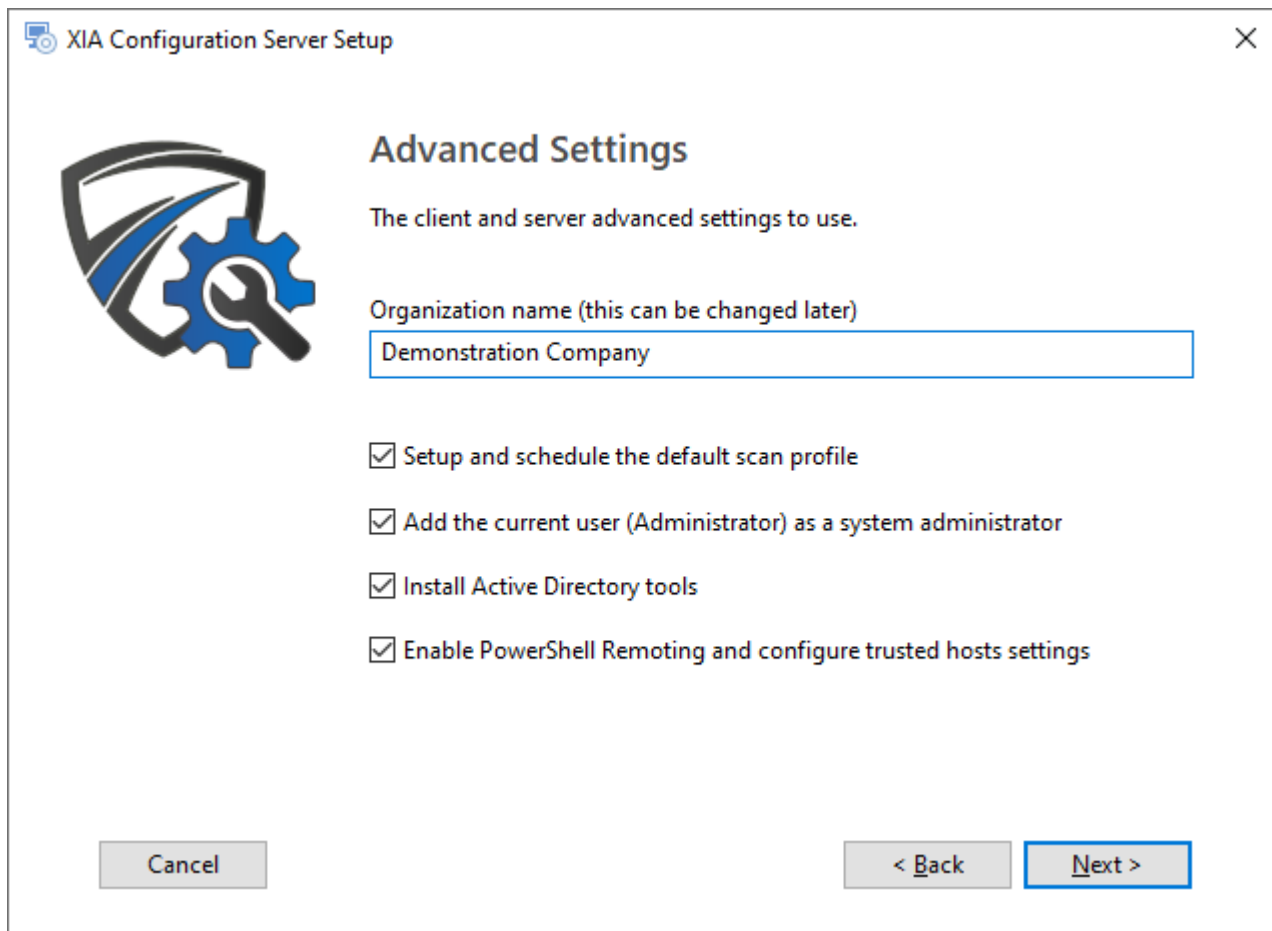
- A [Microsoft SQL server](#) is required - for more information see the [database requirements](#) section.

** This prerequisite is a shared component and not removed when the product is [uninstalled](#).*

*** Please see the [Microsoft .NET Framework 4.8 installation requirements](#) for further information.*

Client and Server Advanced Settings

When installing XIA Configuration Server the following client and server advanced settings are presented.



The screenshot shows a Windows-style dialog box titled "XIA Configuration Server Setup" with a close button (X) in the top right corner. On the left is a shield icon with a gear and a wrench. The main heading is "Advanced Settings". Below it is the text "The client and server advanced settings to use." There is a text input field for "Organization name (this can be changed later)" containing the text "Demonstration Company". Below this are four checked checkboxes: "Setup and schedule the default scan profile", "Add the current user (Administrator) as a system administrator", "Install Active Directory tools", and "Enable PowerShell Remoting and configure trusted hosts settings". At the bottom are three buttons: "Cancel", "< Back", and "Next >".

Organization name

This determines the organization that will be set automatically as the [root container name](#), branding in the [browser title](#), and text in the [PDF footer](#). This can be changed later in the [configuration settings](#). This has no effect if the *Use existing database* setting was checked during the installation.

Setup and schedule the default scan profile

Determines whether the [installation](#) should create a [scan profile](#) which is [scheduled](#) to automatically scan common [items](#).

Add the current user ([Account Name]) as a system administrator

Determines whether the user performing the installation should be automatically added as a [system administrator](#).

Install Active Directory tools

Determines whether the [installation](#) should install the following Active Directory tools that are required by the [Active Directory](#) agent.

- Active Directory module for Windows PowerShell (RSAT-AD-PowerShell)
- DFS Management Tools (RSAT-DFS-Mgmt-Con)
- Group Policy Management (GPMC)

Enable PowerShell Remoting and configure trusted hosts settings

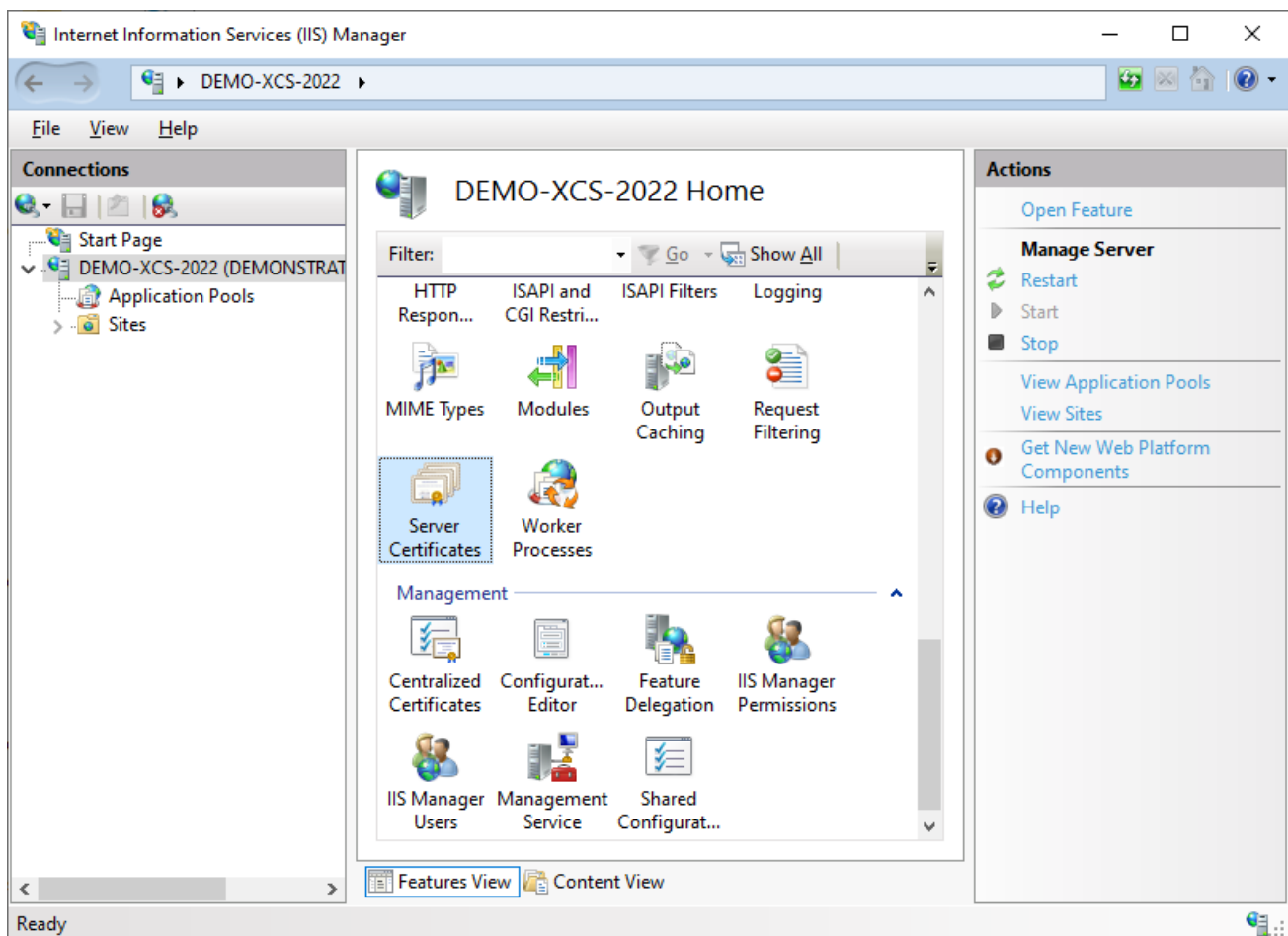
Determines whether the [installation](#) should enable [PowerShell remoting](#) on the local machine, and configure the [trusted hosts](#) setting to allow connections to any host.

Configure SSL (HTTPS)

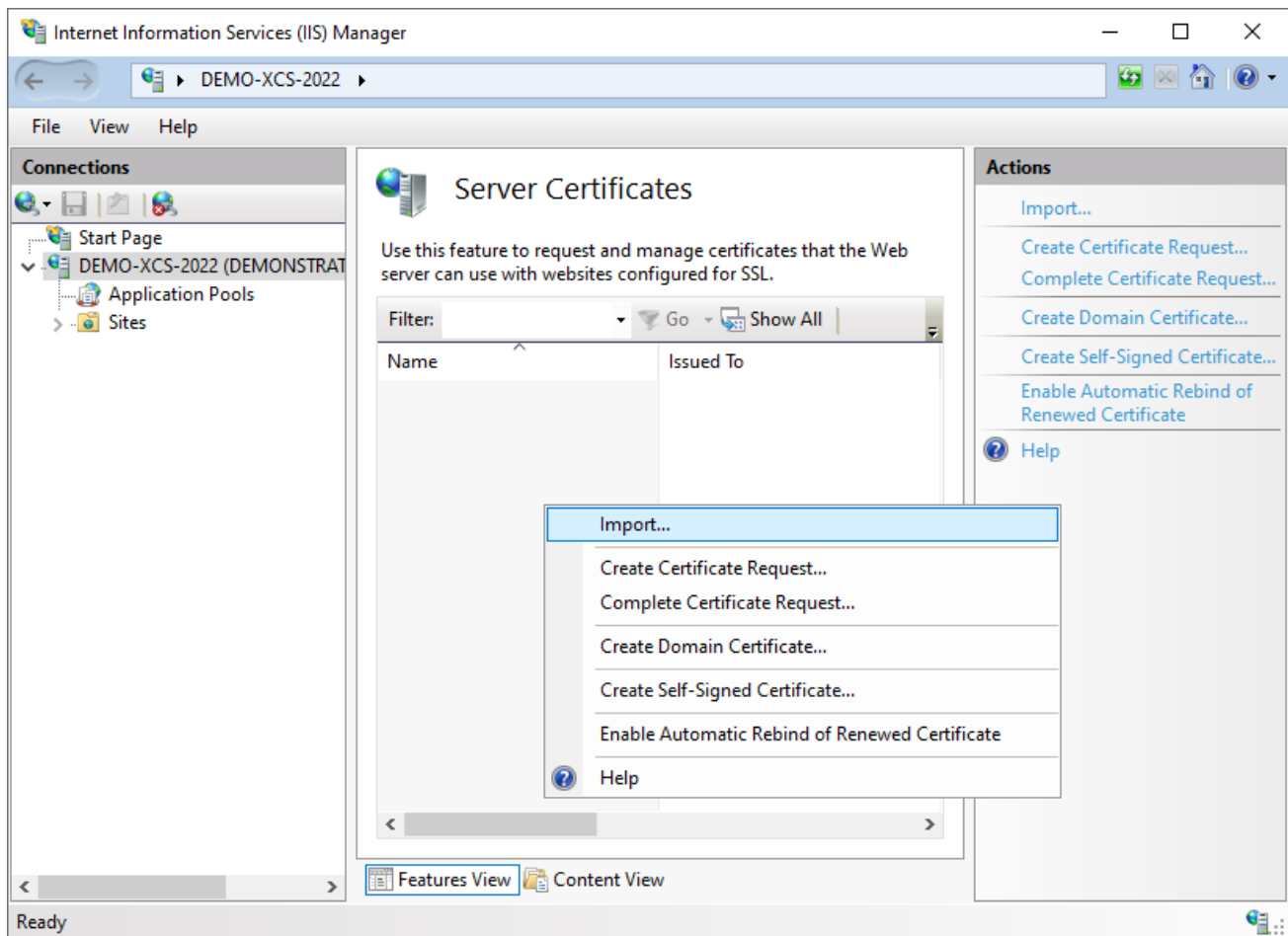
To configure [XIA Configuration Server](#) to use SSL complete the following steps.

NOTE: This section is for guidance only, for more information review the documentation for the version of [Internet Information Server \(IIS\)](#) in use.

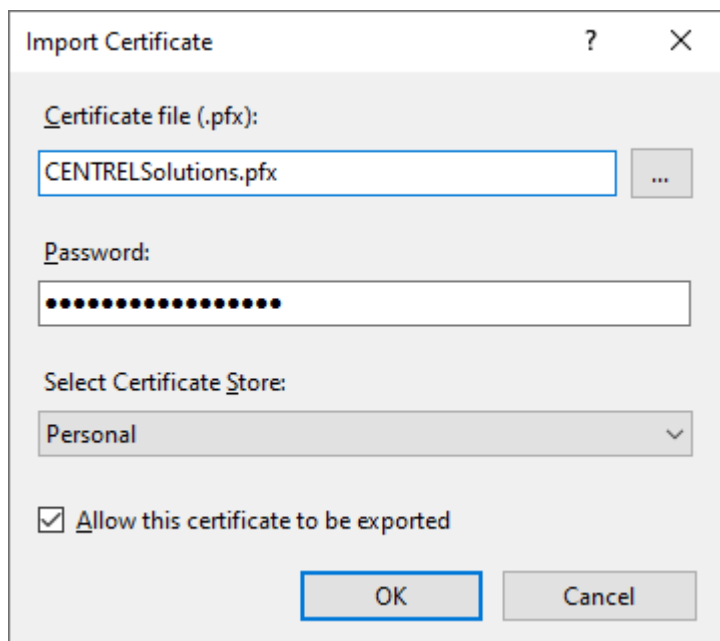
- An SSL certificate in .pfx format is required before proceeding - this can be generated by your network administrator or purchased from a 3rd party.
- Open the [Internet Information Server \(IIS\)](#) Manager tool.
- Select the server node, then double click *Server Certificates*.



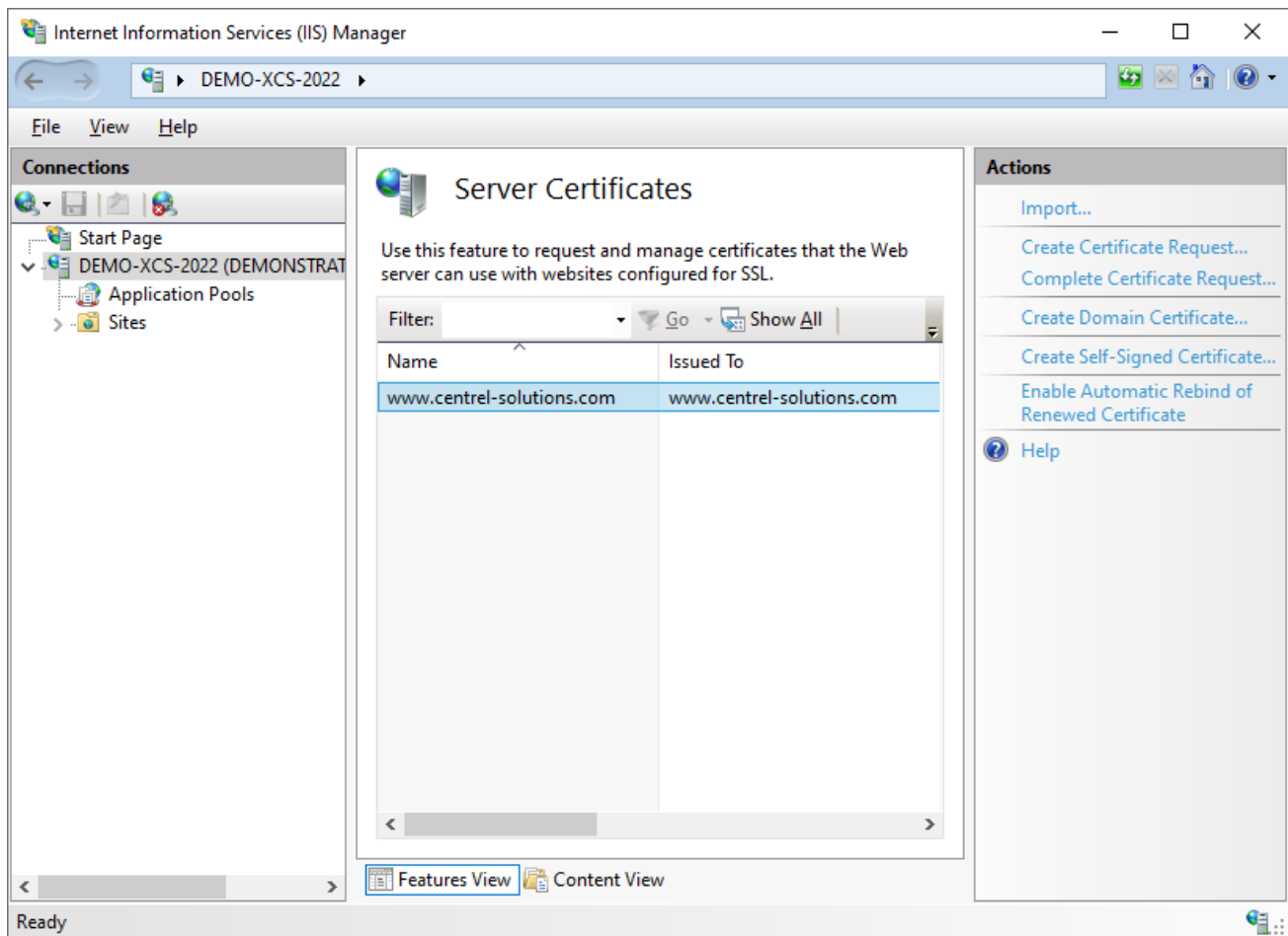
- Right click and select *Import*



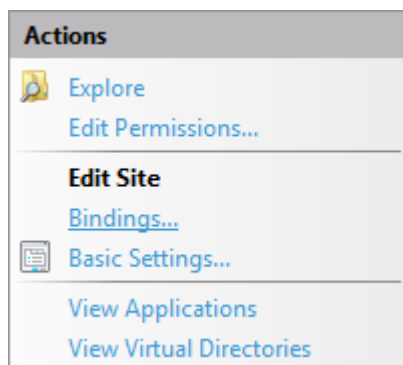
- Browse to the SSL certificate and enter the password.



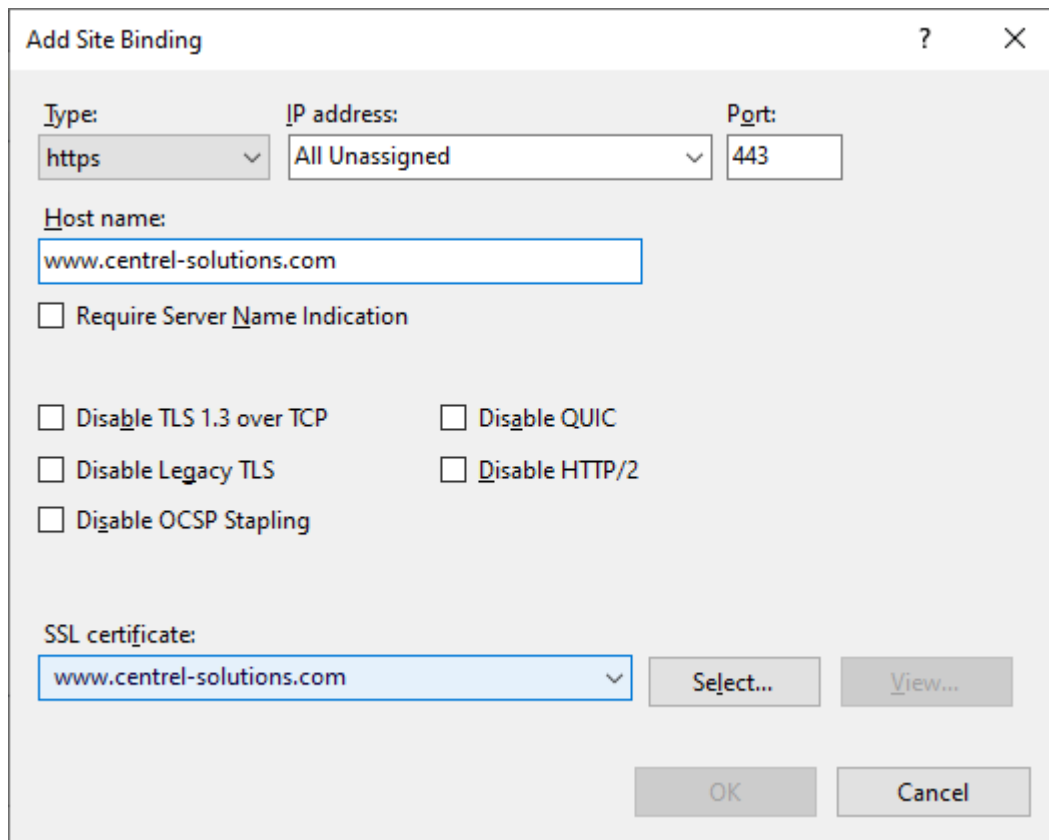
- Ensure that the certificate is installed.



- Select the web site hosting [XIA Configuration Server](#) and click Bindings



- Add a new binding selecting the certificate and assign the host name as required.



The 'Add Site Binding' dialog box is used to configure a new site binding. It includes fields for Type, IP address, Port, Host name, and SSL certificate, along with several checkboxes for disabling specific features.

Type: **https** | IP address: **All Unassigned** | Port: **443**

Host name: **www.centrel-solutions.com**

☐ Require Server Name Indication

☐ Disable TLS 1.3 over TCP | ☐ Disable QUIC

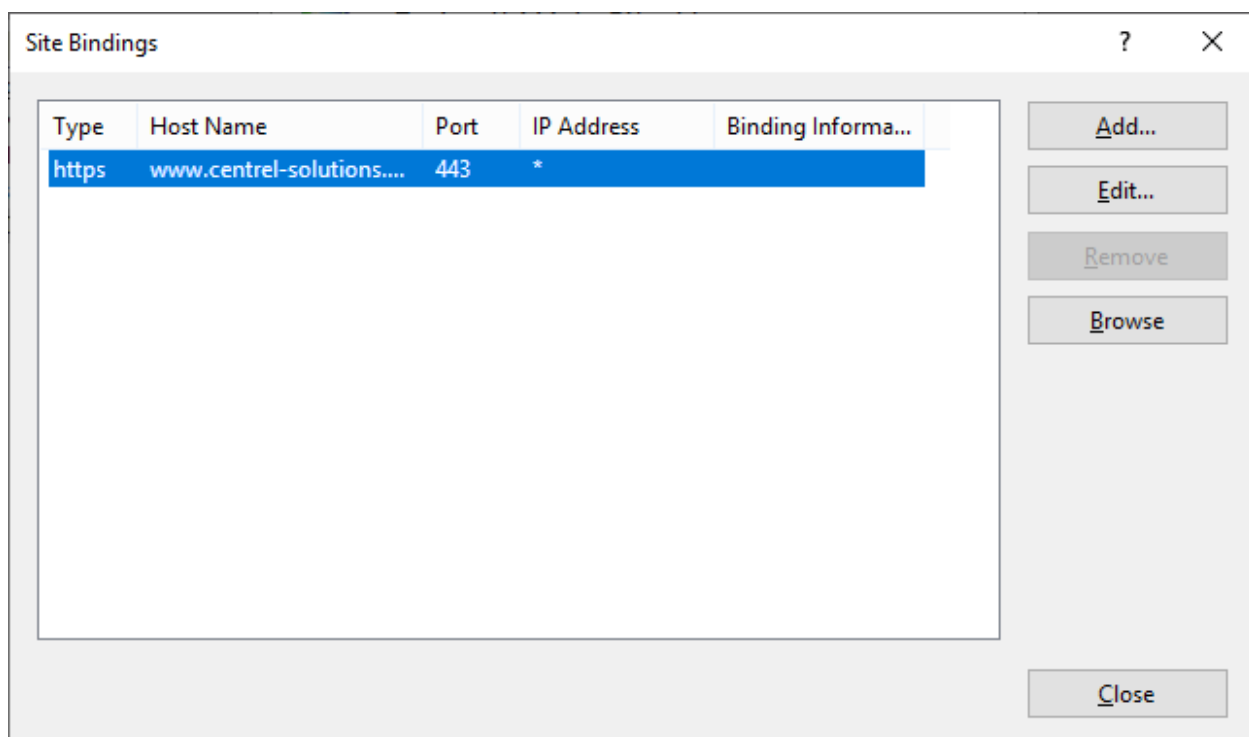
☐ Disable Legacy TLS | ☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate: **www.centrel-solutions.com** | **Select...** | **View...**

OK | **Cancel**

- Optionally remove the default HTTP binding if required.



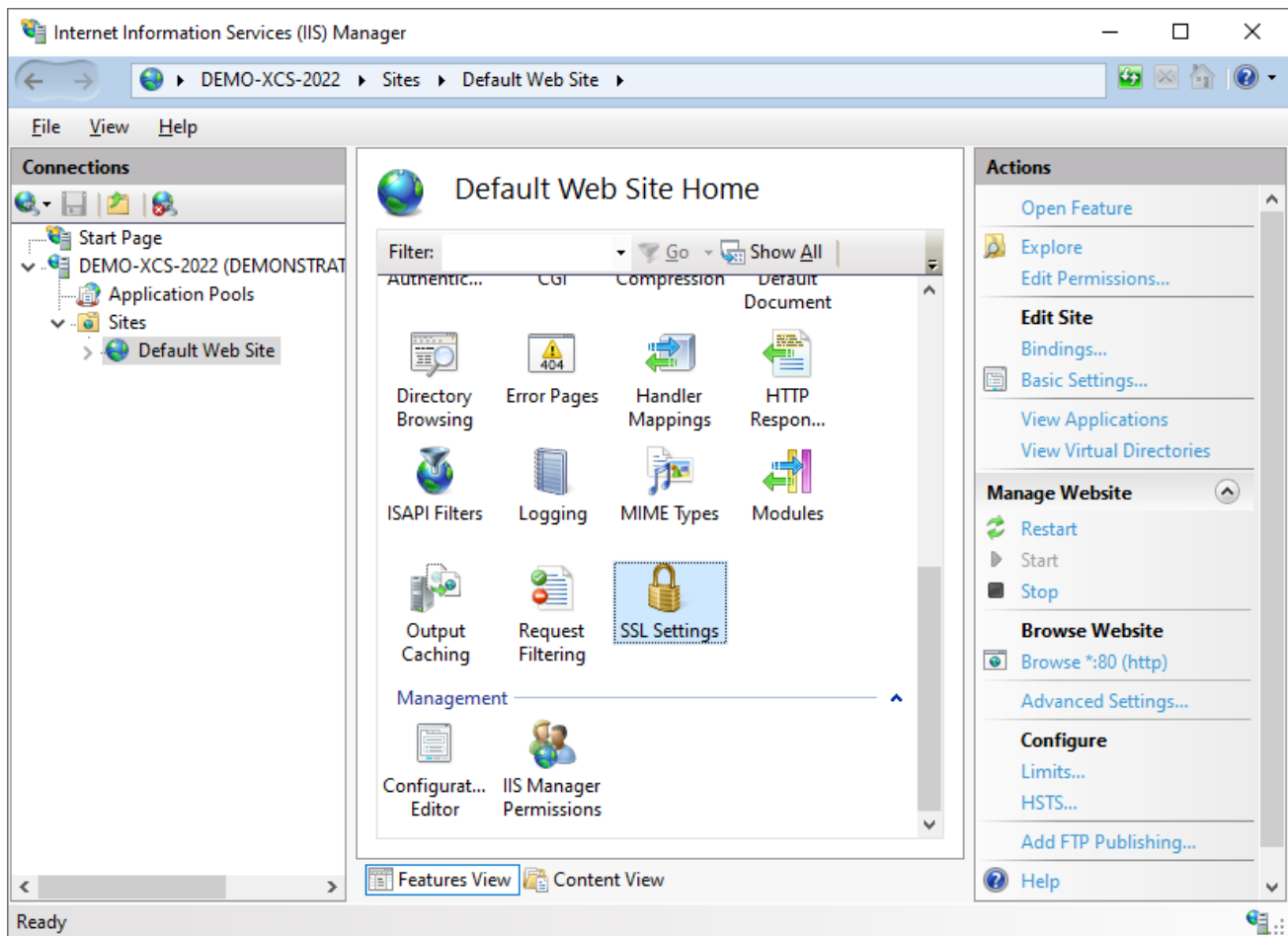
The 'Site Bindings' dialog box displays a list of configured site bindings. The first binding is highlighted in blue.

Type	Host Name	Port	IP Address	Binding Informa...
https	www.centrel-solutions....	443	*	

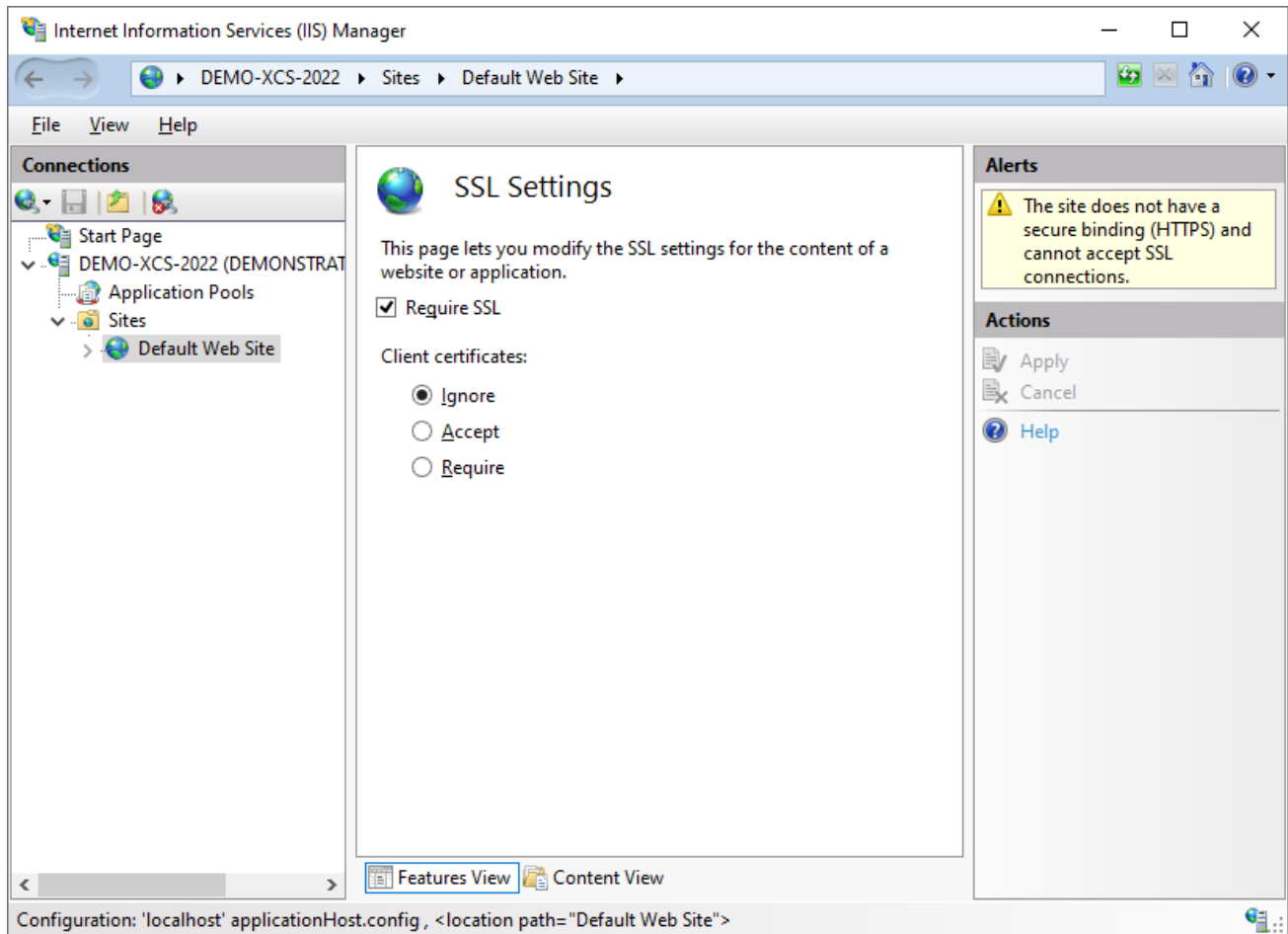
Add... | **Edit...** | **Remove** | **Browse**

Close

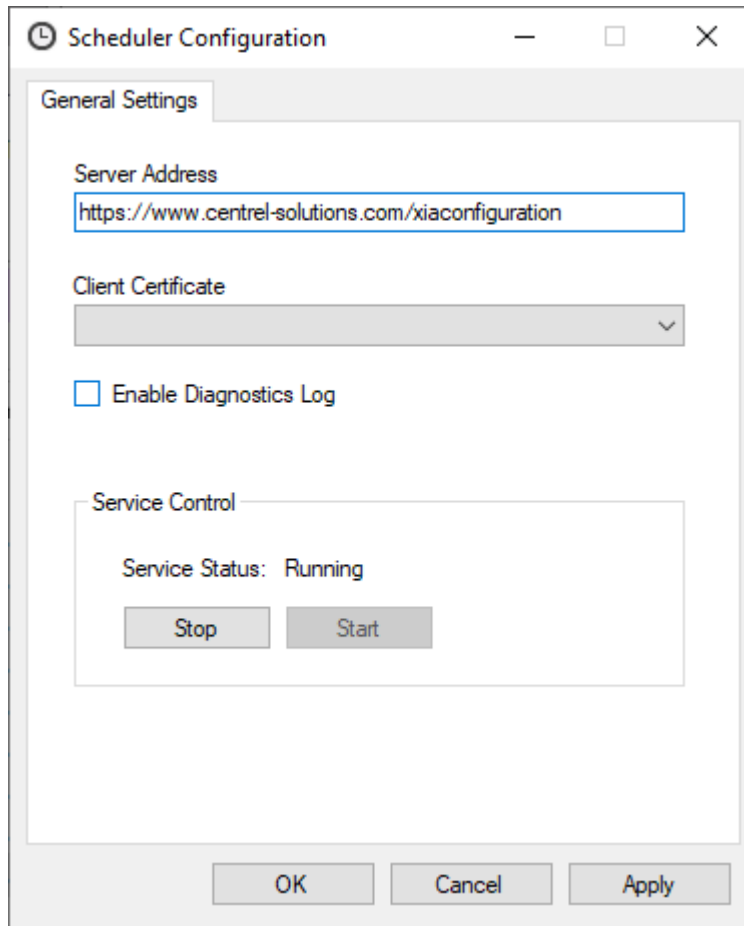
- Select the [XIA Configuration Server](#) application and double click *SSL Settings*.



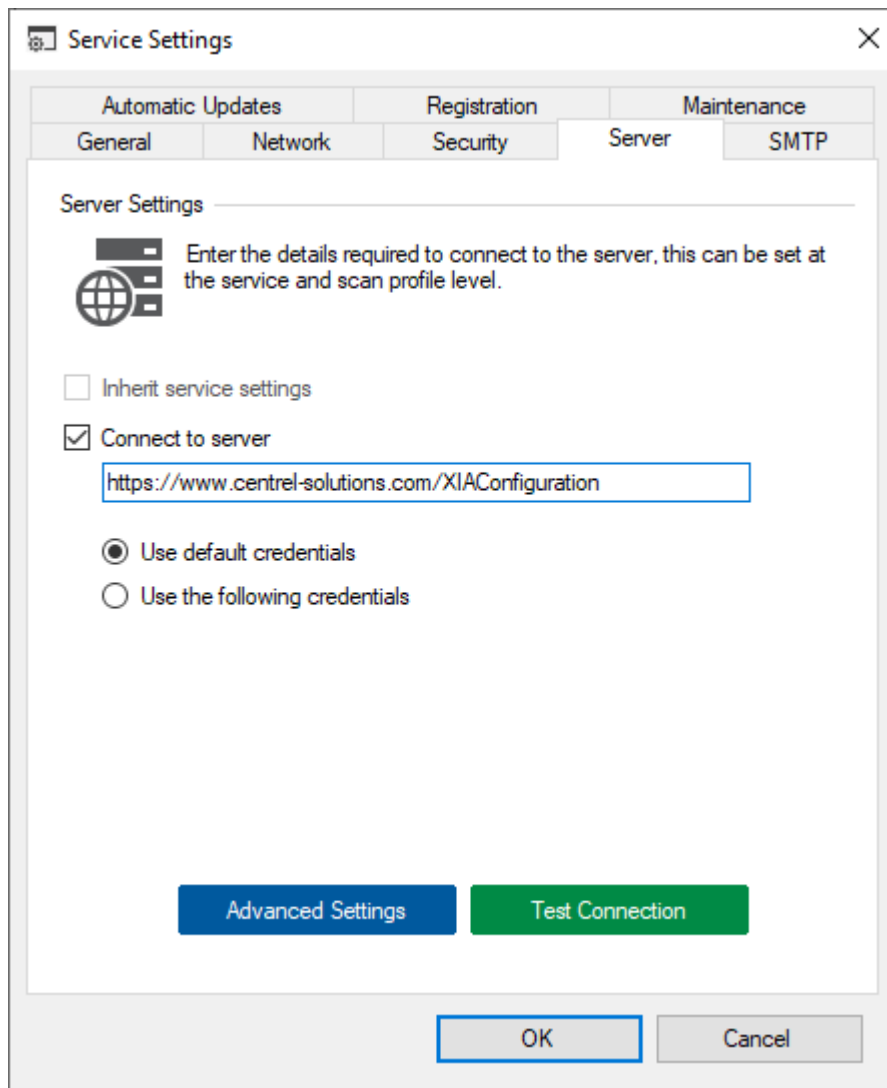
- Select *Require SSL* if required.



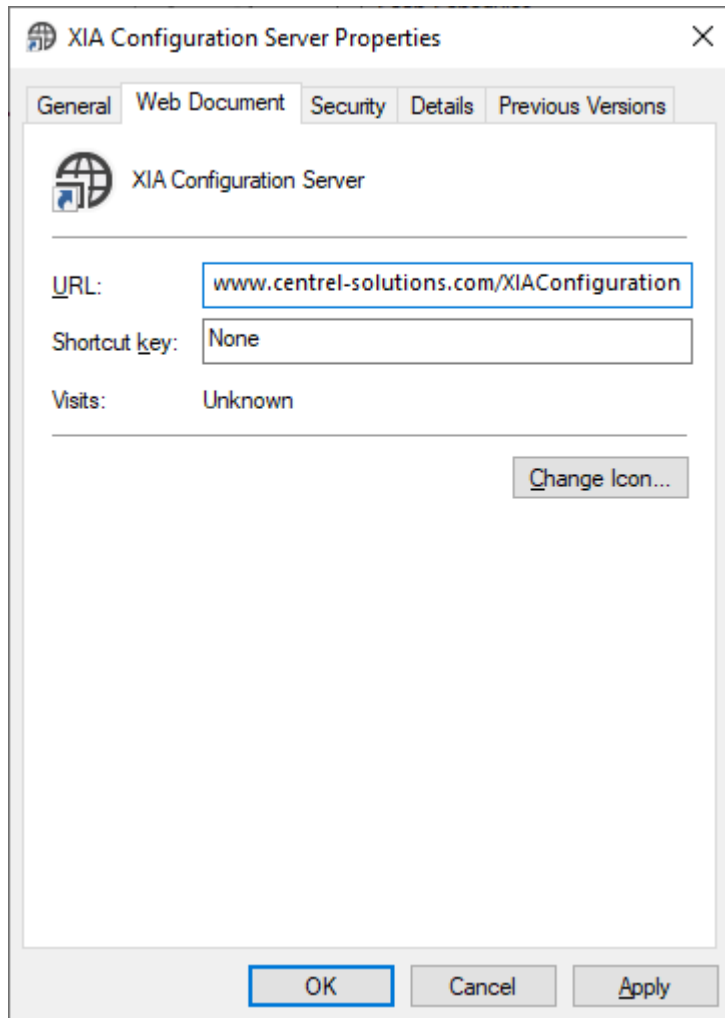
- Ensure that the installation can be accessed from a web browser.
- Open the [scheduler configuration tool](#) and set the server address as required.



- Open the [XIA Configuration Client administration tools](#).
- Goto the [service settings](#), and go to the [server](#) tab.
- Set the server address as required.



- Right click the [XIA Configuration Server](#) shortcut on the desktop, and click properties.
- Set the server address as required.



NOTE: If client certificates are required these must be [configured for the scheduler service](#), and also set on the server [advanced settings](#) within the [XIA Configuration Client](#).

Server Installation Log Files

Server Installation Logging

To enable [server installation](#) logging run the setup command with [MSI command line](#) logging parameters - for example
setup.exe /l*v "C:\setup.log"

Custom Installation Log Files

Please note additional information related to the installation may be logged to the custom actions log files which is stored in the following locations

%temp%\XIA Configuration Database Installation Actions.log
%temp%\XIA Configuration Server Installation Actions.log
%temp%\XIA Configuration Client Installation Actions.log

.NET Framework Installation Log File

If the [.NET Framework 4.8](#) is installed a log file will be created in the following location
%temp%\Microsoft .NET Framework 4.8 Setup_XXXXXXXX_XXXXXXXX.html

Database Requirements

[XIA Configuration Server](#) stores configuration information in a [Microsoft SQL Server](#) database, either locally or on a remote machine.

SQL Server Versions

- SQL Server 2022
- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014
- SQL Server 2012

SQL Server Additional Requirements

- All editions of [Microsoft SQL Server](#) are supported, please review the requirements and limitations of each edition against your storage requirements.
- If you don't have [Microsoft SQL Server](#) installed, [download and install SQL Express](#) for free.
- We recommended that [SQL Server Management Studio \(SSMS\)](#) is installed to allow for troubleshooting.
- Installations with server level, case sensitive [collations](#) are **not** supported.
- For security and performance reasons it is recommended that the [Microsoft SQL Server](#) used should be dedicated for the [XIA Configuration Server](#) installation, however this is not a requirement.
- Clustered installations of [Microsoft SQL Server](#) are supported.

Installed Roles and Features

During the [installation](#) of [XIA Configuration Server](#) the following roles, features and other shared components will be automatically installed.

- [.NET Framework 4.8](#)
- The Group Policy Management Console when selected on the [client and server advanced settings](#).

Web Server (IIS)

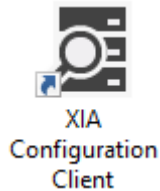
The following Internet Information Server (IIS) roles and features are installed automatically.

- Application Development > .NET Extensibility 4.8
- Application Development > ASP.NET 4.8
- Application Development > ISAPI Extensions
- Application Development > ISAPI Filters
- Common HTTP Features > Default Document
- Common HTTP Features > HTTP Errors
- Common HTTP Features > Static Content
- Security > Request Filtering
- Security > Windows Authentication
- Management Tools > IIS Management Console
- Management Tools > IIS Scripts and Tools

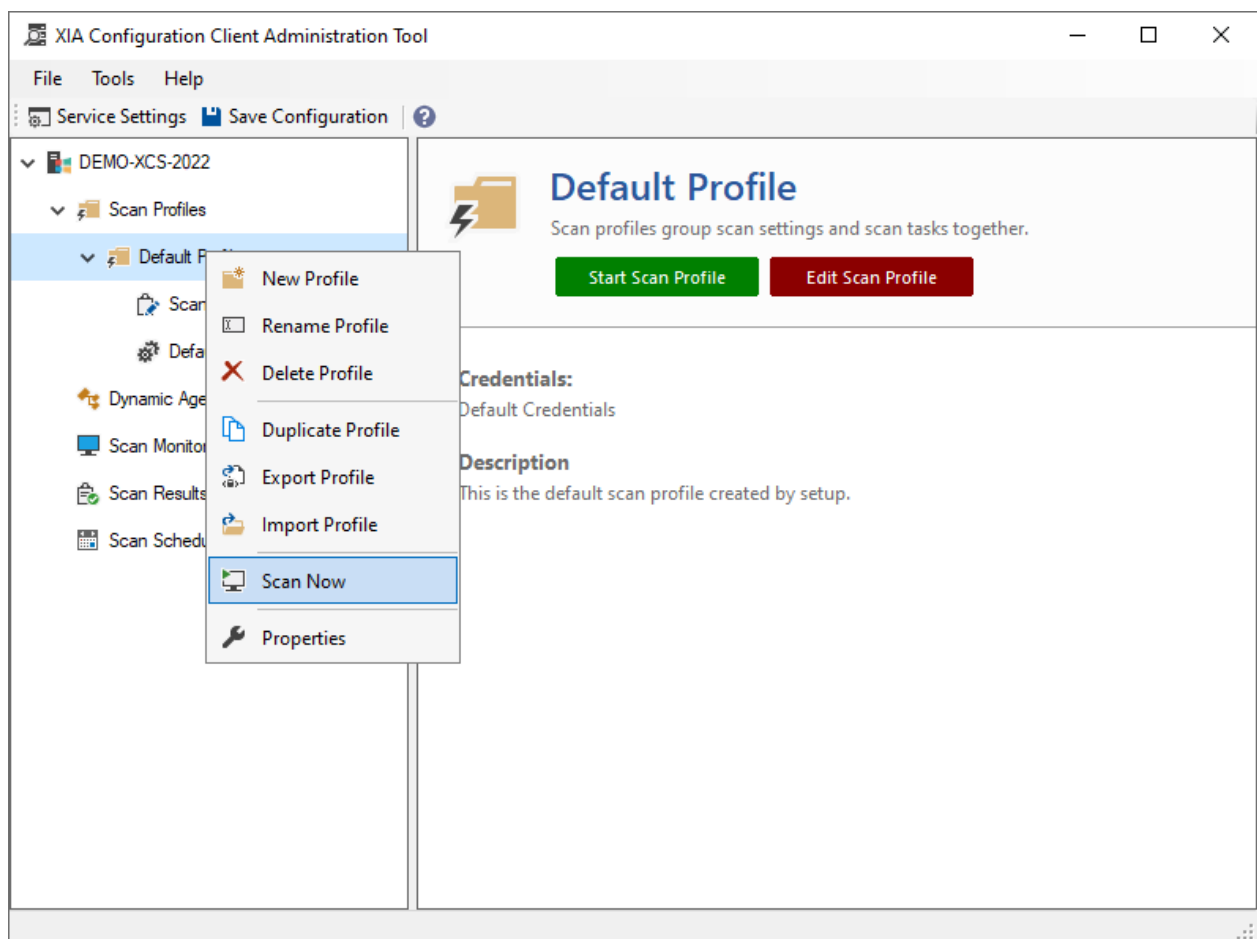
Performing your first scan

Once the [installation](#) has been completed, you are ready to perform a scan of your environment.

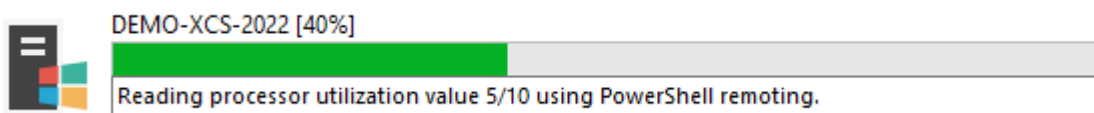
- Start the [XIA Configuration Client](#) by double clicking the desktop icon.



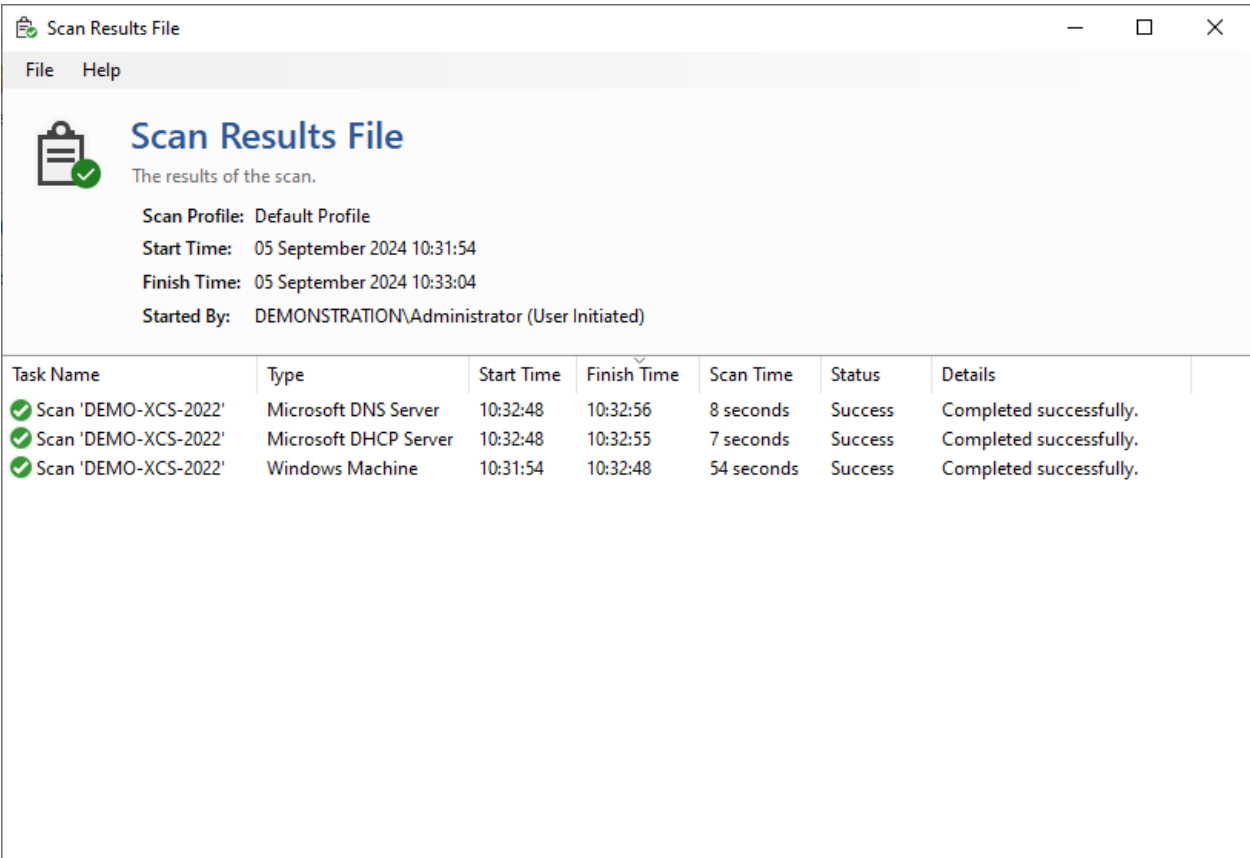
- If you selected the *Setup and schedule the default scan profile* option during the [installation](#) you can simply right click the [Default Profile](#), and select *Scan Now*.



- The [scan monitor](#) will be displayed with the progress of the scan.



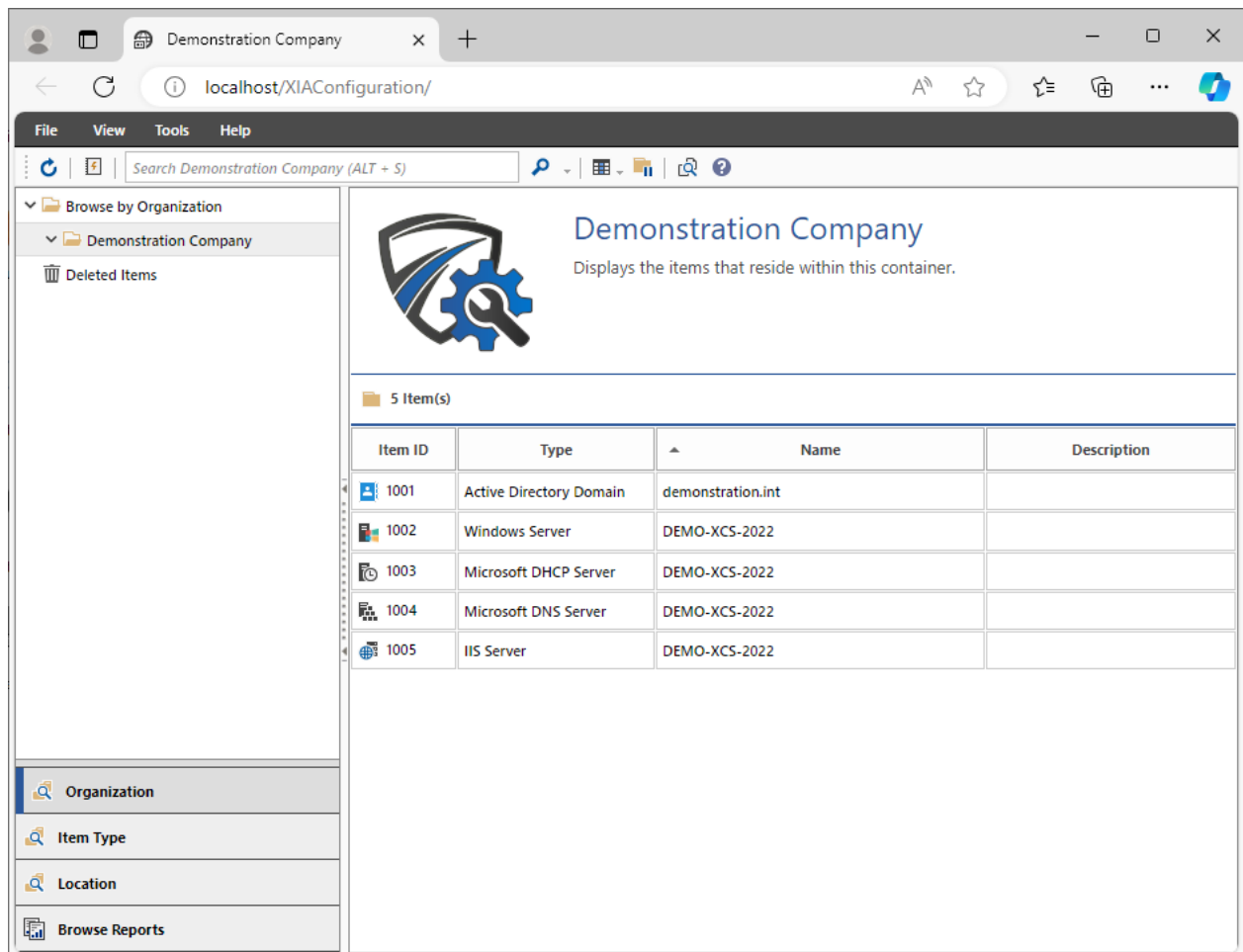
- Click *View Scan Results* to view the [results](#) of the scan.



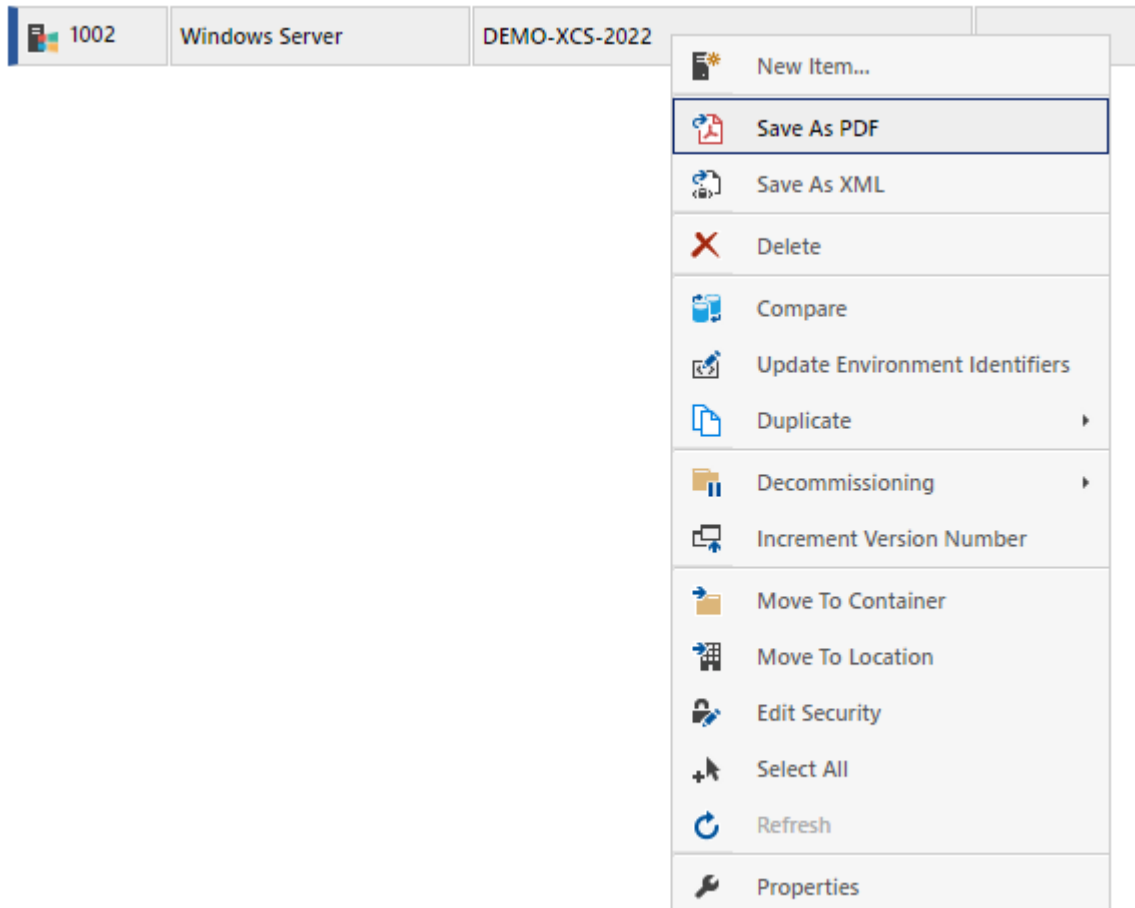
- Once complete, double click the link to [XIA Configuration Server](#) on the desktop.



- The information from the scan will appear in the list.



- Double click an [item](#) in the list to [view information](#) about that [item](#).
- Right click an [item](#), and select *Save as PDF* to [generate a PDF](#) of the [item](#).



Server Installation Troubleshooting

This section provides troubleshooting information for the [installation](#) of the [XIA Configuration Server](#).

- Please ensure that your system meets the [server requirements](#).
- Please ensure that your database meets the [database requirements](#).
- You can request support by going to our [support page](#).
- For additional information about the installation please see the [server installation log files](#).
- For non-installation issues see the [server troubleshooting](#) section.

[A certificate chain could not be built to a trusted root authority](#)

[ODBC Connect: timeout exceeded](#)

[The cabinet file *filename.cab* has an invalid digital signature](#)

[The installation package could not be opened](#)

[There is already an object named '*name*' in the database](#)

Related Client Installation Issues

[Service 'XIA Configuration Service' \(XIAConfigurationSvc\) failed to start](#)

A certificate chain could not be built to a trusted root authority

Symptoms

When [installing XIA Configuration Server](#), the installer reports
A certificate chain could not be built to a trusted root authority.

Issue

This issue is caused by the [.NET Framework 4.8](#) installer when an internet connection is not available and the certificates on the machine have not been updated.

Resolution

- Connect the machine to the internet.

- or -
- Manually update the root certificates and certificate revocation lists (CRLs) on the machine.

More Information

For more information about running Windows machines in disconnected environments see the following Microsoft article.

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn265983\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn265983(v=ws.11))

Encryption not supported on the client

Symptoms

When installing or upgrading the [XIA Configuration Server](#) you see the error

[Microsoft][ODBC Driver 18 for SQL Server]Encryption not supported on the client.

[Microsoft][ODBC Driver 18 for SQL Server]SQL Server Network Interfaces: The parameter is incorrect.

Cause

This can occur when performing the installation on Windows Server 2008 R2 where TLS 1.0 is disabled and the latest security patches are not installed on the machine.

Resolution

Ensure that the latest patches from [Windows Update](#) are installed on the machine.

ODBC Connect: timeout exceeded

Symptoms

When installing or upgrading the [XIA Configuration Server](#) you see the error "ODBC Connect: timeout exceeded".

Cause

There are several reasons

- The SQL Server instance name has been specified incorrectly.
- The SQL Server instance is not available over the network.

Resolution

- Ensure that the SQL server instance name has been specified correctly. When performing an upgrade the following registry keys are used for the instance and database name.
HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup
DatabaseInstance (REG_SZ)
DatabaseName (REG_SZ)
- Ensure that the SQL server instance is available.

The cabinet file filename.cab has an invalid digital signature

Symptoms

When installing or upgrading the [XIA Configuration Server](#) you see the error

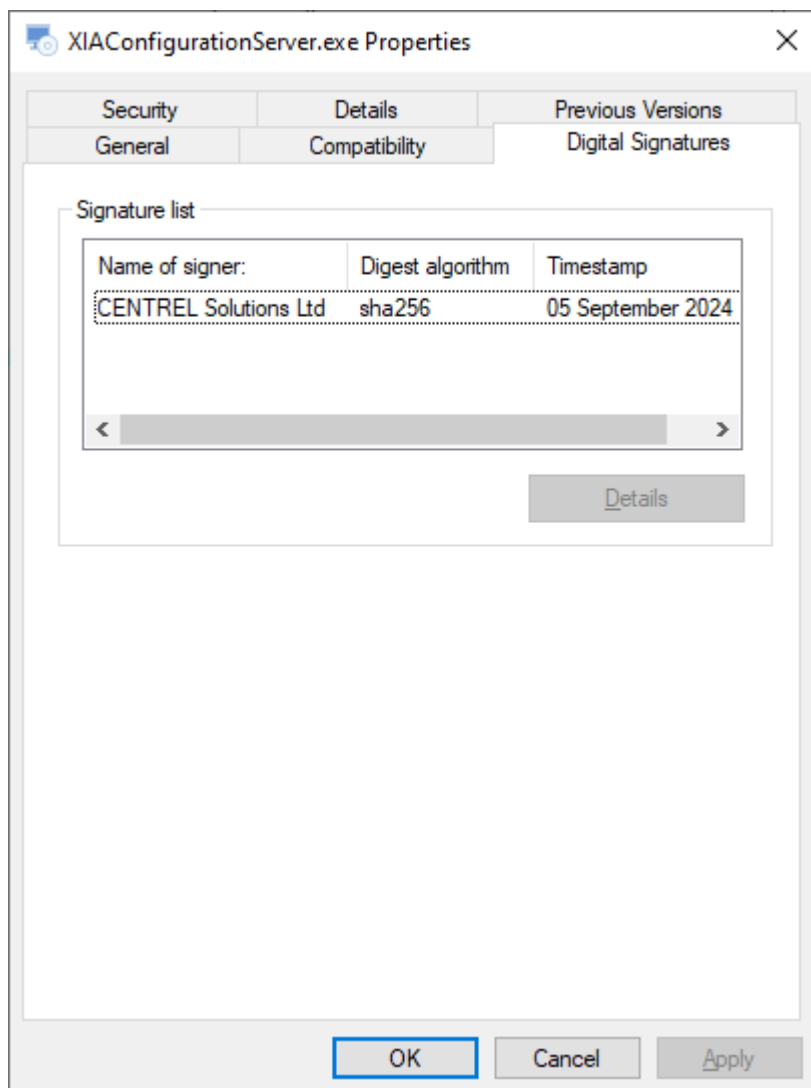
"A file that is required cannot be installed because the cabinet file <path>.cab has an invalid digital signature. This may indicate that the cabinet file is corrupt."

Cause

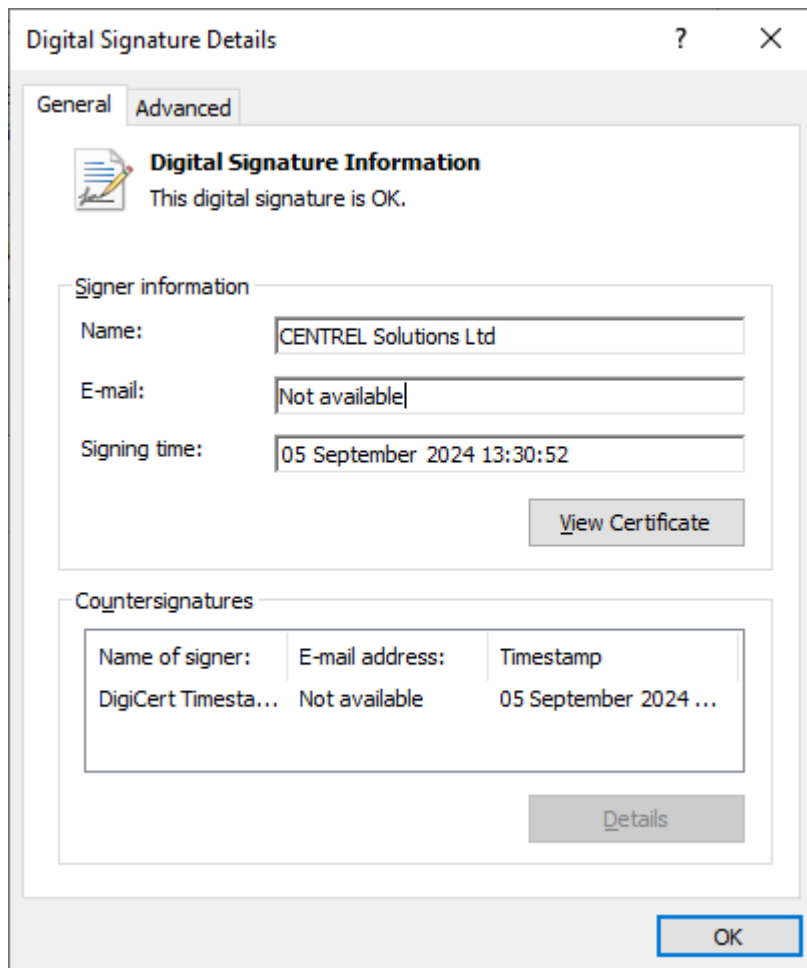
This is typically caused in a disconnected environment where the trusted certificate authorities are not updated automatically. The system can therefore not validate the certificate that was used to sign the [XIA Configuration Server](#) installer.

To validate the signature:

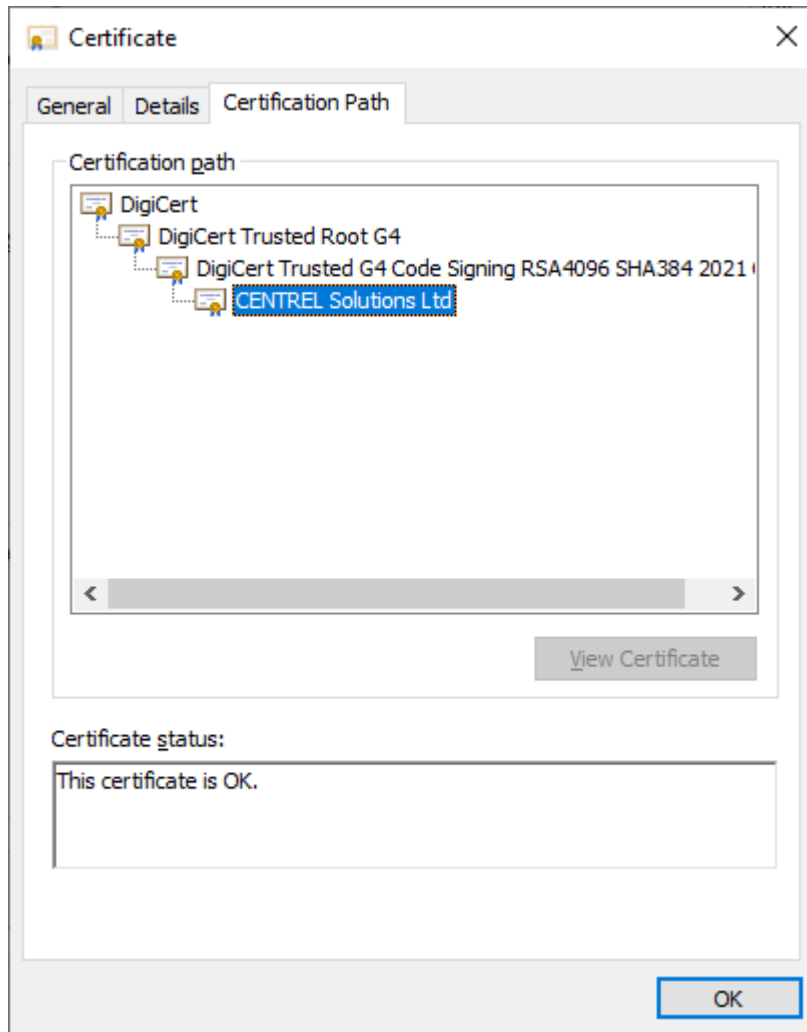
- Right click the installer and select properties.
- Select the *Digital Signatures* tab.



- Select the signature and click *Details*, issues with the signature will be displayed here.



- Clicking *View Certificate* and then viewing the *Certification Path* tab will display the certificates that are required to complete the chain.



More Information

For more information about disconnected environments please see the following Microsoft article <https://support.microsoft.com/en-us/help/2813430>

Resolution

If any of the certificates from the trust chain displayed in the *Certification Path* tab are missing they can be manually downloaded from the DigiCert site.

<https://www.digicert.com/digicert-root-certificates.htm>

The required certificates should then be installed into the *Trusted Root Certification Authorities* certificate store.

The client and server cannot communicate (common algorithm)

Symptoms

When installing or upgrading the [XIA Configuration Server](#) you see the error

A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The client and server cannot communicate, because they do not possess a common algorithm.) (Microsoft SQL Server, Error: -2146893007)

Cause

This can occur when security protocols such as TLS 1.0 are disabled, however other protocols are not available.

The connection from [SQL Server Management Studio \(SSMS\)](#) also fails with the same error.

Resolution

- Review the security configuration of the machine where you are installing [XIA Configuration Server](#) and where SQL Server is installed and ensure that these are set correctly.
- If you have disabled TLS 1.0 ensure that the version of SQL Server that you are running supports newer protocols.

The installation package could not be opened

Symptoms

When [installing XIA Configuration Server](#), the installer reports

This installation package could not be opened. Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package.

Issue

This issue is seen when the installer package has been corrupted, typically during the download process.

Resolution

[Download the installer](#) and start the installation again.

There is a problem with this Windows Installer package

Symptoms

The following error is seen when clicking the **validate** button installing [XIA Configuration Server](#).

There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.

Issue

The issue is seen on Windows 10, Windows Server 2016, or Windows Server 2019 when the [.NET Framework](#) feature has been removed.

More Information

The [.NET Framework](#) 4.x is built-in to these operating systems as a Windows feature and is enabled by default. When the feature is removed operating system functionality such as Server Manager and PowerShell may be affected.

Resolution

The [.NET Framework](#) 4.x can be enabled on the server without access to Server Manager by using the [DISM command](#).

```
DISM /Online /Enable-Feature /FeatureName:NetFx4 /all
```

There is already an object named 'name' in the database

Symptoms

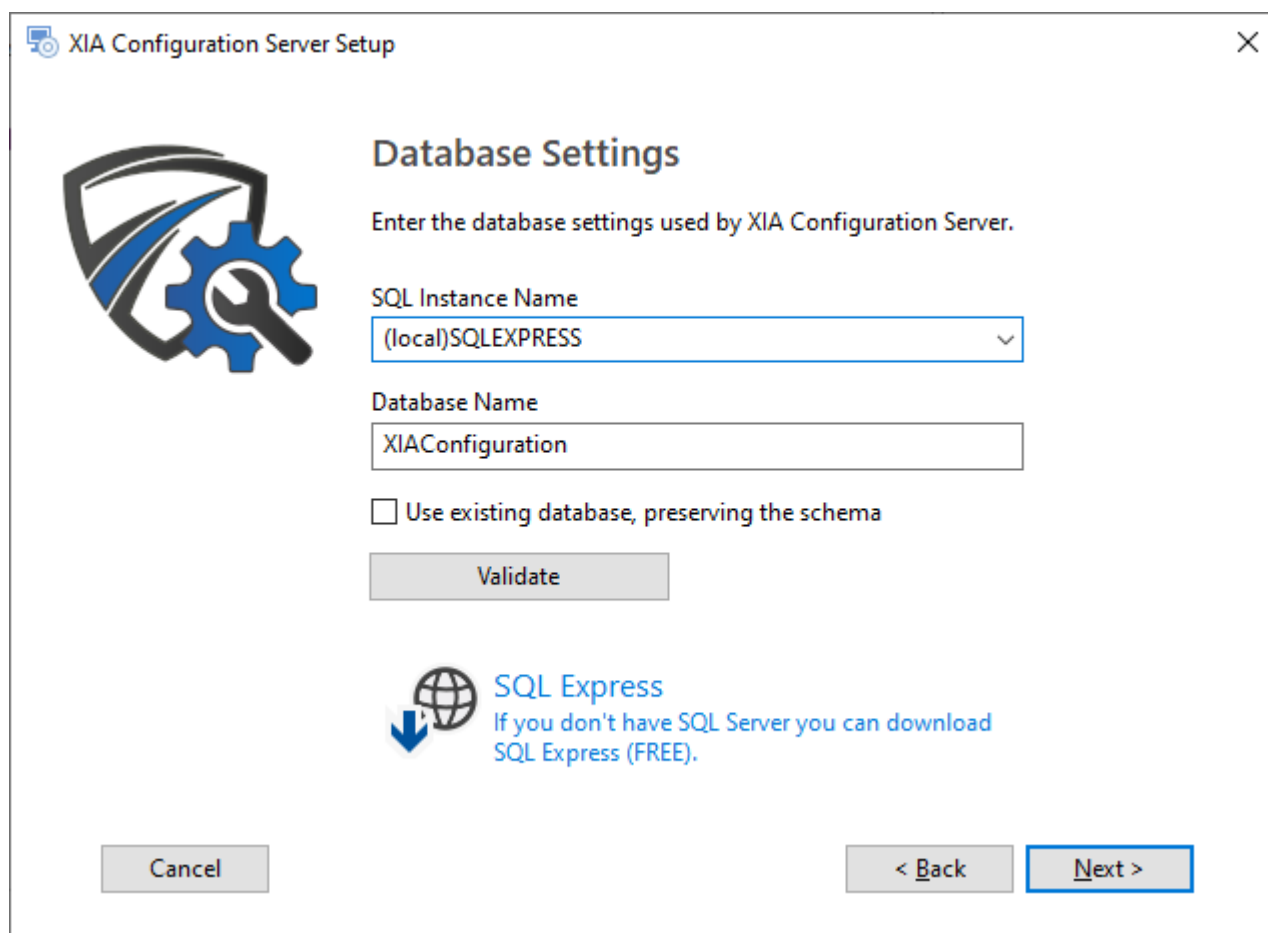
When [installing XIA Configuration Server](#), the installer reports
{SQL_ERROR}: {SQL_STATE: 42S01} There is already an object named '*name*' in the database.

Issue

This issue is seen when performing a new [installation](#) of [XIA Configuration Server](#) where the database already exists.

Resolution

When performing a new [installation](#) and the database already exists ensure the *Use existing database, preserving the schema* is selected.



The screenshot shows the 'XIA Configuration Server Setup' window with the 'Database Settings' tab selected. On the left is a shield and gear icon. The main area contains the following elements:

- Database Settings** header.
- Instruction: 'Enter the database settings used by XIA Configuration Server.'
- SQL Instance Name**: A dropdown menu showing '(local)SQLEXPRESS'.
- Database Name**: A text box containing 'XIAConfiguration'.
- ☐ **Use existing database, preserving the schema** (This checkbox is currently unchecked).
- Validate** button.
- SQL Express** section with a globe icon and a download arrow, containing the text: 'If you don't have SQL Server you can download SQL Express (FREE).'

At the bottom are three buttons: **Cancel**, **< Back**, and **Next >** (the 'Next >' button is highlighted with a blue border).

There was an error during the Windows features configuration process

Symptoms

When [installing XIA Configuration Server](#), the installer reports

There was an error during the Windows features configuration process. Your original configuration will be restored.

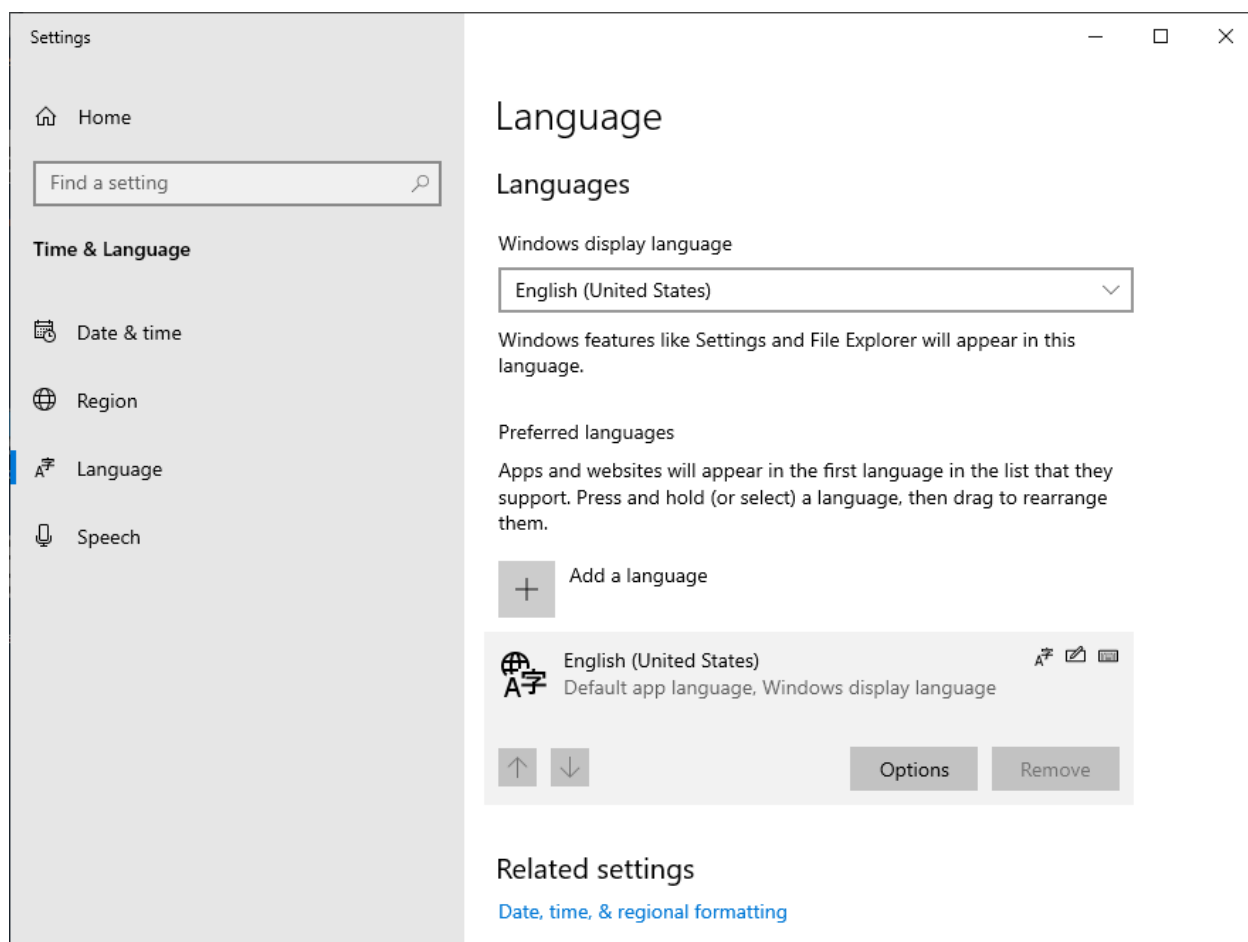
Issue

This issue is caused by a problem with the Windows component based servicing (CBS) system.

Resolution

It may be possible to determine more information about this issue by completing the following steps.

- Attempt to install the required [roles and features](#) manually using Server Manager or the [Install-WindowsFeature](#) cmdlet.
- Review the component based servicing (CBS) log file.
%windir%\Logs\CBS\CBS.log
- The issue may be caused by additional language packs being installed.



Server Migration

In the event that you need to migrate your [XIA Configuration Server installation](#) to a new physical or virtual machine, you should complete the following steps:

Server Migration

For information on migrating the [XIA Configuration Server installation](#), see the [server migration](#) section.

Database Migration

For information on migrating the [XIA Configuration Server database](#), see the [database migration](#) section.

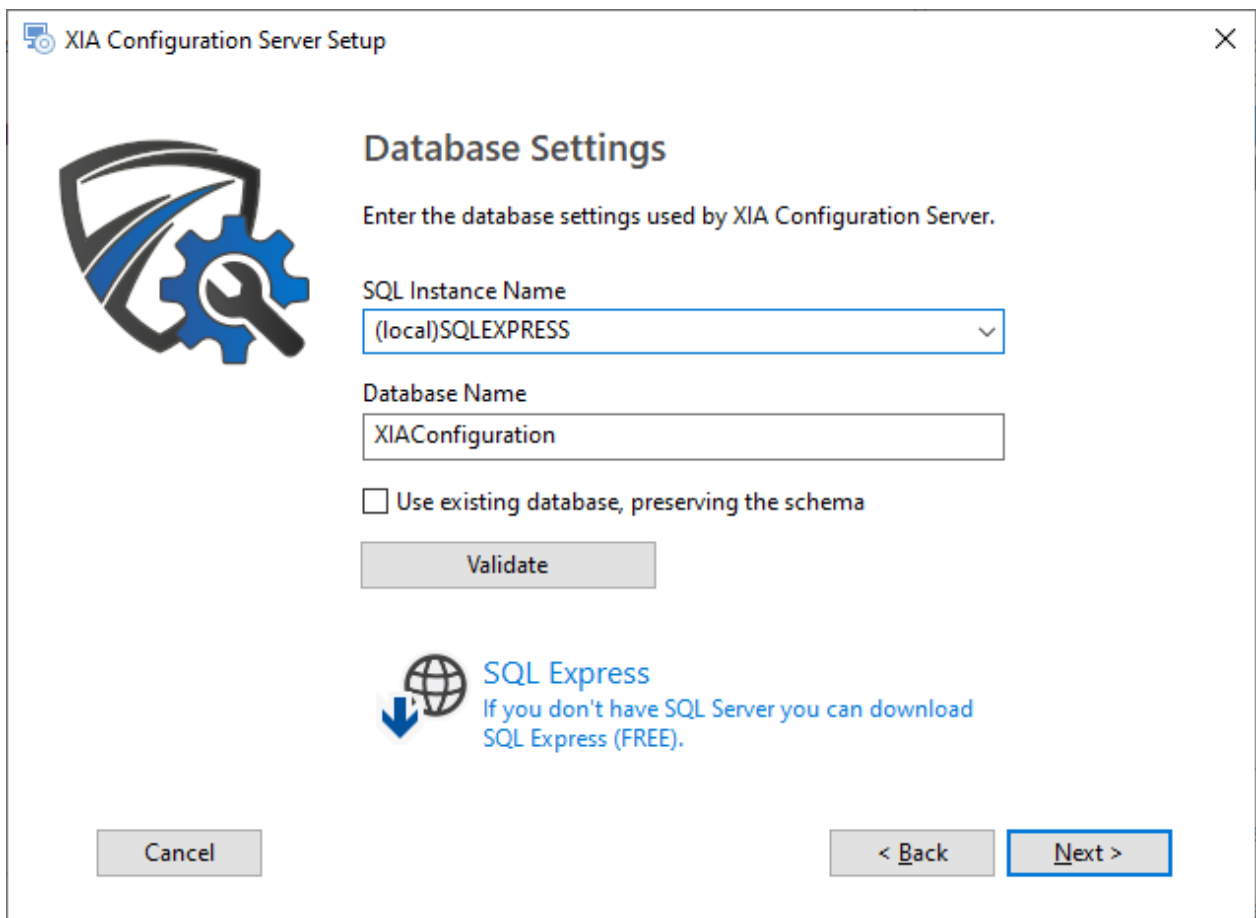
Client Migration

For information on migrating the [XIA Configuration Client](#) that is installed with the server see the [client migration](#) section.

Server Migration

The following steps describe how to move the [XIA Configuration Server installation](#) to a different physical or virtual machine:

- Ensure you have a **full system backup** of the existing and new server.
- If the new server is on a different Active Directory domain, or you have a named server [license](#), you may need to contact [CENTREL Solutions Support](#) for an updated [license](#) file before proceeding.
- On the new server, [install](#) the **same version** of [XIA Configuration Server](#) as is installed on the existing machine. If you are using an existing [SQL Server database](#), ensure that you tick the "Use existing database, preserving the schema" option during the [installation](#).



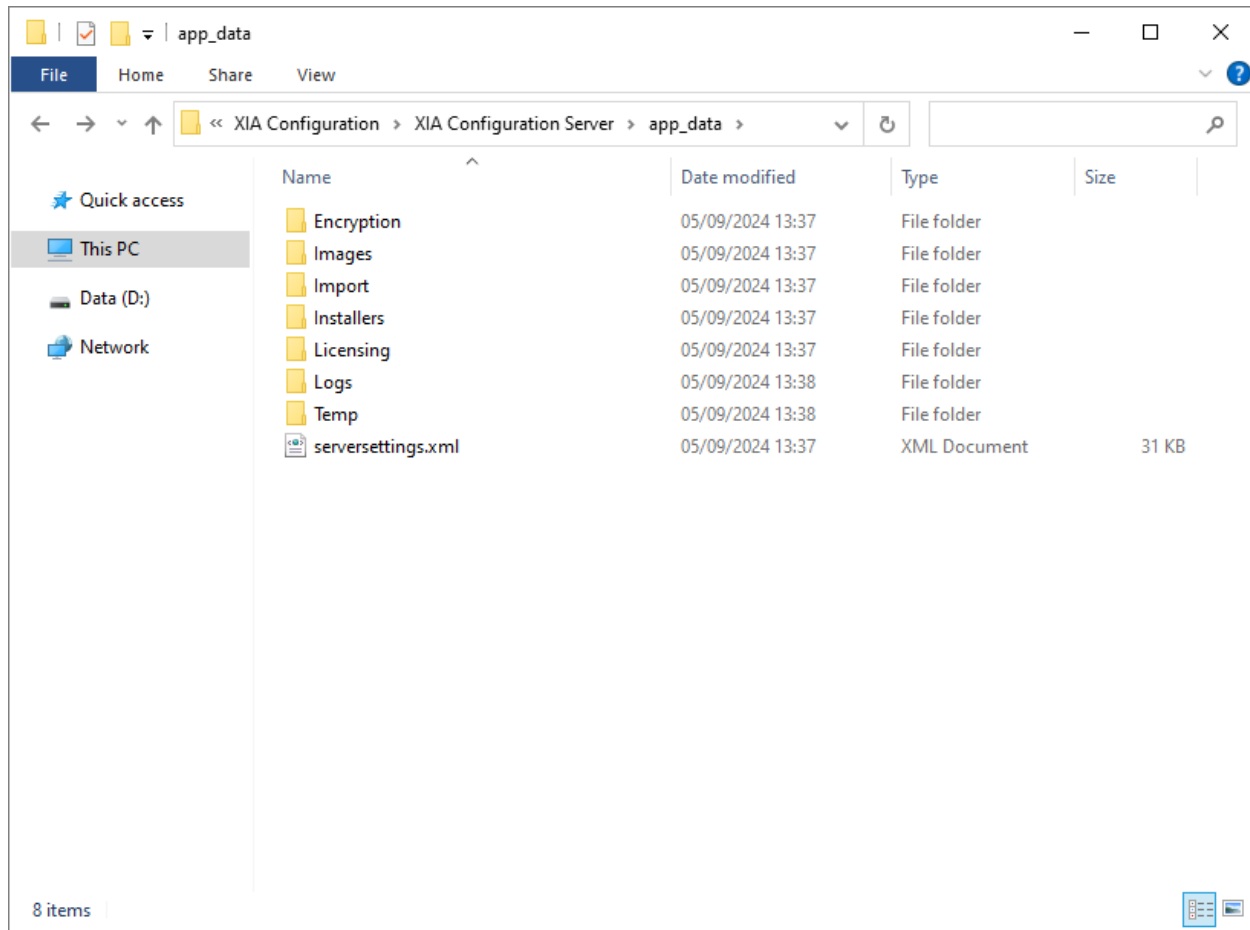
The screenshot shows the 'XIA Configuration Server Setup' window with the 'Database Settings' tab selected. On the left is a logo featuring a shield and a gear. The main area contains the following elements:

- Database Settings** header.
- Instruction: 'Enter the database settings used by XIA Configuration Server.'
- SQL Instance Name**: A dropdown menu showing '(local)SQLEXPRESS'.
- Database Name**: A text box containing 'XIAConfiguration'.
- ☐ **Use existing database, preserving the schema**
- Validate** button.
- SQL Express** section with a globe icon and a download arrow, containing the text: 'If you don't have SQL Server you can download SQL Express (FREE).'
- Navigation buttons at the bottom: **Cancel**, **< Back**, and **Next >**.

- Ensure that you can access the installation on the new server and that it performs correctly.

NOTE: If you wish to use a newer version of [XIA Configuration Server](#), upgrade the existing server **before** performing the new installation. This may require you to obtain an updated [license](#) file from [CENTREL Solutions Support](#).

- Copy the files from the App_Data folder on the existing server to the new server, overwriting any existing files:



By default, these files are found in this location:

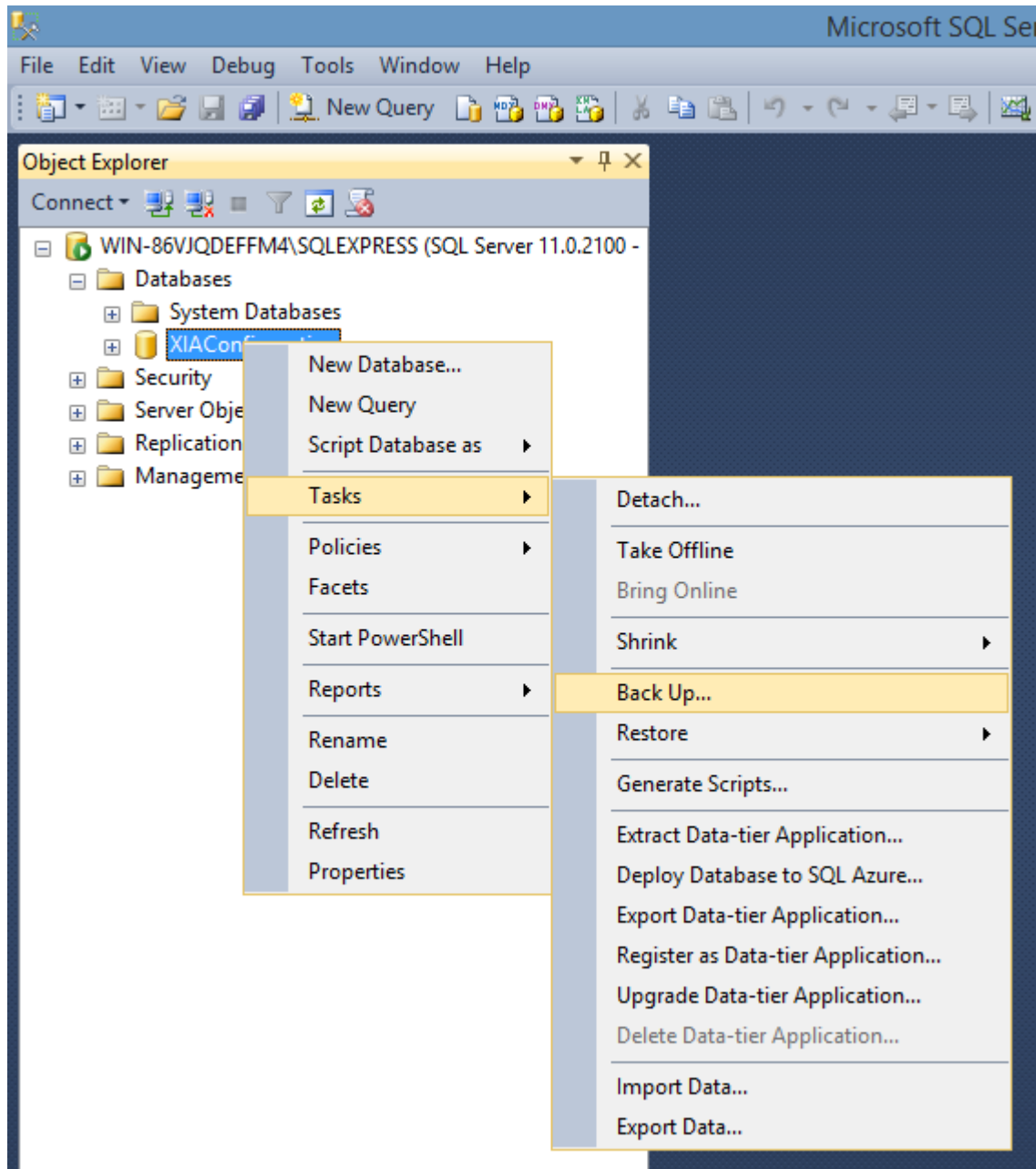
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\App_Data

- If you have made any custom modifications to the [Web.Config](#) file, copy the file from the existing server to the new server.
- If you have installed any SSL certificates on the existing server, these must be migrated manually to the new server. Please see the documentation from your SSL certificate provider for more information.
- If you are hosting the database on a **separate server** and that server is **not** being migrated, you should now be able to access the [XIA Configuration Server](#).
- If you also wish to migrate the [XIA Configuration Client](#) settings, please complete the steps in the [client migration](#) section.
- If you are also migrating the database, please complete the steps in the [database migration](#) section.
- Once complete, **uninstall** the existing [XIA Configuration Server](#).

Database Migration

The following steps describe how to move the [XIA Configuration Server](#) database to a different physical or virtual machine.

- On the **existing** database server, start SQL Server Management Studio.
- Right click the XIA Configuration Server database and select Tasks > Back Up:

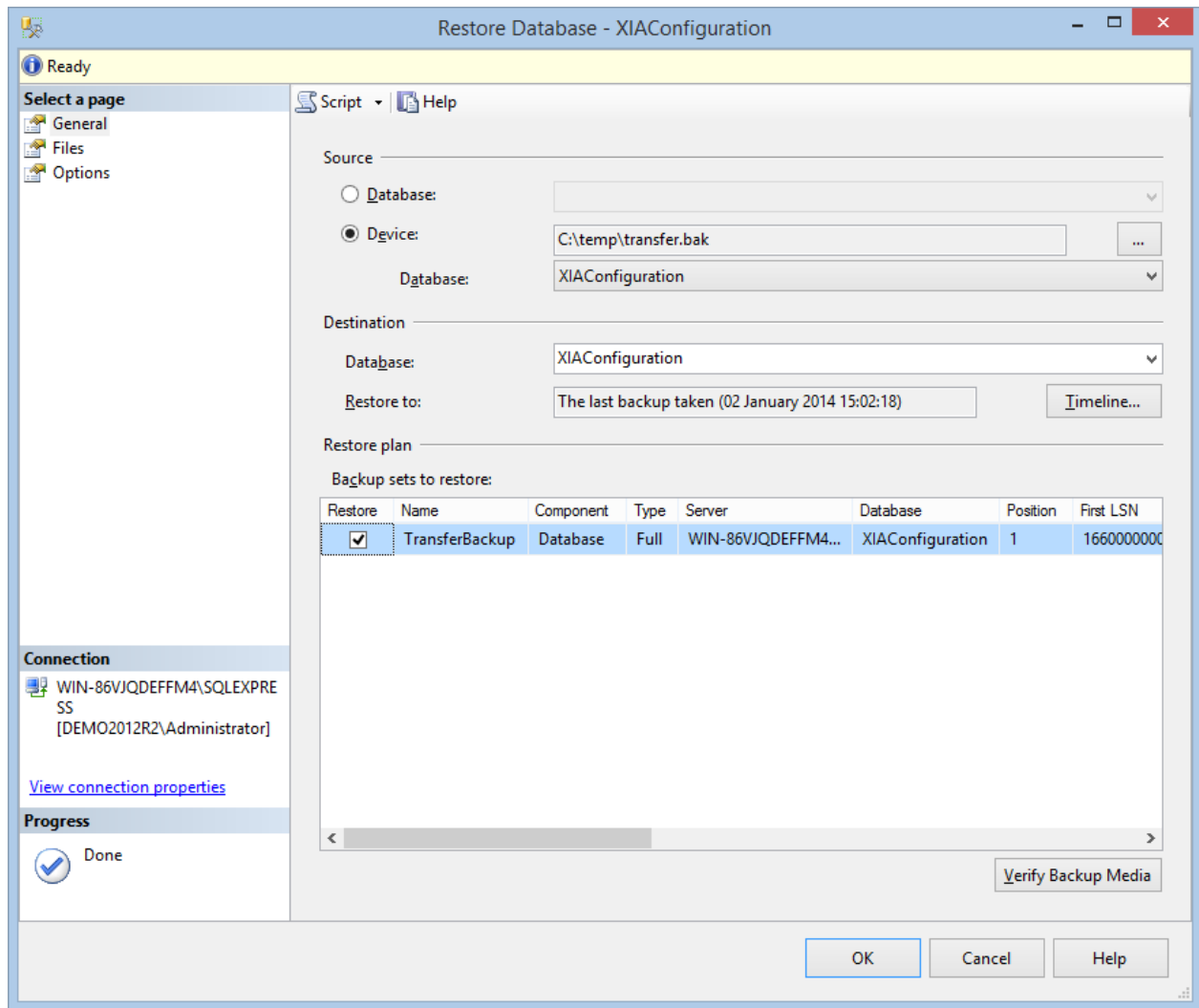


- Ensure you are performing a **Full** backup and select an appropriate backup destination:

The screenshot shows the 'Back Up Database - XIAConfiguration' dialog box. On the left, there is a 'Select a page' pane with 'General' and 'Options' tabs. Below this is a 'Connection' section showing the server 'WIN-86VJQDEFFM4\SQLEXPRESS' and connection 'DEMO2012R2\Administrator'. A 'Progress' section at the bottom left shows a 'Ready' status. The main area is divided into sections: 'Source' (Database: XIAConfiguration, Recovery model: SIMPLE, Backup type: Full, Copy-only Backup: unchecked, Backup component: Database), 'Backup set' (Name: TransferBackup, Description: empty, Backup set will expire: After 0 days), and 'Destination' (Back up to: Disk, c:\temp\transfer.bak). There are 'Add...', 'Remove', and 'Contents' buttons next to the destination path. At the bottom right are 'OK' and 'Cancel' buttons.

- Click OK to start the backup.
- Copy the backup file to the new database server.
- On the **new** database server, start SQL Server Management Studio.
- Right click databases and click **Restore**.

- Select the backup file that you are restoring:

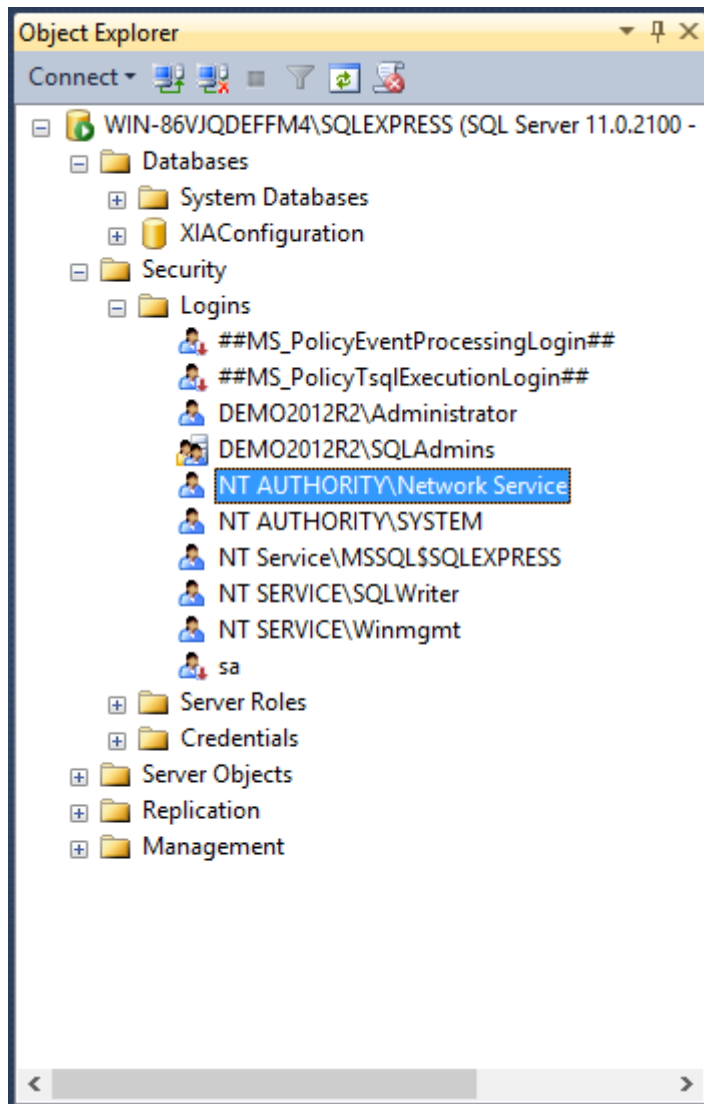


- On the **Files** tab, ensure that the database files are going to be restored to the correct location.
- Click **OK** to begin the restore.

- Expand the restored database > Security > Logins and ensure that the service account (*by default* the [Network Service](#) account) is listed correctly.

NOTE: If you used the [Network Service](#) account during the installation, by default, the account name should be "NT AUTHORITY\Network Service" for English versions of Windows. For other language versions, you may have to use the localized variant of this built-in account.

NOTE: If you used the [Network Service](#) account during the installation and the database server is on a **different** machine to the computer running the [XIA Configuration Server](#) product, you should use the computer account of the computer running the [XIA Configuration Server](#) product in the format DOMAIN\ComputerName\$ - for example "CORP\DEMO-SRV01\$".



- If the user doesn't exist right click Logins > New Login.

- Enter the login name as determined above and select the default database:

Login - New

Script Help

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: WIN-86VJQDEFFM4\SQLEXPRESS

Connection: DEMO2012R2\Administrator

[View connection properties](#)

Progress

Ready

Login name: NT AUTHORITY\NETWORK SERVICE Search...

☒ Windows authentication

☐ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Add

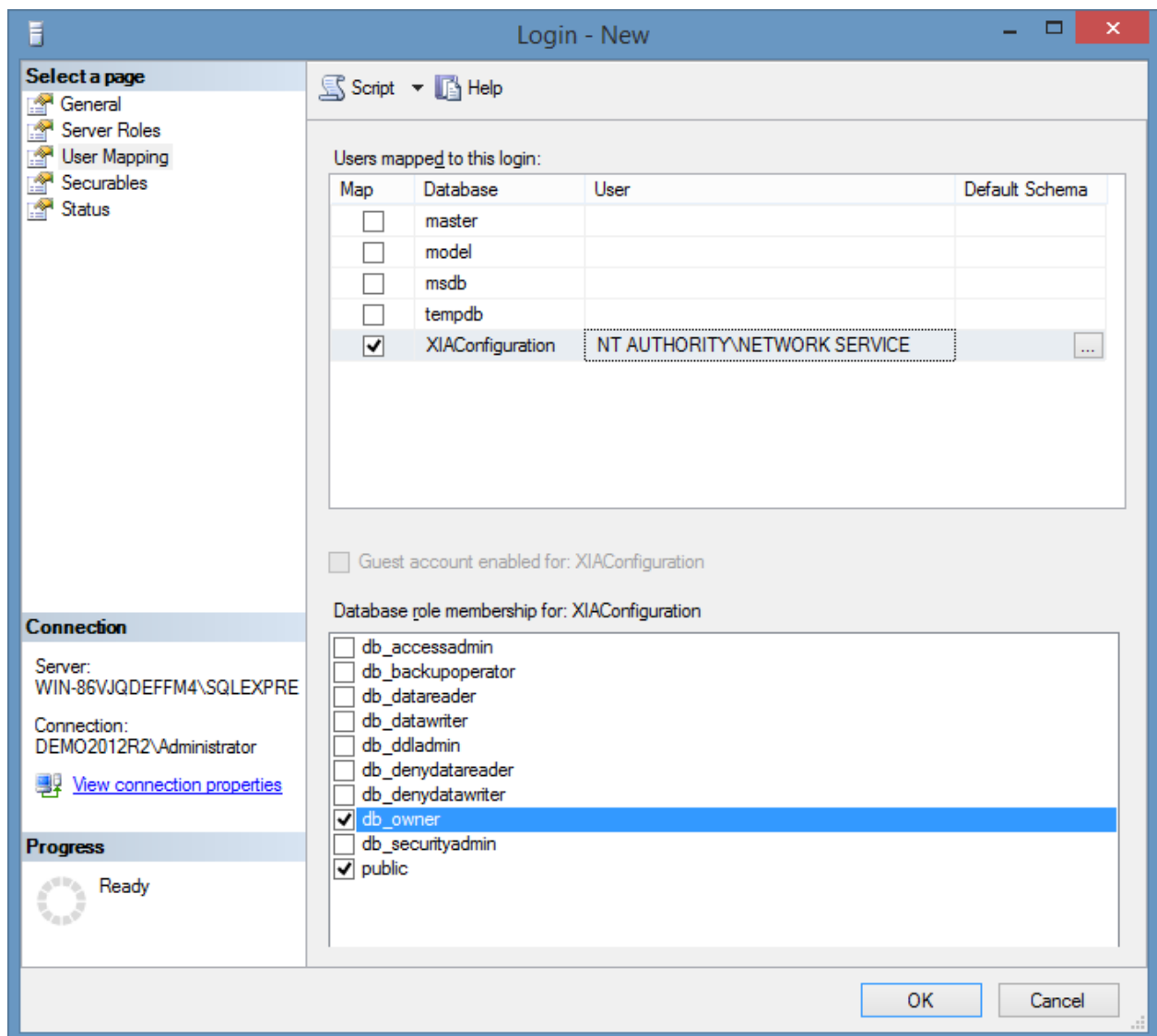
Remove

Default database: XIAConfiguration

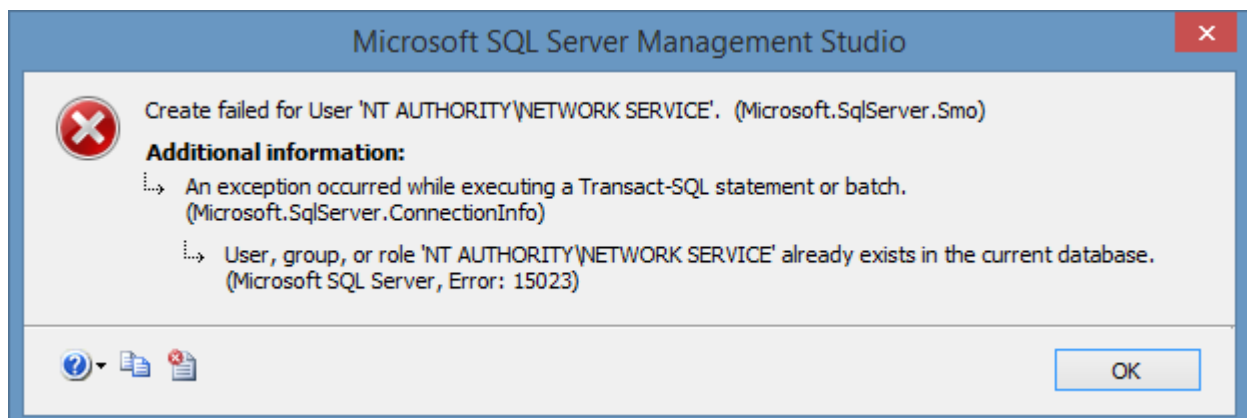
Default language: <default>

OK Cancel

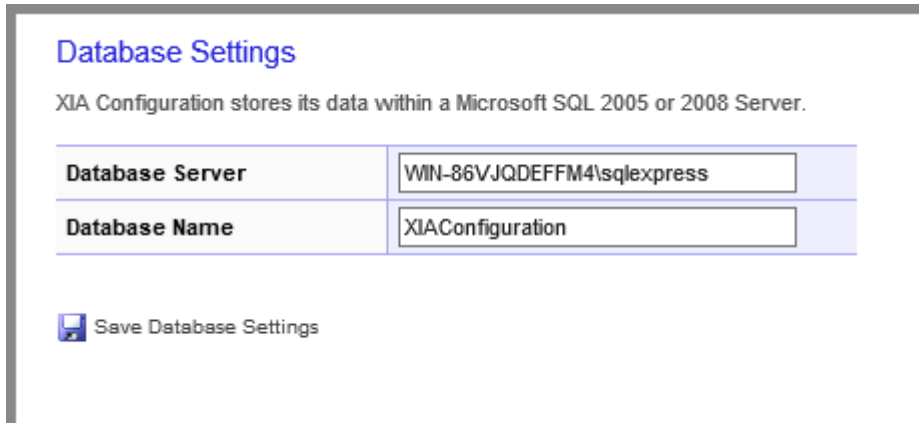
- On the **User Mapping** tab, select the XIA Configuration database and ensure that **db_owner** is ticked:



- Click **OK** to create the login.
- If you are informed that the login already exists within the database, browse to "Databases > Database Name > Security > Users" and remove the user and repeat the steps above to create the login.



- Open the XIA Configuration Server web interface.
NOTE: There may be a delay as the system attempts to locate the previous SQL server instance if this is no longer available on the network.
- On the **Database Settings** tab, enter the new database server instance name and ensure the database name is correct.
- Click **Save Database Settings**.



Database Settings

XIA Configuration stores its data within a Microsoft SQL 2005 or 2008 Server.

Database Server	WIN-86VJQDEFFM4\sqlexpress
Database Name	XIAConfiguration

 Save Database Settings

- To ensure that upgrades are performed correctly, open **regedit.exe** and modify the following registry key values to match the values in the web interface:

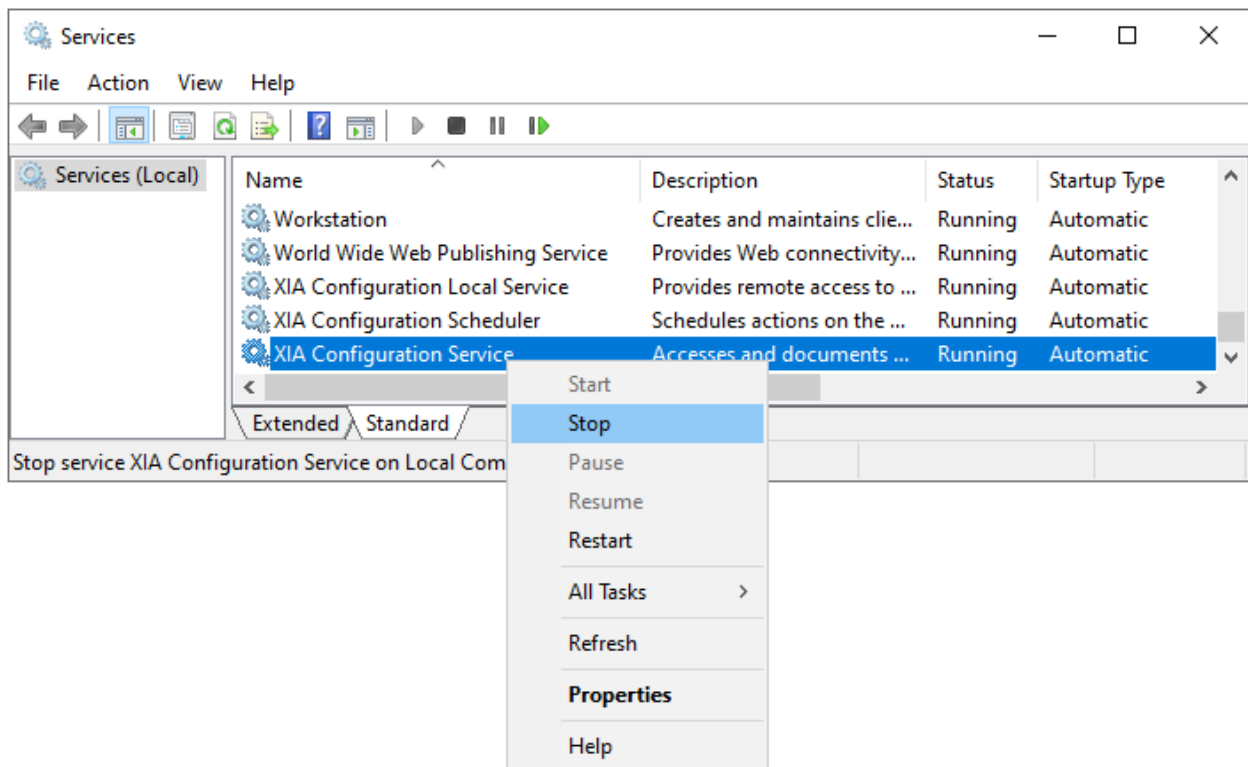
HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup
 DatabaseInstance [REG_SZ]
 DatabaseName [REG_SZ]

- It should now be possible to access the [XIA Configuration Server](#) web interface.

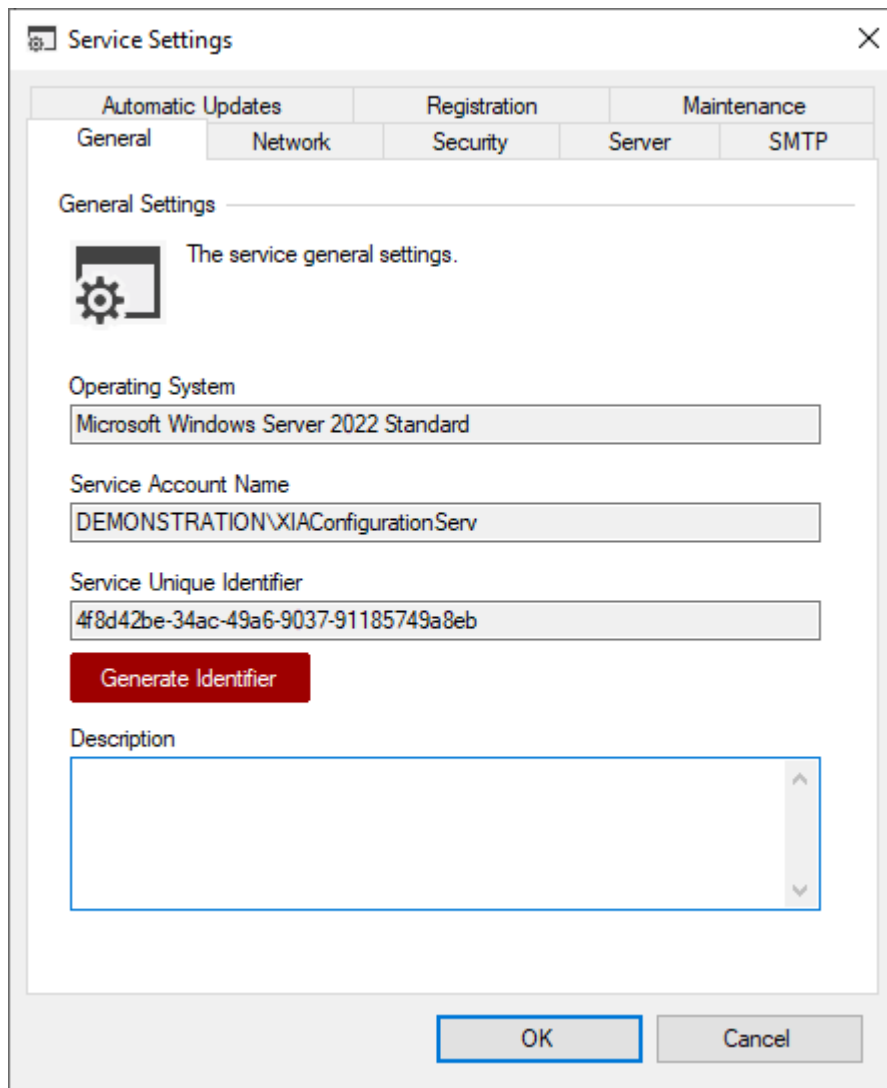
Client Migration

The following steps describe how to migrate the [XIA Configuration Client](#) settings following a [server migration](#). For the migration of a stand-alone [installation](#) of the [XIA Configuration Client](#) see the [client migration](#) section.

- Ensure you have a **full system backup** of the existing and new server.
- On the new server, stop the XIA Configuration Service.



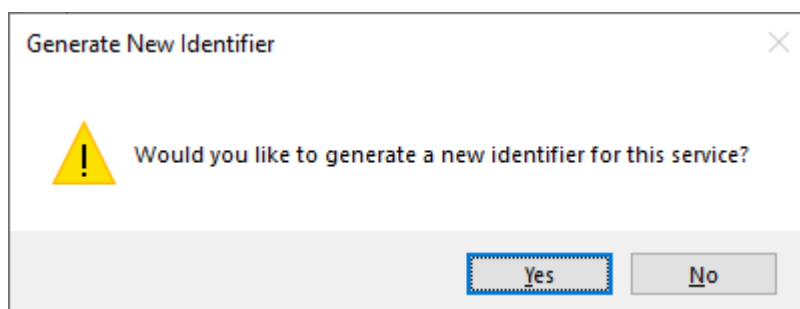
- Copy the **encryption** and **configuration** directories from the existing server to the new server, overwriting any existing files.
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Configuration
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Encryption
- On the new server, start the XIA Configuration Service.
- Open the [administration tools](#), go to the [service settings, general tab](#) and click the *Generate Identifier* button.



The Service Settings dialog box is shown with the 'General' tab selected. It contains the following fields and controls:

- General Settings**: A section header with a gear icon and the text 'The service general settings.'
- Operating System**: A text field containing 'Microsoft Windows Server 2022 Standard'.
- Service Account Name**: A text field containing 'DEMONSTRATION\XIAConfigurationServ'.
- Service Unique Identifier**: A text field containing '4f8d42be-34ac-49a6-9037-91185749a8eb'.
- Generate Identifier**: A red button located below the Service Unique Identifier field.
- Description**: A large, empty text area for entering a description.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

- Click yes when prompted.



The 'Generate New Identifier' dialog box is shown. It contains the following elements:

- Warning Icon**: A yellow triangle with a black exclamation mark.
- Text**: 'Would you like to generate a new identifier for this service?'
- Buttons**: 'Yes' and 'No' buttons at the bottom right.

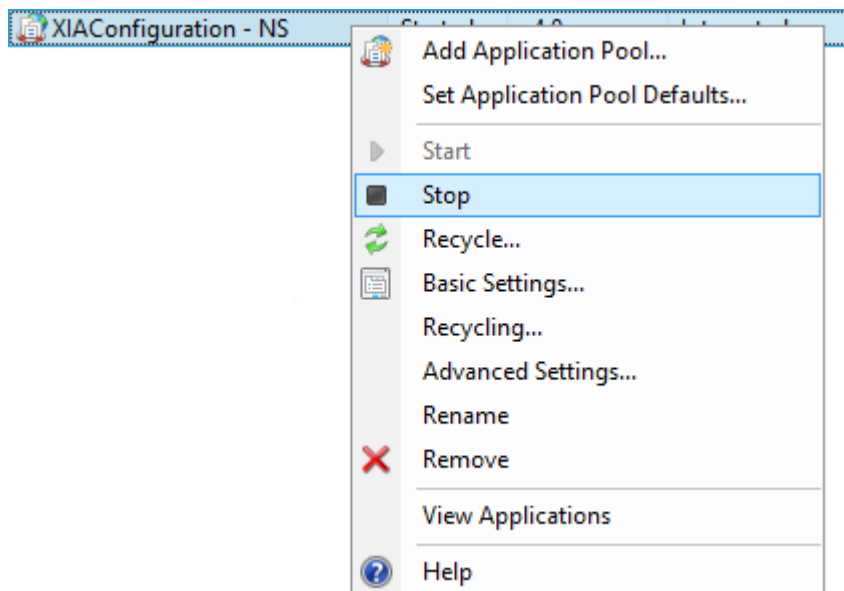
- Save the settings and close the [administration tools](#).

Web Server Account Migration

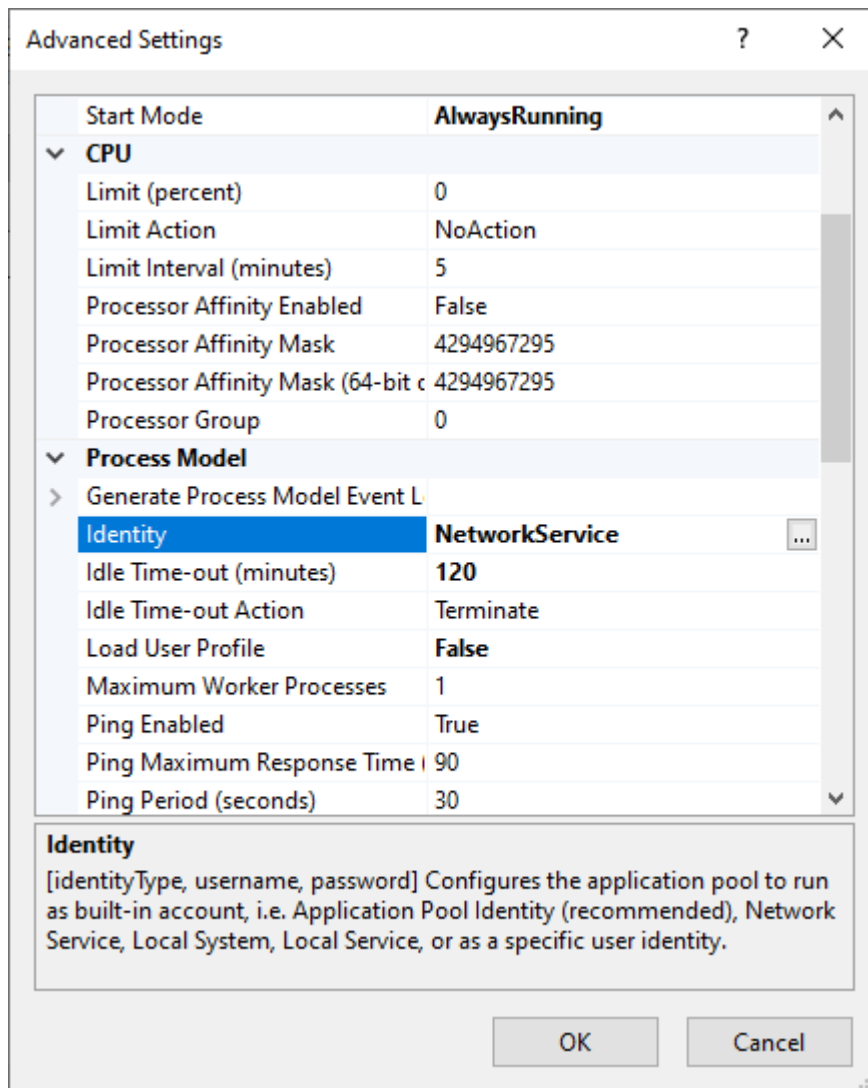
The following steps describe how to manually change the [web server account](#) after [XIA Configuration Server](#) has been [installed](#).

WARNING: This process is not recommended, the [installer](#) should be used to assign the [web server account](#).

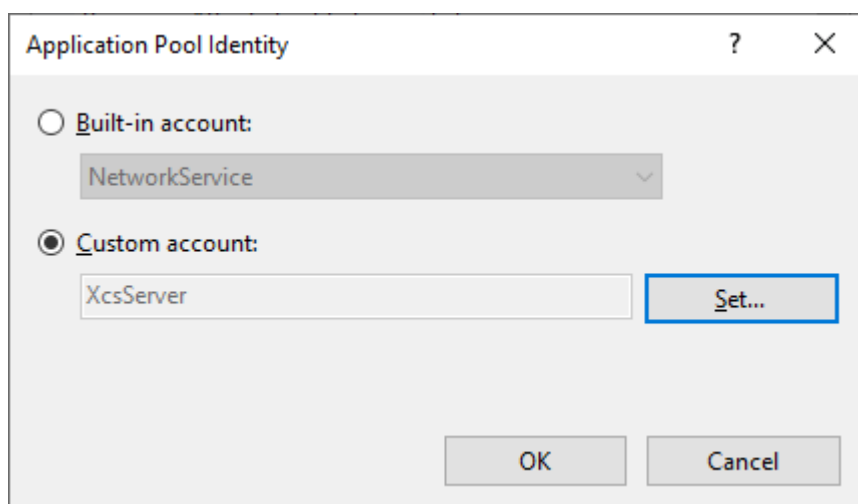
- Ensure you have a **full system backup** of the server.
- If you wish to use a custom account, create the user account that is to be used as the [web server account](#) following the guidelines in the [web server account](#) section.
- Add the [web server account](#) to the IIS_USRS group. This is not necessary when using the [Network Service](#) account.
- Open the Internet Information Services (IIS) Manager tool, and stop the [XIA Configuration](#) application pool.



- If you wish to use the [Network Service](#) account ensure that application pool is named "*VirtualDirectoryName* - NS", renaming if necessary.
NOTE: You will have to reassign the [XIA Configuration](#) application to a different application pool temporarily while renaming.
- If you wish to use custom account ensure that application pool is named "*VirtualDirectoryName*", renaming if necessary.
NOTE: You will have to reassign the [XIA Configuration](#) application to a different application pool temporarily while renaming.
- In the advanced settings of the application pool modify the **Identity** property.

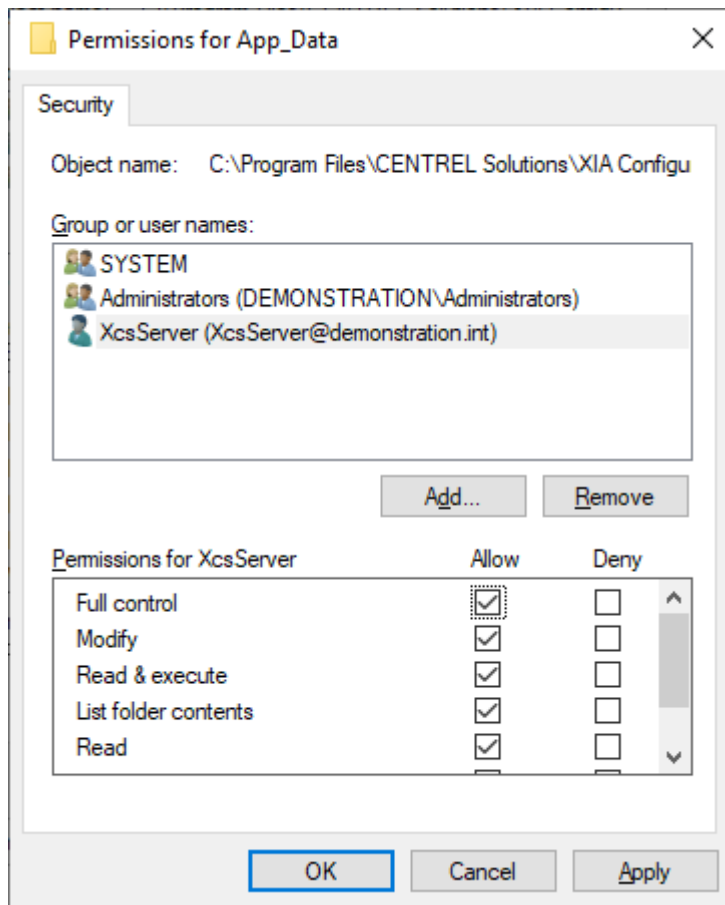


- Set the credentials for the [web server account](#) or select [Network Service](#) from the built-in account drop-down.

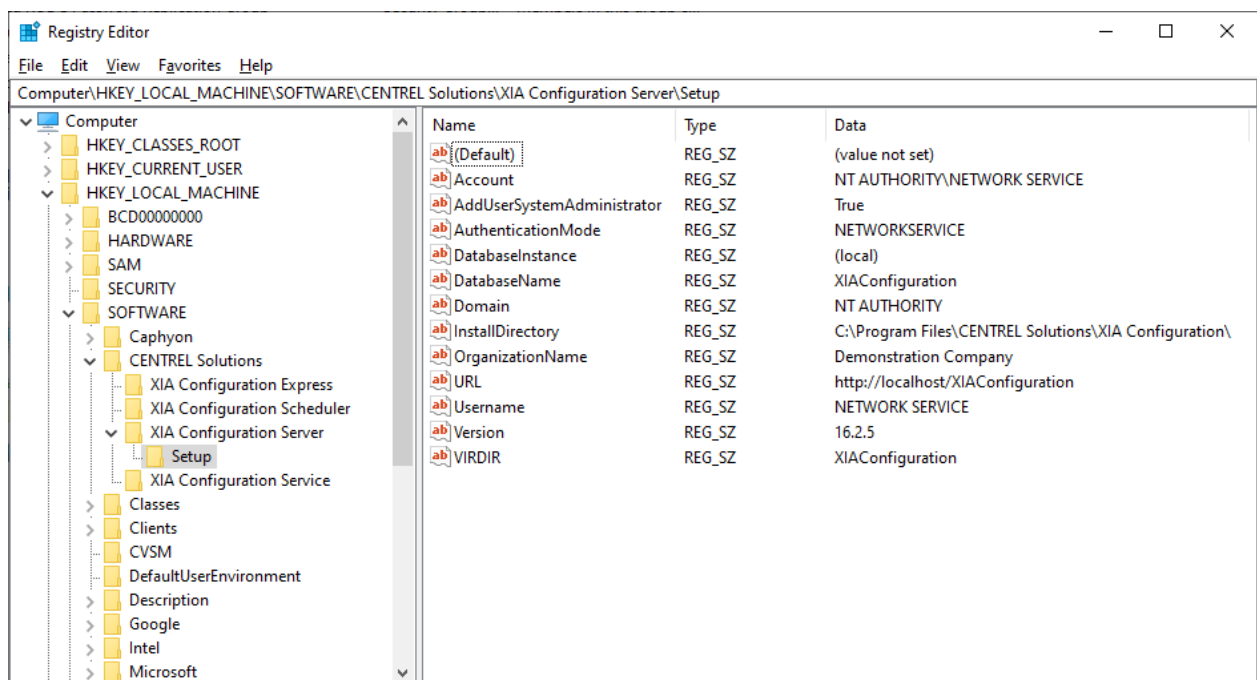


- Modify the NTFS permissions on the App_Data directory, this is located by default in the following location.
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\App_Data

- Remove the previous [web server account](#) from the access control list, and ensure that the new [web server account](#) has full control.



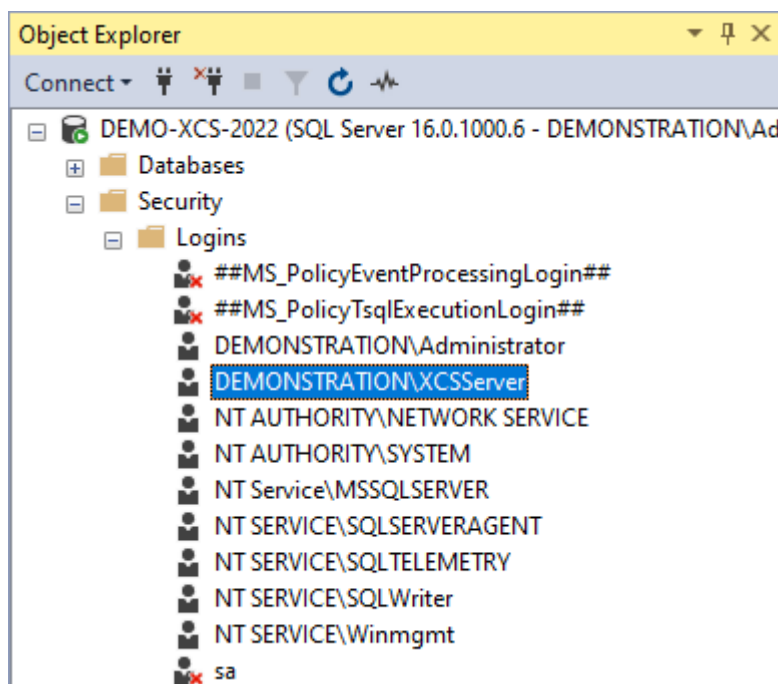
- Open Regedit and locate the following registry key
HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup



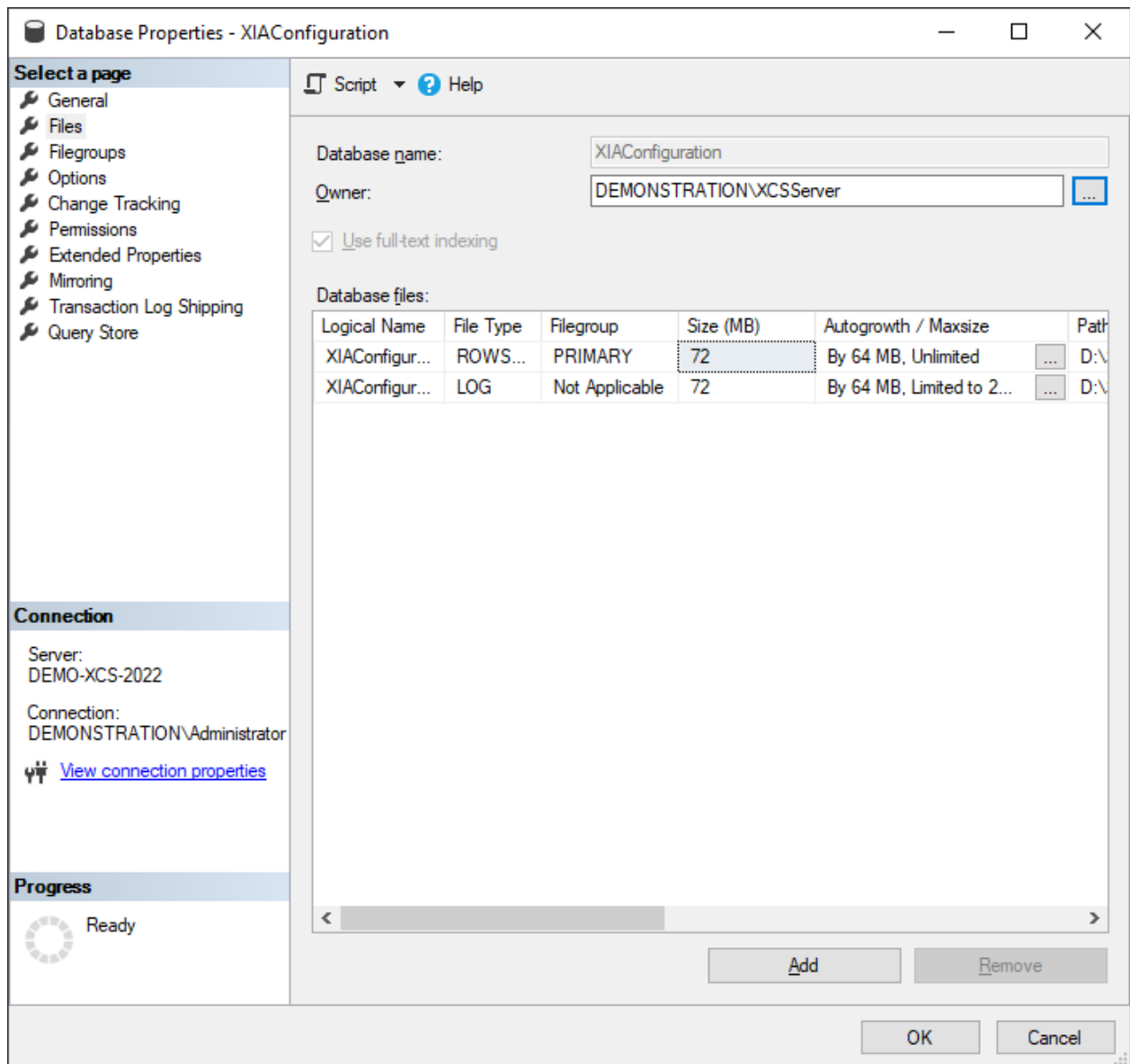
- Set the AuthenticationMode value to "NETWORKSERVICE" when using the [Network Service](#)

account, or "CUSTOM" when using a custom [web server account](#).

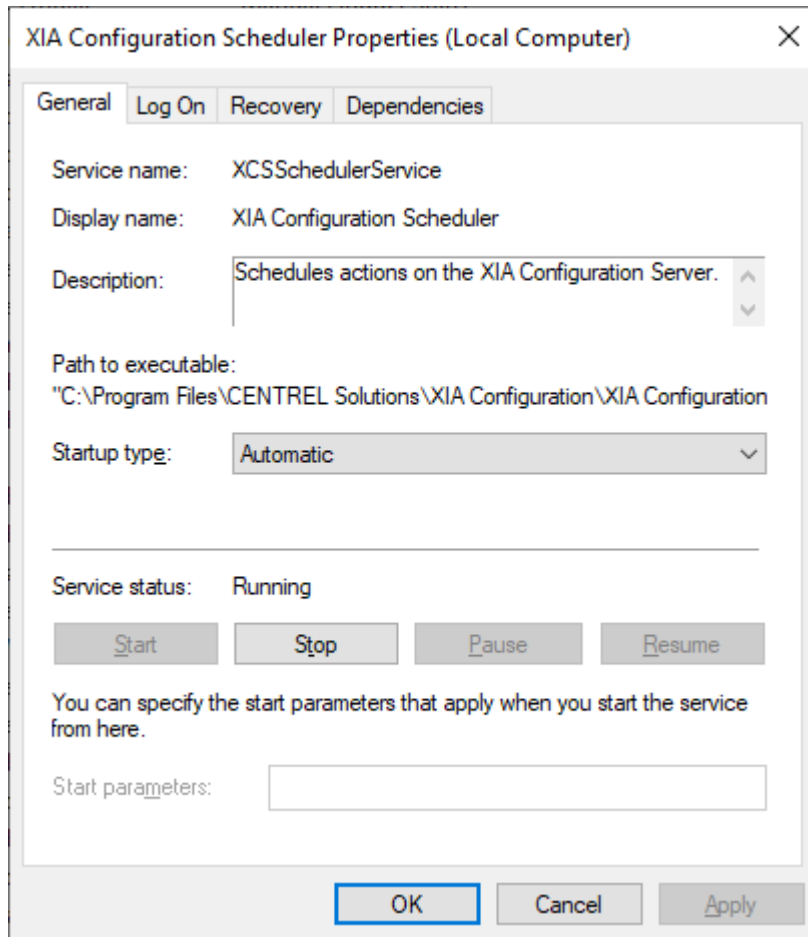
- Set the Account value to be "NT AUTHORITY\NETWORKSERVICE" when using the [Network Service](#)* account, or the full account name of the custom [web server account](#)**.
- Set the Domain value to be "NT AUTHORITY" when using the [Network Service](#)* account, or the domain name of the custom [web server account](#)**.
- Set the Username value to be "NETWORKSERVICE" when using the [Network Service](#)* account, or the username of the custom [web server account](#)**.
- Open [SQL Server Management Studio \(SSMS\)](#).
- Expand Security > Logins and ensure that the appropriate account exists, creating the account if required.



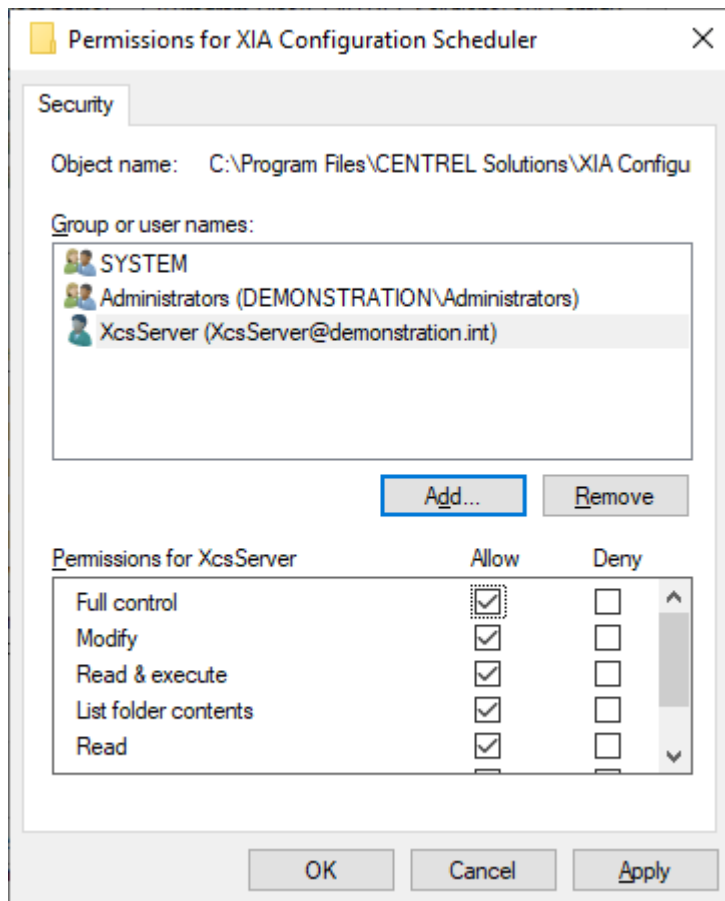
- "NT AUTHORITY\NETWORKSERVICE" when using the [Network Service](#)* account locally.
 - "*DOMAINNAME\ComputerName\$*" when using the [Network Service](#)* account over the network.
 - The account name of the custom [web server account](#)**.
- Modify the properties of the [XIA Configuration Server database](#), setting the owner to the server login from the previous step.



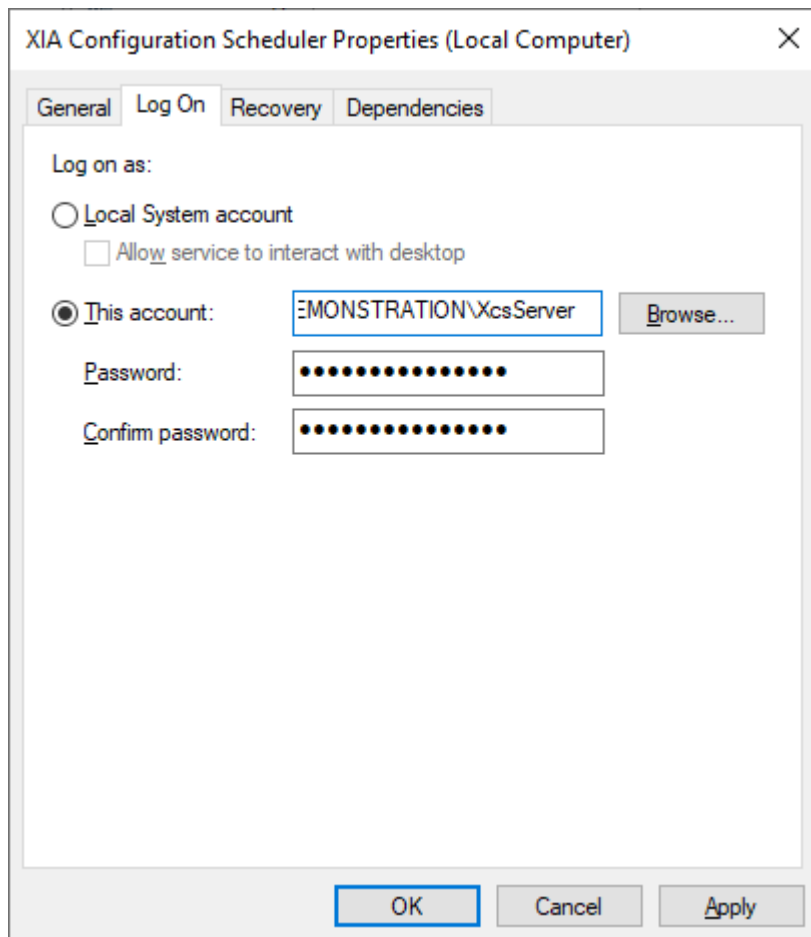
- Start the [XIA Configuration](#) application pool.
- Stop the [XIA Configuration Scheduler](#) service.



- Modify the NTFS permissions on the [XIA Configuration Scheduler](#) directory, this is located by default in the following location.
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler
- Remove the previous [web server account](#) from the access control list, and ensure that the new [web server account](#) has full control.



- Modify the logon properties and set to use the [Network Service](#)* account or account name and password of the custom [web server account](#)**.



- Start the [XIA Configuration Scheduler](#) service.
- Test that the [XIA Configuration Server](#) can be accessed through a web interface, and that scheduled tasks work as expected before proceeding.

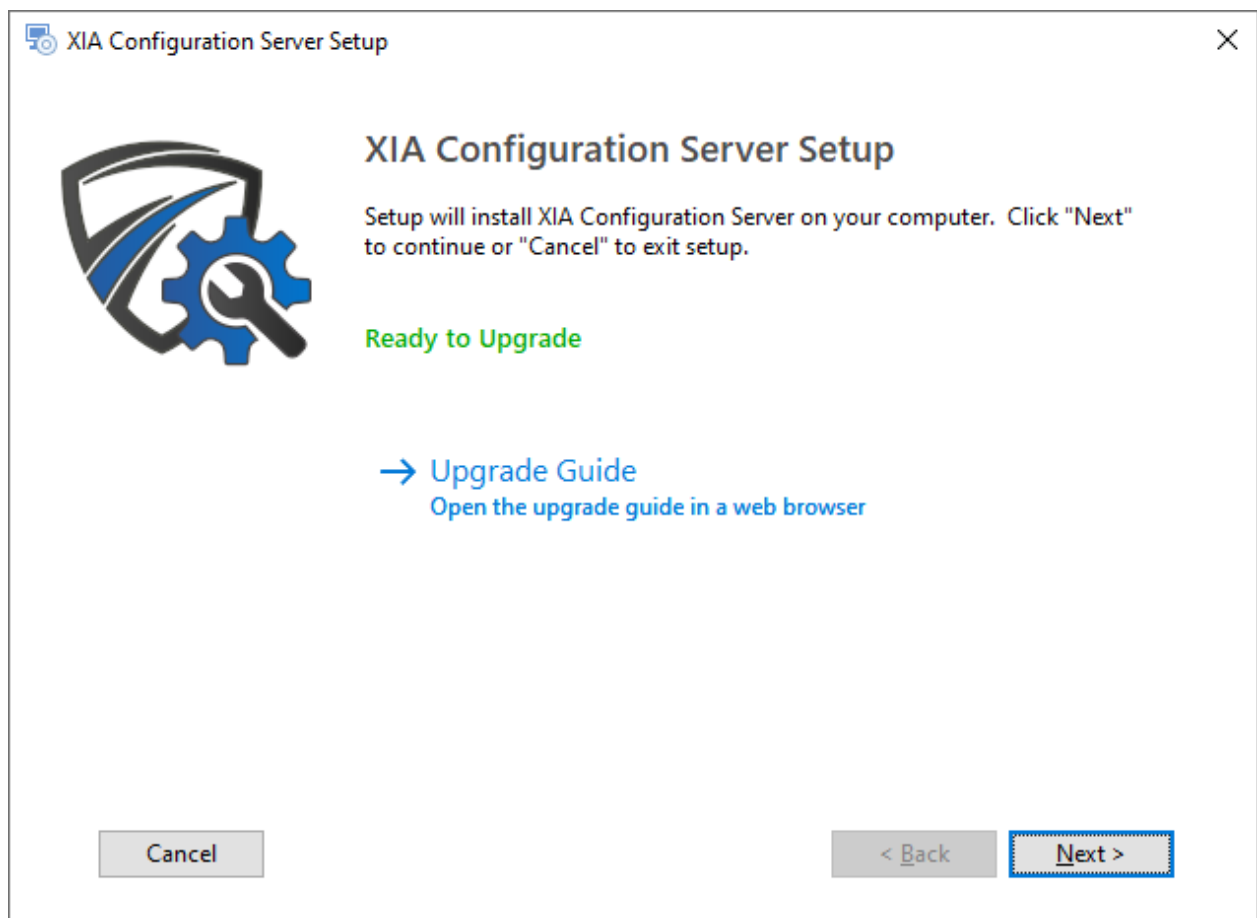
* **WARNING:** The Network Service account name differs for non-English versions of Windows.

** **WARNING:** When the [web server account](#) is on a WORKGROUP use the local computer's NetBIOS name for the domain name.

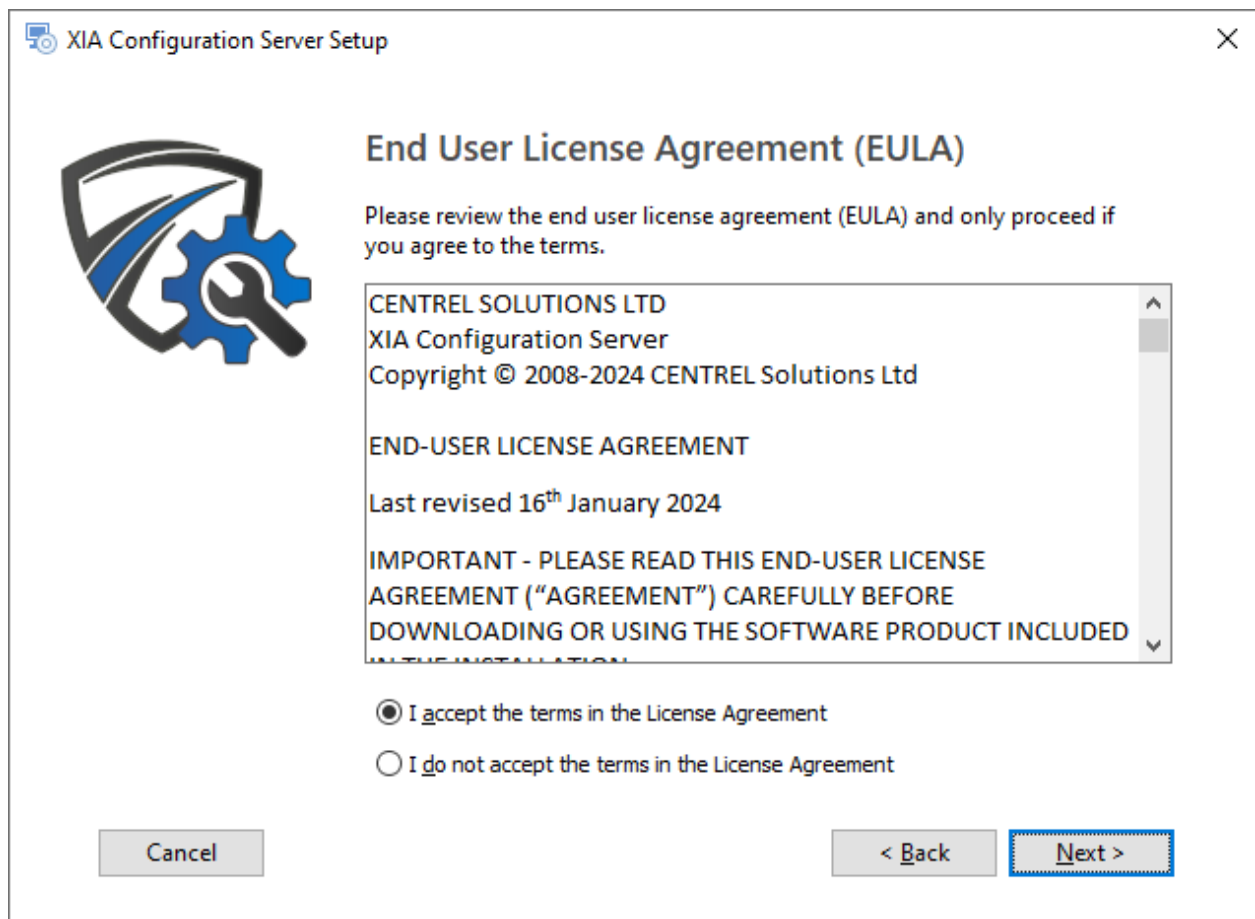
Server Upgrade

This section describes the upgrade process of [XIA Configuration Server](#), for new installations please see the [installation](#) section.

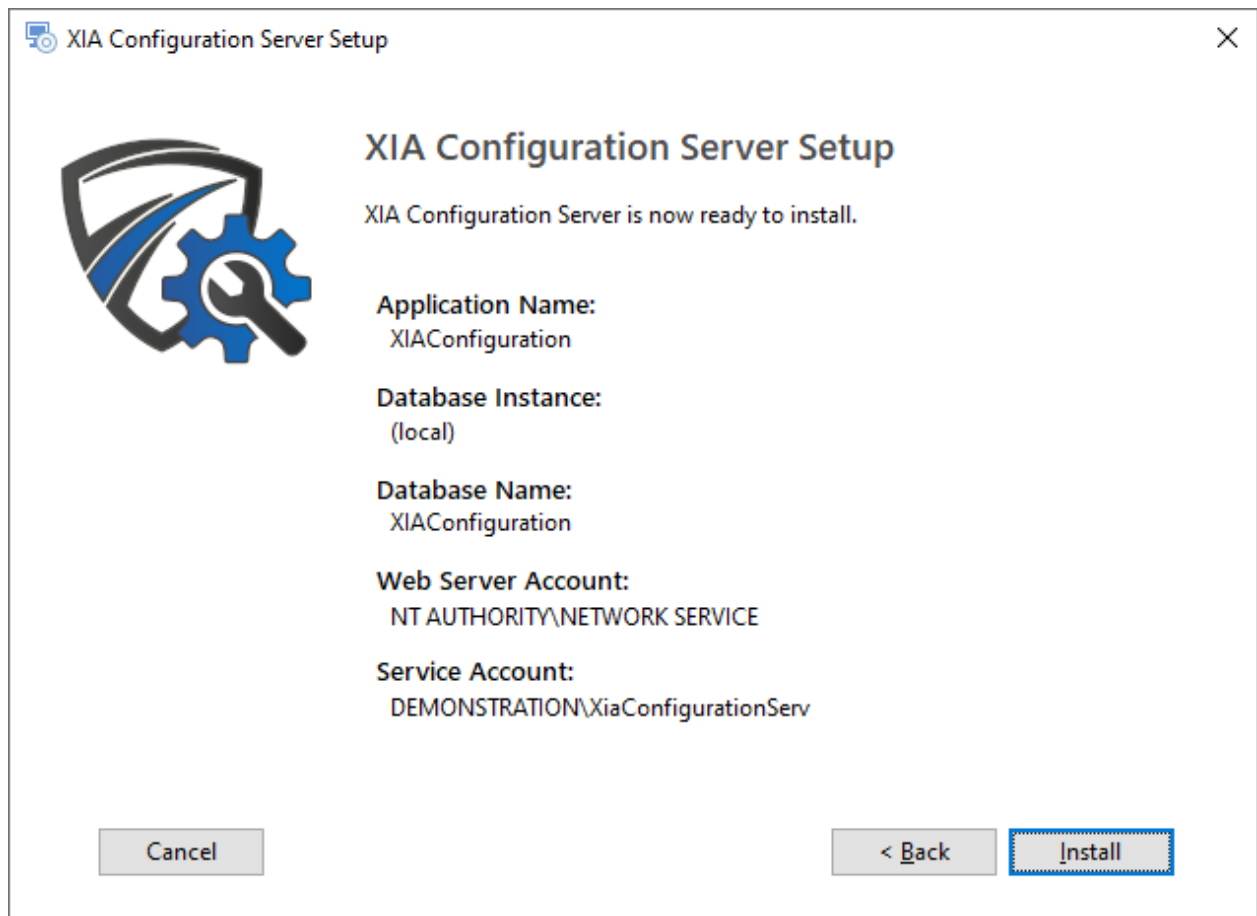
- Ensure that you have a full system backup.
- Ensure that the support expiry date of your [license](#) file is still valid, or if support has expired, later than the release date of the upgrade.
- Review the [upgrade notes](#) for the version being installed.
- Review the [roles and features](#) that will be automatically installed.
- Check that the system you are installing on meets the current [server requirements](#).
- Check that you have a database server that meets the current [database requirements](#).
- Download the [latest installation package](#).
- Start the installation, the system should report *Ready to Upgrade*, click *Next*.



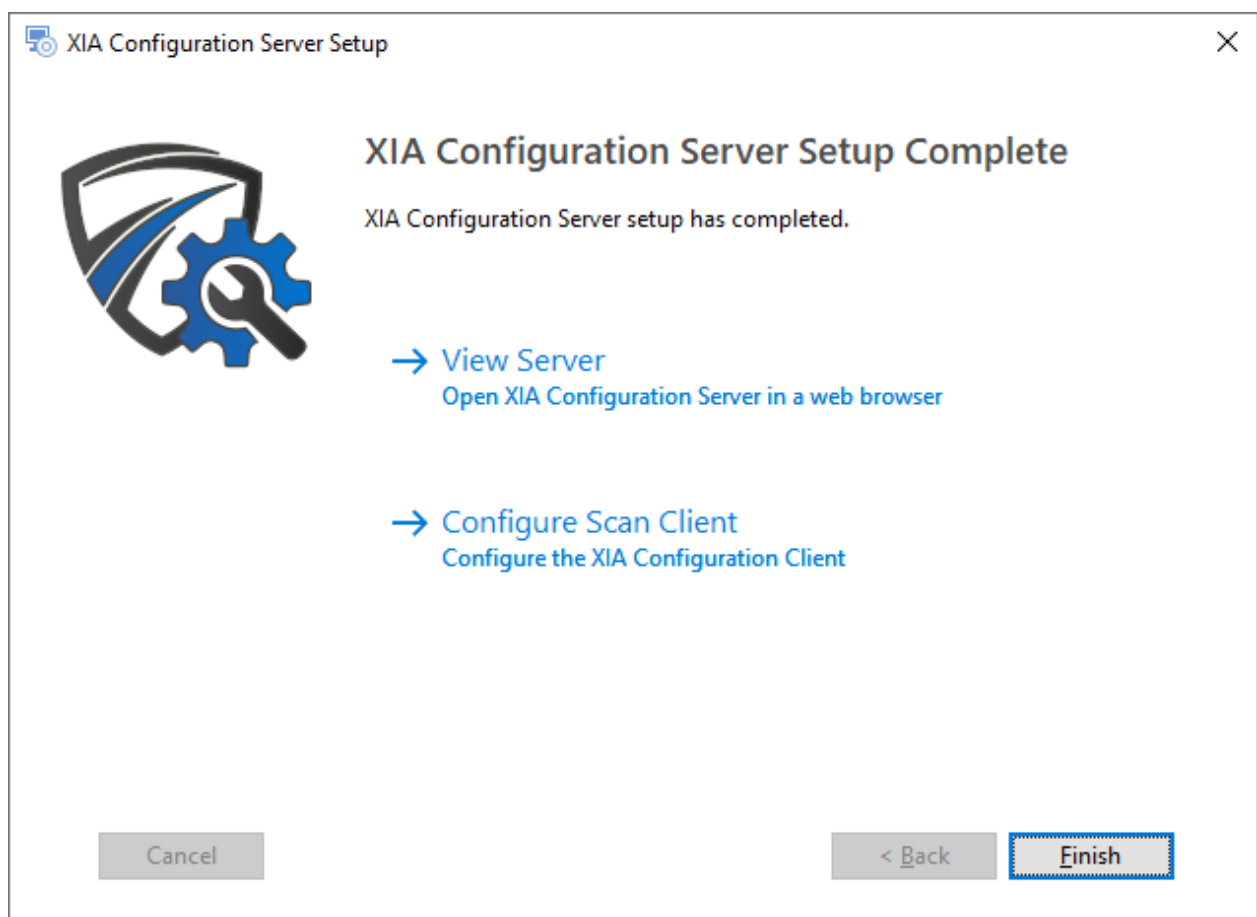
- Review the end user license agreement (EULA) and only accept if you agree to the terms. If you do not accept the terms of the agreement please cancel the upgrade.



- The *Ready to Install* dialog will be shown, click *Install* to start the installation.



- Click *Finish* to complete the upgrade.



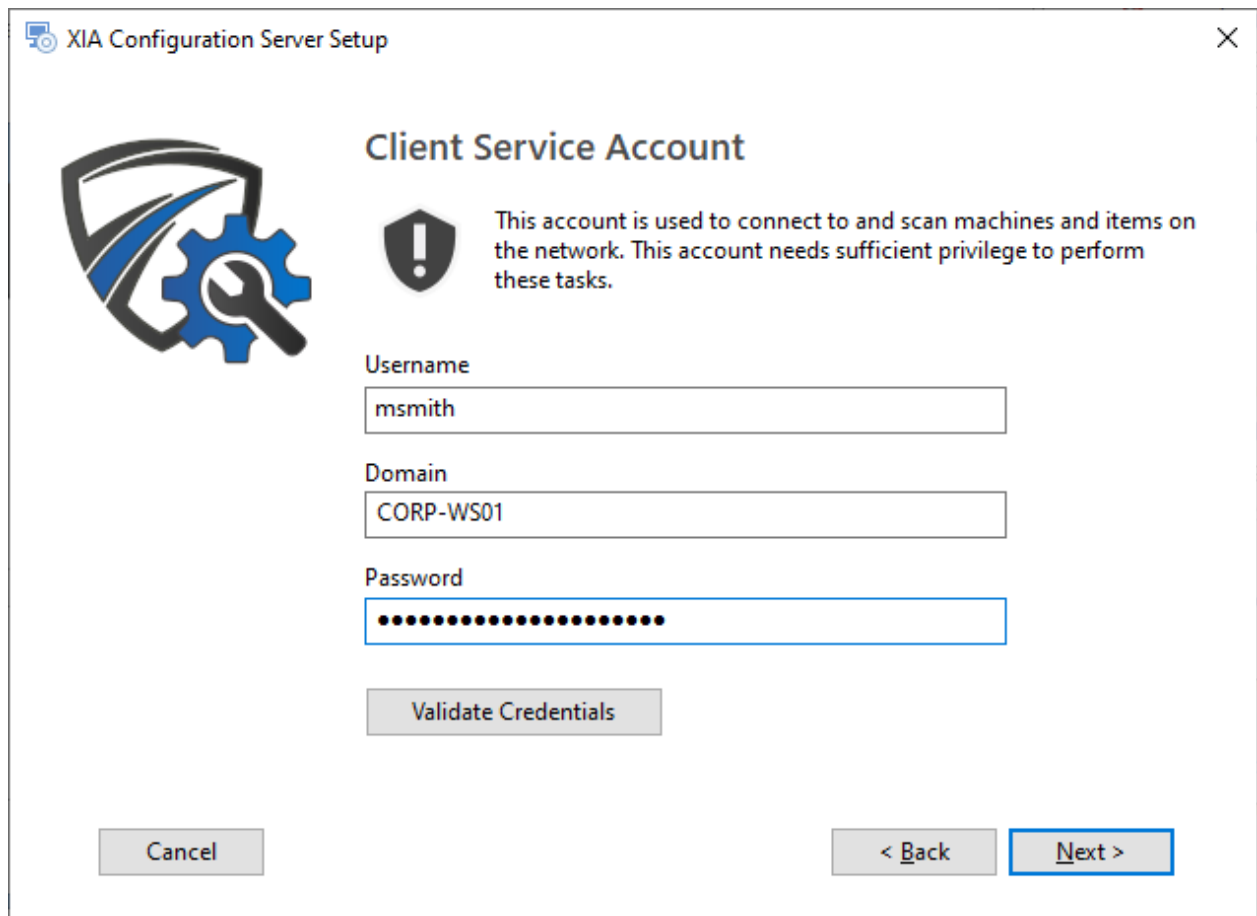
Technician License Installation Best Practice

The [technician license](#) is designed for use by IT professionals to perform an audit of customer, or prospective customer environments.

NOTE: Each technician license may be used by one IT professional on a single machine only, the machine cannot be shared or used by others. For more information see the [End User License Agreement \(EULA\)](#).

The following process describes the best practice for the installation and use of the [technician license](#).

- Select a laptop or virtual machine that will be used for the [installation](#) that meets the [server requirements](#).
- Ensure that the NetBIOS computer name of the machine matches the name specified in the [technician license](#) that you have purchased - for example "CORP-WS01".
- If you are planning to [scan customer environments directly](#) the machine should be a WORKGROUP member rather than a member of a domain to simplify its connection to customer environments.
- Create a local user account in the name of the technician - for example "msmith". It is also possible to use an Active Directory domain account if the machine is not a WORKGROUP member. Ensure that this user account name matches the name specified in the [technician license](#) that you have purchased - for example "CORP-WS01\msmith".
- Add the user account to the local Administrators group.
- Logon as the user account and follow the [installation instructions](#). The user account will be automatically added as a [system administrator](#). Only the user account specified in the [technician license](#) is able to access the [server](#) installation.
- When prompted the same user account can be specified for the [service account](#) or a dedicated account created if required. This account will be used to run the [XIA Configuration Client service](#), however [custom credentials](#) will need to be specified when [scanning customer environments directly](#).



The screenshot shows the 'XIA Configuration Server Setup' window. On the left is a logo featuring a shield and a gear. The main title is 'Client Service Account'. Below the title is a warning icon and a text box stating: 'This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks.' There are three input fields: 'Username' with the value 'msmith', 'Domain' with the value 'CORP-WS01', and 'Password' which is masked with dots. Below these fields is a 'Validate Credentials' button. At the bottom, there are three buttons: 'Cancel', '< Back', and 'Next >'. The 'Next >' button is highlighted with a blue border.

XIA Configuration Server Setup

Client Service Account

This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks.

Username
msmith

Domain
CORP-WS01

Password
.....

Validate Credentials

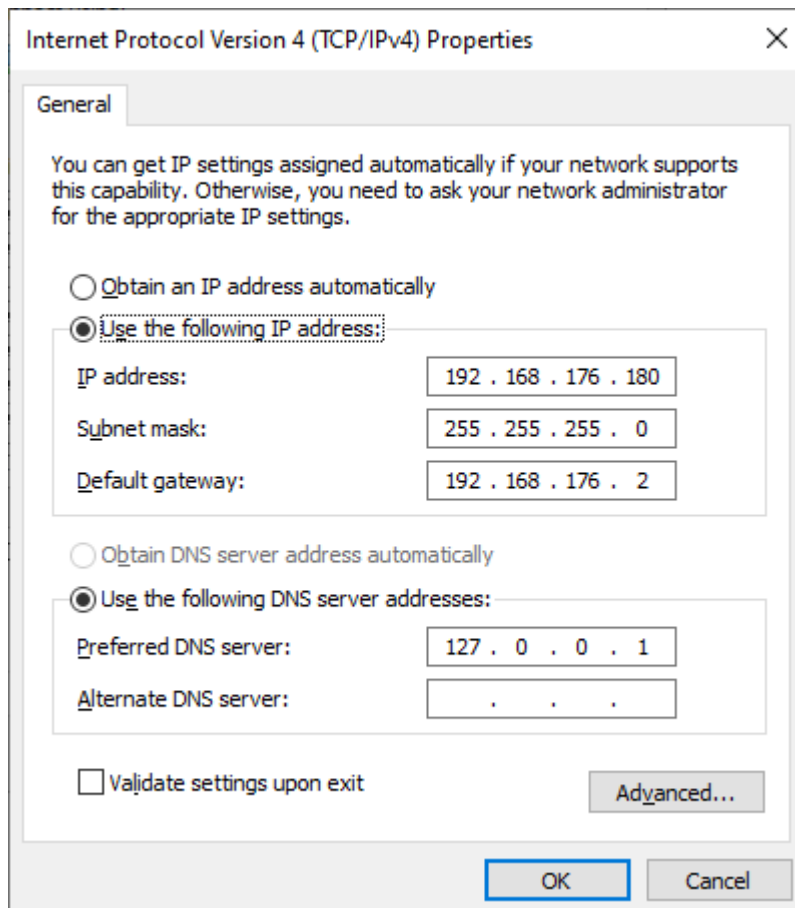
Cancel < Back Next >

- If using [scan tasks](#) that require [PowerShell remoting](#) it is recommended to configure the [trusted hosts setting](#). This is done automatically by the [installer's "Enable PowerShell Remoting and configure trusted hosts settings" advanced option](#).
- When the installation is complete, follow the steps in the [scanning customer environments \(directly\)](#) or [scanning customer environments \(with XIA Configuration Client\)](#) section to perform a scan.

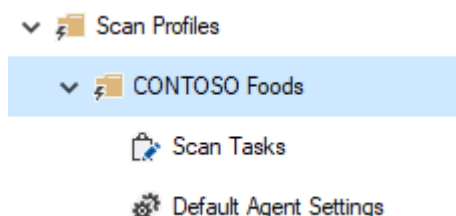
Scanning Customer Environments (Directly)

Once the steps in the [technician license installation best practice](#) have been completed the following steps describe how to connect to, and scan a customer environment directly from the computer where the [XIA Configuration Server](#) is installed.

- Connect the machine to the customer network and ensure that valid IP addressing information is provided by DHCP, otherwise this may have to be configured manually.



- Create a new [scan profile](#) for the customer.



- Configure the [credentials](#) to scan the customer environment as required in the [scan profile](#) settings.

Scan Profile Settings

Exclusions

Email Notifications

Performance

General

Credentials

Server Upload

File Output

Credentials

The credentials to use for the scan profile.

☐ Use default credentials

☒ Use the following credentials

Username

xiaconfiguration

Domain

contosofoods.int

Password

••••••••••••••••

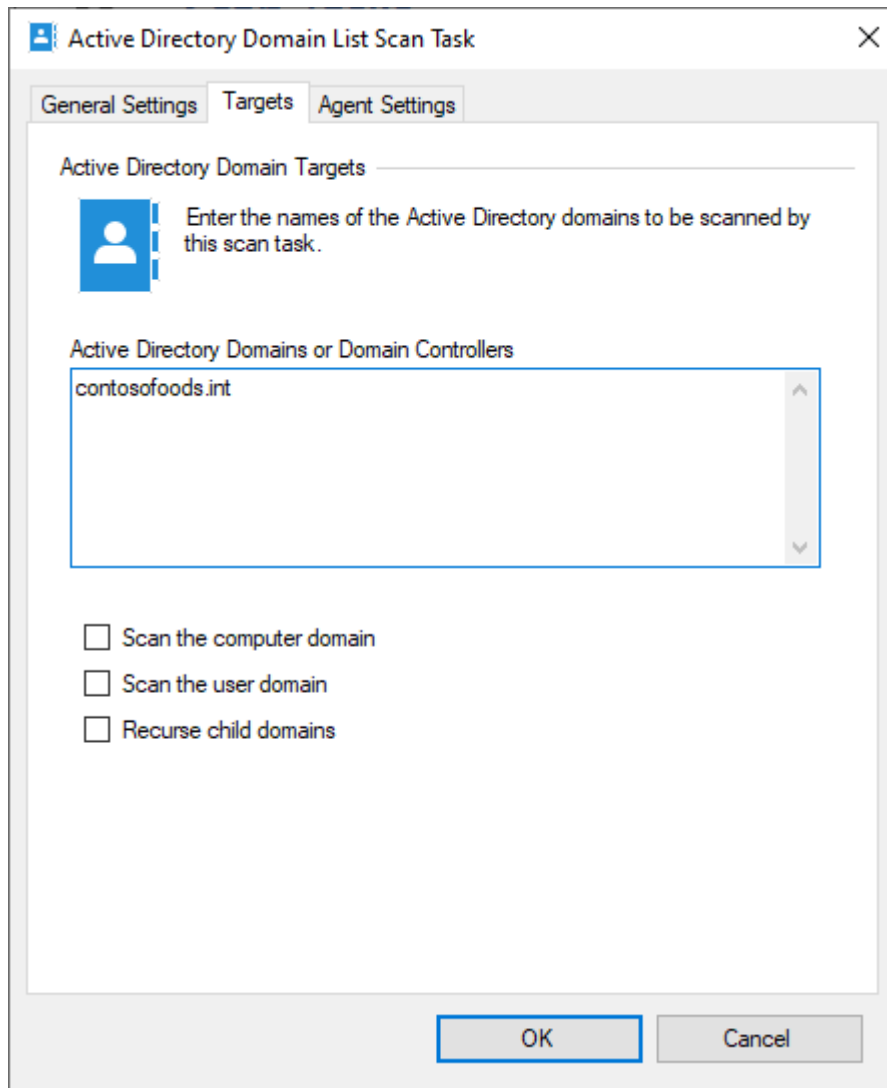
The specified credentials will be used to scan remote systems and upload to the XIA Configuration Server when hosted on a remote machine.

OK

Cancel

- Create an [Active Directory Domain](#) scan task to document the [Active Directory](#) domain if required.

NOTE: The *Scan default computer domain* option cannot be used as the computer is not a domain member.



The screenshot shows a dialog box titled "Active Directory Domain List Scan Task" with a close button (X) in the top right corner. The dialog has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the "Targets" tab, there is a section titled "Active Directory Domain Targets" with a blue icon of a person. Below the icon, it says "Enter the names of the Active Directory domains to be scanned by this scan task." Below this text is a list box titled "Active Directory Domains or Domain Controllers" containing the text "contosofoods.int". At the bottom of the list box are up and down arrow buttons. Below the list box are three checkboxes: "Scan the computer domain", "Scan the user domain", and "Recurse child domains", all of which are currently unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons.

- Create an [Active Directory Search](#) scan task to search the Active Directory domain if required.
NOTE: The *[Default Computer Domain]* option cannot be used as the computer is not a domain member.

The screenshot shows the 'Active Directory Search Scan Task' dialog box with the 'Search Settings' tab selected. The dialog has three tabs: 'General', 'Search Settings', and 'Agent Settings'. The 'Search Settings' tab contains a search icon and the text 'The search settings for the scan task.' Below this is a 'Search Paths' section with a table:

Path	Recurse
LDAP://contosofoods.int	True

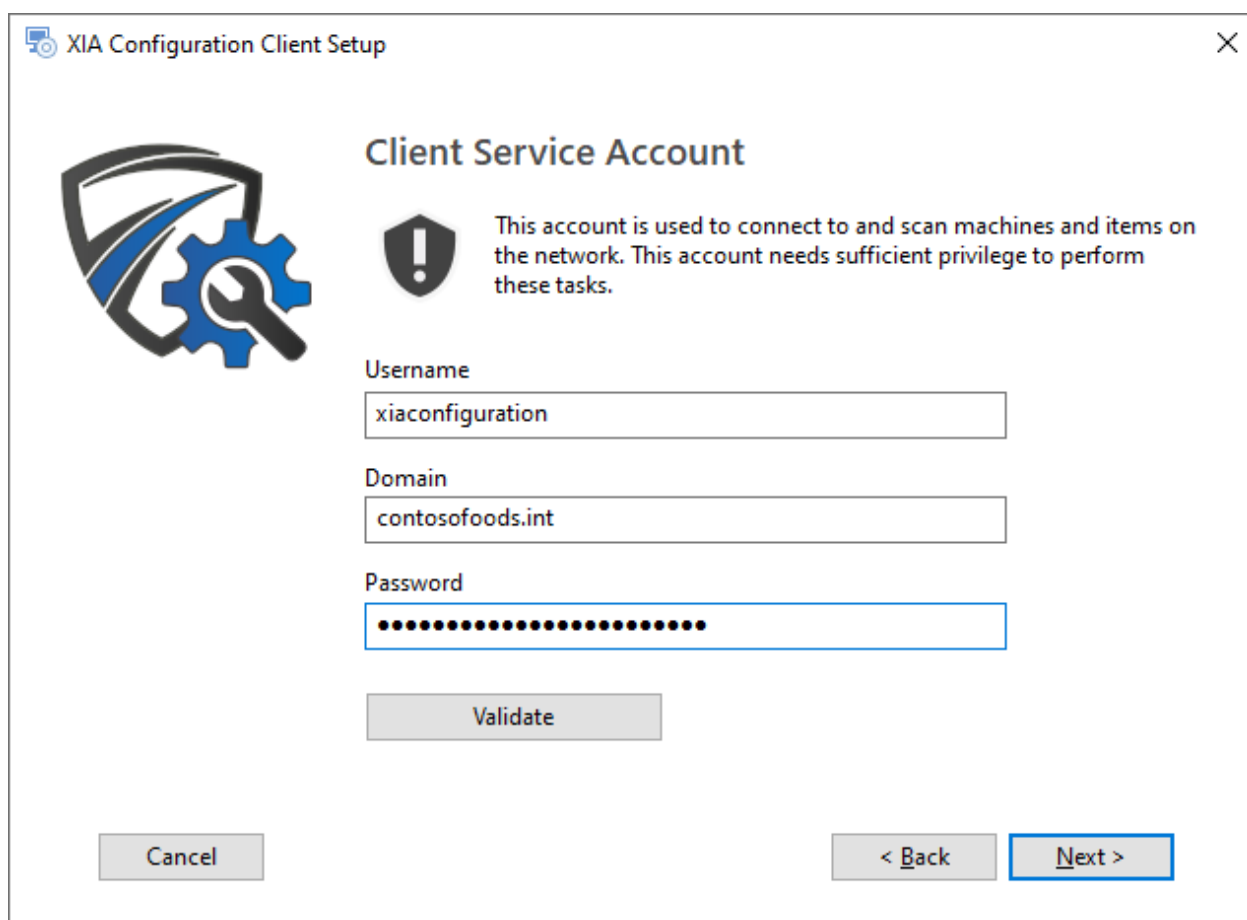
Below the table is a 'Search Type' dropdown menu set to 'Windows Servers'. Underneath is a 'Search Filter' text box containing the LDAP filter: `(&(&(objectCategory=computer)(objectClass=user)(!useraccountcontrol:1.2.840.113556.1.4.803:=2)(operatingSystem=*server*)))`. At the bottom of the dialog are 'OK' and 'Cancel' buttons, and an 'Advanced' button is located above the 'OK' button.

- Create any additional [scan tasks](#) as required.
- **NOTE:** Due to the default configuration of a [Microsoft Exchange](#) on-premises organization, you may need to manually enter the [credentials](#) in the [Exchange on-premises scan task](#).
- **NOTE:** Due to scanning across domains it may be necessary to [configure the TrustedHosts setting](#) for [PowerShell remoting](#). This is configured by default by the [installation](#).

Scanning Customer Environments (with XIA Configuration Client)

Once the steps in the [technician license installation best practice](#) have been completed the following steps describe how to install a copy of the XIA Configuration Client in the customer environment, scan the customer environment and send the data to the [XIA Configuration Server](#).

- Select a machine in the customer environment that meets the [client installation requirements](#).
- [Install](#) the [XIA Configuration Client](#) specifying [credentials](#) appropriate for the customer environment when prompted.



The screenshot shows the 'XIA Configuration Client Setup' window. The title bar includes a gear icon and the text 'XIA Configuration Client Setup'. The main content area is titled 'Client Service Account'. On the left is a shield icon with a gear and a magnifying glass. To the right of the icon is a warning icon (shield with an exclamation mark) and the text: 'This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks.' Below this text are three input fields: 'Username' with the value 'xiaconfiguration', 'Domain' with the value 'contosofoods.int', and 'Password' with a masked password (dots). Below the password field is a 'Validate' button. At the bottom left is a 'Cancel' button. At the bottom right are two buttons: '< Back' and 'Next >', with the 'Next >' button highlighted with a blue border.

- Modify the [server](#) settings and specify the appropriate connection settings for the [XIA Configuration Server](#).

Service Settings

Automatic Updates Registration Maintenance

General Network Security **Server** SMTP

Server Settings

Enter the details required to connect to the server, this can be set at the service and scan profile level.

☐ Inherit service settings

☒ Connect to server

☐ Use default credentials

☒ Use the following credentials

Username

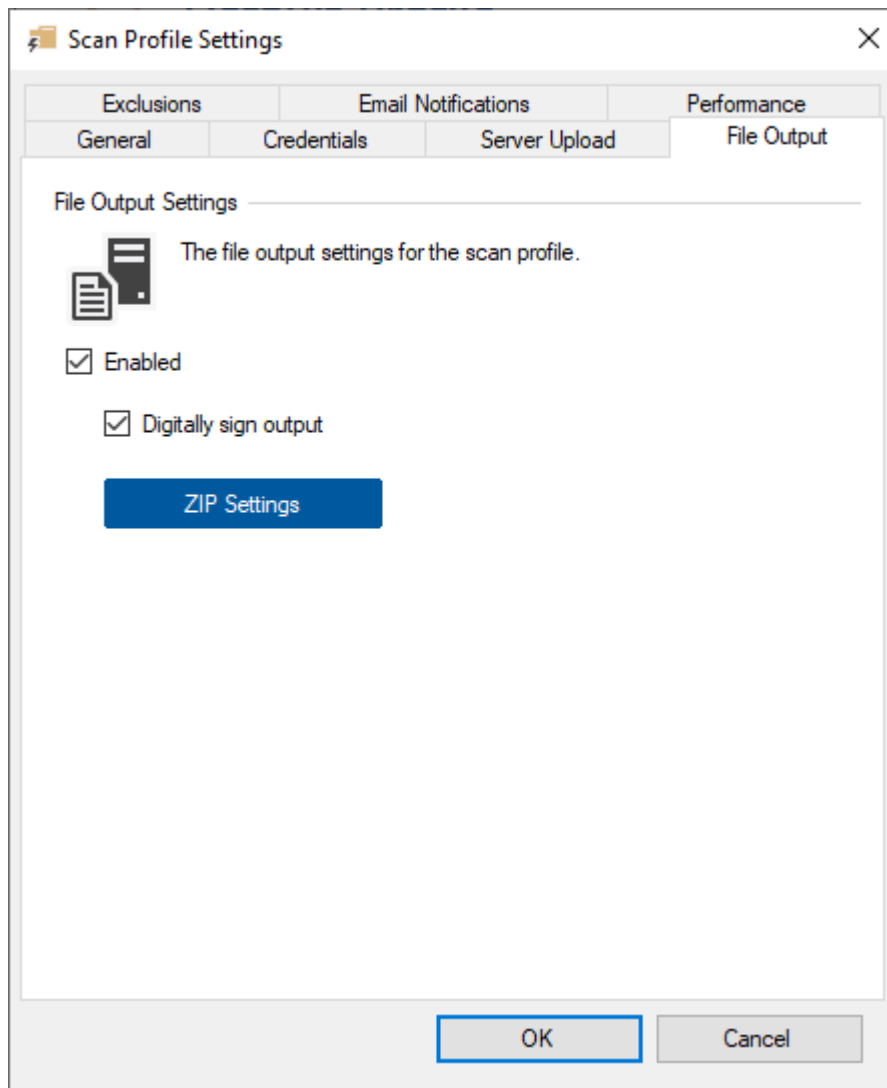
Domain

Password

Advanced Settings **Test Connection**

OK **Cancel**

- If the machine running [XIA Configuration Server](#) is not accessible through HTTP/S it is possible to transfer the data from the [XIA Configuration Client](#) manually by following the steps below.
- Modify the [scan profile](#) and ensure that the [file output settings](#) are enabled.

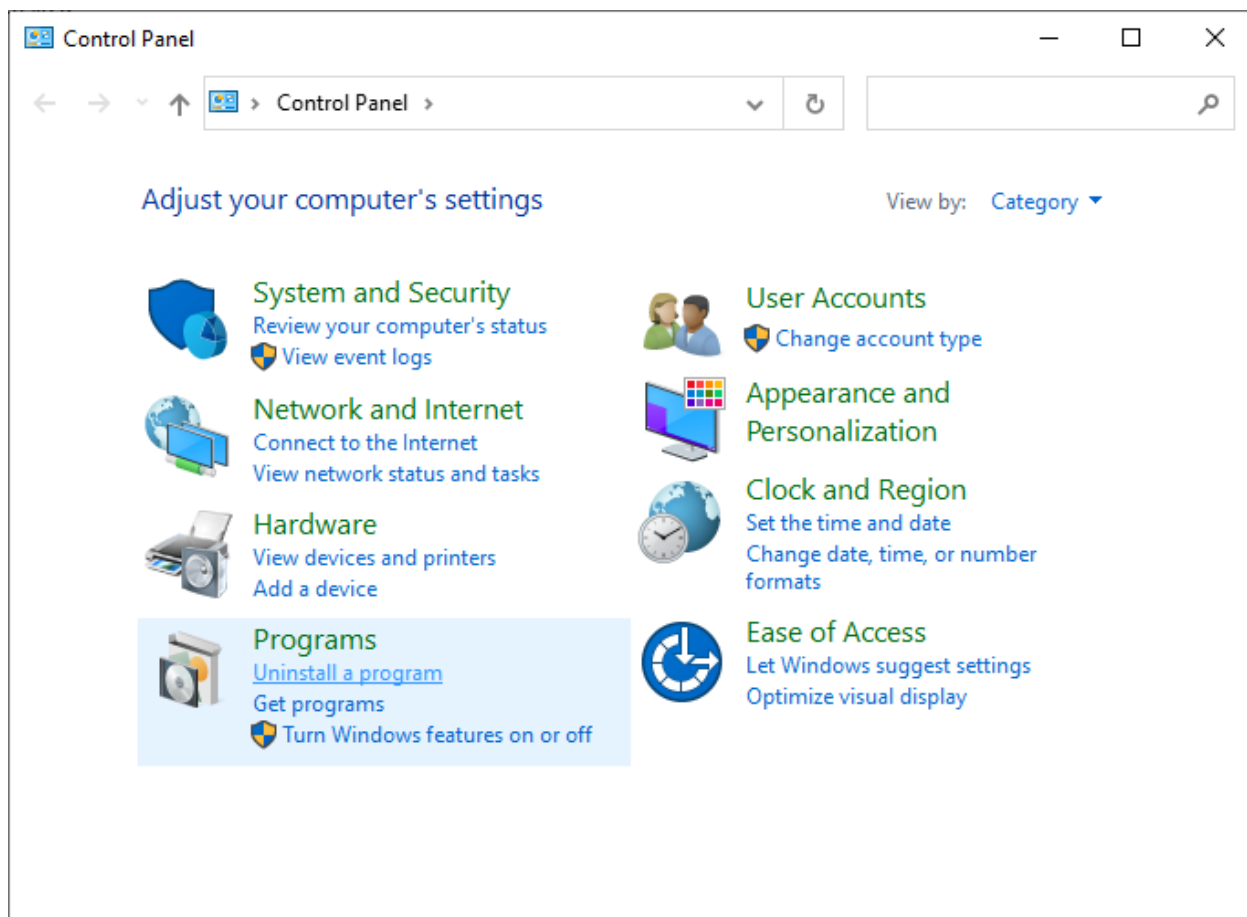


- This will save the scan data to the file system on the machine running the [XIA Configuration Client](#) by default in the following location.
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Data\data.zip
- Copy the data file to the computer running [XIA Configuration Server](#) and [upload the data manually](#).

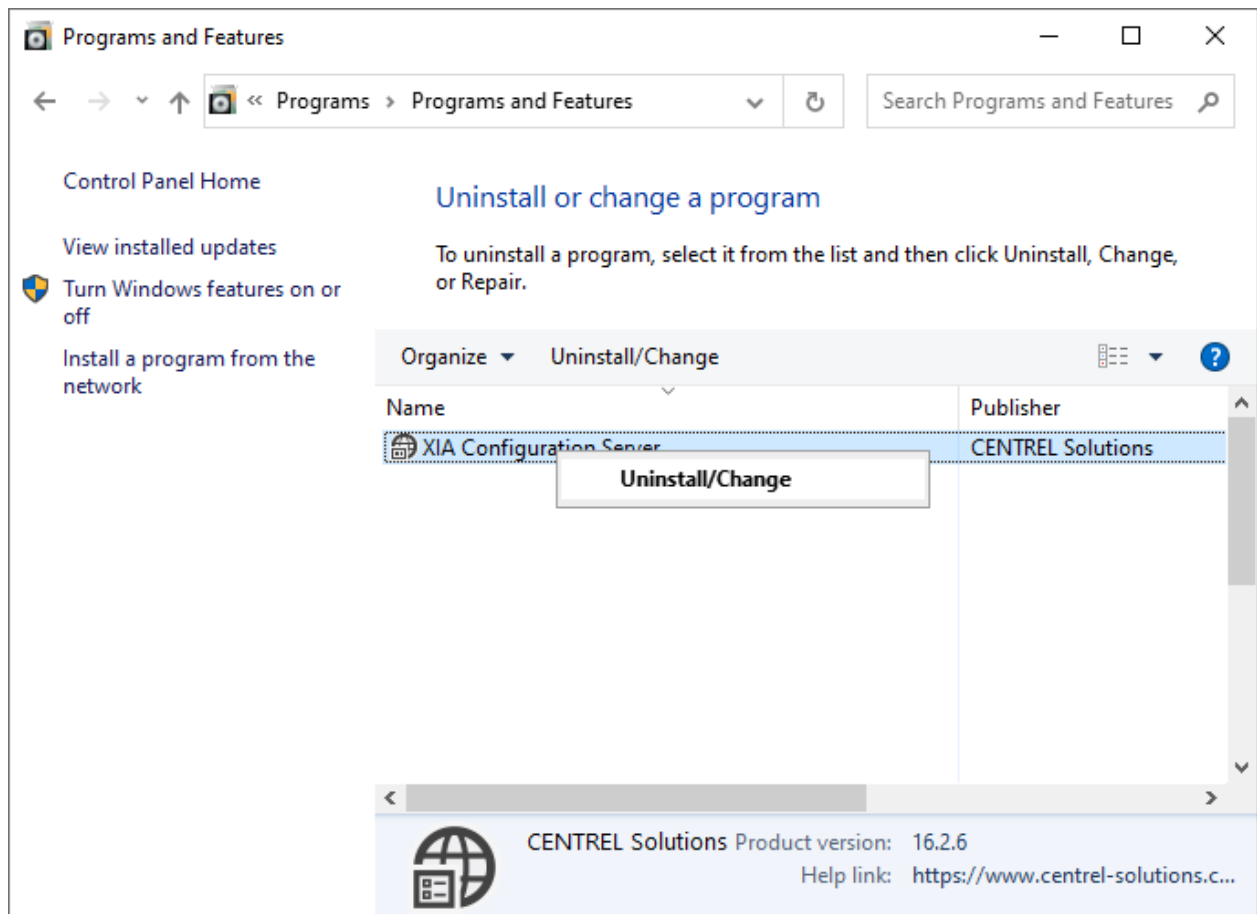
Uninstallation

To uninstall *XIA Configuration Server*

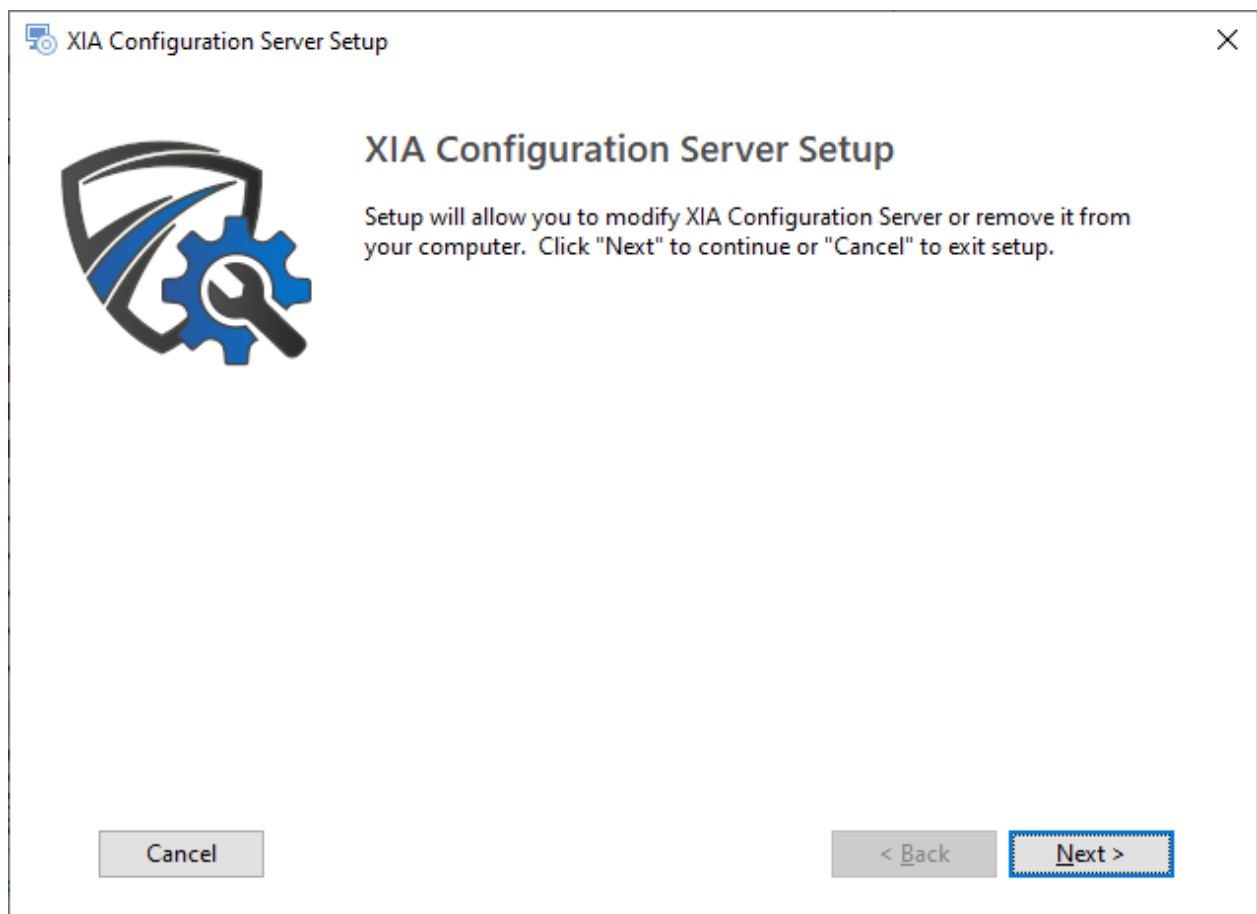
- Go to Control Panel, *Programs*, *Uninstall a program*.



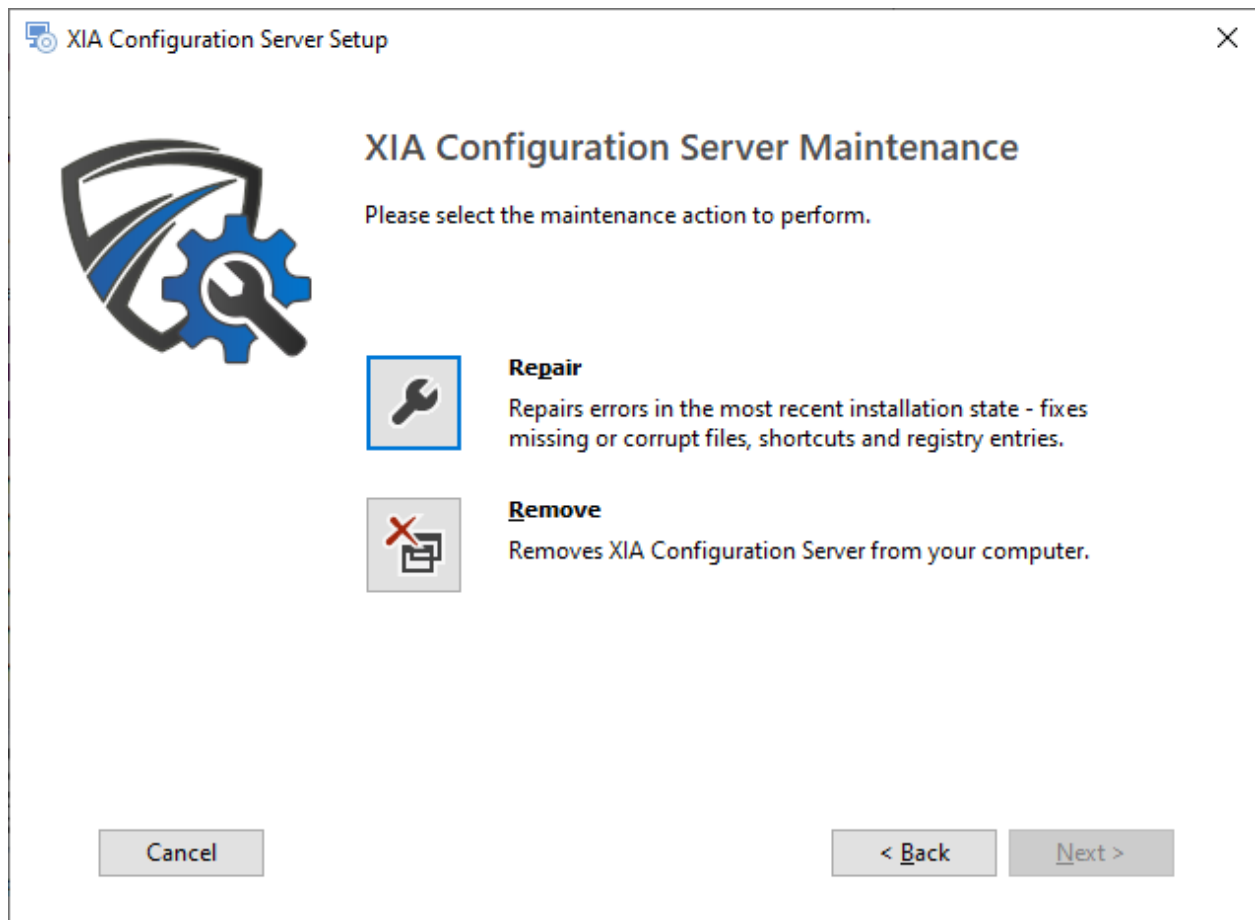
- Right click *XIA Configuration Server* and select *Uninstall/Change*.



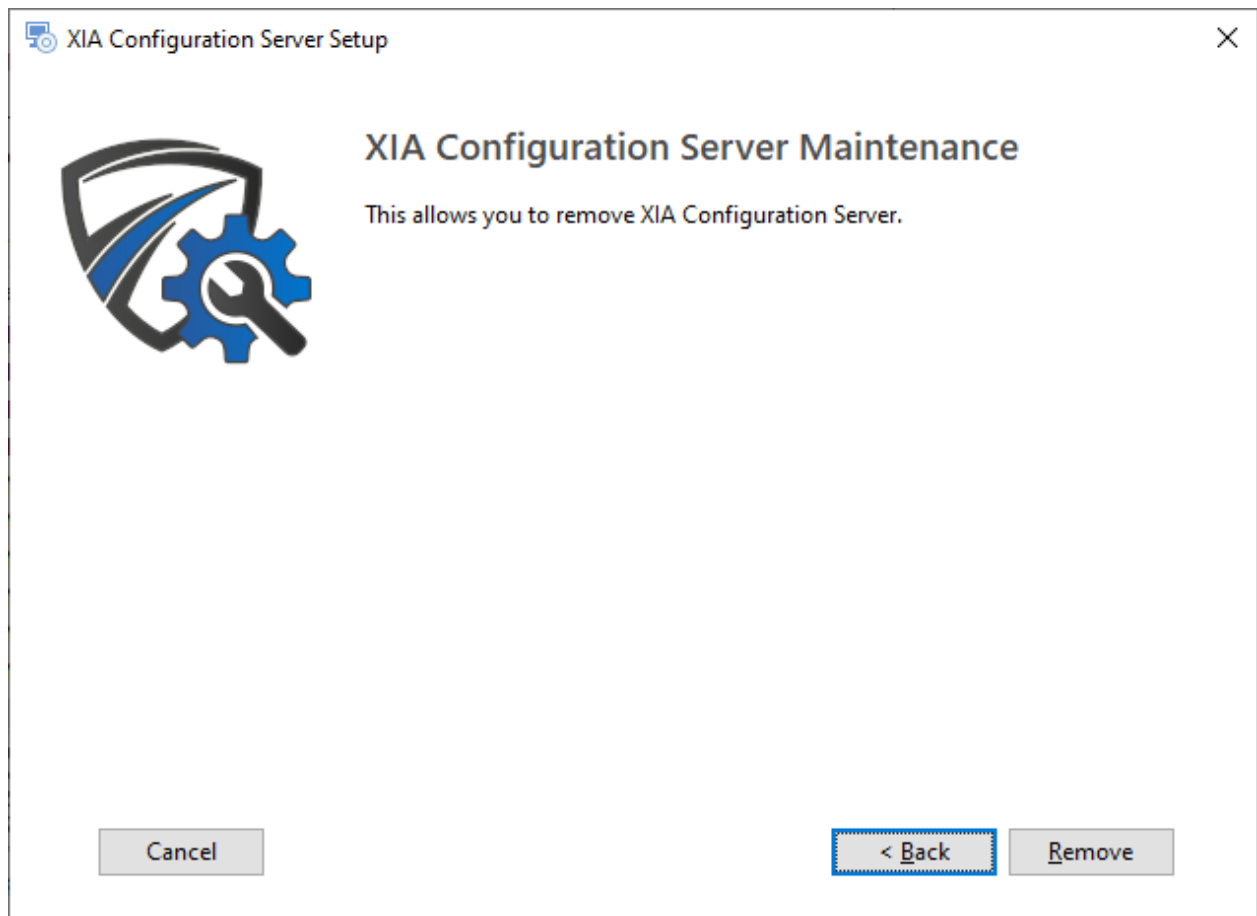
- The wizard welcome screen will be displayed, click Next to continue.



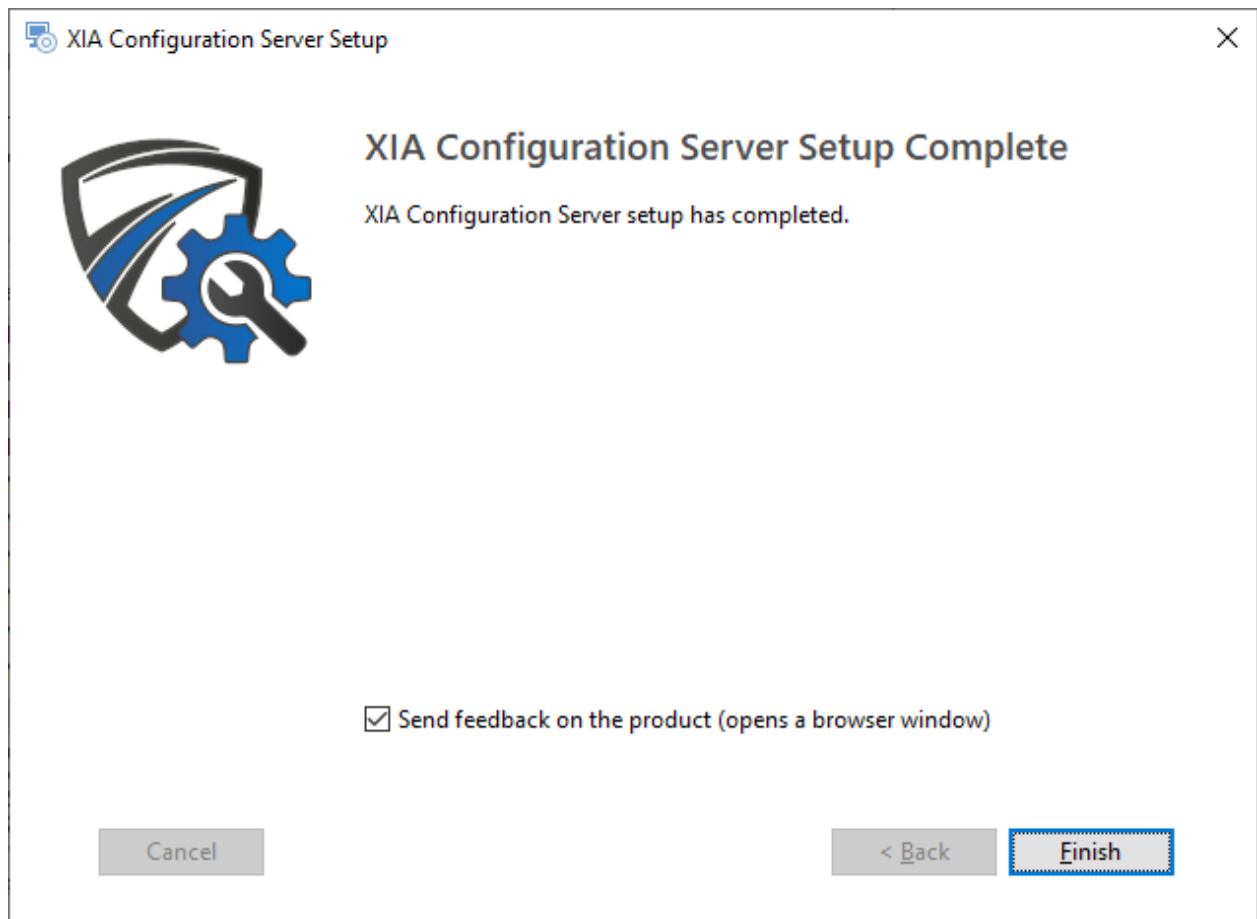
- Click the *Remove* button.



- To continue with the removal, click the *Remove* button.



- Click *Finish* to complete the removal. The *show feedback on the product* checkbox automatically launches a web browser when you click the *Finish* button allowing you to provide feedback on the product.



NOTE: Certain shared [roles and features](#) are automatically installed by the product, you may need to review these and remove them manually if they are no longer required.

If you experience any problems, please see the [manual uninstallation instructions](#).

Manual Uninstallation Instructions

WARNING:

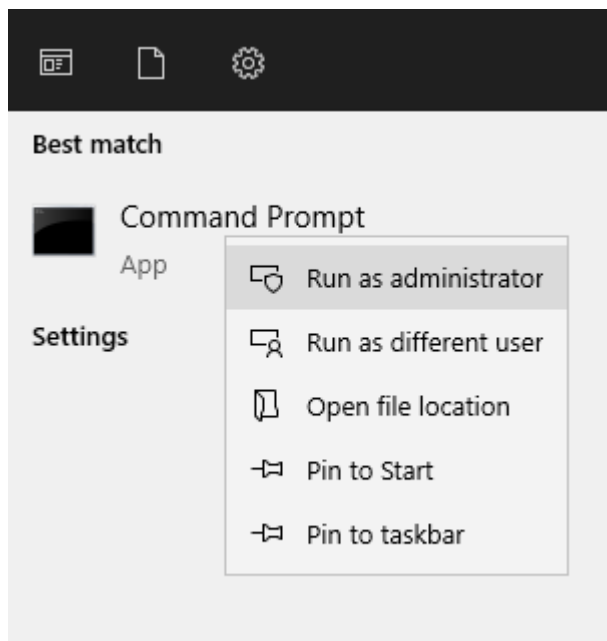
You should always remove XIA Configuration Server using the [uninstallation instructions](#) unless there is a problem preventing this process from completing.

Using **Registry Editor** incorrectly can cause serious problems that may require you to reinstall your operating system.

These instructions are provided as guidance only and are completed at your own risk. If you have any questions or concerns, do not proceed, instead, log a support call at the following address <https://www.centrel-solutions.com/support/logsupportcall.aspx>.

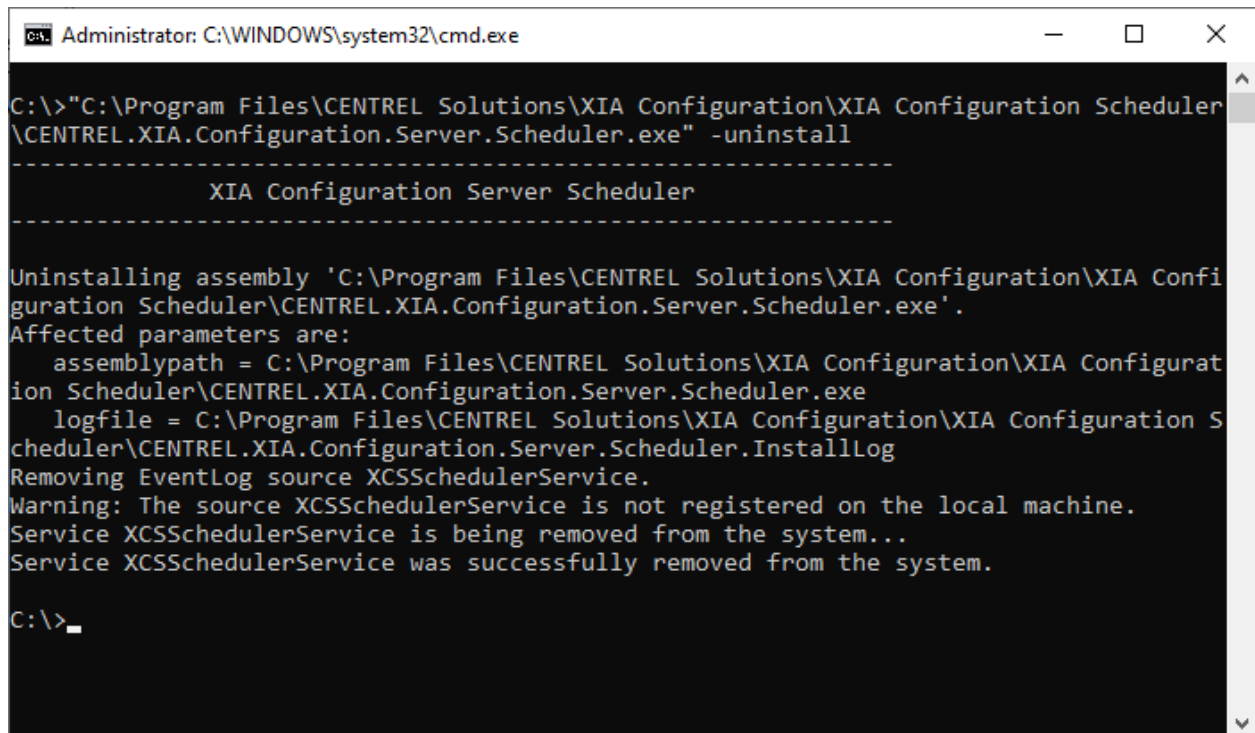
Manual Uninstallation Steps

- Ensure you have a full backup of your system.
- Logon as an administrator.
- Start a command prompt as administrator:



- Remove the scheduler service with the following command (replacing the path with your installation path):

"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe" -uninstall



```

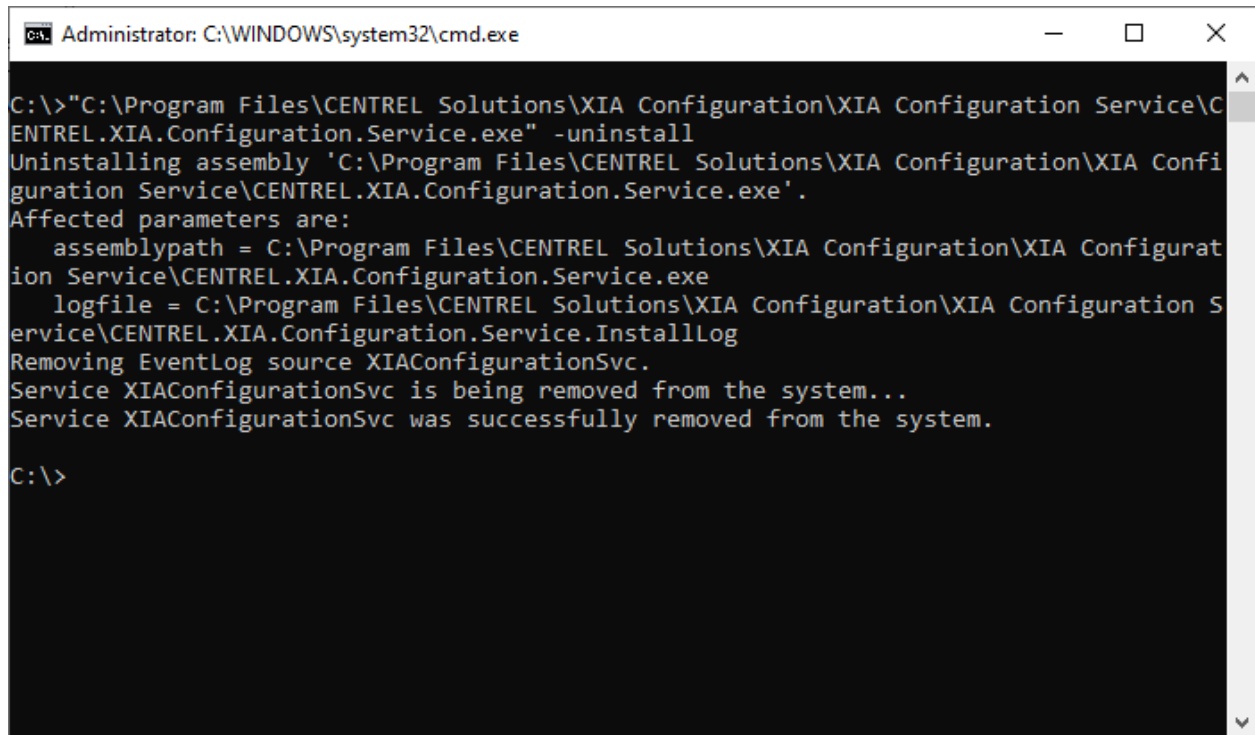
Administrator: C:\WINDOWS\system32\cmd.exe

C:\>"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe" -uninstall
-----
XIA Configuration Server Scheduler
-----

Uninstalling assembly 'C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe'.
Affected parameters are:
    assemblypath = C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.exe
    logfile = C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Scheduler\CENTREL.XIA.Configuration.Server.Scheduler.InstallLog
Removing EventLog source XCSSchedulerService.
Warning: The source XCSSchedulerService is not registered on the local machine.
Service XCSSchedulerService is being removed from the system...
Service XCSSchedulerService was successfully removed from the system.

C:\>_
  
```

- Ensure that the command states that the service has been successfully removed from the system.
- Remove the client service with the following command (replacing the path with your installation path):
"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe" -uninstall



```
Administrator: C:\WINDOWS\system32\cmd.exe

C:\>"C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe" -uninstall
Uninstalling assembly 'C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe'.
Affected parameters are:
    assemblypath = C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.exe
    logfile = C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Service.InstallLog
Removing EventLog source XIAConfigurationSvc.
Service XIAConfigurationSvc is being removed from the system...
Service XIAConfigurationSvc was successfully removed from the system.

C:\>
```

- Ensure that the command states that the service has been successfully removed from the system.
- Remove the installation directory (replacing the path with your installation path):
C:\Program Files\CENTREL Solutions\XIA Configuration
- Remove the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions
- Remove the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4943FAD2-E2E0-4071-9830-3B8C0E456C03}
- Start IIS manager and go to the **Application Pools** section.
- Right click the **XIAConfiguration** or **XIAConfiguration - NS** application pool and select Remove:



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

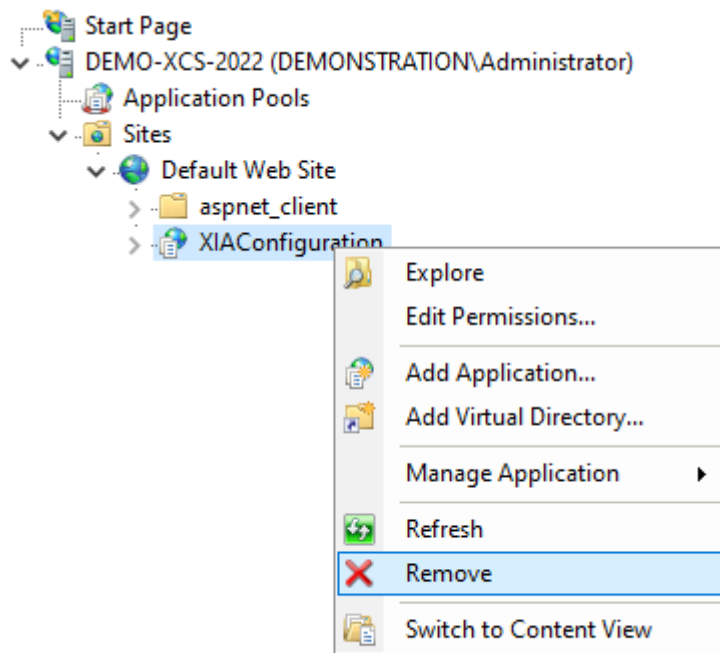
Filter: Go Group by:

Name	Status	.NET CLR ...	Managed Pipeli...
.NET v4.5	Started	v4.0	Integrated
.NET v4.5 Classic	Started	v4.0	Classic
DefaultAppPool	Started	v4.0	Integrated
XIAConfiguration	Started	v4.0	Integrated

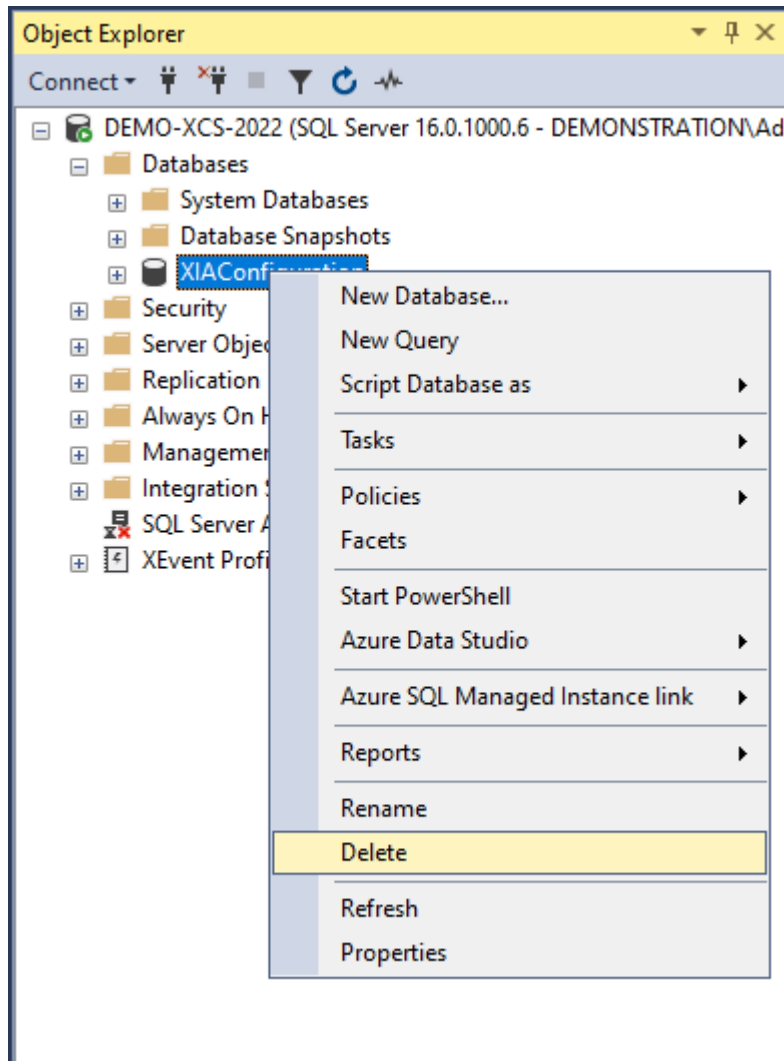
Add Application Pool...
Set Application Pool Defaults...
Start
Stop
Recycle...
Basic Settings...
Recycling...
Advanced Settings...
Rename
Remove
View Applications
Help

- Expand the **Default Web Site**.

- Right click the **XIAConfiguration** virtual directory (or other virtual directory that you selected during the installation) and select Remove:



- Open **SQL Management Studio** on the machine running the SQL database.
- Expand the **Databases** node.
- Right click the **XIAConfiguration** database (or the database you named during the installation) and select delete:



- Certain shared [roles and features](#) and prerequisites are automatically installed by the product, you may need to review these and remove them manually if they are no longer required.
- Reboot the system when ready.

Web Server Account

When [installing XIA Configuration Server](#), a user account is selected that is used to run the [XIA Configuration Server](#) web application. By default this account is the [Network Service](#) account, however a specific account can be selected.

When using a specific account the following should be considered

- The account must be created manually, it will not be created by the [installer](#).
- The account should be dedicated for this purpose.
- The account should not have privileges other than those configured by the [installer](#) - for example the account should **not** be an *Administrator*.
- The account will be assigned to the application pool created by the [installer](#).
- The account has access to the potentially sensitive data within the [XIA Configuration Server](#) database, such as user accounts and IP addresses and should therefore should have a suitably complex password.
- The account will be configured as the [database owner \(db_owner\)](#) of the [XIA Configuration Server](#) database.
- The account will be added to the IIS_IUSRS group.
- The account can be a domain or local account if the [Microsoft SQL Server](#) is hosted on the same machine as the [XIA Configuration Server](#), however should be a domain account if the [XIA Configuration Server](#) is hosted on another machine.

Compare Items

The compare function allows the comparison of any two **items** of the same **type**, or two **versions** of the same **item**, and display the differences.

To do this, select one or more **items**, right click, and click the Compare context menu item.

NOTE: If more than two **items** are selected, the first two **items** in the list are compared.

2 Item(s)

Item ID	Type	Name
1007	Windows Server	DEMO-SRV01
1002	Windows Server	DEMO-SRV02

New Item...

Save As PDF

Save As XML

Delete

Compare

Update Environment Identifiers

Duplicate

Decommissioning

Increment Version Number

Move To Container

Move To Location

Edit Security

Select All

Refresh

Properties

If the two **items** are not visible in the list at the same time, select the first **item** and click Compare, then browse to and select the second **item** and click Compare. Both **items** will now be visible in the **item comparison dialog**.

Item Comparison Dialog

The item comparison dialog allows you to compare any two items of the same [type](#), or two [versions](#) of the same item to see the differences.

To display items for comparison, see the [compare items](#) section.



Compare Items

Provides the ability to compare items for differences or compare two versions of the same item for changes.

 DEMO-SRV01 [1007]
Demonstration Windows server.

Clear Selection

Select Version

Version	Date	Time
 1.00	9/6/2024	3:18 PM

Compare

Report

XML

 DEMO-SRV02 [1002]
Demonstration Windows server.

Clear Selection

Select Version

Version	Date	Time
 1.02	9/6/2024	3:18 PM
 1.01	9/6/2024	3:00 PM
 1.00	9/6/2024	3:00 PM

- Select the source and destination version from the [version history](#).
- Hovering over a version displays additional information about that version.
- Click **Compare** to compare the two items and display the results in the browser window.
- Click **Report** to compare the two items and display the results in the PDF report.
- Click **XML** to compare the two items and display the results in an XML file.
- Click the swap icon to swap the source and destination items.

Comparing Components

Certain [item types](#), such as VMware systems, have components which can be compared directly.

This allows, for example, two individual virtual machines within a VMware system to be directly compared.



DEMO-XCS-2022 [1005]
Demonstration IIS server.

Clear Selection

 Select Version

Version	Date	Time
 1.02	9/6/2024	3:20 PM
 1.01	9/6/2024	3:01 PM
 1.00	9/6/2024	3:01 PM

 Select Component

Name	Component Type
 DEMO-XCS-2022	Entire IIS Server
 DEMO-XCS-2022	Server Configuration
 Default Web Site	Site
 Default Web Site/XIAConfigur...	Application

Compare

Report

XML

When an item supports components, the component can be selected from the list.

Hovering over the component displays additional information for that component:

Select Component

Name	Component Type
 DEMO-XCS-2022	Entire IIS Server
 DEMO-XCS-2022	Server Configuration
 Default Web Site	Site
 Default Web Site/XIAConfigur...	Application

Default Web Site/XIAConfiguration
dc41ee7c-e1b7-41fe-a871-845289f9cbb3
Application

Item Comparison Dialog Parameters

The item comparison dialog can be accessed directly using a URL, for example:

<http://localhost/xiaconfiguration/tools/compareitems.aspx?SourceItemIdentifier=1578&DestinationItemIdentifier=2631>

ItemID

The item to add to the comparison dialog, for example, 1072. If a source is not currently configured, the item is set as the source for the item. If a source is currently configured, the destination item is set to the value.

VersionID

The [version](#) of the item to compare, for example, 1.31. If a source is not currently configured, the item is set as the source version. If a source is currently configured, the destination version is set to the value.

ComponentIdentifier

The unique identifier of the [component](#) to compare, where appropriate.

SourceItemIdentifier

Specifies the unique identifier of the source item, for example, 1552.

SourceVersion

The [version](#) of the source item to compare, for example, 1.31. When this value is not set or configured as zero, the current live version of the item will be selected.

SourceComponentIdentifier

The unique identifier of the source [component](#) to compare, where appropriate.

DestinationItemIdentifier

Specifies the unique identifier of the destination item, for example, 1056.

DestinationVersion

The [version](#) of the destination item to compare, for example, 1.31. When this value is not set or configured as zero, the current live version of the item will be selected.

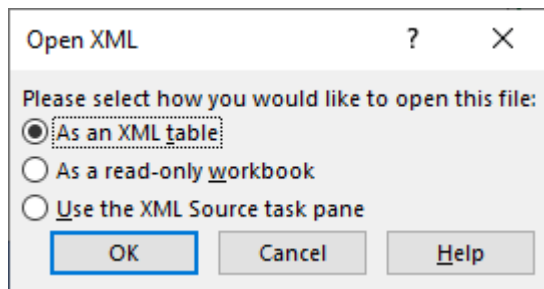
DestinationComponentIdentifier

The unique identifier of the destination [component](#) to compare, where appropriate.

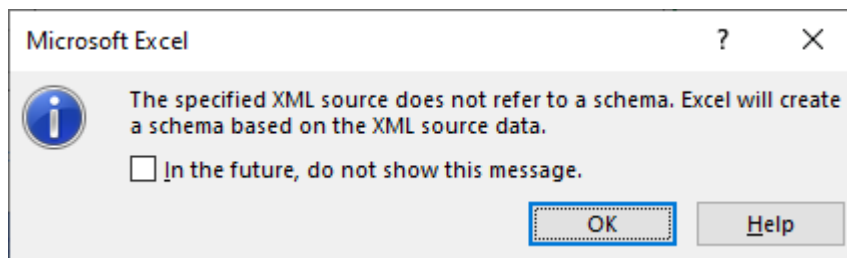
Viewing Results in Excel

To view comparison results in [Microsoft Excel](#), perform a comparison, then export the data to **XML** using the [item comparison dialog](#).

- Open [Microsoft Excel](#).
- Click *Open* and browse to the XML file.
- When prompted, select to open **As an XML table**:



- If prompted with a schema warning, click **OK**:



- The results will be displayed in [Microsoft Excel](#) where you can remove columns and sort as required:

	A	B	C	D	E
	Path	PropertyDisplayName	SourceValue	DestinationValue	ChangeType
2	General Settings > Motherboard > BIOS	Vendor		Phoenix Technologies LTD	Value Changed
3	General Settings > Motherboard > BIOS	Version		6.00	Value Changed
4	General Settings > Motherboard > BIOS	Release Date	[Not Configured]	02 June 2011	Value Changed
5	General Settings > Motherboard	Manufacturer		Intel Corporation	Value Changed
6	General Settings > Motherboard	Product Name		440BX Desktop Reference Platform	Value Changed
7	General Settings > Motherboard	Version		None	Value Changed
8	General Settings > Motherboard	Status	Complete	Complete	Value Changed
9	General Settings	Location	"Head office"	"System administrators office"	Value Changed
10	General Settings	Platform	Linux	Solaris	Value Changed
11	General Settings	Kernel Version	3.0.0-12-generic	5.11	Value Changed
12	General Settings	Operating System Version	Ubuntu 11.10	11.1	Value Changed
13	General Settings	Total Memory	995.24KB	1023.56KB	Value Changed
14	General Settings > Logical Drives > /	Size	18.70GB	13.73GB	Value Changed
15	General Settings > Logical Drives > /	Space Used	2.41GB	1.98GB	Value Changed
16	General Settings > Logical Drives > /	Free Space	16.29GB	11.74GB	Value Changed
17	General Settings > Logical Drives	/sys/fs/fuse/connections			Item Removed
18	General Settings > Logical Drives > /dev	Size	489.89MB	0 bytes	Value Changed
19	General Settings > Logical Drives > /dev	Space Used	4KB	0 bytes	Value Changed
20	General Settings > Logical Drives > /dev	Free Space	489.89MB	0 bytes	Value Changed
21	General Settings > Logical Drives	/home/dhomer/.gvfs			Item Removed
22	General Settings > Logical Drives	/devices			Item Added
23	General Settings > Logical Drives	/etc/dfs/sharetab			Item Added
24	General Settings > Logical Drives	/export			Item Added

Compliance Benchmarks

Compliance benchmarks provide the ability to determine how various [item types](#) adhere to predefined configuration and security standards.

For more information on the results breakdown see the [result types](#) section.

▲ Ref.	Title	Configured Value
📁 Section 1: Password Policy		
✓ 1.01	Set "Enforce password history" to remember at least 24 passwords	24
✓ 1.02	Set "Maximum password age" to 60 days or less	42 days
✓ 1.03	Set "Minimum password age" to at least 1 day(s)	1 days
✗ 1.04	Set "Minimum password length" to 14 or more characters	7
✓ 1.05	Set "Password must meet complexity requirements" to "Enabled"	Enabled
✓ 1.06	Set "Store passwords using reversible encryption" to "Disabled"	Disabled
✗ 1.07	Set "Relax minimum password length limits" to "Enabled" on supported operating systems	Not Configured

For more information see the [compliance benchmarks](#) section for the [XIA Configuration Client](#).

Result Types

[Compliance benchmark](#) results are displayed by the following result types

Unknown

The system was unable to determine whether this compliance benchmark test passed as the information was not collected by the [XIA Configuration Client](#).

Passed

The compliance benchmark test passed.

Failed

The compliance benchmark test is flagged with a warning.

Excluded by Configuration

The compliance benchmark test was excluded because the [XIA Configuration Client](#) agent settings have been configured to exclude it.

Excluded by Platform

The compliance benchmark test was excluded because of the platform being scanned - for example the test was excluded because the target platform was a domain controller, however the test does not apply to domain controllers.

Unavailable (not supported by scan client)

The test result is unavailable as the [XIA Configuration Client](#) is unable to read the configuration, this can be caused by the information being unavailable through any suitable API.

Manual Validation Required

The test result was obtained, however manual validation is required - for example if the test reads text that must be validated to ensure that it meets organizational requirements.

Configuration Settings

This section describes the various settings that can be configured within [XIA Configuration Server](#).

To access the configuration settings, select Tools > Configuration from the drop down menu in the main [XIA Configuration Server](#) interface.

You must be a [system administrator](#) to access the settings interface.

Automatic Update Settings

Automatic updates configures the ability to automatically update the [XIA Configuration Client](#) on remote machines that are configured for [automatic updates](#).

NOTE: This does not update the [XIA Configuration Server](#) product. When the [XIA Configuration Server](#) product is [upgraded](#) the locally installed [XIA Configuration Client](#) is automatically updated.

NOTE: If the [.NET Framework](#) version on the machine being updated is not [.NET Framework 4.8](#), this will be automatically updated, however the machine must be rebooted for the automatic update to complete.

Enable automatic updates

Determines whether automatic updates are enabled from this [server](#).

Automatically Approve Updates

When the [XIA Configuration Server](#) is [upgraded](#), the corresponding client update is also upgraded. When this option is enabled, the newly available update is immediately available for deployment to client machines.

Approved Update

When the [XIA Configuration Server](#) is [upgraded](#), the corresponding client update is also upgraded. When this option is enabled, the newly available update must be manually approved.

Automatically Update All Client Machines

All client machines that request updates are permitted to download and install them.

Automatically Update These Client Machines

Only the client machines specified (using their NetBIOS computer name or [GUID](#)) are permitted to download and install them.

Save Settings

Saves the settings.

Cache

Information is stored in the memory cache to increase performance.

Cache

Information is stored in the memory cache to increase performance.

 3 Cached Objects

▼ Key Name	Data Type
 System.Web.Script.Services.WebServiceD...	System.Web.Script.Services.WebServiceData
 ServerSettings	Server Settings
 aspxDXTemporaryUploadFolderCleaner	DevExpress.Web.Internal.TemporaryFolderCleaner

Refresh

Clear Cache

Key Name

The name of the key in the cache.

Data Type

The type of data stored in the cache.

Refresh

Reloads information about objects currently stored in the cache.

Clear Cache

Deletes all objects from the cache.

Check Out

When [items](#) are edited by a user, they are automatically [checked out](#) so that they cannot be edited by other users.

Automatically check in items that have been checked out for (minutes)

Determines whether the [scheduler](#) should automatically check in [items](#) that have been checked out for the number of minutes specified or greater.

The default value is enabled and set to 60 minutes.

Checked Out Items

This section displays information about [items](#) that are currently [checked out](#).

Checked Out Items

Provides a user interface to view checked out items.

 1 Checked Out Items

Identifier	Name	Type	Check Out Date	Username
 1007	DEMO-SRV01	Windows Server	09 September 2024 10:40:02	DEMONSTRATION\Administrator

Check In Items

Identifier

The unique identifier of the [item](#) that is [checked out](#).

Name

The name of the [item](#) that is [checked out](#).

Type

The type of [item](#) that is [checked out](#).

Check Out Date

The date and time that the [item](#) was [checked out](#).

Username

The username of the user that [checked out](#) the [item](#).

Check In Items

Automatically checks in all currently [checked out items](#). Changes to [items](#) currently being [edited](#) may be lost.

Client Installations

The client installations [configuration](#) section allows the managing of the [XIA Configuration Client](#) installations that are configured to [register](#) with the [server](#).

The [client](#) installations are listed by machine name by default, with manually created client installations displayed with a pencil icon.

Client Installations

This section provides information about the client installations that have registered with the server.

 1 Client Installations

Machine Name	Operating System	Last Registration	Last Poll	Version
 DEMO-XCS-2022	Microsoft Windows Server 2022 Standard	09 September 2024 10:46:42	09 September 2024 10:46:42	16.2.5.0

New Client Installation

Refresh

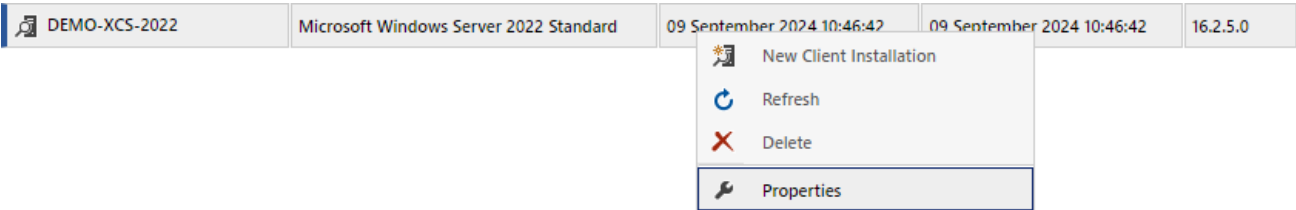
Right clicking a client installation shows the [context menu](#).

New Client Installation

Displays the [client installation properties](#) to manually create a new [client installation](#).

Context Menu

Right clicking a [client installation](#) shows the context menu.



New Client Installation

Displays the [client installation properties](#) to manually create a new [client installation](#).

Refresh

Refreshes the list of [client installations](#).

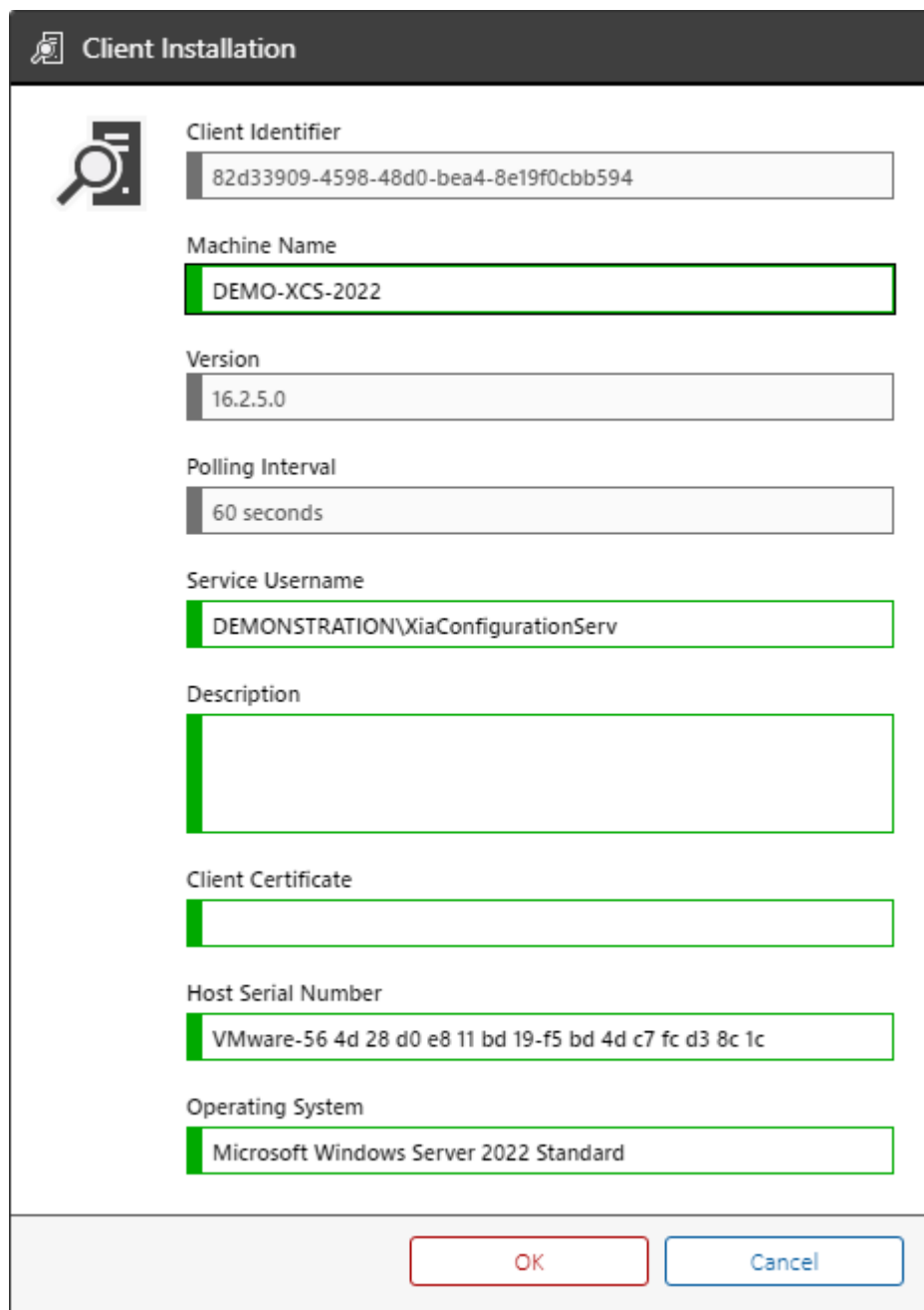
Delete

Deletes the currently selected [client installation](#).

Properties

Displays the [client installation properties](#) of the currently selected [client installation](#).

Client Installation Properties



The image shows a 'Client Installation' dialog box with a dark header bar containing a magnifying glass icon and the title 'Client Installation'. The main area is white and contains several labeled text input fields. On the left side of the main area is a large magnifying glass icon. The fields are: 'Client Identifier' with the value '82d33909-4598-48d0-bea4-8e19f0cbb594'; 'Machine Name' with the value 'DEMO-XCS-2022'; 'Version' with the value '16.2.5.0'; 'Polling Interval' with the value '60 seconds'; 'Service Username' with the value 'DEMONSTRATION\XiaConfigurationServ'; 'Description' which is an empty text area; 'Client Certificate' which is an empty text area; 'Host Serial Number' with the value 'VMware-56 4d 28 d0 e8 11 bd 19-f5 bd 4d c7 fc d3 8c 1c'; and 'Operating System' with the value 'Microsoft Windows Server 2022 Standard'. At the bottom right are two buttons: 'OK' and 'Cancel'.

Property	Value
Client Identifier	82d33909-4598-48d0-bea4-8e19f0cbb594
Machine Name	DEMO-XCS-2022
Version	16.2.5.0
Polling Interval	60 seconds
Service Username	DEMONSTRATION\XiaConfigurationServ
Description	
Client Certificate	
Host Serial Number	VMware-56 4d 28 d0 e8 11 bd 19-f5 bd 4d c7 fc d3 8c 1c
Operating System	Microsoft Windows Server 2022 Standard

Client Identifier

The unique identifier of the [client](#) in GUID format, configured on the [service settings general](#) tab.

Machine Name

The NetBIOS name of the computer running the [client](#).

Version

The registered version of the [client](#).

Polling Interval

The interval (in seconds) at which the [client](#) will poll the [server](#).

Service Username

The username configured as the [service account](#) on the [client](#).

Description

The administrator configured description of the [client](#), configured on the [service settings general](#) tab.

Client Certificate

The thumbprint of the SSL client certificate if [configured](#).

Host Serial Number

The serial number of the host machine.

Operating System

The name of the operating system running on the host machine.

Custom Sections and Attributes

Custom sections and attributes allow additional information to be assigned to [items](#).

Custom Sections and Attributes

Provides the ability to extend items with custom sections and attributes.

 2 Custom Sections

Display Name	Item Types	Custom Attributes
 CONTOSO Windows Support	All item types	Operating System Details Operating System Expiry Date Support Contract Type
 House Keeping	All item types	Server Maintenance

New Custom Section

Save Custom Sections

Display Name

The display name of the custom section.

Item Types

The types of [items](#) to which the custom section applies.

Custom Attributes

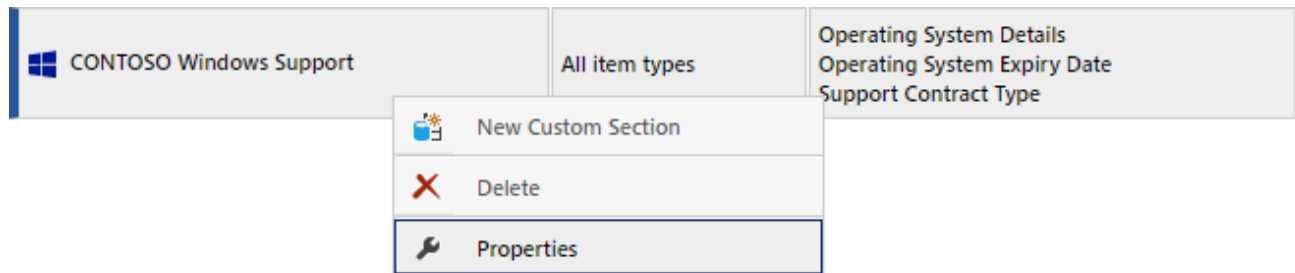
The names of the custom attributes assigned to this section.

Right clicking an item shows the custom sections [context menu](#).

Clicking new custom section displays the [custom section dialog](#).

Context Menu

The context menu is displayed when right clicking a [custom section](#) in the listview.



New Custom Section

Displays the [custom section dialog](#) to allow a new [custom section](#) to be created.

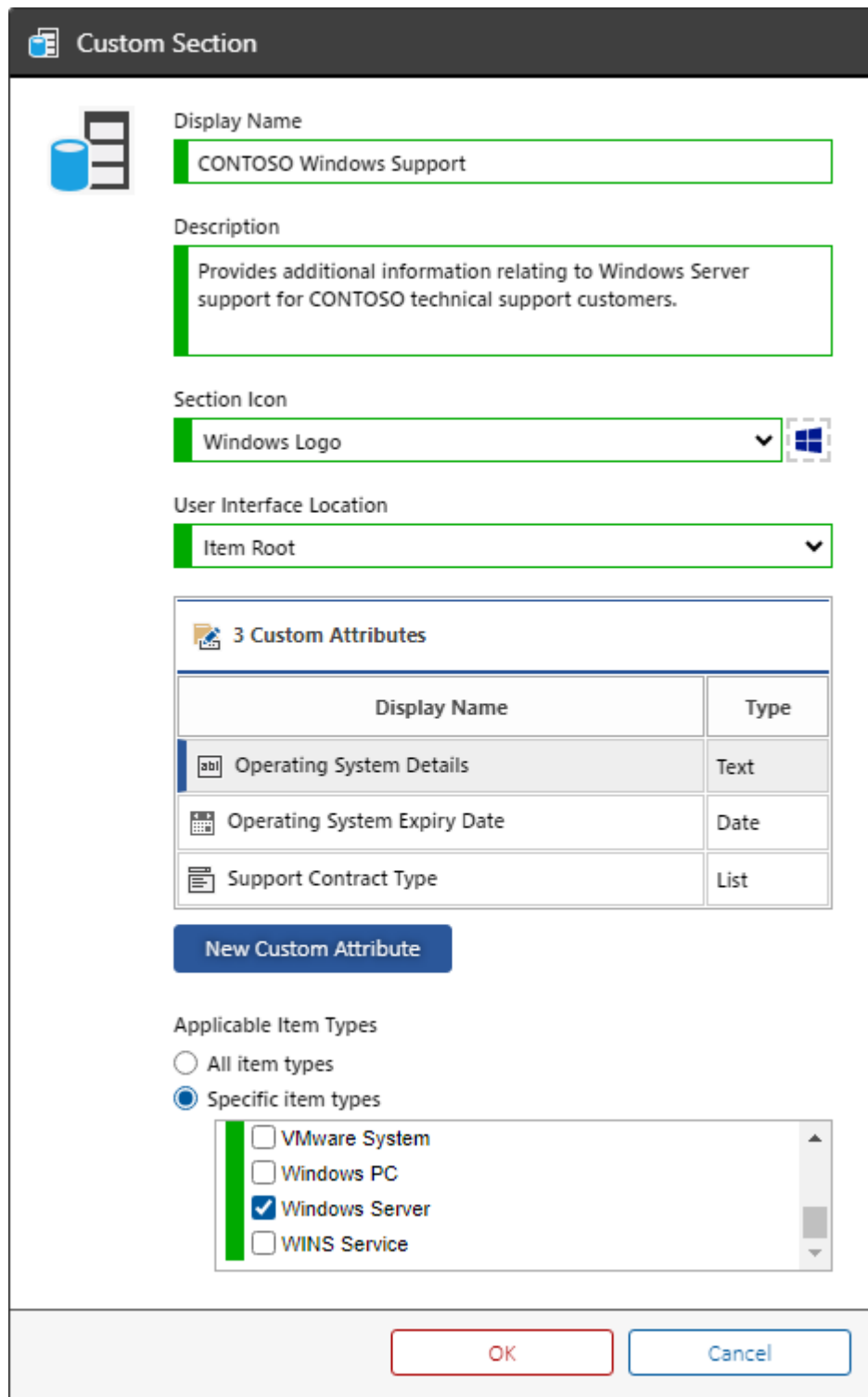
Delete

Deletes the currently selected [custom section](#).

Properties

Displays the currently selected [custom section](#) in the [custom section dialog](#).

Custom Section Dialog



The Custom Section dialog box is used to configure a custom section in the XIA Configuration Administrator. It features a dark header bar with the title "Custom Section" and a small icon. The main area is white and contains several sections: "Display Name" with a text input field containing "CONTOSO Windows Support"; "Description" with a text area containing "Provides additional information relating to Windows Server support for CONTOSO technical support customers."; "Section Icon" with a dropdown menu showing "Windows Logo" and a small icon; "User Interface Location" with a dropdown menu showing "Item Root"; a table titled "3 Custom Attributes" with columns "Display Name" and "Type", containing three rows: "Operating System Details" (Text), "Operating System Expiry Date" (Date), and "Support Contract Type" (List); a "New Custom Attribute" button; "Applicable Item Types" with radio buttons for "All item types" and "Specific item types" (selected), and a list box showing "VMware System", "Windows PC", "Windows Server" (checked), and "WINS Service". At the bottom are "OK" and "Cancel" buttons.

Display Name
CONTOSO Windows Support

Description
Provides additional information relating to Windows Server support for CONTOSO technical support customers.

Section Icon
Windows Logo

User Interface Location
Item Root

3 Custom Attributes

Display Name	Type
Operating System Details	Text
Operating System Expiry Date	Date
Support Contract Type	List

New Custom Attribute

Applicable Item Types
☐ All item types
☒ Specific item types

☐ VMware System
☐ Windows PC
☒ Windows Server
☐ WINS Service

OKCancel

Display Name

The display name of the [custom section](#).

Description

The description of the [custom section](#).

Section Icon

The icon to display for the [custom section](#).

User Interface Location

Determines where in the user interface the [custom section](#) should be displayed.

Custom Attributes

The custom attributes assigned to this [custom section](#).

Applicable Item Types

The types of [items](#) to which the [custom section](#) applies.

Custom Attributes

Custom attributes can be created within [custom sections](#) and allow addition information to be stored within that [section](#).

 2 Custom Attributes

Display Name	Type
 Operating System Details	Text

 HTML

 Additional Information	HTML
--	------

Display Name

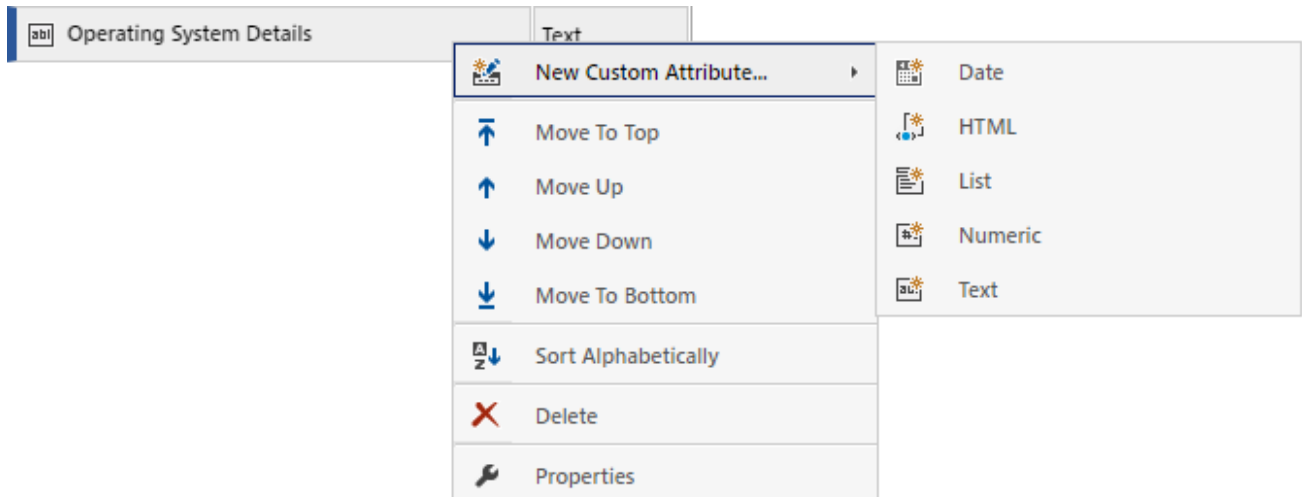
The display name of the custom attribute.

Type

The type of custom attribute.

Right clicking an item shows the custom attributes [context menu](#).

Context Menu



New Custom Attribute

Creates a new [custom attribute](#) of the specified [custom attribute type](#).

Move To Top ¹

Moves the currently selected [custom attribute](#) to the top of the list.

Move Up ¹

Moves the currently selected [custom attribute](#) up the list.

Move Down ¹

Moves the currently selected [custom attribute](#) down the list.

Move To Bottom ¹

Moves the currently selected [custom attribute](#) to the bottom of the list.

Sort Alphabetically ¹

Sorts the [custom attributes](#) alphabetically.

Delete

Deletes the currently selected [custom attribute](#).

Properties

Displays the currently selected [custom attribute](#).

¹ HTML custom attributes are sorted separately to other [custom attribute types](#).

Custom Attribute Types

Date

The [date custom attribute](#) allows the user to select a date using the [date picker](#). The information is stored as a [System.DateTime](#).

HTML

The [HTML custom attribute](#) allows the user to enter HTML using the [HTML editor](#). The information is stored as a [System.String](#).

List

The [list custom attribute](#) allows the user to select a value from a drop down list. The information is stored as a [System.String](#).

Numeric

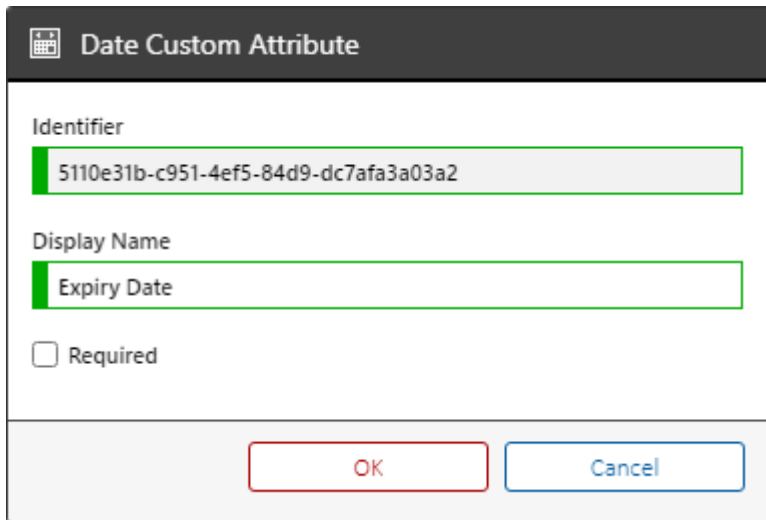
The [numeric custom attribute](#) allows the user to enter a numerical value between 0 and 9223372036854775807. The information is stored as a [System.Int64](#).

Text

The [text custom attribute](#) allows the user to enter a text value. The information is stored as a [System.String](#).

Date Custom Attribute

The date [custom attribute type](#) allows the user to select a date using the [date picker](#). The information is stored as a [System.DateTime](#).

A dialog box titled "Date Custom Attribute" with a calendar icon. It contains three input fields: "Identifier" with the value "5110e31b-c951-4ef5-84d9-dc7afa3a03a2", "Display Name" with the value "Expiry Date", and a "Required" checkbox which is unchecked. At the bottom are "OK" and "Cancel" buttons.

Date Custom Attribute

Identifier
5110e31b-c951-4ef5-84d9-dc7afa3a03a2

Display Name
Expiry Date

☐ Required

OK Cancel

Identifier

The unique identifier of the [custom attribute](#) in [GUID format](#).

Display Name

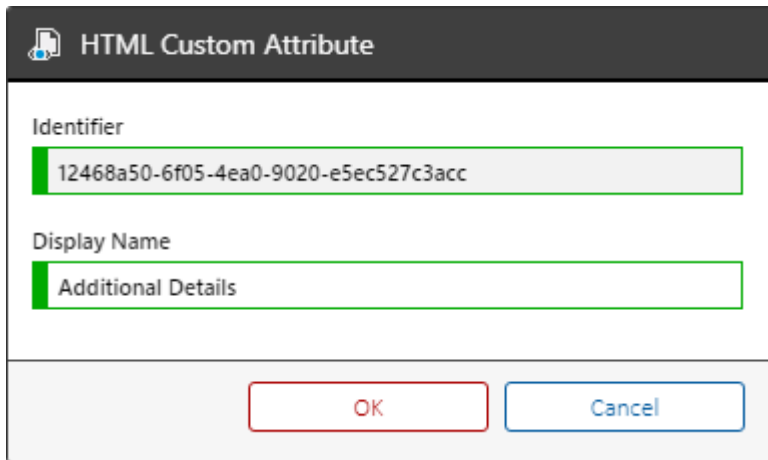
The display name of the [custom attribute](#).

Required

Determines whether the [custom attribute](#) is mandatory and must have a value assigned.

HTML Custom Attribute

The HTML [custom attribute type](#) allows the user to enter HTML using the [HTML editor](#). The information is stored as a [System.String](#).

A screenshot of a dialog box titled "HTML Custom Attribute". The dialog has a dark header bar with a document icon and the title. Below the header, there are two text input fields. The first field is labeled "Identifier" and contains the GUID "12468a50-6f05-4ea0-9020-e5ec527c3acc". The second field is labeled "Display Name" and contains the text "Additional Details". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

HTML Custom Attribute	
Identifier	12468a50-6f05-4ea0-9020-e5ec527c3acc
Display Name	Additional Details
OK Cancel	

Identifier

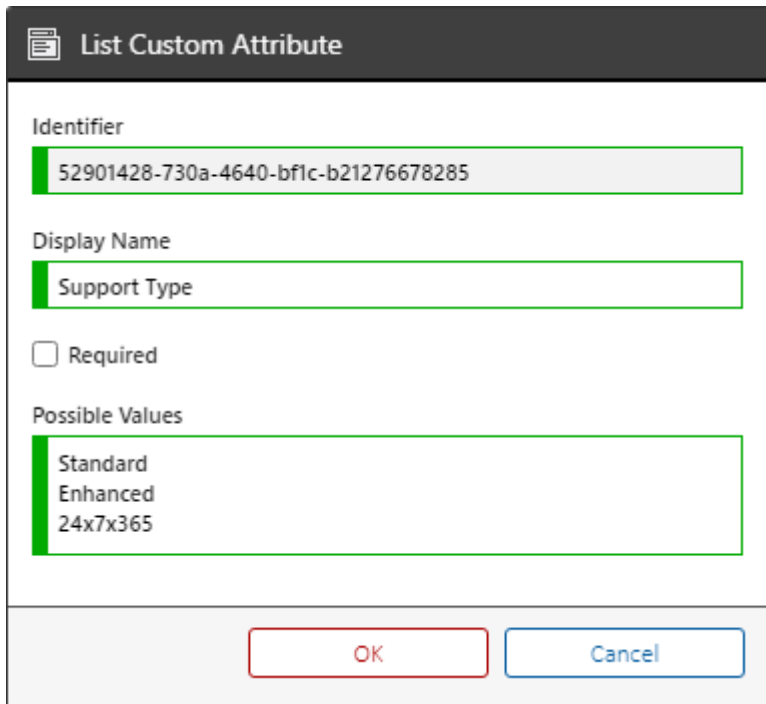
The unique identifier of the [custom attribute](#) in [GUID format](#).

Display Name

The display name of the [custom attribute](#).

List Custom Attribute

The list [custom attribute type](#) allows the user to select a value from a drop down list. The information is stored as a [System.String](#).



List Custom Attribute

Identifier
52901428-730a-4640-bf1c-b21276678285

Display Name
Support Type

☐ Required

Possible Values
Standard
Enhanced
24x7x365

OK Cancel

Identifier

The unique identifier of the [custom attribute](#) in [GUID format](#).

Display Name

The display name of the [custom attribute](#).

Required

Determines whether the [custom attribute](#) is mandatory and must have a value assigned.

Possible Values

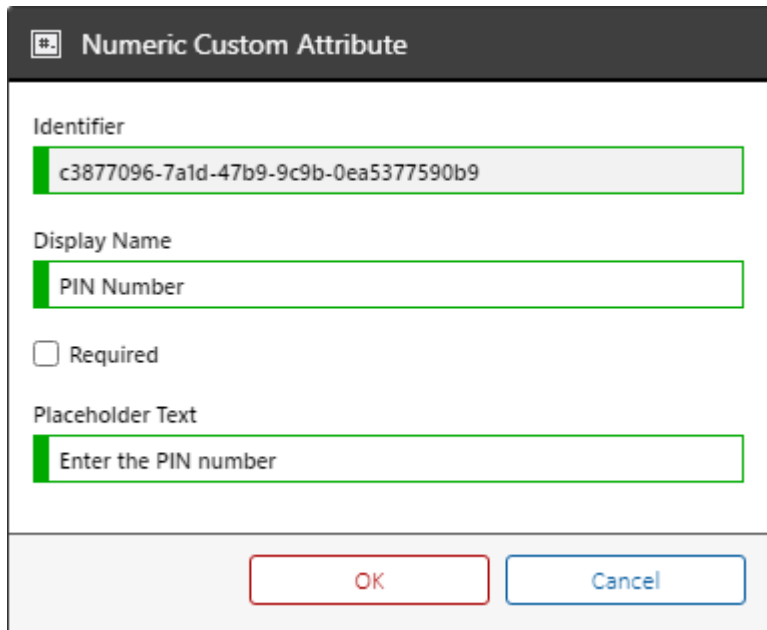
The possible values that can be assigned to the [custom attribute](#).

Numeric Custom Attribute

The numeric [custom attribute type](#) allows the user to enter a numerical value between 0 and 9223372036854775807.

The information is stored as a [System.Int64](#).

NOTE: Versions of [XIA Configuration Server](#) prior to v16 used a [System.Int32](#) data type.



The screenshot shows a dialog box titled "Numeric Custom Attribute" with a close button (X) in the top-left corner. The dialog contains four input fields: "Identifier" with the value "c3877096-7a1d-47b9-9c9b-0ea5377590b9", "Display Name" with the value "PIN Number", "Required" with an unchecked checkbox, and "Placeholder Text" with the value "Enter the PIN number". At the bottom, there are two buttons: "OK" (outlined in red) and "Cancel" (outlined in blue).

Identifier

The unique identifier of the [custom attribute](#) in [GUID format](#).

Display Name

The display name of the [custom attribute](#).

Required

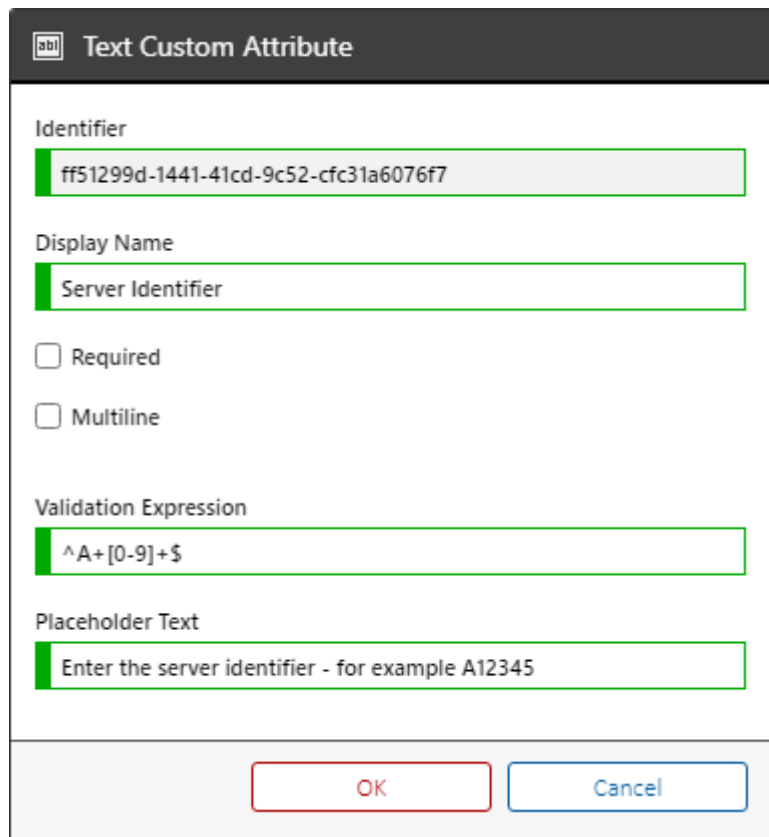
Determines whether the [custom attribute](#) is mandatory and must have a value assigned.

Placeholder Text

The placeholder text to display in the input control to the user for the [custom attribute](#).

Text Custom Attribute

The text [custom attribute type](#) allows the user to enter a text value.
The information is stored as a [System.String](#).



The screenshot shows a dialog box titled "Text Custom Attribute" with a dark header bar containing a small icon and the title. The dialog has several input fields and checkboxes. The "Identifier" field contains a GUID string. The "Display Name" field contains "Server Identifier". There are two unchecked checkboxes labeled "Required" and "Multiline". The "Validation Expression" field contains a regular expression. The "Placeholder Text" field contains a descriptive text string. At the bottom, there are "OK" and "Cancel" buttons.

Field	Value
Identifier	ff51299d-1441-41cd-9c52-cfc31a6076f7
Display Name	Server Identifier
Required	☐
Multiline	☐
Validation Expression	^A+[0-9]+\$
Placeholder Text	Enter the server identifier - for example A12345

Identifier

The unique identifier of the [custom attribute](#) in [GUID format](#).

Display Name

The display name of the [custom attribute](#).

Required

Determines whether the [custom attribute](#) is mandatory and must have a value assigned.

Multiline

Determines whether the [custom attribute](#) will allow the user to enter text over multiple lines.

Validation Expression

Determines the [regular expression](#) to use to validate the input for the [custom attribute](#).

Placeholder Text

The placeholder text to display in the input control to the user for the [custom attribute](#).

Database Settings

This section configures the database connection and timeout settings.

This is initially configured by the [installer](#), and changes should only be made to the instance name, or database name after reviewing the [system migration](#) guide.

Instance Name

Enter the [SQL server](#) instance name for example "(local)", "CORP-SQL01" or "CORP-SQL01\SQLExpress".

Database Name

Enter the name of the database.

- This database must be an existing XIA Configuration database.
- The default database name is **XIAConfiguration**.
- The database is accessed using the [web server account](#) that was configured during [installation](#). By default the account used is the Network Service account.

Report Execution Timeout

The timeout value in seconds in which a [report](#) must execute.

Delete Previous Versions Execution Timeout

The timeout value in seconds in which deleting [previous versions](#) must execute.

Diagnostics

The diagnostics section is provided to assist with troubleshooting issues with [XIA Configuration Server](#).

Diagnostics Settings

Configures the server side diagnostics logging settings.

Logging to file 'C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\AppData\Logs\Trace\Trace.log'

Disable Logging

Clicking the enable logging or disable logging button enables or disables trace logging of actions performed to text file. The file path, local to the server, is displayed in the interface and can be viewed in a standard text editor or followed by a tail application.

Note:

- As all actions performed by [XIA Configuration Server](#) will be written to this trace file, it is recommended to minimize access to a single user while troubleshooting.
- Diagnostics should be disabled when not in use and by default diagnostics will be automatically disabled the next time that the [XIA Configuration Server](#) application is restarted.

Event Log Settings

The event log settings determine the behaviour of the [event log](#).

Audit PDF export

Determines whether the system should log an [event](#) to the [event log](#) when a user generates a PDF document of an [item](#).

Audit user account logon success

Determines whether the system should log an [event](#) to the [event log](#) when a user logs on successfully.

Audit password list entry changes

Determines whether the system should log an [event](#) to the [event log](#) when changes are made to individual [password list](#) entries.

General Settings

Browser and Home Page Title

Allows you to customise the title of the web browser shown to users when viewing the home page. The title for the reporting section home page can be configured in the [reporting settings](#) section.

Home Page Description

Provides a descriptive message to be displayed on the home page. The description for the reporting section home page can be configured in the [reporting settings](#) section.

Allow the drag and drop of items in the treeview

Determines whether users can drag and drop [items](#) in the tree view of the organization and location sections.

Hardware Definitions

Hardware definitions allow information such as a description and image to be automatically detected for any hardware [items](#).

Hardware Definitions

Configures the definitions for hardware devices.

 1 Hardware Definitions

 Display Name	System Managed	Image
 VMware Virtual Platform	True	500 x 175

New Hardware Definition

Import

Display Name

The display name of the hardware definition.

System Managed

Determines whether the hardware definition is managed by the system.

Image

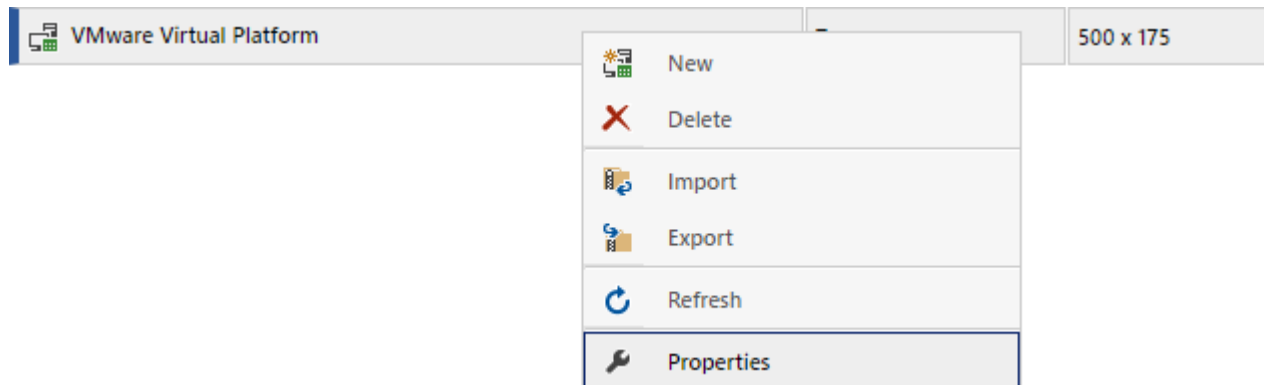
Determines whether an image is available for the hardware definition, and it's size in pixels.

Right clicking an item shows the hardware definitions [context menu](#).

Clicking import displays the hardware definitions [import dialog](#).

Context Menu

The context menu is displayed when a user right clicks a [hardware definition](#).



New

Displays the [hardware definition dialog](#), to create a new [hardware definition](#).

Delete

Deletes the currently selected [hardware definition](#).

Import

Displays the hardware definitions [import dialog](#), allowing [hardware definitions](#) to be imported from a ZIP file.

Export

Exports the configured [hardware definitions](#) to a ZIP file.

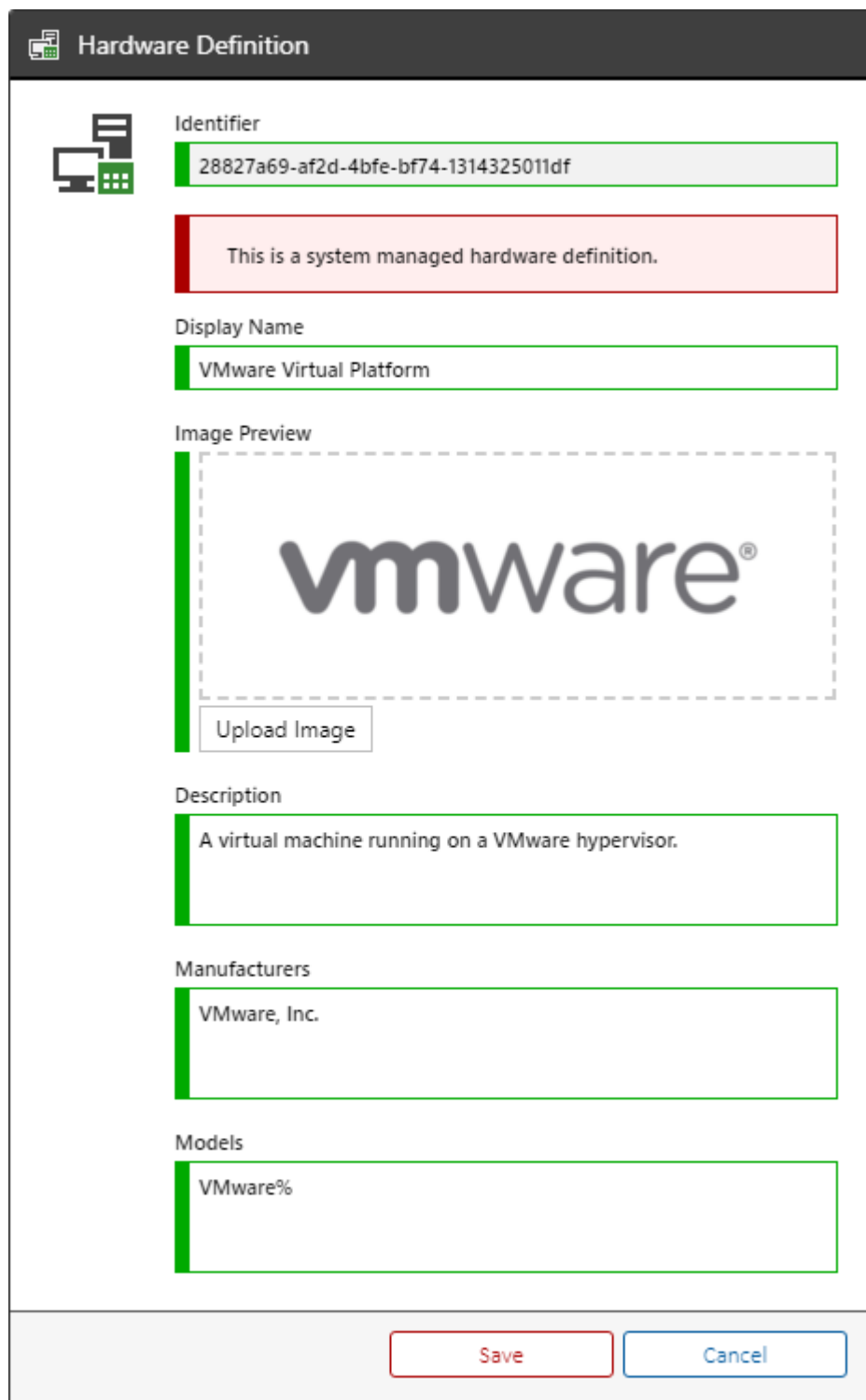
Refresh

Refreshes the [hardware definitions](#).

Properties

Displays the currently selected [hardware definition](#) in the [hardware definition dialog](#).

Hardware Definition Dialog

The image shows a 'Hardware Definition' dialog box. It has a dark header bar with a computer icon and the title 'Hardware Definition'. On the left, there is a sidebar icon. The main area contains several input fields: 'Identifier' with a UUID, a red message box stating 'This is a system managed hardware definition.', 'Display Name' with 'VMware Virtual Platform', 'Image Preview' with a VMware logo and an 'Upload Image' button, 'Description' with 'A virtual machine running on a VMware hypervisor.', 'Manufacturers' with 'VMware, Inc.', and 'Models' with 'VMware%'. At the bottom are 'Save' and 'Cancel' buttons.

Hardware Definition



Identifier

28827a69-af2d-4bfe-bf74-1314325011df

This is a system managed hardware definition.

Display Name

VMware Virtual Platform

Image Preview



Upload Image

Description

A virtual machine running on a VMware hypervisor.

Manufacturers

VMware, Inc.

Models

VMware%

Save

Cancel

Identifier

The unique identifier of the [hardware definition](#).

Display Name

The display name of the [hardware definition](#).

Image Preview

A preview of the image associated with the [hardware definition](#).

Upload Image

Uploads a new image for the [hardware definition](#).

Description

The description of the [hardware definition](#).

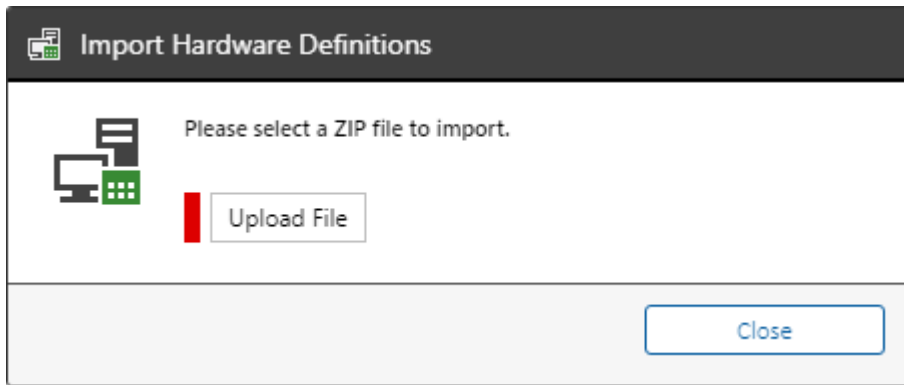
Manufacturers

The manufacturer names that match this [hardware definition](#), one per line. These can include the % wildcard.

Models

The model names that match this [hardware definition](#), one per line. These can include the % wildcard.

Import Dialog



The import dialog allows [hardware definitions](#) to be imported from a ZIP file.

Full details of the import can be viewed in the [event log](#).

HTML Editor Settings

This section describes the settings that affect the operation of the [HTML editor](#).

HTML Editor Settings

This section provides settings related to the HTML editor.

☒ Show CSS style controls

☒ Show insert and remove hyperlink controls

☒ Show full screen controls

☒ Show image controls

☒ Show preview tab

☒ Show table controls

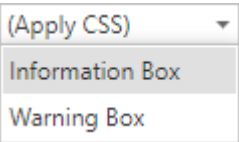
 View Source HTML

☐ All Users ☒ System Administrators ☐ Specified Users

Save Editor Settings

Show CSS style controls

Determines whether the editor should display the CSS drop down, allowing the user to select from predefined CSS styles.



Show insert and remove hyperlink controls

Determines whether the insert hyperlink and remove hyperlink buttons should be displayed on the toolbar of the [editor](#).

Show full screen controls

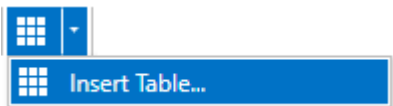
Determines whether the full screen button should be displayed on the toolbar, allowing the user to view the [editor](#) full screen within the browser.

Show image controls

Determines whether the insert [image](#) button should be displayed on the toolbar of the [editor](#).

Show table controls

Determines whether the table controls should be displayed on the toolbar of the [editor](#). Existing tables will still be displayed when this setting is unchecked.



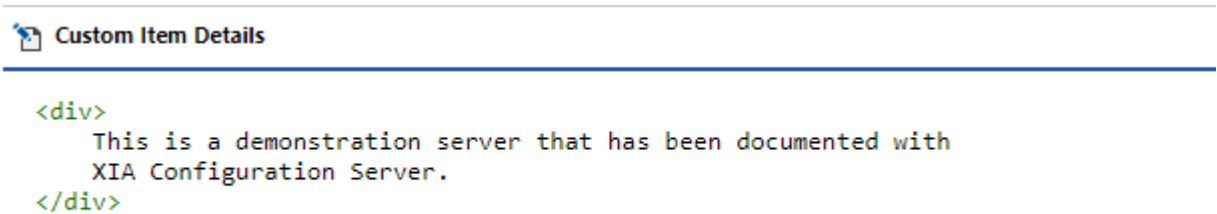
Show preview tab

Determines whether the preview tab should be displayed in the [editor](#).



View source HTML

Determines the [server permission](#) of which users can view and modify the underlying source HTML by selecting the HTML tab in the [editor](#).



Import Engine Settings

Configures the ability to import data into the [XIA Configuration Server](#) from the [XIA Configuration Client](#).

Allow all client machines

Data will be accepted from any [XIA Configuration Client](#) machine.

Allow only the following client machines

Data will only be accepted from the specified [XIA Configuration Client](#) machines with the specified NetBIOS names.

Verify RSA signatures

Determines whether the digital signature should be validated to help to ensure that the data has not been modified. This should be enabled on the [advanced tab](#) of the [XIA Configuration Client](#) machine.

Create VMware Physical ESX Hosts

Determines whether [VMware physical ESX host items](#) should be automatically created or updated when importing [VMware systems](#).

Automatically import data files found in the import directory

When enabled, the [scheduler](#) will [automatically import](#) any Zip or XML data files found in the import directory.

Default Zip Password

The password to use to unzip Zip files when [automatically importing](#) data.

Item Comparer Settings

The section determines the settings to use when [items](#) are compared using the [item comparer](#).

Maximum Text Length

Determines the maximum text length to display for results in characters. The default value is to display a maximum of 200 characters.

When the maximum text length is exceeded in the web interface on desktop machines the result is displayed with the option to double click the result to see the full information.

11 differences detected		
Description	[Double Click]	[Double Click]

When the maximum text length is exceeded in an exported PDF report the "Too long to display" text is displayed.

General Settings		
Property or Action	Source Item	Destination Item
Description	Too long to display	Too long to display

Item Creation Rules

When [XIA Configuration Server](#) receives [item](#) data from the [XIA Configuration Client](#) the [import engine](#) locates the [item](#) using its [item identifiers](#).

If the [item](#) does not exist, by default a new [item](#) is created within the [root container](#), however it is possible to modify this behaviour using item creation rules.

NOTE: Rules are processed from top to bottom, once a matching rule has been found that rule is actioned and no further rule processing is performed. If no matching rule is located a new [item](#) is created within the [root container](#).

Item Creation Rules

Item creation rules determine which container a new item will be created in. This allows new items to be routed to a container based on the item type or the client which first scanned the item.

 3 Item Creation Rules

Priority	Rule Name	Host Name	Username	Environment	Item Types	Destination Container
 1	Customer 1	DEMO-SRV01	*	*	All	Customer 1
 2	Customer 2	DEMO-SRV02	*	*	All	Customer 2
 Lowest	Default Rule	*	*	*	All	Lost and Found

Create New Rule

Save Rules

Rule Name
The unique descriptive name for the [rule](#).

Rule Identifier
The unique identifier of the rule in [GUID](#) format.

Host Name
The NetBIOS computer name of the machine running the [XIA Configuration Client](#) to match.

Username
The name of the user account including domain name that was used to upload the data to the [XIA Configuration Server](#) to match.

Environment Identifier
The name of the [environment identifier](#) to match.

Item Types
The [item types](#) to match.

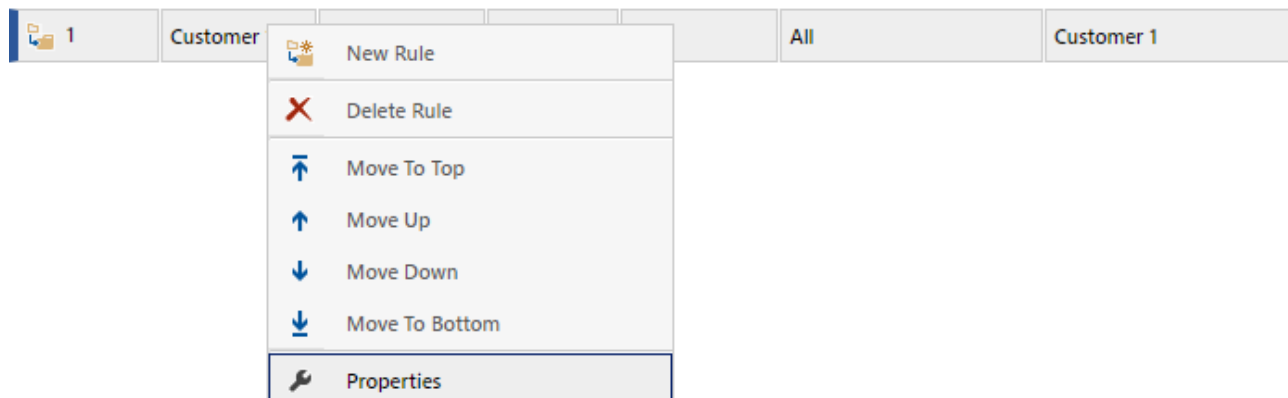
Destination Container

The [container](#) or [customer](#) into which matching [items](#) are to be created.

Right clicking an item shows the item creation rules [context menu](#).

Context Menu

The context menu is displayed when a user right clicks an [item creation rule](#).



New

Displays the [item creation rule dialog](#) to create a new [item creation rule](#).

Delete

Deletes the currently selected [item creation rule](#).

Move To Top

Moves the currently selected [item creation rule](#) to the top of the list.

Move Up

Moves the currently selected [item creation rule](#) up the list.

Move Down

Moves the currently selected [item creation rule](#) down the list.

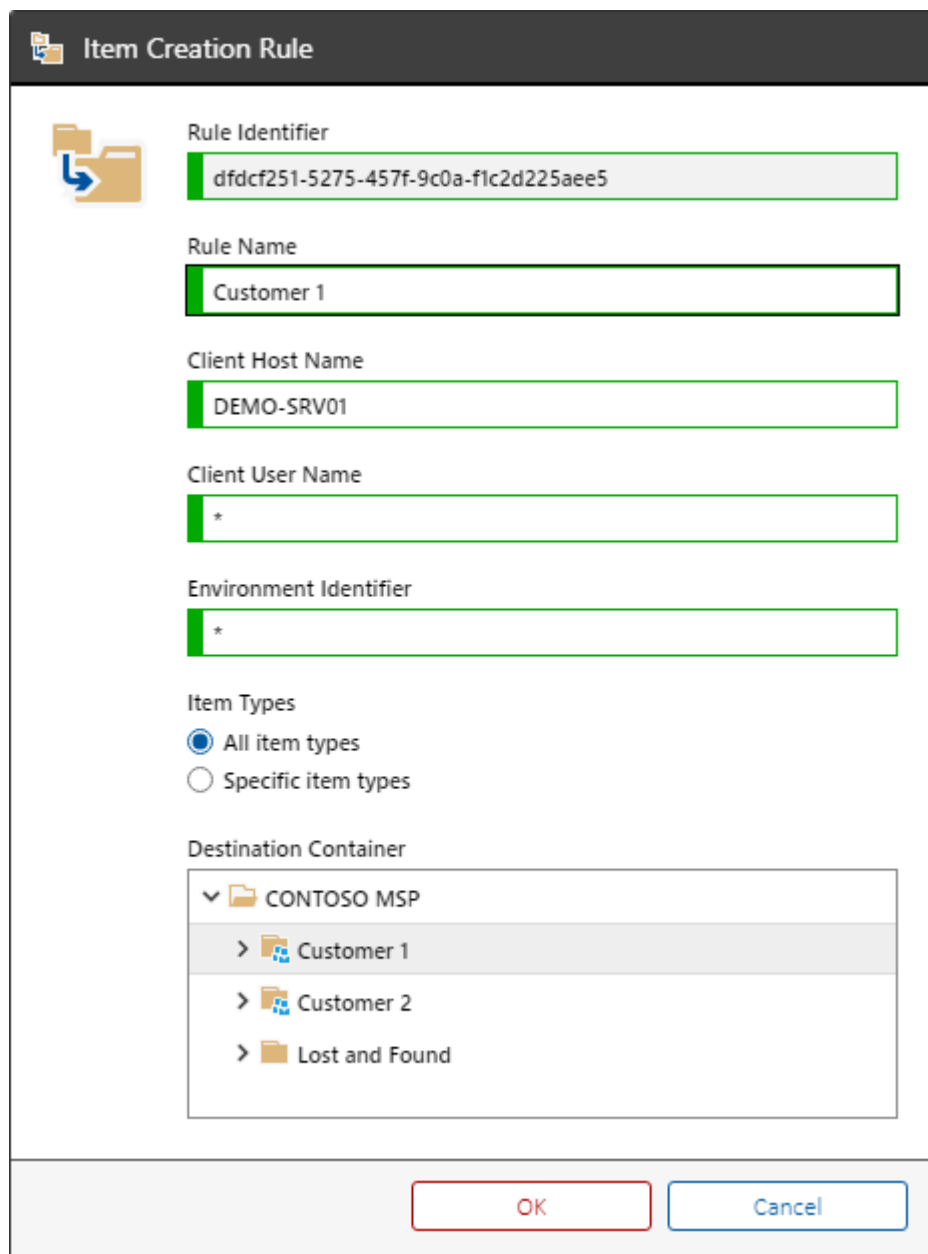
Move To Bottom

Moves the currently selected [item creation rule](#) to the bottom of the list.

Properties

Displays the currently selected [item creation rule](#) in the [item creation rule dialog](#).

Item Creation Rule Dialog



The dialog box is titled "Item Creation Rule" and contains several input fields and a list. On the left side, there is a folder icon with a blue arrow pointing into it. The fields are: "Rule Identifier" with the value "dfdcf251-5275-457f-9c0a-f1c2d225aee5"; "Rule Name" with the value "Customer 1"; "Client Host Name" with the value "DEMO-SRV01"; "Client User Name" with the value "*"; and "Environment Identifier" with the value "*". Below these fields are two radio buttons for "Item Types": "All item types" (selected) and "Specific item types". At the bottom is a "Destination Container" list showing a tree structure: "CONTOSO MSP" (expanded) containing "Customer 1", "Customer 2", and "Lost and Found". At the bottom right are "OK" and "Cancel" buttons.

Rule Identifier
dfdcf251-5275-457f-9c0a-f1c2d225aee5

Rule Name
Customer 1

Client Host Name
DEMO-SRV01

Client User Name
*

Environment Identifier
*

Item Types
☒ All item types
☐ Specific item types

Destination Container
▼ CONTOSO MSP
 > Customer 1
 > Customer 2
 > Lost and Found

OK Cancel

Rule Identifier

The unique identifier of the [rule](#) in [GUID](#) format.

Rule Name

The unique descriptive name for the [rule](#).

Host Name

The NetBIOS computer name of the machine running the [XIA Configuration Client](#) that performed the scan to match - for example "DEMO-SRV01". This field is not case sensitive. A value of "*" matches any client host name.

Username

The name of the user account including domain name that was used to upload the data to the [XIA Configuration Server](#) to match - for example "CORP\svcXIAServer".

- By default, this is the same as the user account running the [XIA Configuration Client](#).
- If [custom credentials](#) were configured for the [server connection settings](#) then this account name is used.
- If [custom credentials](#) were not configured for the [server connection settings](#), but [custom credentials](#) were specified for the [scan profile](#), and the [XIA Configuration Server](#) is running on a different machine to the [XIA Configuration Client](#) then this account name is used.

This field is not case sensitive. A value of "*" matches any username.

Environment Identifier

The name of the [environment identifier](#) assigned to the [item](#) to match. This field is not case sensitive. A value of "*" matches any environment identifier. If the field is blank, only [items](#) with a blank [environment identifier](#) will match this rule.

Destination Container

The [container](#) or [customer](#) into which matching [items](#) are to be created.

Item Types

The [item types](#) to match. This allows different [item types](#) to be created in different [containers](#) or [customers](#).

Integration

The integration section provides the configuration settings to integrate with 3rd party systems.

ServiceNow Connector Settings

Provides the ability to connect to a [ServiceNow instance](#).

ServiceNow Connector Settings

The [ServiceNow](#) connector allows integration between [XIA Configuration Server](#) and a [ServiceNow instance](#).

Enable ServiceNow connector

Determines whether to enable integration between [XIA Configuration Server](#) and a [ServiceNow instance](#).

Instance URL

The URL of the [ServiceNow instance](#).

Authentication Type

The authentication type, this is currently limited to credentials.

Username

The username to use to connect to the [ServiceNow instance](#).

Password

The password to use to connect to the [ServiceNow instance](#).

Language

The two-character ISO language code. This setting is used when creating new choices in the [ServiceNow instance](#) such as operating system names.

Timeout (seconds)

The timeout to use when communicating with the [ServiceNow instance](#).

Enable Windows server synchronization

Determines whether [Windows server](#) items in [XIA Configuration Server](#) should be synchronized with the [ServiceNow instance](#).

Matching Method

The matching method to use to match the [Windows server](#) items in [XIA Configuration Server](#) with the Windows server configuration items in the [ServiceNow instance](#).

- Server Name and Serial Number
- Server Name Only

Operating System Choice Not Found Action

The [action to take](#) if the operating system configured for the [Windows server](#) item in [XIA Configuration Server](#) is not available as a choice in the [ServiceNow instance](#).

Referenced Company Not Found Action

The [action to take](#) if a referenced company (such as the manufacturer) configured for the [Windows server](#) item in [XIA Configuration Server](#) is not available as a company in the [ServiceNow instance](#).

Referenced Hardware Model Not Found Action

The [action to take](#) if a referenced hardware mode configured for the [Windows server](#) item in [XIA Configuration Server](#) is not available in the [ServiceNow instance](#).

Automatically synchronize with ServiceNow

Determines whether the [scheduler](#) should automatically synchronize [XIA Configuration Server](#) with the [ServiceNow instance](#).

Interval (minutes)

The interval in minutes at which the [scheduler](#) should automatically synchronize [XIA Configuration Server](#) with the [ServiceNow instance](#).

Test Connection

Tests the connection between the [XIA Configuration Server](#) and the [ServiceNow instance](#) using the settings in the user interface.

Save Connector Settings

Saves the connector settings.

Choice Not Found Action

When a choice value does not exist in the [ServiceNow instance](#) - for example the choice "Windows Server 2022 Enterprise" is not available for selection as a valid operating system name the following actions are available.

Create (Abort on Failure)

The choice value is created and selected - an exception is thrown if the choice cannot be created.

Create (Continue on Failure)

The choice value is created and selected - if the choice cannot be created the system proceeds and the current value is retained in the [ServiceNow instance](#).

Ignore

The system proceeds with the operation and the current value is retained in the [ServiceNow instance](#).

Throw Exception

An exception is thrown.

Referenced Object Not Found Action

When a referenced object such as a company or model does not exist in the [ServiceNow instance](#) - for example the company "Hewlett-Packard" is not available for selection as the manufacturer of an item, the following actions are available.

Create (Abort on Failure)

The referenced object is created and selected - an exception is thrown if the referenced object cannot be created.

Create (Continue on Failure)

The referenced object is created and selected - if the referenced object cannot be created the system proceeds and the currently referenced object selection is retained in the [ServiceNow instance](#).

Ignore

The system proceeds with the operation and the currently referenced object selection is retained in the [ServiceNow instance](#).

Throw Exception

An exception is thrown.

Synchronization

The section allows the manual synchronization between [XIA Configuration Server](#) and the [ServiceNow instance](#) using the [ServiceNow](#) connector.

Force the resynchronization of all items that have already been synchronized

When this option is set all [supported item types](#) are synchronized between [XIA Configuration Server](#) and the [ServiceNow instance](#) even if the item has already been synchronized and no changes are required.

Simulate the synchronization

Simulates the synchronization between [XIA Configuration Server](#) and the [ServiceNow instance](#), allowing a system administration to evaluate what actions would be taken by the [ServiceNow](#) connector such as matching and item creation.

Run Synchronization

Starts the synchronization or simulation of the synchronization between [XIA Configuration Server](#) and the [ServiceNow instance](#).

Abort Synchronization

Aborts synchronization or simulation.

View Results

Opens the [results](#) in CSV file format.

Results

The results of the [synchronization](#) or [simulation](#) between [XIA Configuration Server](#) and the [ServiceNow instance](#) can be viewed in CSV format.

AutoSave Off Results.csv Search

File Home Insert Page Layout Formulas Data Review View Automate Help

Clipboard Font Alignment Number Styles Cells Analysis Sensitivity

Comments Share

Calibri 11

B I U A A

General

Conditional Formatting

Format as Table

Cell Styles

Insert

Delete

Format

Editing

Analyze Data

Sensitivity

A3

	A	B	C	D	E	F	G	H
1	[Item Identifier]	[Name]	[Type]	[ServiceNow Identifier]	[Action]	[Exception Message]		
2	1001	DEMO-XCS-12R2	Windows Server	9f55890b97331110c030f7a6f053aff1	Update Matched Item			
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								

Results

Ready Accessibility: Unavailable

Item Identifier

The unique identifier of the **item** in XIA Configuration Server.

Name

The name of the [item](#) in [XIA Configuration Server](#).

ServiceNow Identifier

The unique identifier of the **item** in the **ServiceNow** instance.

Action

The action taken or simulated by the [synchronization](#).

Exception Message

The exception message if an error occurred during the [synchronization](#) or [simulation](#).

Troubleshooting

This section highlights the known issues for the [ServiceNow connector](#), and provides details of the solutions.

The 'meta' start tag does not match the end tag

Symptoms

When attempting to connect to a [ServiceNow instance](#) you receive the error.
The 'meta' start tag on line 3 position 10 does not match the end tag of 'head'.

Cause

This can occur when the [ServiceNow instance](#) you are connecting to is a developer instance and the instance is currently hibernating.

Resolution

Log into the [ServiceNow instance](#) instance to wake it from hibernation.

More Information

For more information see the following ServiceNow blog article.

<https://developer.servicenow.com/blog.do?p=/post/hibernation-and-developer-instances/>

The underlying connection was closed

Symptoms

When attempting to connect to a [ServiceNow instance](#) you receive the error.

"Error connecting to the ServiceNow instance. The underlying connection was closed: An unexpected error occurred on a receive."

or

"Error connecting to the ServiceNow instance. The request was aborted: Could not create SSL/TLS secure channel."

Cause

This can occur when using older operating systems such as Windows Server 2012 R2 that are not configured to use newer TLS protocols.

Resolution

Ensure the following registry keys are set on the machine running [XIA Configuration Server](#), and reboot if required.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
```

```
"SystemDefaultTlsVersions"=dword:00000001
```

```
"SchUseStrongCrypto"=dword:00000001
```

- or -

[Install XIA Configuration Server](#) on a more modern operating system.

More Information

For more information see the following article.

<https://learn.microsoft.com/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

Item Naming

Each item type within XIA Configuration has an item naming restriction which sets the format to which an item of that type's name must adhere to.

Modifying Item Naming Settings

Enter the naming convention for each type in regular expression format.

To save the settings click **Save Item Naming Settings**

NOTE: This setting cannot be modified for [knowledge base articles](#) as these are named automatically.

NOTE: Naming conventions are applied only when creating a new item or renaming an existing Item.

Licensing Configuration

The licensing configuration allows you to view the current license configuration for the [XIA Configuration Server](#), which must comply with the terms of the [End User License Agreement \(EULA\)](#).

There are several [license types](#) available depending on the requirements of your organization.

Within the user interface are the following settings.

 Licensing	
Is Licensed	True
Last Validated	Monday, September 9, 2024 1:21:52 PM

Is Licensed

Determines whether the product is currently licensed.

Last Validated

Determines the date and time on which the license was last validated.

 Enterprise License	
Customer Name	Demonstration
Allows Remote Connections	True
Creation Date	Monday, September 9, 2024 1:21:24 PM
License Identifier	a4d67a2e-a123-4b6b-a01e-f4df1e723c4d
Support Expiry Date	Tuesday, September 9, 2025

Customer Name

The name of the customer to which the product is licensed and their unique identifier in GUID format.

Allow Remote Connections

Determines whether remote connections are permitted for this license.

Creation Date

The date and time on which the license was crated.

License Identifier

The unique identifier of the license in GUID format.

Notes

Any additional notes, terms or conditions that apply to this license.

Other Information

Addition information is presented depending on the [license type](#).

Support Expiry Date

The date and time on which the support expires for this license.

License Usage

Determines the currently used licenses, certain [license types](#) provide an unlimited item count. For more information see the [license usage count](#) section.

Reload License File

Reloads the license file and recalculates the license count.

Replace License File

Allows you to [select a new license file](#) to replace the one that is currently installed.

License Types

There are several license types available depending on the requirements of your organization.

This section provides a summary of those license types, however for detailed information please review the [End User License Agreement \(EULA\)](#).

Enterprise License

The *Enterprise license* is designed for customers who wish for centralized server reporting, and [purchase licenses](#) for only [what is used](#).

Technician License

The *Technician license* is designed for engineers or IT technicians who wish to install [XIA Configuration Server](#) on a single machine and perform single audits of environments, generating the subsequent information to [PDF](#) to be presented to the end customer.

Trial License

The *Trial license* is time limited and designed for the evaluation of the [XIA Configuration Server](#) product. [PDF output](#) will be generated with a "Trial" watermark and certain information will be replaced by "Trial" messages. These can only be removed by [purchasing a production license](#).

Unlimited License

The *Unlimited license* is designed for customers who wish for centralized server reporting without needing to specify exact license counts.

Workgroup License

The *Workgroup license* is a free, but limited license designed for small businesses that have only a basic network.

Enterprise License

The *Enterprise* [license type](#) is ideal for customers who wish for centralized server reporting, and [purchase licenses](#) for only [what is used](#).

 License Coverage	
Coverage Type	Active Directory Domain DNS Name
Coverage Values	demonstration.int

Coverage Type

The type of coverage provided by this license. This is either the Active Directory Domain DNS Name of which the computer running [XIA Configuration Server](#) is a member, or the NetBIOS name of computer running [XIA Configuration Server](#).

Coverage Values

The coverage values of the license.

Technician License

The *Technician license type* is ideal for engineers or IT technicians who wish to install [XIA Configuration Server](#) on a single machine and perform single audits of environments, generating the subsequent information to PDF to be presented to the end customer. For more information see the [technician license installation best practice](#).

 License Coverage	
User Full Name	Demonstration User
Account Name	demonstration\administrator
Machine Name	DEMO-XCS-2022

User Full Name

The named Technician can access the software as per the [End User License Agreement \(EULA\)](#).

Account Name

The name of the user account who is permitted to access the software.

Machine Name

The NetBIOS name of the computer on which the software is permitted to be run.

Trial License

The *Trial* license is time limited and ideal for the evaluation of the [XIA Configuration Server](#) product.

There is no limit to the number of [items](#) being documented which allows you to quickly determine the amount of licenses you require to [purchase](#) to use the product in a product environment. [PDF output](#) will be generated with a "Trial" watermark and certain information will be replaced by "Trial" messages. These can only be removed by [purchasing a production license](#).

License Usage		
Category Name	Available	Used
 Cloud Infrastructure Subscriptions	200	0
 Enterprise Application Instances	200	0
 Microsoft 365 Organizations	50	0
 Network Devices	5000	0
 Server Application Instances	400	0
 Unix Systems	1000	0
 Virtualization Hosts	1000	0
 Windows Servers and Roles	10000	2
 Windows Workstations	0	0

As with all [license types](#), the *Trial* license is subject to the terms of the [End User License Agreement \(EULA\)](#).

Unlimited License

The *Unlimited* [license type](#) is ideal for customers who wish for centralized server reporting without needing to specify exact license counts.

 License Coverage	
Coverage Type	Active Directory Domain DNS Name
Coverage Values	demonstration.int

Coverage Type

The type of coverage provided by this license. This is either the Active Directory Domain DNS Name of which the computer running [XIA Configuration Server](#) is a member, or the NetBIOS name of computer running [XIA Configuration Server](#).

Coverage Values

The coverage values of the license.

As with all [license types](#), the *Unlimited* license is subject to the terms of the [End User License Agreement \(EULA\)](#).

Workgroup License

The *Workgroup* [license type](#) is a free, but limited license ideal for small businesses that have only a basic network.

License Coverage

Machine Name	DEMO-XCS-2022
--------------	---------------

Machine Name

The NetBIOS name of which the computer running [XIA Configuration Server](#) that is permitted by this license.

The *Workgroup* license has several limitations

- You cannot [compare items](#) with the *Workgroup* license
- [PDF output](#) will be generated with a watermark
- You cannot use the [Web Services SDK or PowerShell API](#) with the *Workgroup* license

License Usage Count

Determines the currently used license counts, certain [license types](#) provide an unlimited item count.

License Usage		
Category Name	Available	Used
 Cloud Infrastructure Subscriptions	Unlimited	24
 Enterprise Application Instances	Unlimited	15
 Microsoft 365 Organizations	Unlimited	6
 Network Devices	Unlimited	13
 Server Application Instances	Unlimited	58
 Unix Systems	Unlimited	47
 Virtualization Hosts	Unlimited	426
 Windows Servers and Roles	Unlimited	231
 Windows Workstations	Unlimited	27

The licenses are broken down in to categories:

Cloud Infrastructure Subscriptions

The total number of subscriptions in all cloud infrastructure platforms scanned including all subscriptions in scanned [Azure tenants](#).

Enterprise Application Instances

The total number of scanned [Exchange on-premises organizations](#).

Microsoft 365 Organizations

The total number of [Microsoft 365 organizations](#) scanned which may include any or all of the supported Microsoft 365 services [Entra directories](#) and [Exchange Online organizations](#).

Network Devices

The total number of scanned [network storage devices](#) and [network switches](#).

Server Application Instances

The total number of scanned [Backup Exec servers](#) and [SQL instances](#).

Unix Systems

The total number of scanned [Unix or Linux Systems](#).

Virtualization Hosts

The total number of **hosts** in all scanned [Citrix XenApp Farms](#), [Citrix XenDesktop Sites](#), [Hyper-V Servers](#), and [VMware systems](#).

Windows Servers and Roles

The total number of [Windows machines](#), running a server operating system, and supported roles. If any of the individual scanned roles ([Active Directory domain controllers](#), [DHCP](#), [DNS](#), [Failover Cluster](#), [IIS](#), [NLB Cluster](#), [Remote Desktop Session Host](#) or [WINS](#)) exceeds the count of the scanned [Windows Server Machines](#), this number is used as the count instead.

Windows Workstations

The total number of scanned [Windows machines](#), running a desktop operating system.

Show License Count Details

This button displays the full license count of each individual [item type](#), instead of by the license categories.

 License Usage

Category Name	Available	Used
 Cloud Infrastructure Subscriptions	Unlimited	24
 Azure Subscriptions		24
 Enterprise Application Instances	Unlimited	15
 Exchange On-Premises Organizations		15
 Microsoft 365 Organizations	Unlimited	6
 Entra Directories		6
 Exchange Online Organizations		6
 Network Devices	Unlimited	13
 Network Storage Devices		4
 Network Switches		9
 Server Application Instances	Unlimited	58
 Backup Exec Servers		11
 SQL Instances		47
 Unix Systems	Unlimited	47
 Virtualization Hosts	Unlimited	426
 ESX Hosts		386
 Hyper-V Hosts		7
 XenApp Farm Servers		25
 XenDesktop Delivery Controllers		8
 Windows Servers and Roles	Unlimited	231
 Domain Controllers		51
 Failover Clusters		12
 IIS Servers		26
 Microsoft DHCP Servers		19
 Microsoft DNS Servers		18
 Microsoft NLB Clusters		1
 Remote Desktop Session Hosts		9
 WINS Servers		9
 Windows Servers		231
 Windows Workstations	Unlimited	27

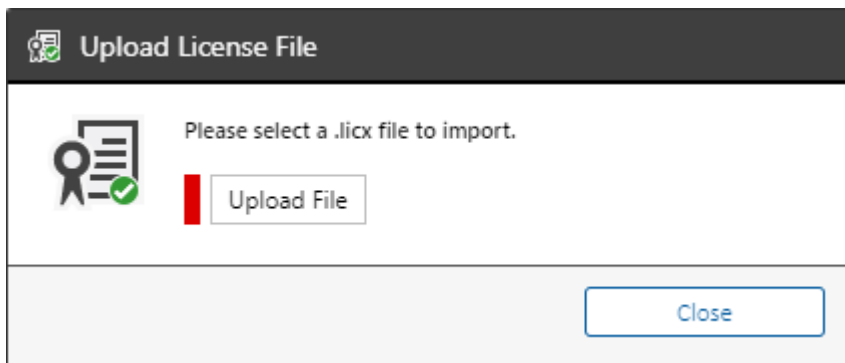
Replacing the License File

To replace the current license file, perform the following steps.

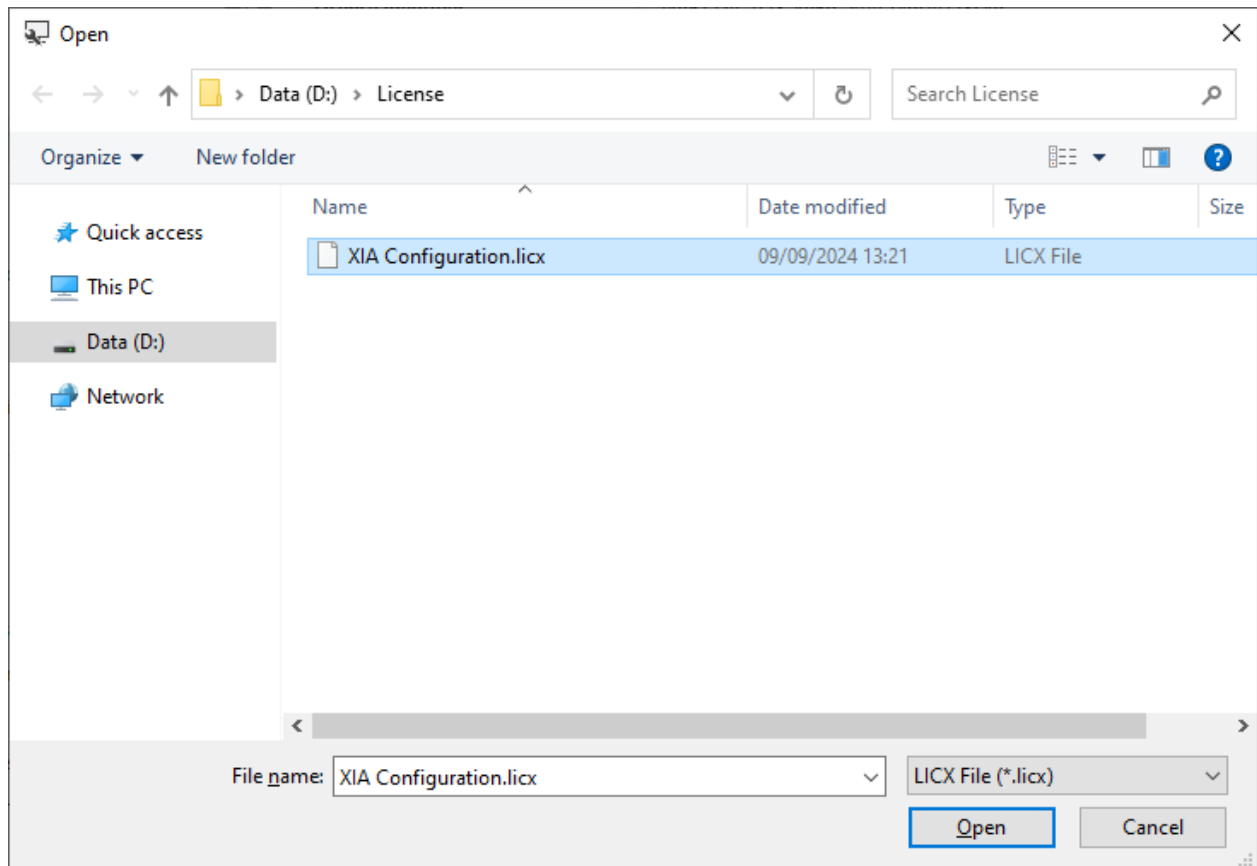
- Go to the [licensing configuration](#) section within the [configuration settings](#).
- Click the Replace License File button

Replace License File

- On the following dialog click the upload file button.



- Select the [license file](#), which must have a .licx extension.



- Click the Open button to replace the existing [license file](#) with the selected file.

NOTE: The current license file will be renamed with a .backup file extension.

Manual Item Creation

Determines the [item types](#) that can be [created manually](#).

Default Item Types

The system automatically determines which [item types](#) can be [created manually](#).

Specific Item Types

The specific [item types](#) that can be [created manually](#).

Manufacturer Definitions

Manufacturer definitions allow information such as a warranty lookup hyperlinks to be automatically detected for hardware [items](#).

Manufacturer Definitions

Configures manufacturer related information for hardware devices.

 2 Manufacturer Definitions

 Display Name	System Managed
 Dell Inc.	True
 HP	True

New Manufacturer Definition

Save Manufacturer Definitions

Display Name

The display name of the manufacturer definition.

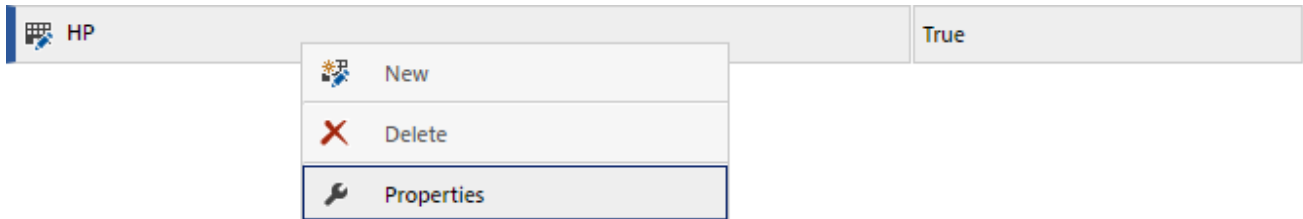
System Managed

Determines whether the manufacturer definition is managed by the system.

Right clicking an item shows the manufacturer definitions [context menu](#).

Context Menu

The context menu is displayed when a [manufacturer definition](#) is right clicked.



New

Displays the [manufacturer definition dialog](#), to create a new [manufacturer definition](#).

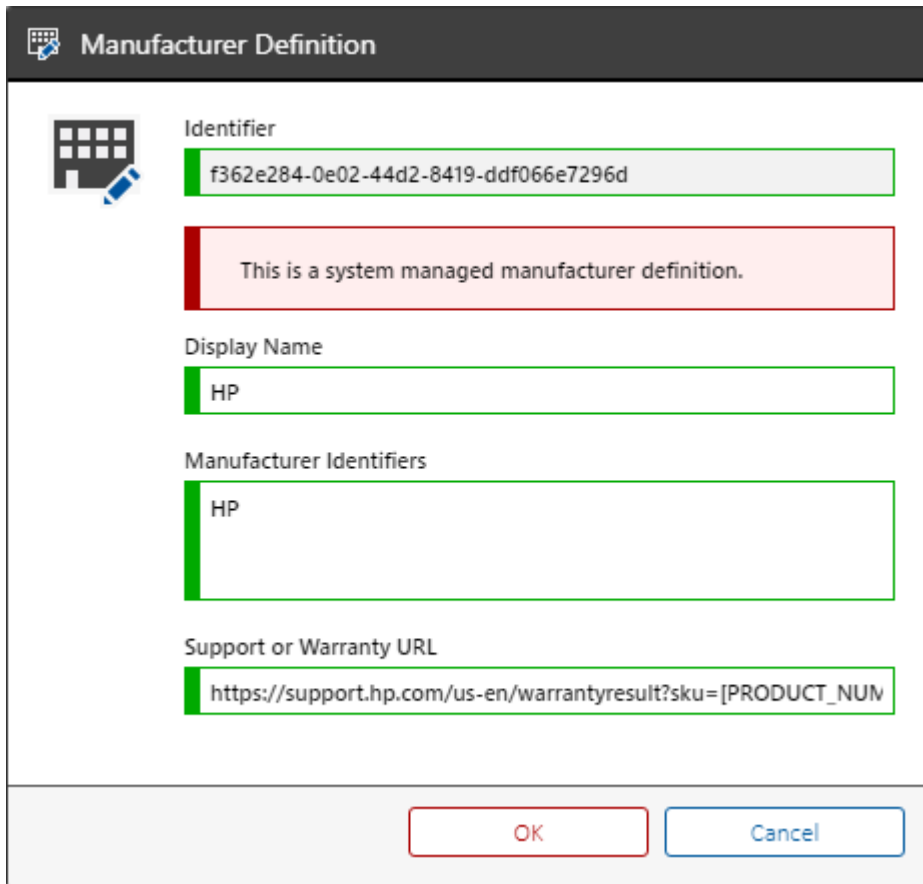
Delete

Deletes the currently selected [manufacturer definition](#).

Properties

Displays the currently selected [manufacturer definition](#) in the [manufacturer definition dialog](#).

Manufacturer Definition Dialog

The image shows a 'Manufacturer Definition' dialog box. It has a dark header bar with a grid icon and the title 'Manufacturer Definition'. The main area contains several fields: 'Identifier' with a value 'f362e284-0e02-44d2-8419-ddf066e7296d', a red-bordered box with the text 'This is a system managed manufacturer definition.', 'Display Name' with a value 'HP', 'Manufacturer Identifiers' with a value 'HP', and 'Support or Warranty URL' with a value 'https://support.hp.com/us-en/warrantyresult?sku=[PRODUCT_NUM]'. At the bottom, there are 'OK' and 'Cancel' buttons.

Manufacturer Definition

Identifier
f362e284-0e02-44d2-8419-ddf066e7296d

This is a system managed manufacturer definition.

Display Name
HP

Manufacturer Identifiers
HP

Support or Warranty URL
https://support.hp.com/us-en/warrantyresult?sku=[PRODUCT_NUM]

OK Cancel

Identifier

The unique identifier of the [manufacturer definition](#).

Display Name

The display name the [manufacturer definition](#).

Manufacturer Identifiers

The manufacturer names that match this [manufacturer definition](#), one per line. These can include the % wildcard.

Support or Warranty URL

The link to the support or warranty information for the hardware [item](#).

This can include the variables

[SERIAL_NUMBER]

[PRODUCT_NUMBER]

Password List

This section provides the [configuration settings](#) relating to [password list items](#).

NOTE: For security settings relating to [password list items](#) see the [security settings](#) section.

Validate password list entry types when password lists are updated

Determines whether the entry type of [password list entries](#) should be validated when the [password list](#) is saved or restored from a [previous version](#).

Entry Type Definitions

The system automatically manages a number of [password list](#) entry types, however additional [password list](#) entry types can be defined.

Entry Type Definitions

Password list entry type definitions allow custom entry types to be created for use within password list items.

 1 Custom Entry Types

 Display Name	Enable Account Name
 Custom Entry Type	True

New Entry Type Definition

Save Entry Type Definitions

 10 System Managed Entry Types

 Display Name	Enable Account Name
 Application Login	True
 FTP Account	True
 Network Device Login	True
 Product Key	True
 SNMP Community String	False
 SQL Account	True
 Unix Account	True
 Website Login	True
 Windows Domain User	True
 Windows Local User	True

Display Name

The display name of the [password list](#) entry type.

Enable Account Name

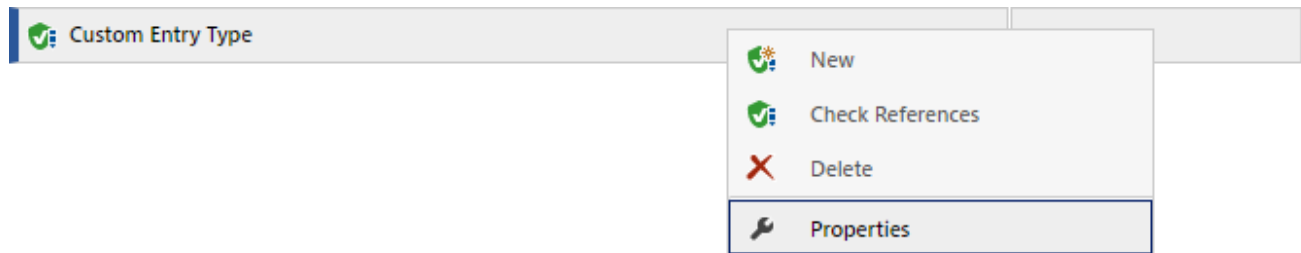
Determines whether the account name field should be enabled for [password list](#) entries of this type.

Right clicking a [password list](#) entry type displays the [password list entry type context menu](#).

Clicking the new entry type definition button displays the [password list entry type dialog](#).

Context Menu

The context menu is displayed when a user right clicks a custom [password list entry type definition](#).



New

Displays the [password list entry type dialog](#), to create a new [password list entry type](#).

Check References

Determines whether the currently selected [password list entry type](#) is in use by any [password lists](#). The Custom Password List Entry Type Usage [report](#) can be used to provide additional information.

Delete

Deletes the currently selected [password list entry type](#).

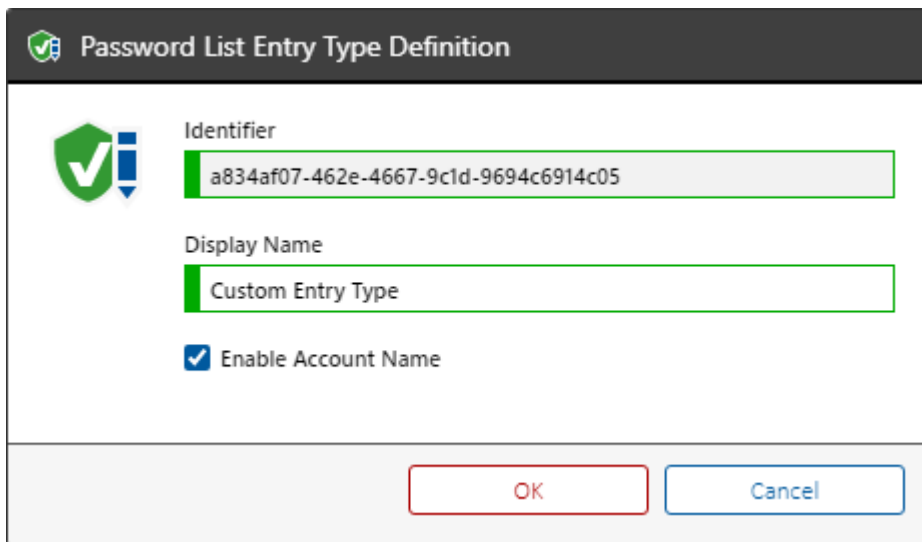
WARNING: Deleting a [password list entry type](#) can lead to password entries displaying as an unknown entry type. Use the check references above to validate whether the password list entry type is in use by any [password lists](#) before proceeding.

Properties

Displays the currently selected [password list entry type](#) in the [password list entry type dialog](#).

Password List Entry Type Dialog

The password list entry type definition dialog allows a [password list entry type](#) to be created or modified.



The dialog box is titled "Password List Entry Type Definition" and features a green checkmark icon. It contains three input fields: "Identifier" with the value "a834af07-462e-4667-9c1d-9694c6914c05", "Display Name" with the value "Custom Entry Type", and a checked checkbox labeled "Enable Account Name". At the bottom right, there are "OK" and "Cancel" buttons.

Field	Value
Identifier	a834af07-462e-4667-9c1d-9694c6914c05
Display Name	Custom Entry Type
Enable Account Name	☒

Display Name

The display name of the [password list](#) entry type.

Identifier

The unique identifier in [GUID](#) format of this [password list entry type](#).

Enable Account Name

Determines whether the account name field should be enabled for [password list](#) entries of this type.

Password List Audit Events

In addition to the events generated by all [item types](#), [password lists](#) also generate the following events to the [event log](#).

Password list entry creation

When an entry is added to a [password list](#).

Password list entry deletion

When an entry is removed from a [password list](#).

Password list entry update

When any of the settings in an entry is modified in a [password list](#). This includes the change of password which also generates a dedicated event.

Password list entry password update

When the password is modified in a [password list](#). If a password entry is modified and the password reset to the same value as is currently set a "Password list entry update" event will be logged as the encrypted value will be updated, but a "Password list entry password update" event will not be logged as the actual password has not been updated.

The audit of the above events can be disabled in the [event log settings](#).

Password list password decryption

When a password is decrypted in a [password list](#) allowing the user to view the plain text password.

Password list decryption

When all passwords are decrypted in a [password list](#) allowing the user to view all plain text passwords.

PDF Output Settings

This section allows the configuration of various aspects of the [PDF documentation](#) of [items](#), and [report](#) output.

Cover Image

Determines the image to write to the cover of the PDF. The options include:

- None
- Blue Waves (default)
- Red Waves
- Custom



When **Custom** is selected, the user can browse to an image to use. The image is automatically saved in .PNG file format and scaled to the size of the PDF. Once selected you will be prompted to overwrite any existing image immediately.

Cover Logo

The cover logo allows for the selection of a company logo to be displayed in the bottom left of the PDF document, though this does not preclude a logo being used as the primary cover image. The options for cover logo include

- None
- Custom

When **Custom** is selected the user can browse to an image to use. The image is automatically saved in .PNG file format and scaled to the appropriate size. Once selected you will be prompted to overwrite any existing image immediately.

PDF Disclaimer Message

Determines the disclaimer message that is shown in a special disclaimer page in the PDF document.

Confidentiality Level

Determines the confidentiality level warning written in red text on the cover of all PDF documents, by default this is set to "Company Confidential".

Footer Text

Determines the text to be written in the footer of every page of the PDF document except for the cover and table of contents pages.



Audit Export to PDF

When selected, this option ensures that every time a user exports an item to PDF the action is audited within the XIA Configuration event log. This option is disabled by default. The event ID recorded by this action is 3031.

Character Support (requires Windows 2008 R2 or above)

Determines which of the following character sets are supported when exporting to PDF.

- Default
- Traditional Chinese
- Simplified Chinese

When this setting is changed, the **application pool** running the XIA Configuration Server site must be restarted for the changes to take effect.

PDF Watermark

Determines the Watermark that is rendered on all pages within the PDF Document.

NOTE: When using the Trial or Workgroup edition of XIA Configuration Server this option is ignored and the default watermark for that license type is applied automatically.

To save the settings click the **Save PDF Settings** action point.

PDF Color Settings

The colour settings determine the colours used for the various sections of the [PDF documentation](#) of [items](#), and [report](#) output.

Heading

Determines the colour to use for the headings in the PDF document.

Table Heading Cell

Determines the colour to use for table heading cells.

Cover Page

Determines the colour settings to use on the cover page.



Footer Background

Determines the colour of the footer of the cover page. By default this is white. When setting the footer colour and using a cover logo you should ensure that the logo has a transparent background, or that the logo background colour matches that of the footer.

Heading

The colour to use for the heading text on the cover page.

Subheading

The colour to use for the subheading text on the cover page.

Bullet Points

The colour to use for the bullet points on the cover page.

Date	06/03/2014 12:45:15
Author	[redacted]
Version	1.0.0
Product	XIA Configuration Server [5.3.0.19702]

Table of Contents

Determines the colour settings to use on the table of contents pages.



The image shows a screenshot of a 'Table of Contents' page with a solid blue background and white text. The title 'Table of Contents' is at the top left. Below it, the word 'Document' is followed by a list of topics and their corresponding page numbers. The topics are organized into sections: 'General Information' (Operations Monitor, 8), 'Groups' (Access Control Assistant Operations, 12; Account Operations, 12; Administration, 12; Admins BCOE Password Replication Group, 16; Backup Operations, 16; Cert Publishers, 16; Certificate Services BCOE Admins, 16; Certificate Services Controllers, 14; Cryptographic Operations, 16; Remote BCOE Password Replication Group, 16; Distribution COO Admins, 16; Distributions, 16; EncryptionPolicy, 16; Domain Admins, 16; Domain Computers, 17; Domain Controllers, 17; Domain Groups, 17; Domain Users, 17; Enterprise Admins, 16; Enterprise Read-only Domain Controllers, 16; Event Log Readers, 16; Group Policy Creator Owners, 16; Guests, 16; HelpAndRecoveryAdmins, 16; Users of Administrators, 20; and XIA Admins, 20).

Document	
General Information	
Operations Monitor	8
Groups	
Access Control Assistant Operations	12
Account Operations	12
Administration	12
Admins BCOE Password Replication Group	16
Backup Operations	16
Cert Publishers	16
Certificate Services BCOE Admins	16
Certificate Services Controllers	14
Cryptographic Operations	16
Remote BCOE Password Replication Group	16
Distribution COO Admins	16
Distributions	16
EncryptionPolicy	16
Domain Admins	16
Domain Computers	17
Domain Controllers	17
Domain Groups	17
Domain Users	17
Enterprise Admins	16
Enterprise Read-only Domain Controllers	16
Event Log Readers	16
Group Policy Creator Owners	16
Guests	16
HelpAndRecoveryAdmins	16
Users of Administrators	20
XIA Admins	20

Heading

The colour to use for the heading text for the table of contents.

Subheading

The colour to use for the subheading text for the table of contents.

Text

The colour to use for the text on the table of contents.

Restore Default Settings

Restores the default colour settings to the blue colour scheme.

To save the settings click the **Save Colour Settings** action point.

Relationship Settings

Filter By Environment Identifier

Determines whether system managed [relationships](#) should be filtered if the [items](#) have different [environment identifiers](#). This prevents [relationships](#) being detected between [items](#) that belong in separate environments but have the same identifiers - for example when a disaster recovery environment contains [items](#) with the exact same name and serial number as in a production environment.

Filter By Immediate Parent Customer

Determines whether system managed [relationships](#) should be filtered if the [items](#) have different parent [customers](#). This prevents [relationships](#) being detected between [items](#) that belong in separate [customers](#) but have the same identifiers - for example when two distinct [customers](#) have used the same naming convention for [items](#).

Relationship Types

The system automatically manages a number of relationship types between [items](#), however additional relationship types can be defined.

Relationship Types

Relationship type definitions allow custom relationship types to be created.

1 Custom Relationship Types

Display Name	Inbound Creation	Valid Source Types	Valid Target Types
 Primary Contact	Optional	Any	Contact

[New Relationship Type](#)[Save Relationship Types](#)

52 System Managed Relationship Types

Display Name	Inbound Creation	Valid Source Types	Valid Target Types
 Connected Disk Shelf	Optional	Any	Disk Shelf
 Connected Network Device	Prevent	Network Switch	Any
 Connected Network Storage Device	Optional	Any	Network Storage Device
 Connected Tape Library	Optional	Any	Tape Library
 Connected to Network Device	Prevent	Any	Network Switch
 Contained Within	Prevent	Any	Any
 Contains Delivery Controller	Prevent	Citrix XenDesktop Site	Windows Server

Display Name

The display name of the relationship type.

Inbound Creation Mode

Determines whether a reciprocal [relationship](#) should be automatically created from the target [item](#) to the source [item](#).

Valid Source Types

The valid [item types](#) for the source [item](#).

Valid Target Types

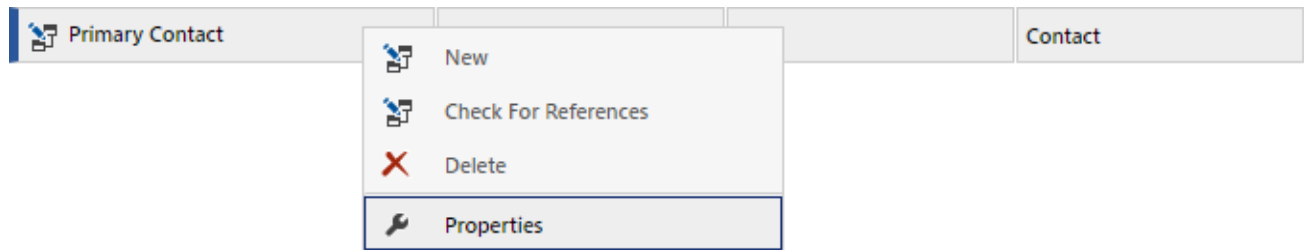
The valid [item types](#) for the target [item](#).

Right clicking a custom relationship type displays the [relationship type context menu](#).

Clicking the new relationship type button displays the [relationship type dialog](#).

Context Menu

The context menu is displayed when a user right clicks a [custom relationship type](#).



New

Displays the [relationship type dialog](#), to create a new [custom relationship type](#).

Check For References

Determines whether the currently selected [custom relationship type](#) is referenced by any [items](#). The Custom Relationship Type Usage [report](#) can be used to provide additional information.

Delete

Deletes the currently selected [custom relationship type](#).

Properties

Displays the currently selected [custom relationship type](#) in the [relationship type dialog](#).

Deleting Relationship Types

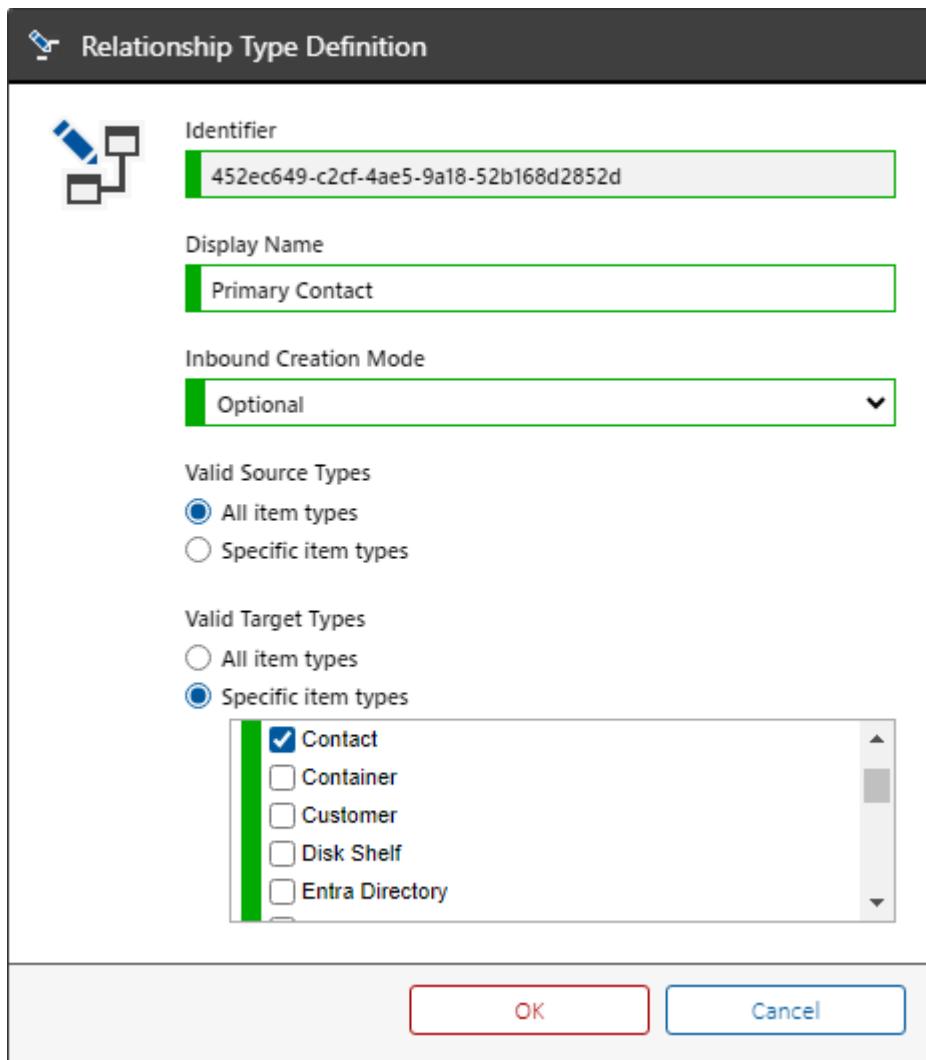
When a [relationship type](#) definition is deleted any [relationships](#) that reference the [relationship type](#) will display as **** Unknown Relationship Type ****.

If you attempt to save changes to the [relationships](#) of an item that contains an unknown [relationship type](#) the system will display an error stating that the [relationship type](#) was not found.

The [relationship](#) must be deleted or modified to use a valid [relationship type](#).

Relationship Type Dialog

The relationship type definition dialog allows a [relationship type](#) to be created or modified.



The screenshot shows the 'Relationship Type Definition' dialog box. It has a dark header bar with a pencil icon and the title 'Relationship Type Definition'. The main area is white and contains several fields and options. On the left, there is a small icon of a document with a pencil. The fields are: 'Identifier' with a text box containing '452ec649-c2cf-4ae5-9a18-52b168d2852d'; 'Display Name' with a text box containing 'Primary Contact'; 'Inbound Creation Mode' with a dropdown menu showing 'Optional'; 'Valid Source Types' with two radio buttons, 'All item types' (selected) and 'Specific item types'; 'Valid Target Types' with two radio buttons, 'All item types' and 'Specific item types' (selected). Below the 'Valid Target Types' section is a list box containing five items: 'Contact' (checked), 'Container', 'Customer', 'Disk Shelf', and 'Entra Directory'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Definition Identifier

The unique identifier in GUID format of this [relationship type](#).

Display Name

The display name of the relationship type.

Inbound Creation Mode

Determines whether a reciprocal [relationship](#) should be automatically created from the target [item](#) to the source [item](#).

- Optional
The user is prompted whether they wish to create a reciprocal inbound [relationship](#) when they [create or modify a relationship](#).
- Prevent
An inbound [relationship](#) cannot be created on the target system

- **Require**
An inbound [relationship](#) must be created on the target system.

Valid Source Types

The valid [item types](#) for the source [item](#) of the [relationship](#).

Valid Target Types

The valid [item types](#) for the target [item](#) of the [relationship](#).

Reporting Settings

This section defines the global reporting settings.

Home Page Title

Determines the title to display in the reporting section. The title for the other section home pages can be configured in the [general settings](#) section.

Home Page Description

Provides a descriptive message to be displayed on the reporting section home page. The description for the other section home pages can be configured in the [general settings](#) section.

CSV Encoding

Determines the encoding to use when writing [report](#) CSV data to a file. The available settings are [UTF-8](#) (default) or [Unicode \(UTF-16\)](#) encoding.

Allow system administrators to drag and drop objects in the reporting treeview

Determines whether [system administrators](#) can drag and drop reports, report binders and report in the reporting treeview.

Hide reports and report binders from users who do not have permissions to execute them

Determines whether reports and report binders are hidden from users who do not have permissions to execute them.

Show Customer Names

When checked displays the name of the owning [customer](#) in reports where this is available. To display customer names in reports, see the [output and charting](#) section.

Scheduler

The scheduler allows the automated execution of [scheduled tasks](#) and the [import of data files](#) on the [XIA Configuration Server](#).

The scheduler is dependent on the [scheduler service](#).

The scheduler writes information to the [event log](#).

Scheduler Status

Scheduler Status

The scheduler allows the automated execution of scheduled tasks and the import of data files.

 Scheduler Status

Executing	True
Last Updated	09 September 2024 14:13:15
Summary	Executing scheduled task 'Usage and Diagnostics Data' with identifier '84231f31-fde1-4dff-8367-c3502bf265ef'.

 Execution Queue

Display Name	Scheduled Task Type
 Usage and Diagnostics Data	Report Binder Execution Scheduled Task

Refresh

The scheduler status provides a user interface to display the current status of the [scheduler](#). The status of the [scheduler](#) can also be accessed using the [PowerShell API](#).

Executing

Determines whether the scheduler is currently executing. The execution is started every 60 seconds by the [scheduler service](#).

Last Updated

The date and time that the status displayed was last updated.

Summary

The current action being performed by the [scheduler](#).

Execution Queue

The [scheduled tasks](#) that are currently queued for execution, the [scheduled task](#) currently executing is displayed with a "play" icon.

Scheduled Tasks

Scheduled Tasks

This section allows tasks to be scheduled for automatic execution.

 2 Scheduled Tasks

▲	Display Name	Scheduled Task Type	Next Execution Date
	Sample Report	Report Execution Scheduled Task	15 September 2024 16:08
	Usage and Diagnostics Data	Report Binder Execution Scheduled Task	01 October 2024 22:00

Refresh

New Scheduled Task

Scheduled tasks can be configured to be executed by the [scheduler](#) on the specified [schedule](#). [Scheduled tasks](#) can also be managed using the [PowerShell API](#).

Report Execution Scheduled Task

Executes a [report](#) on the specified schedule.

Report Binder Execution Scheduled Task

Executes a [report binder](#) on the specified schedule.

Report Execution Scheduled Task

Executes a [report](#) on the specified [schedule](#).

General Settings



General Settings

The general settings of this scheduled task.

Display Name

Sample Report

Scheduled Task Identifier

5fcc77d2-2ee6-487b-ab0f-8c779d1ca264

Creation Date

09 September 2024 16:08:51

Date Last Modified

09 September 2024 16:08:51

Description

Sample report execution scheduled task.

Display Name

The display name of the [report execution scheduled task](#).

Scheduled Task Identifier

The unique identifier of the [report execution scheduled task](#) in [GUID](#) format.

Creation Date

The date and time on which the [report execution scheduled task](#) was created.

Date Last Modified

The date and time on which the [report execution scheduled task](#) was last modified.

Description

A description of the [report execution scheduled task](#).

Schedule



Schedule

The schedule on which the scheduled task is to execute.



☐ Once ☒ Weekly ☐ Monthly

☒ Enabled

Start Date

09/09/2024	20:00
------------	-------

☐ Expires

09/09/2025	20:00
------------	-------

Days Of Week

☐	Sunday
☒	Monday
☐	Tuesday
☐	Wednesday
☐	Thursday
☐	Friday
☐	Saturday

Determines the [schedule](#) on which the [report execution scheduled task](#) will execute.

Report Execution Settings



Report Execution Settings

The report execution settings of this scheduled task.

Report

Windows Service Summary Report

Container

> Demonstration Inc

Service Name

(e.g. Spooler)

Machine Name

(e.g. DEMO-SRV01)

Service Display Name

(e.g. Spooler Service)

Report

The [report](#) that is to be executed by the [report execution scheduled task](#).

Container

The [container](#) or [customer](#) against which the [report](#) is to be executed.

Report Parameter Values

The [report parameter values](#) to use for the execution of the [report](#).

Report Output Format



Report Output Format

The output format for this report.



Save the report in PDF format



Save the report in CSV format

Save the report in PDF format

The [report](#) is executed by the [report execution scheduled task](#) in PDF format.

Save the report in CSV format

The [report](#) is executed by the [report execution scheduled task](#) in CSV (comma separated values) format.

Assigned Output Targets



Assigned Output Targets

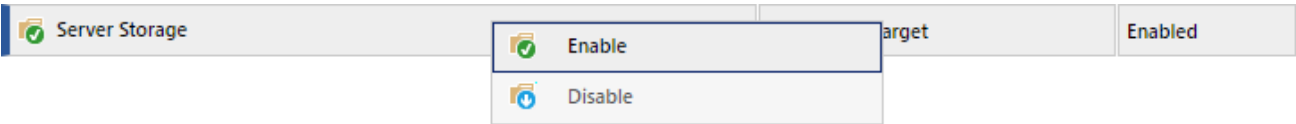
The output targets assigned to this scheduled task.

1 Output Targets Assigned

Display Name	Task Output Target Type	Status
Server Storage	File System Target	Enabled
Usage and Diagnostics Data	SMTP Target	Disabled

Assigns the [task output targets](#) for this [report execution scheduled task](#).

Right click the [task output target](#) and select the appropriate option to enable or disable it.



NOTE: At least one [task output target](#) must be assigned.

Report Binder Execution Scheduled Task

Executes a [report binder](#) on the specified [schedule](#).

General Settings



General Settings

The general settings of this scheduled task.

Display Name

Technical Overview Report Binder

Scheduled Task Identifier

80f504d9-9c52-48c7-93c6-4110f1238e53

Creation Date

[Not Configured]

Date Last Modified

[Not Configured]

Description

Executes the technical overview report binder and sends to the technical support team.

Display Name

The display name of the [report binder execution scheduled task](#).

Scheduled Task Identifier

The unique identifier of the [report binder execution scheduled task](#) in [GUID](#) format.

Creation Date

The date and time on which the [report binder execution scheduled task](#) was created.

Date Last Modified

The date and time on which the [report binder execution scheduled task](#) was last modified.

Description

A description of the [report binder execution scheduled task](#).

Schedule



Schedule

The schedule on which the scheduled task is to execute.



☐ Once ☐ Weekly ☒ Monthly

☒ Enabled

Start Date

09/09/2024	09:00
------------	-------

☐ Expires

09/09/2025	09:00
------------	-------

Months

☒ January
☒ February
☒ March
☒ April
☒ May
☒ June
☒ July
☒ August
☒ September
☒ October
☒ November
☒ December

Days

☒ 1	☐ 8	☐ 14	☐ 20	☐ 26
☐ 2	☐ 9	☐ 15	☐ 21	☐ 27
☐ 3	☐ 10	☐ 16	☐ 22	☐ 28
☐ 4	☐ 11	☐ 17	☐ 23	☐ 29
☐ 5	☐ 12	☐ 18	☐ 24	☐ 30
☐ 6	☐ 13	☐ 19	☐ 25	☐ 31
☐ 7				

Determines the [schedule](#) on which the [report binder execution scheduled task](#) will execute.

Report Binder Execution Settings



Report Binder Execution Settings

The report binder execution settings of this scheduled task.

Report Binder

Technical Overview ▼

Container

▼ CONTOSO MSP

> Customer 1

> Customer 2

> Lost and Found

Report Binder

The [report binder](#) that is to be executed by the [report binder execution scheduled task](#).

Container

The [container](#) or [customer](#) against which the [report binder](#) is to be executed.

Report Parameter Values

The [report parameter values](#) to use for the execution of the [report binder](#).

Assigned Output Targets



Assigned Output Targets

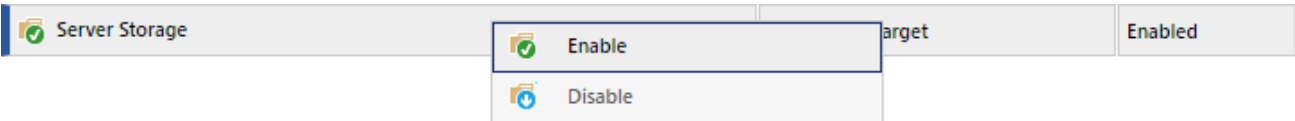
The output targets assigned to this scheduled task.

1 Output Targets Assigned

Display Name	Task Output Target Type	Status
Server Storage	File System Target	Enabled
Usage and Diagnostics Data	SMTP Target	Disabled

Assigns the [task output targets](#) for this [report binder execution scheduled task](#).

Right click the [task output target](#) and select the appropriate option to enable or disable it.



NOTE: At least one [task output target](#) must be assigned.

Task Output Targets

Task Output Targets

The configured task output targets.

 2 Task Output Targets

 Display Name	Creation Date	Task Output Target Type
 Server Storage	09 September 2024 16:17	File System Target
 Usage and Diagnostics Data	09 September 2024 14:12	SMTP Target

Refresh

New Task Output Target

Task output targets are used by [scheduled tasks](#). [Task output targets](#) can also be managed using the [PowerShell API](#).

File System Target

Saves the output of a [scheduled task](#) on the local file system or UNC path.

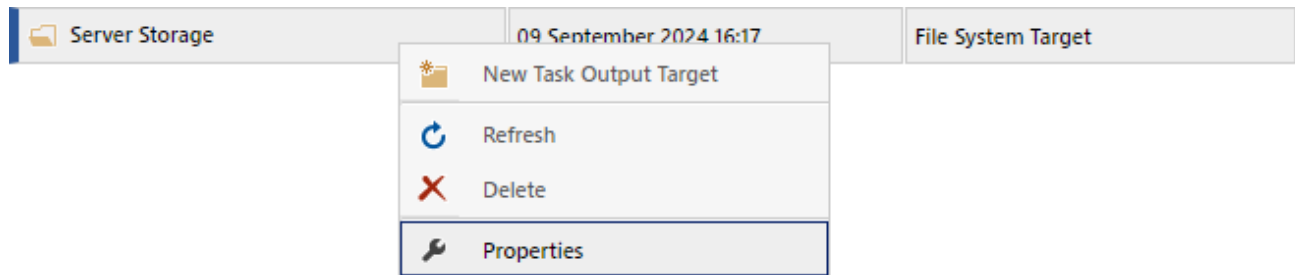
SMTP Target

Sends the output of a [scheduled task](#) to the specified addresses by email using an SMTP mail server.

Right clicking a task output target shows the [context menu](#).

Context Menu

The context menu is displayed when a user right clicks a [task output target](#).



New Task Output Target

Displays the menu to create a new [task output target](#).

Refresh

Reloads the list of [task output targets](#).

Delete

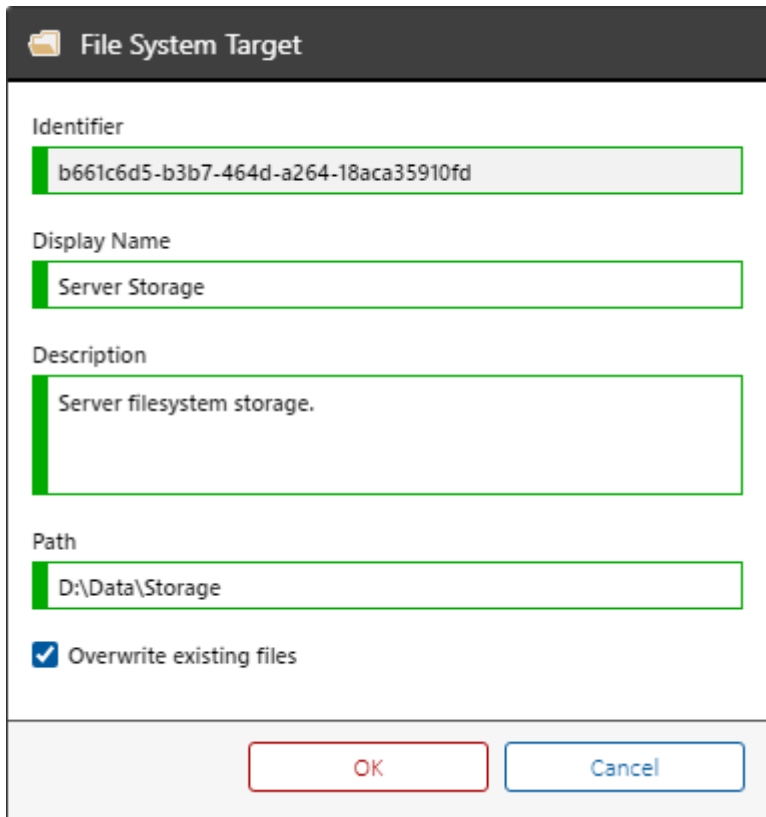
Deletes the currently selected [task output target](#).

Properties

Displays the properties of the currently selected [file system target](#) or [SMTP target](#).

File System Target

The file system target is a [task output target](#) that saves the output of a [scheduled task](#) on the local file system or UNC path.



The image shows a 'File System Target' configuration dialog box. It has a title bar with a folder icon and the text 'File System Target'. Inside, there are five text input fields: 'Identifier' with the value 'b661c6d5-b3b7-464d-a264-18aca35910fd', 'Display Name' with 'Server Storage', 'Description' with 'Server filesystem storage.', and 'Path' with 'D:\Data\Storage'. Below these fields is a checkbox labeled 'Overwrite existing files' which is checked. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Identifier	b661c6d5-b3b7-464d-a264-18aca35910fd
Display Name	Server Storage
Description	Server filesystem storage.
Path	D:\Data\Storage
Overwrite existing files	☒

Display Name

The display name of the [task output target](#).

Identifier

The unique identifier of the [task output target](#) in GUID format.

Description

The description of the [task output target](#).

Path

The local or UNC path of a directory in which to save the output of the [scheduled task](#).
The directory will be created if it does not exist.

Overwrite existing files

Determines whether existing files should be overwritten.

SMTP Target

The SMTP target is a [task output target](#) that sends the output of a [scheduled task](#) to the specified addresses by email using the [configured SMTP mail server](#).

 **SMTP Target**

Identifier

1720f1c2-9971-40b6-9093-ec90be878fc4

Display Name

Usage and Diagnostics Data

Description

Provides a task output target to send usage and diagnostics data to CENTREL Solutions.

To Addresses

support@centrel-solutions.com

CC Addresses

Subject

Usage and Diagnostics Data: Demonstration

Message

Please find attached the current usage and diagnostics data.
Customer: Demonstration

OK

Cancel

Display Name

The display name of the [task output target](#).

Identifier

The unique identifier of the [task output target](#) in [GUID](#) format.

Description

The description of the [task output target](#).

To Addresses

The addresses to which the mail should be sent.

CC Addresses

The addresses to which the mail should be copied.

Subject

The subject of the email.

Message

The message to assign to the email.

Security Settings

Require an SSL Connection when viewing Password List Items

Determines whether a [password list](#) item must be viewed using a HTTPS connection. When enable the Microsoft IIS server must be configured with an SSL certificate, for more information see the Microsoft documentation for your operating system.

Hide items in the organization view when the user doesn't have read permission

This setting determines whether [items](#) should be hidden from users that do not have at least read [permissions](#) when in the organization view.

System Administrators

Determines the users who are [system administrators](#) of the [XIA Configuration Server](#).

Check Names

Checks the names entered in the *System Administrators* field.

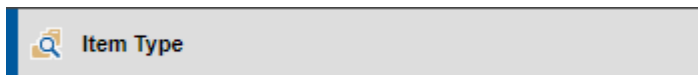
Browse Items by Location

The [server permission](#) that determines which users are permitted to browse by location.



Browse Items by Type

The [server permission](#) that determines which users are permitted to browse by item type.



Client Access

The [server permission](#) that determines the users who are permitted to connect from the [XIA Configuration Client](#) to upload data, use [automatic updates](#) and perform other client related functions. The user account is specified within the [XIA Configuration Client](#) within the [server settings](#) and [server upload](#) sections.

Decrypt Password Lists

The [server permission](#) that determines which users can decrypt an entire [password list](#) and generate a PDF document of all passwords within it. The user must still have read permission to the [password list](#).

Download Client Installer

Determines the users who are permitted to download the [XIA Configuration Client](#) installer either through the web interface or using [automatic updates](#).

Manage ServiceNow Item Synchronization

Determines the users who are permitted to modify ServiceNow item [synchronization settings](#) for which they have also [write permission](#), as well as manually synchronizing items for which they also have [read permission](#) with a [ServiceNow instance](#).

Synchronize Items With ServiceNow

Determines the users who are permitted to manually synchronize items for which they also have [read permission](#) with a [ServiceNow instance](#).

Saving Settings

To save settings click the *Save Security Settings* action point.

Server Permissions

Server permissions determine which users can perform a specific function and are assigned within the [security settings](#) of the [XIA Configuration Server](#).

 Browse Items by Type

☐ All Users ☐ System Administrators ☒ Specified Users

DEMONSTRATION\Managers

Permission Name

The descriptive name of the server permission to be assigned.

All Users

All users are permitted to perform this function.

System Administrators

[System administrators](#) are permitted to perform this function.

Specific Users

Determines the specific users that can perform this action in the format *domain\username*. [System administrators](#) are automatically permitted to perform this function.

Validate Account Names

Validates and formats the account names.

SMTP

SMTP settings on the server can be configured to allow the sending of emails to specified users.

Enable SMTP

Determines whether SMTP should be enabled.

SMTP Server Hostname

The hostname or IP address of the SMTP server.

Port

The TCP port that should be used for communication.

Use SSL/TLS Connection

Determines whether an SSL or TLS connection should be used.

Timeout (Milliseconds)

The timeout for the SMTP connection in milliseconds.

From Email Address

A valid email address that is accepted by the SMTP server

Message Body Encoding

The encoding to use for the message body. The available settings are [UTF-8](#) (default), [Unicode \(UTF-16\)](#), or [ASCII](#) encoding.

Authentication Settings

The [authentication settings](#) for the SMTP connection.

Test Email Address

The email address to send a test email.

Send Test Email

Sends a test email to the address specified in the *test email address* field.

SMTP Authentication Settings

☐ Use default credentials

☒ Use the following credentials

Username

smtp@demostration.com

Domain

Password

.....

Use Default Credentials

Determines whether the connection to the SMTP server should use the [server account](#).

Use Specific Credentials

Determines whether to use the specified credentials.

Username

The username to use for the connection.

Domain

The domain name to use for the connection. If specifying an email address for the username, the domain field can be left blank.

Password

The password to use for the connection.

Usage and Diagnostics Data

Usage and diagnostics data allows information such as [licensing](#) and [item](#) operating system information to be automatically sent to [CENTREL Solutions](#) using the [scheduler](#).

Usage and Diagnostics Data

Provides the ability to send usage and diagnostics information to CENTREL Solutions.

 Usage and Diagnostics Data

Enabled	True
To Addresses	support@centrel-solutions.com
CC Addresses	
Information Level	Default (Licensing and Operating System Information)
Schedule	The schedule is configured to run on day 1 of every month at 22:00:00 starting 09 September 2024 22:00:00. The schedule never expires.

Disable

Enabled

Determines whether usage and diagnostics data is enabled. [SMTP](#) must be enabled and configured before usage and diagnostics data can be used.

To Addresses

The [SMTP](#) addresses to which usage and diagnostics data will be sent.

CC Addresses

The [SMTP](#) addresses to which usage and diagnostics data will be CC'd.

Information Level

The detail level of usage and diagnostics data that is to be sent.

Schedule

The [schedule](#) on which the usage and diagnostics data is to be sent.

Enable

Enables usage and diagnostics data, creating the required [scheduled task](#) and [task output target](#). A default [monthly schedule](#) is assigned to send usage and diagnostics data on the first of each month.

Disable

Disables usage and diagnostics data, removing the [scheduled task](#) and [task output target](#).

Usage and diagnostics data can also be managed using the [PowerShell API](#).

Version Control Settings

Version control automatically creates new, numbered versions of [items](#) when they are modified by a user or updated by the [XIA Configuration Client](#).

Require Version Description

Determines whether users must enter a description when saving changes to an [item](#).

Enable Version Control

Determines whether new, numbered versions of [items](#) should be created when they are modified.

Allow items to be edited or updated without creating a new version

Determines whether additional, new, numbered versions of [items](#) should be created when the [item](#) has been modified multiple times by the same user within the specified number of hours. This does not apply to new versions created by the [XIA Configuration Client](#).

Automatically delete previous versions older than (days)

Determines whether the [scheduler](#) should automatically delete previous versions for [items](#), where the previous versions are older than the specified number of days. By default this option is disabled.

Previous Versions Management

Version control automatically creates new, numbered versions of items when they are modified by a user or updated by the XIA Configuration Client.

This section displays storage information and management controls for previous versions created by version control.

 **Storage Information**

Previous Versions Count	13
Used Space	3.16 MB

Refresh

Previous Versions Count *

The total number of previous versions currently stored in the database for all items.

Used Space *

The total amount of space currently used to store previous versions in the database for all items.

Minimum Age

The minimum age of previous versions of items that are to be deleted from the database.

Item Type

The type of items for which previous versions are to be deleted from the database.

Delete Previous Versions **

Deletes the previous versions from the database that match the criteria.

NOTE: Storage information may take a short period of time to be updated following the deletion of previous versions of items.

Clear Previous Versions

Deletes all previous versions for all items, and resets the version identifier for all items to "1.00".

* Additional information can be found in the reporting section "Internal System Reports" > "Previous Versions Storage".

** Previous versions can be deleted automatically by the scheduler when configured in the version control settings.

Web Proxy Settings

Web proxy settings on the [server](#) can be configured for remote connections.

Use a proxy server

Determines whether a proxy server should be used.

Address

The address of the proxy server - for example "http://proxy.demonstration.int:8080".

Bypass proxy server for local addresses

Determines whether the proxy server should be bypassed for local addresses.

Credentials

The credentials to use when connecting to the proxy server.

Web Service Settings

Enable SDK web services access

Determines whether the web services that form the [web services SDK](#) should be enabled and accessible.

Enable client access web service

Determines whether the web services that form the access point for the [XIA Configuration Client](#) should be enabled and accessible. Disabling this setting will prevent any clients from accessing the [XIA Configuration Server](#).

Enable scheduler access web service

Determines whether the web services that form the access point for the [scheduler service](#) should be enabled and accessible. Disabling this setting will prevent the [scheduler service](#) from operating.

Decommissioned Items

All [items](#) support the ability to be [decommissioned](#).

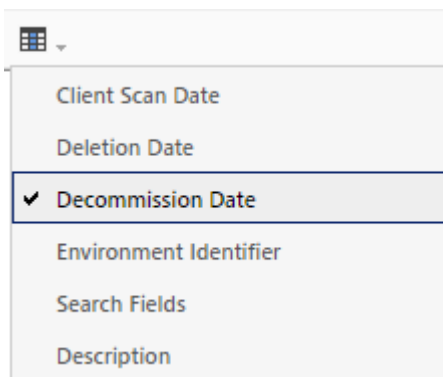
This allows you to maintain information about systems that are no longer in use within your organization.

Please note that [decommissioned](#) items

- Require a valid [license](#).
- Can be [viewed](#).
- Cannot be [edited](#).
- Cannot be [checked in](#) or [checked out](#).
- Are displayed in the treeview if they are [customer](#) or [container items](#), however are marked as "Decommissioned".

>  Customer 1 (Decommissioned)

- Are hidden from the list by default.
- To view decommissioned items, select the show [decommissioned items](#)  toolbar button.
- To view the date on which items were [decommissioned](#) check the decommission date field from the view menu of the toolbar.



Decommissioning Items

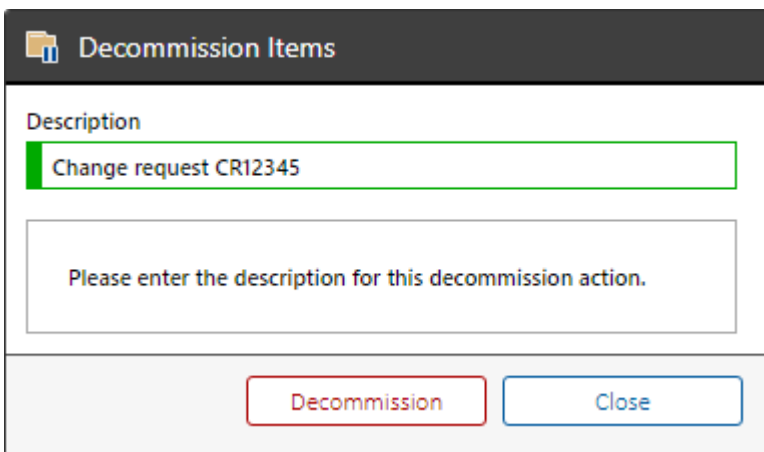
To decommission an [item](#), select the [item](#) or [items](#) within the user interface, right click, and select decommission within the decommissioning context menu.

The user must have the [decommission and recommission security permission](#) to perform this action.

The [item](#) must not be [checked out](#).



When prompted enter a description for the decommissioning action.

A screenshot of a dialog box titled 'Decommission Items'. It has a dark header bar with a folder icon and the title. Below the header is a 'Description' label and a text input field containing 'Change request CR12345'. Below the input field is a larger text area with the placeholder text 'Please enter the description for this decommission action.' At the bottom of the dialog are two buttons: 'Decommission' (outlined in red) and 'Close' (outlined in blue).

NOTE: When you decommission a [customer](#) or [container](#) all [items](#) stored within that [customer](#) or [container](#) are also decommissioned.

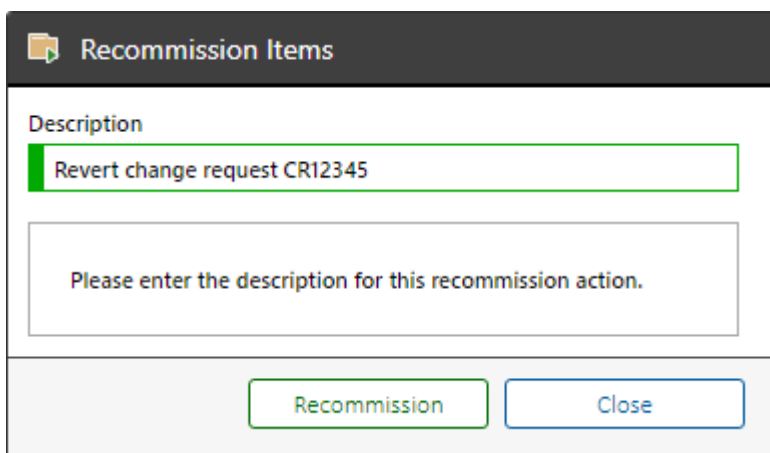
Recommissioning Items

To recommission an [item](#), select the [item](#) or [items](#) within the user interface, right click, and select recommission within the decommissioning context menu.

The user must have the [decommission and recommission security permission](#) to perform this action.



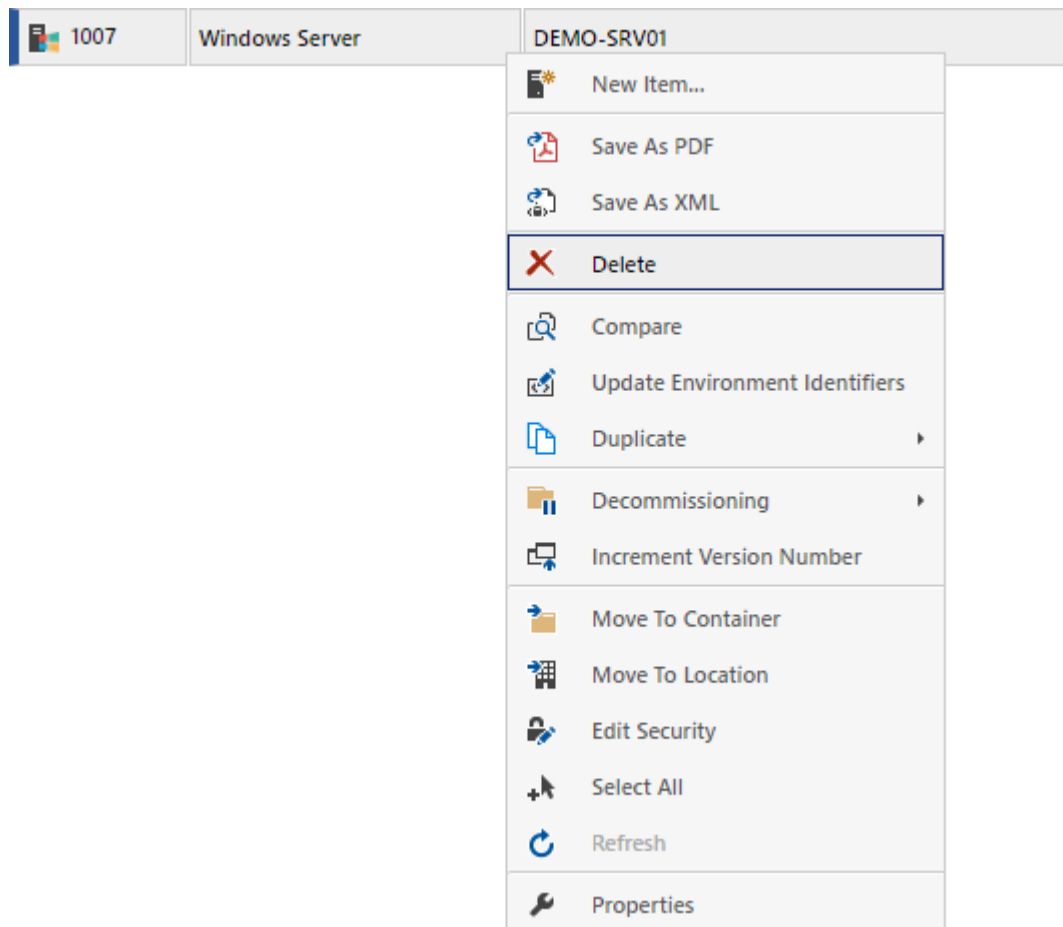
When prompted enter a description for the recommissioning action.

A screenshot of a dialog box titled 'Recommission Items'. The dialog box has a dark header bar with the title. Below the header, there is a 'Description' label and a text input field containing the text 'Revert change request CR12345'. Below the input field, there is a message box that says 'Please enter the description for this recommission action.' At the bottom of the dialog box, there are two buttons: 'Recommission' and 'Close'.

NOTE: When you recommission a [customer](#) or [container](#) all [items](#) stored within that [customer](#) or [container](#) are also recommissioned.

Deleting Items

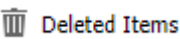
To delete an [item](#) click the item and select delete.



The item is then visible only through the [deleted items](#) section.

Deleted Items

System administrators are able to view deleted items by selecting deleted items in the treeview.



This shows the deleted items list.



Deleted Items

Displays items which have been deleted, and can be restored or permanently deleted.

 1 Item(s)

Item ID	Type	Name	Description
 1007	Windows Server	DEMO-SRV01	Demonstration Windows server.

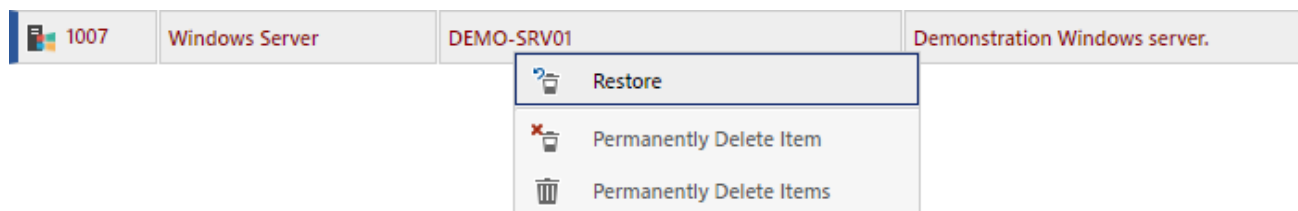
When items have been deleted they

- Do not require a license.
- Cannot be viewed.
- Cannot be edited.

Right clicking an item displays the deleted items context menu.

Deleted Items Context Menu

The context menu is displayed when a user right clicks a [deleted item](#).



Restore

Restores the [deleted item](#). This requires a [license](#).

Permanently Delete Item

Permanently deletes the [item](#). This action cannot be undone.

Permanently Delete Items

Permanently deletes all [deleted items](#). This action cannot be undone.

Diagnostics

The following chapters cover the diagnostics available within [XIA Configuration Server](#).

This includes the [diagnostics logs](#) and the [diagnostics test page](#).

For information about specific issues see the [troubleshooting](#) section.

Diagnostics Logs

[XIA Configuration Server](#) supports the ability to write trace information to a diagnostics log.

Configuration Tools

The diagnostics log can be enabled or disabled using the [diagnostics configuration page](#). This page will display the path on the server where the log file is written.

Web.Config

The diagnostics log can also be enabled or disabled at startup using the Web.Config file. For more information see the [enable diagnostics in the Web.Config file](#) section.

Enable Diagnostics in Web.Config

The diagnostics can be enabled by configuring the [Web.Config](#) file which by default can be found at the following path

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\Web.Config

When diagnostics are disabled the section of the Web.Config file resembles the following

```
<system.diagnostics>
  <trace autoflush="true">
    <listeners>
      <clear />
      <!-- Uncomment the following line to enable trace logging from startup. This is not
required normally as this can be enabled from the web interface once the application is
running. -->
      <!-- <add name="TextTracer" type="CENTREL.XIA.Support.AdvancedTextWriterTraceListener,
CENTREL.XIA.Support" initializeData="~\App_Data\Logs\Trace\Trace.log" /> -->
    </listeners>
  </trace>
</system.diagnostics>
```

To enable diagnostics, the comment characters `<!--` and `-->` must be removed so that the section of Web.Config file resembles the following.

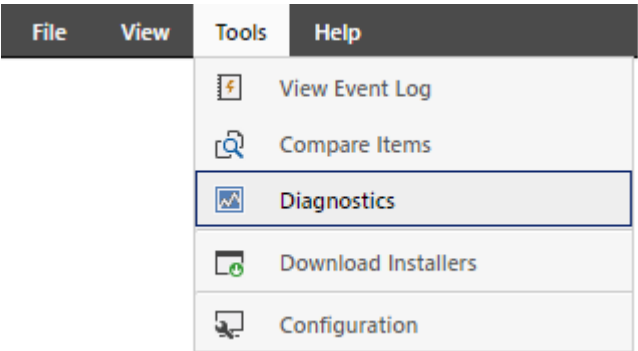
```
<system.diagnostics>
  <trace autoflush="true">
    <listeners>
      <clear />
      <!-- Uncomment the following line to enable trace logging from startup. This is not
required normally as this can be enabled from the web interface once the application is
running. -->
      <add name="TextTracer" type="CENTREL.XIA.Support.AdvancedTextWriterTraceListener,
CENTREL.XIA.Support" initializeData="~\App_Data\Logs\Trace\Trace.log" />
    </listeners>
  </trace>
</system.diagnostics>
```

To avoid unnecessary disk space usage, diagnostics should be disabled when not in use.

Diagnostics Test Page

The diagnostics page provides basic diagnostics and performance tests for [XIA Configuration Server](#).

To access the diagnostics page, select the **Tools > Diagnostics** menu item.



The diagnostics page provides the following information:

Show Information

Provides basic information about the remote sever and browser accessing the system. This can be performed by any user.

Show Configuration

Shows basic server configuration information and the results of repeated load performance testing of the configuration file. This can be performed by [system administrators](#) only.

Test Licensing

Clears cached licensing information and performs a reload of the licensing configuration. This can be performed by [system administrators](#) only.

Event Log

The event log allows [system administrators](#) to view the history of actions performed on the [system](#). The event log can be configured with the [event log settings](#).

FileViewToolsHelp



Event Log

The event log records the events that have occurred on the system.

Filter

2 Event Log Entries

Creation Date	Entry Type	Entry Code	Summary	Username
09 September 2024 16:50:50	Success Audit	2014	Item recommission	DEMONSTRATION\Administrator
09 September 2024 16:50:38	Success Audit	1001	Clear event log	DEMONSTRATION\Administrator

Creation Date

The date and time that the entry was created.

Entry Type

The [entry type](#).

Entry Code

The unique [code](#) for the entry.

Summary

The summary of the [entry code](#).

Username

The name of the user that performed the action.

Double clicking an entry displays the [entry details](#).

Filter

The filter allows the events displayed in the [event log](#) to be filtered by the following criteria

 Filter Events



From Date

09/08/2024

00:00

To Date

10/09/2024

00:00

Entry Type

[All Event Types]

Entry Code

[All Event Codes]

Message

Username

Maximum Result Count

1000

Reset

Apply

Close

From Date

The date and time from which events should be displayed.

To Date

The date and time to which events should be displayed.

Entry Type

The [entry types](#) to display.

Entry Code

The entry code to display.

Message

The message to filter by. This may include wildcards - for example "**deleted**".

Username

The user to filter by. This may include wildcards - for example "**admin**".

Maximum Result Count

The maximum number of entries to return based on the criteria.

Entry Types

The [event log](#) records events of the following types

Information

Informational events.

Failure Audit

An action was performed by the user for which they did not have permission.

Success Audit

An action was successfully performed by the user for which they had permission.

Warning

Warning events.

Error

An action failed to be performed because of an error.

Entry Codes

The following are the entry codes generated by the [event log](#).

- 1000 - User account logon.
- 1001 - Clear event log.
- 1002 - Clear cache.
- 1003 - User interface update.
- 2000 - Item creation.
- 2001 - Item update.
- 2002 - Item move.
- 2003 - Item deletion.
- 2004 - Item check out.
- 2005 - Item check in.
- 2006 - Items check in.
- 2007 - Item security update.
- 2008 - Item restoration.
- 2009 - Item permanent deletion.
- 2010 - Item location move.
- 2011 - Item upload.
- 2012 - Item decommissioning information read.
- 2013 - Item decommission.
- 2014 - Item recommission.
- 2015 - Item PDF export.
- 2016 - Item relationships render.
- 2017 - Item read.
- 2018 - Item rename.
- 2019 - Item duplication.
- 2020 - Item major version number increment.
- 2021 - Item relationships update.
- 4000 - Report creation.
- 4001 - Report update.
- 4002 - Report deletion.
- 4003 - Report folder creation.
- 4004 - Report folder update.
- 4005 - Report folder deletion.
- 4006 - Report binder creation.
- 4007 - Report binder update.
- 4008 - Report binder deletion.
- 5000 - Scheduled tasks directory import.

5001 - Scheduled tasks execution.
5002 - Scheduled task execution.
5003 - Scheduled task creation.
5004 - Scheduled task deletion.
5005 - Scheduled task update.
5006 - Scheduled tasks automated check in.
5006 - Scheduled tasks automated check in.
6000 - Task output target creation.
6001 - Task output target update.
6002 - Task output target deletion.
7000 - Client automatic update execution.
7001 - Client scan task execution.
8000 - Password list password decryption.
8001 - Password list decryption.
8002 - Password list entry creation.
8003 - Password list entry update.
8004 - Password list entry password update.
8005 - Password list entry deletion.
9000 - Hardware definitions read.
9001 - Hardware definition read.
9002 - Hardware definition creation.
9003 - Hardware definition update.
9004 - Hardware definition image update.
9005 - Hardware definition deletion.
9006 - Hardware definitions import.
10001 - Previous version deletion.
10002 - Previous versions deletion.
10003 - Previous versions clear.
11001 - ServiceNow item synchronization.
11002 - ServiceNow item creation.

Entry Details



Success Audit | Event Log Entry



Creation Date

09 September 2024 16:50:50

Entry Code

Item recommission

Machine Name

DEMO-XCS-2022

Username

DEMONSTRATION\Administrator

Message

Recommissioned item with identifier '1008'.
Reason: Change CR12345

Additional Information

Property	Value
 Browser	Chrome 128.0
 Remote Address	localhost

Close

Creation Date

The date and time that the entry was created.

Entry Type

The [entry type](#) is displayed in the title bar.

Entry Code

The summary of the entry code.

Machine Name

The NetBIOS name of the computer running [XIA Configuration Server](#) that logged the event.

Username

The name of the user that performed the action.

Message

The message that was logged.

Browser

The browser name and version, if available.

Remote Address

The address of the remote machine from where the action was performed, if available.

Client Name

The NetBIOS name of the [client](#) machine, if applicable.

Client Identifier

The [unique identifier](#) of the [client](#) machine, if applicable.

Scan Profile Name

The name of the [scan profile](#), if applicable.

Scan Target

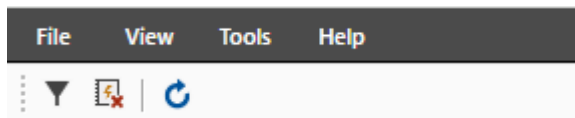
The name of the target being scanned by the [client](#), if applicable.

Scan Task Name

The name of the [scan task](#), if applicable.

Toolbar

The [event log](#) has the following toolbar commands



 Display the event log filter.

 Clears the event log.

 Refreshes the current view.

Files

This section provides a technical reference for the files contained with the [XIA Configuration Server installation](#).

Data Files

The following details the configuration files used by [XIA Configuration Server](#). These files are stored within the **App_Data** folder which can, by default, be found in
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\app_data

To ensure that these files are secured from unauthorized access, the [XIA Configuration Server installation](#) sets the NTFS permissions on the **App_Data** folder to the following:

- Administrators - Full Control
- SYSTEM - Full Control
- [Web Server Account](#) - Full Control

Encryption

Stores the [encryption keys](#).

Images

Stores built in icons such as [custom section](#) icons and operating system images.

Import

Provides a directory into which data from the [XIA Configuration Client](#) can be placed to be [imported](#) into the system.

Installers

Stores the [XIA Configuration Client](#) and other installers.

Licensing

Stores the license.licx license file.

Logs

Stores the [diagnostics trace](#) log files.

Server Settings

The serversettings.xml is stored in the root of the App_Data directory and stores all of the [configuration settings](#) for the system. The file should not be modified directly.

Temp

Provides a [temporary folder](#) used by the system.

Encryption Keys

[XIA Configuration Server](#) uses 2048bit RSA Keys to secure passwords within [password list](#) items and [configuration settings](#). The keys are generated by [XIA Configuration Server](#) setup during installation and are stored in the App_Data\Encryption folder.

The files are named pub.key and priv.key for the public and private keys respectively.

NOTE:

These keys are essential for the security of the XIA Configuration System and should be kept secure. Should you lose these encryption keys you will not be able to decrypted passwords stored in [password lists](#) or access certain [configuration settings](#).

Temp Folder

The temp folder resides within the App_Data folder and provides a location to store sensitive temporary files.

Manual Data Upload

During the [manual data upload](#) process the selected ZIP or XML files are stored and processed within the temp directory "`\ManualFileUpload\GUID`" where GUID is a unique identifier created for each upload. The directory and the files it contained are deleted when the [manual data upload](#) process is complete.

Web.Config

The web.config file is found in the root of the XIA Configuration Server installation directory, by default in the following location

`C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\web.config`

This file is used by ASP.NET to determine the configuration of a web application. Changes to this file should be made only under the direction of CENTREL Solutions as this could affect the normal operation of the application.

NOTE: Changes made to the web.config file are overwritten by upgrades to XIA Configuration Server.

A backup of the latest version of the web.config file is stored in the following location:

`C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\default-web.config`

Generating PDF Documents

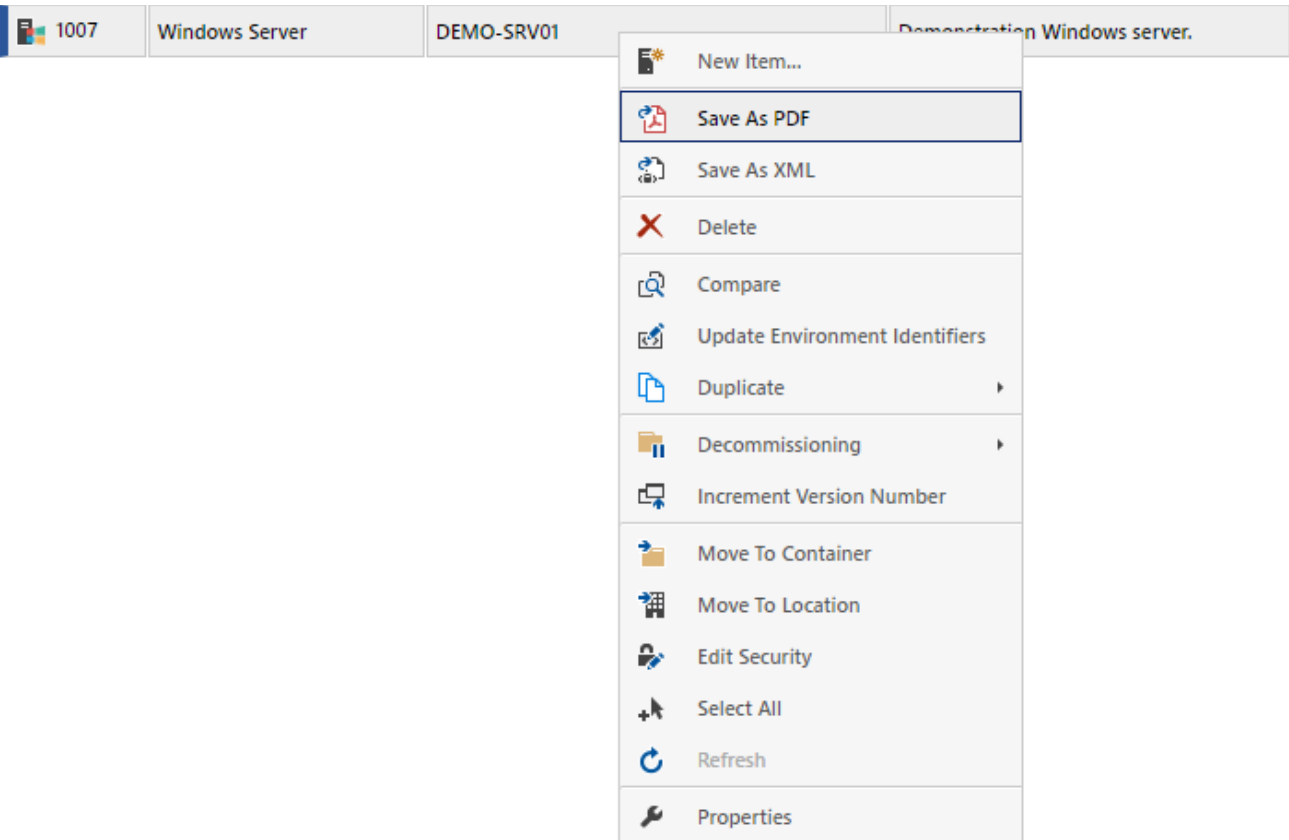
All [items](#) within [XIA Configuration Server](#) can be written to [PDF documents](#) which can be read using [Adobe Acrobat Reader](#), or other compatible products. The system ensures that all items are displayed in a consistent style and format, regardless of the [item type](#). The global style can be configured in the [PDF output settings](#) and [PDF color settings](#) sections within the [configuration settings](#) by a [system administrator](#).



There are several ways to generate a [PDF document](#) of an [item](#).

Main Interface

Right click the selected [items](#) within the main view and click *Save as PDF* to display the [generate documents dialog](#).



Item Page

When an [item](#) is being viewed, click the PDF icon to display the [generate documents dialog](#).



Programmatically

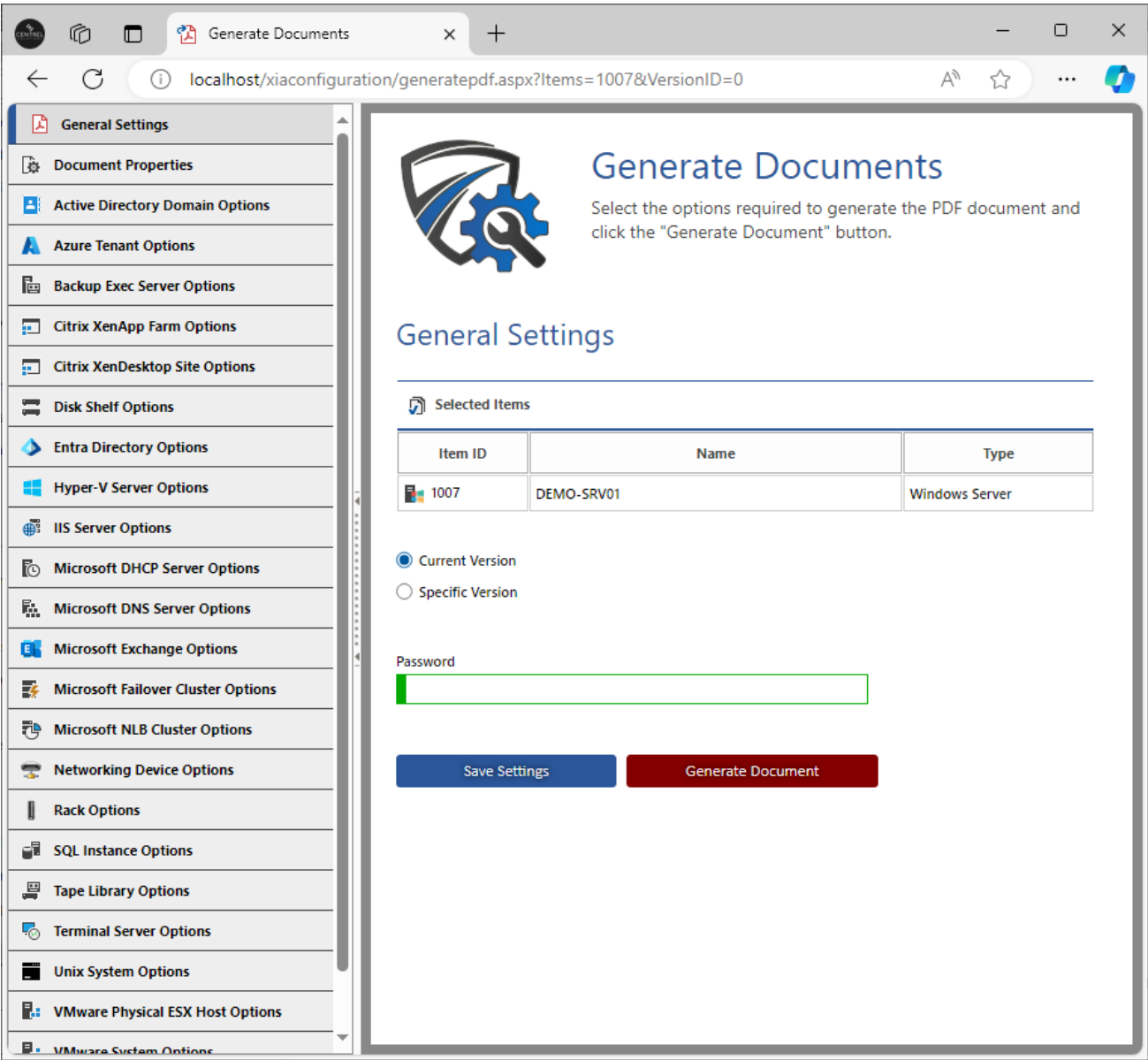
A [PDF document](#) can also be created using the [Web Services SDK](#). For more information see the [Generating a PDF Document](#) example within [Windows PowerShell](#) section.

```
Connecting to XIA Server at http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx
Getting PDF data...

Handles  NPM(K)  PM(K)  WS(K) VM(M)  CPU(s)  Id ProcessName
-----  -
58        6      880    3532   61     0.03   5724 AcroRd32
```

Generate Documents Dialog

The generate documents dialog allows you to generate PDF documents of items within XIA Configuration Server.



Selected Items

The items for which PDF documents are to be generated. If a single item is selected a single PDF document is generated and returned. If multiple items are selected multiple PDF documents are generated and a ZIP file containing the PDF documents is returned.

See the generating PDF documents section for information about selecting items.

Current Version

The current version of the items is used to generate the document.

Specific Version

The [version](#) of the [items](#) specified is used to generate the document. This should be entered in decimal format - for example "1.05".

Password

The password used to protect the [PDF document\(s\)](#) that are generated.

Save Settings

The current settings in the generate documents dialog are saved as the default for all users. This is only available for [system administrators](#).

Generate Document

Generates the [PDF document\(s\)](#) using the current settings.

Document Properties

The screenshot shows a web browser window with the address bar displaying `localhost/xiaconfiguration/generatepdf.aspx?Items=1007&VersionID=0`. The page title is "Generate Documents". On the left, a sidebar lists various configuration options, with "Document Properties" highlighted. The main content area features a gear icon and the heading "Generate Documents". Below this, it says "Select the options required to generate the PDF document and click the 'Generate Document' button." The "Document Properties" section includes a text field for "Author" with the value "CONTOSO MSP" and a checkbox for "Show Thumbnails". The "Optional Sections" section lists several options, all of which are checked: "Assigned Support Provisions", "Assigned Support Provision Details", "Client Information", "Custom Sections", "Relationships", "Relationship Map", "ServiceNow Synchronization Information", and "System Information".

Author

The author to display on the cover of the [PDF document\(s\)](#) that are generated. If this property is left blank the login name of the user that generates the [PDF document\(s\)](#) is used - for example "CONTOSO\tsmith".

Show Thumbnails

Determines whether thumbnail images are displayed in the [PDF document\(s\)](#).

Assigned Support Provisions

Determines whether information about the [support provisions](#) that are assigned to the selected [items](#) should be written to the [PDF document\(s\)](#).

Assigned Support Provision Details

Determines whether detailed information each [support provisions](#) that is assigned to the selected [items](#) should be written to the [PDF document\(s\)](#).

Client Information

Determines whether [client information](#) for the selected [items](#) should be written to the [PDF document\(s\)](#).

Custom Sections

Determines whether the [custom sections](#) for the selected [items](#) should be written to the [PDF document\(s\)](#).

Relationships

Determines whether the [relationships](#) of the selected [items](#) are written to the [PDF document\(s\)](#).

Relationship Map

Determines whether a graphical map of the [relationships](#) of the selected [items](#) are written to the [PDF document\(s\)](#).

System Information

Determines whether the system information such as item identifier, and path for the selected [items](#) should be written to the [PDF document\(s\)](#).

Version History

Determines whether the [version history](#) of the selected [items](#) are written to the [PDF document\(s\)](#).

Globalization

[XIA Configuration Server](#) supports both UK and US English languages. The language that is displayed is dependent on the language requested by the web browser.

For instructions on how to change the language preference please see the documentation for your specific web browser.

NOTE: If a language setting other than English (United States) [en-US] is selected the system will default to English (British) spelling.

Globalization: Date Formats

Date and time values are automatically displayed by [XIA Configuration Server](#) in the format appropriate for the user.

If the date and time format is not correct, please ensure that the correct language is selected within the user's browser.

For more information see the [globalization](#) section.

Item Identifiers

When the [XIA Configuration Client](#) sends data to the [XIA Configuration Server](#), item identifiers are used to locate an existing item to be updated.

These identifiers are as follows:

Primary Identifier

Provides the primary method for an item to be identified, typically the item name. This field is mandatory for all [item types](#).

Secondary Identifier

Provides the secondary method for this item to be identified. This field is optional and differs based on the [item type](#). For more information see the item identifiers section within each [scan task](#).

Tertiary Identifier

Provides the tertiary method for this item to be identified. This field is optional.

Environment Identifier

An environment identifier is used to distinguish between multiple *identical* items where the primary, secondary and tertiary identifiers are all identical. For example, in a resilient environment where it is possible to have multiple virtual servers with the same name and serial number, the environment identifier allows [XIA Configuration Server](#) to distinguish between these otherwise identical systems.

By default this field is blank however can be configured on the [general tab](#) of the [scan profile](#) within the [XIA Configuration Client](#).

Environment identifiers can also be [updated manually](#).

Item Names

Each item within [XIA Configuration Server](#) is given a display name.

If the [type of item](#) is scanned and created by the [XIA Configuration Client](#), it will be named automatically.

Item ID	Type	Name	Description
 1008	Customer	Customer 1	
 1009	Customer	Customer 2	
 1001	Active Directory Domain	demonstration.int	
 1007	Windows Server	DEMO-SRV01	Demonstration Windows server.
 1002	Windows Server	DEMO-SRV02	Demonstration Windows server.
 1003	Microsoft DHCP Server	DEMO-XCS-2022	
 1004	Microsoft DNS Server	DEMO-XCS-2022	
 1005	IIS Server	DEMO-XCS-2022	Demonstration IIS server.
 1006	WINS Service	DEMO-XCS-2022	
 1010	Container	Lost and Found	

If the item is [manually created](#), it can be given any name that conforms to the [item naming](#) rules.

NOTE: Changing the name of an item scanned by the [XIA Configuration Client](#) does not prevent it from being updated because [item identifiers](#) are used for this purpose, however for constancy within the user interface it is recommend to not rename these items.

Item Types

This section provides information about the various item types supported by XIA Configuration Server.

Active Directory Domains

[XIA Configuration Server](#) is capable of documenting Microsoft on-premises [Active Directory](#) domains automatically using the [Active Directory domain](#) scan tasks and [PowerShell remoting](#).

For more information see the [Active Directory domain](#) agent.

Azure Tenants

[Microsoft Azure](#) is a cloud computing platform and infrastructure created by [Microsoft](#).

For more information see the [Azure Tenant](#) scan task information.

For detailed information about the virtual machine guests see the [Scanning Azure Virtual Machines](#) section.

Backup Exec Servers

The [Backup Exec](#) server scan tasks are able to document Backup Exec version 14.0 and above using PowerShell remoting and WMI.

The data located by these tasks include the following information types:

- Global Configuration
- Global Settings
- Storage Devices
- Agent Servers
- Backup Definitions
- Media Sets
- Media
- Media Vaults

For more information see the [Backup Exec Server](#) agent information.

Citrix XenApp Farms (Classic)

[Citrix XenApp](#) provides centrally managed virtual application delivery enabling users to access Windows applications from a range of devices.

[XIA Configuration](#) can document Citrix XenApp 6.0 and 6.5, creating an item for each farm.

The data located by these tasks include the following information types:

- Farm Configuration
- Applications
- Servers
- Policies

For more information see the [Citrix XenApp Farm Agent](#).

NOTE: For newer versions of [Citrix XenApp and XenDesktop](#) (also known as [Citrix Virtual Apps and Desktops](#)) please see [Citrix XenDesktop sites](#).

Citrix XenDesktop Sites

The [Citrix XenDesktop Site](#) scan tasks are able to document [Citrix XenApp and XenDesktop](#) (also known as [Citrix Virtual Apps and Desktops](#)) sites using [PowerShell remoting](#).

The data located by these tasks includes site configuration, applications, delivery groups, and machine catalogs.

Containers

Containers are used to group [items](#), apply [security](#) and operate in a similar way to [customers](#).

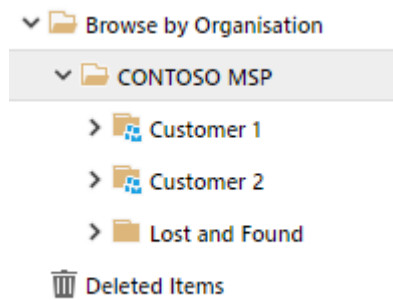
Containers themselves are [items](#) and therefore support the standard [item](#) functionality such as [custom attributes](#).

Root Container

The root container is a special [container](#) in which all other containers and items reside.

Customers

Customer [items](#) operate in a similar way to [containers](#) and can contain items belonging to a customer and can be extended with [custom attributes](#) specific to customers.



Customer [items](#) are typically used by [managed service providers](#) to differentiate their supported customers.

By using customer [items](#) it is also possible to [display the customer name](#) automatically in reports.

Disk Shelves

A disk shelf is a physical enclosure containing multiple disk drives. A disk shelf can be connected to a storage area network (SAN) or directly to a server machine.

XIA Configuration Server supports the [manual creation](#) of disk shelves and can store information relating to:

- Manufacturer
- Model
- Serial Number
- Asset Tag
- Location
- Support and Maintenance

Hardware items can be automatically detected and a representative image displayed by configuring a [hardware definition](#) for the tape libraries in the system.



Entra Directories

XIA Configuration Server is capable of documenting [Microsoft Entra](#) directories (previously known as [Azure Active Directory](#)) using the [Entra Directory scan tasks](#).

For more information see the [Entra Directory](#) agent.

External Links

External links present an easy way to connect to external links via a URL.

External links support the same configuration as all other [items](#) within [XIA Configuration Server](#) including [version control](#) and [security](#).

There is no [license limit](#) to the number of external links that you can create.

To create an external link follow the steps in the [manually creating items](#) section.

NOTE: Unlike other items, when an external link is double clicked, the link itself is launched. To modify the properties of an external link, right click it and select properties.

Generic Network Devices

Within [XIA Configuration Server](#) a generic network device is any SNMP enabled device that does not have a dedicated agent available.

The following information is collected by the agent:

- Name
- Description
- ARP cache
- Network Ports
- IP addresses
- Routing table

Additionally, hardware information can be entered manually.

For more information see the [generic network device agent](#) section.

Hyper-V Servers

XIA Configuration Server is capable of documenting [Hyper-V Servers](#) running on [Windows Server 2012](#) and above and [Microsoft Azure Local](#) (Microsoft Azure Stack HCI) above using [PowerShell remoting](#).

The data located by these [scan tasks](#) include resource pools, server settings, virtual machines, and virtual switches.

For more information see the [Hyper-V Server](#) agent.

IIS Servers

XIA Configuration Server is capable of documenting [Microsoft Internet Information Services \(IIS\) Servers](#) automatically using the [IIS Server scan tasks](#) and [PowerShell remoting](#).

The data located by these tasks include server configuration, application pools, sites, applications and virtual directories as well as ASP.NET, IIS, and management features.

For more information see the [IIS Server](#) agent.

Knowledge Base Articles

[XIA Configuration Server](#) provides the ability to store technical information and troubleshooting guides in the form of knowledge base articles.

Content can be entered into a knowledge base article using the [HTML editor](#) control, and includes the following fields.

Summary

A summary of the information stored in the knowledge base article. This field is required.

Cause

The cause of the issue described in the knowledge base article.

Resolution

The steps required to resolve the issue.

More Information

Additional information relating to the knowledge base article.

Locations

Location [items](#) represent physical locations such as offices or data centers and must be [created manually](#), and can contain [rooms](#).

Microsoft DHCP Servers

XIA Configuration Server is capable of documenting [Microsoft DHCP servers](#) automatically using the [Microsoft DHCP server scan tasks](#) scan tasks and [PowerShell remoting](#).

The data located by these tasks include server settings, superscopes, multicast scopes, options, IPv4 scopes, and IPv6 scopes.

For more information see the [Microsoft DHCP server](#) agent.

Microsoft DNS Servers

XIA Configuration Server is capable of documenting [Microsoft DNS servers](#) automatically using the [Microsoft DNS server scan tasks](#) and [PowerShell remoting](#).

The data located by these tasks include server configuration, conditional forwarders, trust points, and zones.

For more information see the [Microsoft DNS server](#) agent.

Microsoft Exchange Organizations

[XIA Configuration Server](#) is capable of documenting both [Exchange Online](#) and Exchange On-Premises automatically using the [Microsoft Exchange](#) scan tasks.

For more information see the [Microsoft Exchange](#) agent.

Microsoft Failover Clusters

XIA Configuration Server is capable of documenting [Microsoft failover clusters](#) automatically using the [Microsoft failover cluster scan tasks](#) and [PowerShell remoting](#).

The data located by these tasks include cluster configuration, quorum, roles, and storage.

For more information see the [Microsoft failover cluster](#) agent.

Network Storage Devices

A network storage device is used to provide storage, typically to servers, over a Fibre Channel (FC) or Ethernet (iSCSI) network.

For information about automatic detection see the [network storage device](#) section within the [XIA Configuration Client](#) documentation.

Connected Disk Shelves

[Disk shelves](#) can be linked to [network storage devices](#) by using the **connected disk shelf relationship**.

When connected, they are shown under the disk shelves section. As the [disk shelves](#) are stored as a separate item, the user must have read access to both the item and the [disk shelf](#) to view the information.

For more information see the [connecting disk shelves](#) section.

Network Switches

Network Switch tasks are able to document network switches from various manufacturers that support SNMP management. To understand the capabilities of your network equipment please refer to the documentation provided by your switch manufacturer.

The following information can be obtained from all switch manufacturers:

- Switch Name
- Description
- ARP cache
- Ports
- IP addresses
- Base MAC address
- Routing table

Dependant on the capabilities of the switch the following information may also be available:

- Serial number
- Model
- Firmware
- Software Version
- Port speed, duplex and flow control
- Asset Tag
- Product Number / Service Tag
- Stacking information

For more information on scanning network switch using the XIA Configuration Client please see [Network Switch Scan Tasks](#) section.

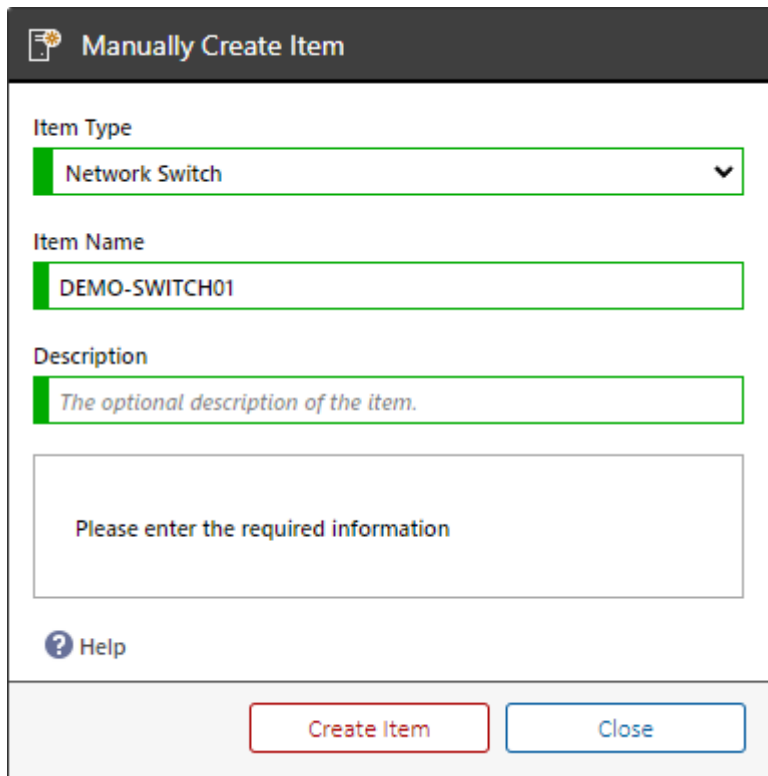
Manually Creating Network Switches

It is recommended that [network switches](#) are created automatically using the [XIA Configuration Client](#).

It is however possible to manually create these devices if the device cannot be scanned - for example if the switch does not support SNMP management.

To [manually create](#) a [network switch](#):

- Select **File > New Item** from the drop down menu.



- Select **Network Switch** from the item type drop down.
(If the *Network Switch* option is not available review the [manual item creation settings](#)).
- Enter an item name and description then press 'Create Item'.
- Double click the newly created [network switch](#).
- Navigate to the **hardware information** section.
- Click the [edit button](#) on the [toolbar](#).
- Enter the required information.
NOTE: only certain information can be entered manually, this includes serial number, manufacturer and model number.
- Click the save button on the [toolbar](#).

Password Lists

XIA Configuration Server allows you to securely store passwords for your systems, applications, and devices.

Password Entries

Provides a list of password entries stored in this password list.

 3 Password Entries

▲	Display Name	Entry Type	Account Name	Expiry Date
	DEMO-SRV01 Administrator	Windows Local User	DEMO-SRV01\Administrator	01 January 2025
	DEMO-SRV02 Administrator	Windows Local User	DEMO-SRV02\Administrator	01 January 2025
	DEMO-SRV03 Administrator	Windows Local User	DEMO-SRV03\Administrator	01 January 2025

New Password Entry

Display Name
The display name of the password entry.

Entry Type
The [password entry type](#).

Account Name
The account name.

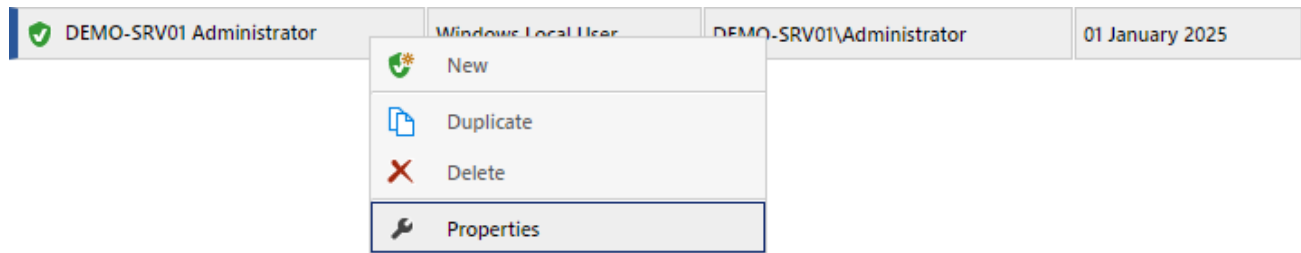
Expiry Date
The optional expiry date of the password entry.

Right clicking a password entry displays the [password entry context menu](#).

Clicking the new password entry button displays the [password entry dialog](#) to create a new password entry.

Context Menu

The context menu is displayed when right clicking a password entry within a [password list](#).



New

When [editing](#), displays the [password entry dialog](#) to create a new password entry.

Duplicate

When [editing](#), displays a duplicate of the currently selected password entry in the [password entry dialog](#).

Delete

When [editing](#), deletes the currently selected password entry.

Properties

Displays the [password entry dialog](#) with the currently selected password entry.

Password Entry Dialog

The password entry dialog displays information about this password entry.

Password Entry Details

Password Entry Details

Display Name	DEMO-SRV01 Administrator
Description	Local administrator account of DEMO-SRV01.
Entry Type	Windows Local User
Expiry Date	01 January 2025

Credentials

Account Name	DEMO-SRV01\Administrator
Password	Reveal Password Copy Password

Close

Reveal Password

Clicking this button decrypts the password and displays it in the user interface.
This action is written as an audit entry in the [event log](#).

Copy Password

Clicking this button decrypts the password and copies it to the clipboard if the browser supports this action.
This action is written as an audit entry in the [event log](#).

When [editing](#) a password entry, the form displays as follows.

Password Entry Details

Password Entry Details

Display Name	DEMO-SRV01 Administrator
Description	Local administrator account of DEMO-SRV01.
Entry Type	Windows Local User
Expiry Date	01/01/2025

Credentials

Account Name	DEMO-SRV01\Administrator
Password	

Apply

Close

Display Name

The display name of the password entry.

Description

The description of the password entry.

Entry Type

The type of password entry. This may include any [custom password list entry types](#).

Expiry Date

The optional expiry date of the password entry. When [editing an item](#), this displays the [date picker](#) control.

Account Name

The optional account name.

Password

The password for the password entry. By default this is only displayed once the user has clicked the reveal password button.

An audit entry is automatically written to the [event log](#).

Password Entry Types

The [password list items](#) can contain password entries of the following built-in types.

Additional custom [entry type definitions](#) can be configured.

Application Login (ApplicationLogin)

A login to a custom application.

Custom

A custom [entry type definition](#).

FTP Account (FtpAccount)

An FTP account login.

Network Device Login (NetworkDeviceLogin)

A login to a network device.

Product Key (ProductKey)

A product key.

SNMP Community String (SnmpCommunity)

An SNMP community string.

SQL Account (SqlAccount)

A SQL login.

Unix Account (UnixAccount)

A login to a Unix or Linux system.

Website Login (WebSiteLogin)

A login to a web site.

Windows Domain User (WindowsDomainUser)

A Windows Active Directory domain user account.

Windows Local User (WindowsLocalUser)

A Windows local (SAM) user account.

Importing Password Entries from CSV

When [editing](#) a [password list](#), it is possible to import information from a comma separated volume (CSV) file.

The following steps should be completed

- [Prepare the CSV file](#)
- [Import the CSV File](#)
- [Map field headings](#)
- [Correct issues, and mport](#)

Preparing the CSV File

To [import password entries from a CSV file](#) you must first prepare the CSV file.

- The file should include the following fields, and can optionally include the field names in the first line of the CSV.

DisplayName

The display name of the password entry.

DefinitionIdentifier

If the [password entry type](#) is set to [custom](#), determines the unique identifier in [GUID format](#) of the [custom entry type definition](#).

Optional when no [password entry type](#) is set to [custom](#).

Description

The description of the password entry. Optional.

EntryType

The [password entry type](#).

Expiry Date

The expiry date of the password entry this should be in a machine readable date format - for example 01-Jan-20. Optional.

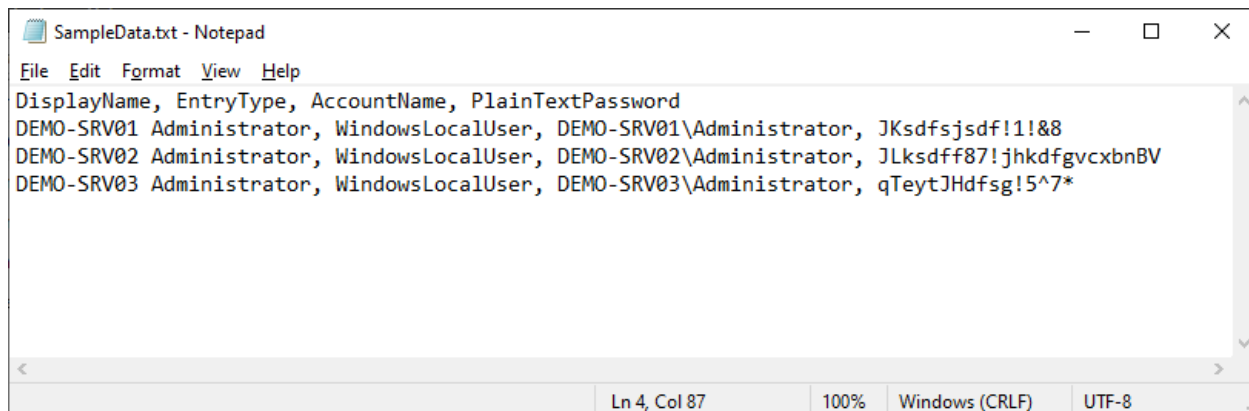
Account Name

The account name. Optional.

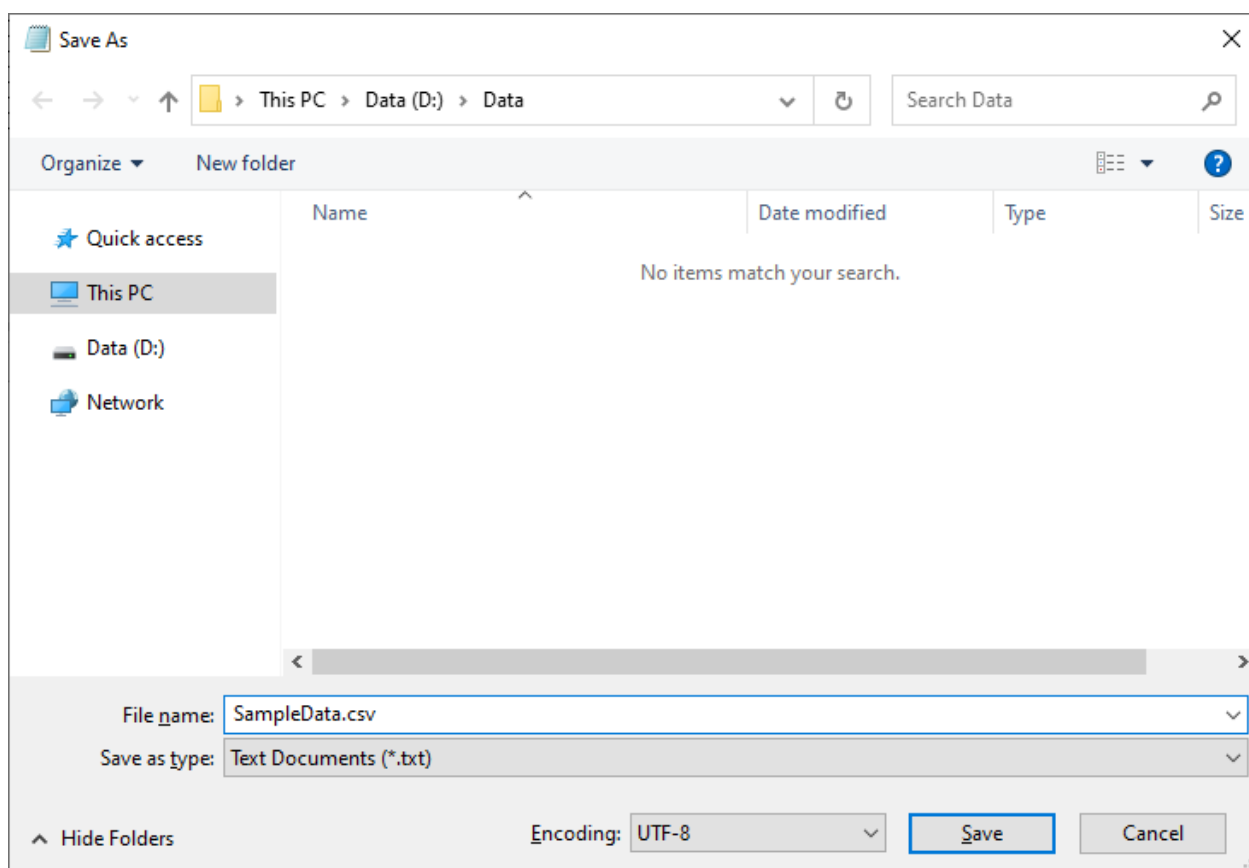
PlainTextPassword

The password to assign to the password entry. This password is automatically encrypted once the file has been imported.

- The file can be created in a simple text editor such as notepad however, in this case the encoding must be handled manually.
- If a value includes a comma then the entire value must be enclosed in double quotation marks.
- If a value includes double quotation marks the entire value must be enclosed in double quotation marks and the double quotation marks replaced with two double quotation marks.



- The file should be saved in UTF-8 encoding.

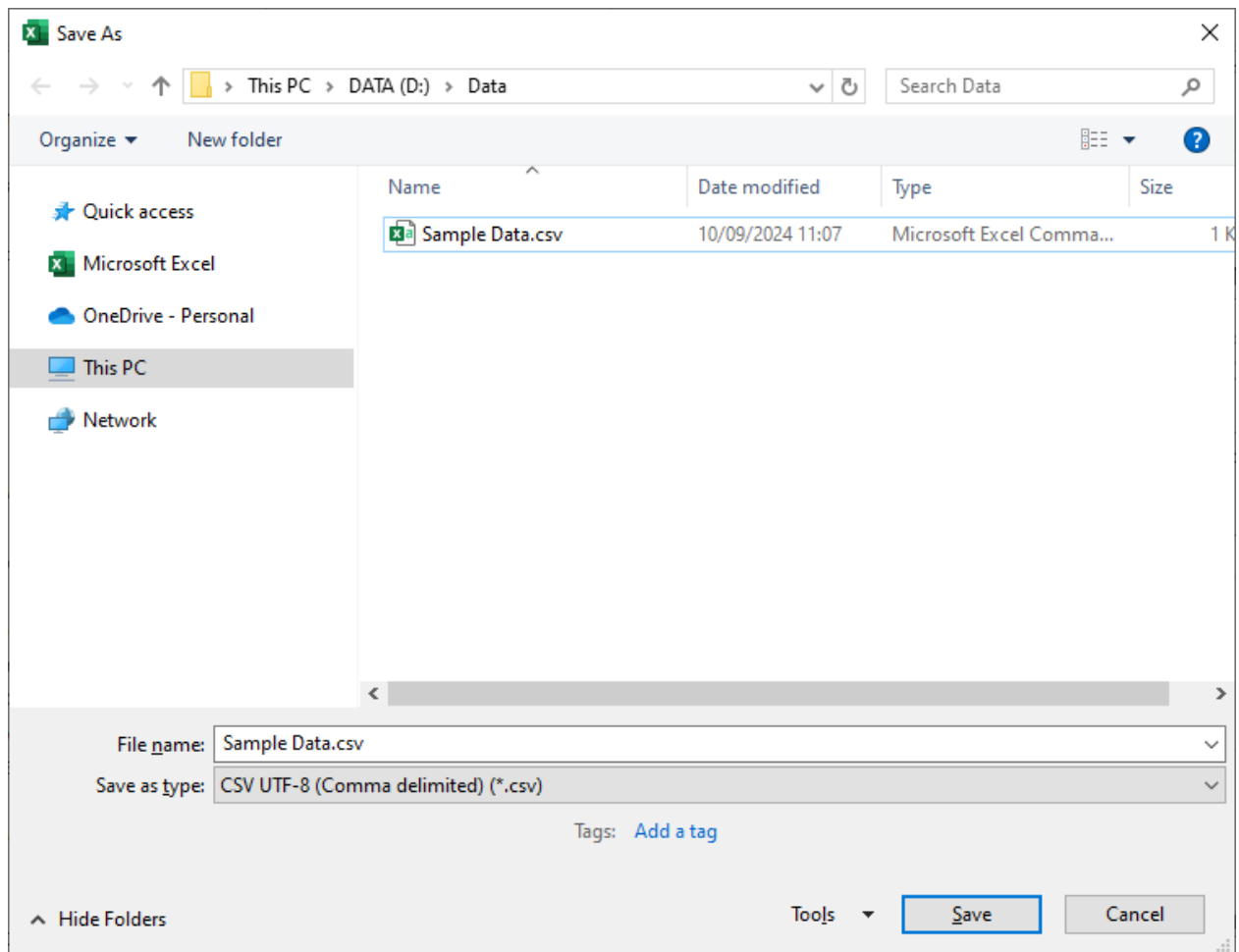


- Alternatively, an application such as [Microsoft Excel](#) can be used. This will automatically encode the values in the CSV file.

The screenshot shows the Microsoft Excel interface with the 'Home' tab selected. The file 'Sample Data.csv' is open and saved to the PC. The data is as follows:

	A	B	C	D
1	DisplayName	EntryType	AccountName	PlainTextPassword
2	DEMO-SRV01 Administrator	WindowsLocalUser	DEMO-SRV01\Administrator	JKsdfsjsdf!1!&8
3	DEMO-SRV02 Administrator	WindowsLocalUser	DEMO-SRV02\Administrator	JLksdff87!jhkdfgvcxbnBV
4	DEMO-SRV03 Administrator	WindowsLocalUser	DEMO-SRV03\Administrator	qTeytJHdfsg!5^7*
5				
6				
7				
8				
9				
10				
11				
12				

- The file should be saved in UTF-8 format.



Importing the CSV File

The [prepared CSV file](#) file can be imported by clicking the browse button, or by dragging file onto the drop area.

Import from CSV

Allows password entries to be imported from a comma separated volume (csv) file.



If the field names were specified in the [CSV file](#) they are automatically mapped to the system, otherwise the field heads must be [manually mapped](#).

Import from CSV

Allows password entries to be imported from a comma separated volume (csv) file.



Browse

3 Password Entries

DisplayName	EntryType	AccountName	PlainTextPassword
DEMO-SRV01 Administrator	WindowsLocalUser	DEMO-SRV01\Administrator	JKsdfsjsdf!!&8
DEMO-SRV02 Administrator	WindowsLocalUser	DEMO-SRV02\Administrator	JLksdff87!jhkdfgvcxbnBV
DEMO-SRV03 Administrator	WindowsLocalUser	DEMO-SRV03\Administrator	qTeytJHdfsg!5^7*

Import Passwords

Mapping Field Headings

If the field names were specified in the [CSV file](#) they are automatically mapped to the system, otherwise the field heads must be [manually mapped](#).

Right clicking on a column header will display the available fields to assign to the data.

For more information on the field names see the [preparing the CSV file](#) page.

3 Password Entries

▲	{Not Assigned}	{Not Assigned}	{Not Assigned}	{Not Assigned}
✖	DEMO-SRV01 Administrator	Unassign	D-SRV01\Administrator	JKsdfsjsdf!1!&8
✖	DEMO-SRV02 Administrator	AccountName	D-SRV02\Administrator	JLksdff87!jhkdfigvcxnbBV
✖	DEMO-SRV03 Administrator	DefinitionIdentifier	D-SRV03\Administrator	qTeytJHdfsg!5^7*
		Description		
		DisplayName		
		EntryType		
		ExpiryDate		
		PlainTextPassword		

Correcting Issues and Import

If the import displays any errors more information can be found by hovering the row, and viewing the tooltip text.

If the issue is caused by fields not being assigned, see the [mapping field headings](#) section.

3 Password Entries

Display Name	Entry Type	Account Name	(Not Assigned)
DEMO-SRV01 Administrator	WindowsLocalUser	DEMO-SRV01\Administrator	JKsdfsjsdf!1!&8
DEMO-SRV02 Administrator	WindowsLocalUser	DEMO-SRV02\	bnBV
DEMO-SRV03 Administrator	WindowsLocalUser	DEMO-SRV03\Administrator	qTeytJHdfsg!5^7*

If information is missing from the source data, please correct the information when [preparing the CSV file](#) and [import the CSV file](#) again.

3 Password Entries

Display Name	Entry Type	Account Name	PlainTextPassword
	WindowsLocalUser	DEMO-SRV01\Administrator	JKsdfsjsdf!1!&8
DEMO-SRV02 Administrator		ministrator	JLksdff87!jhkdfgvcbnBV
DEMO-SRV03 Administrator	WindowsLocalUser	DEMO-SRV03\Administrator	qTeytJHdfsg!5^7*

Once complete click the import passwords button.

3 Password Entries

Display Name	Entry Type	Account Name	PlainTextPassword
DEMO-SRV01 Administrator	WindowsLocalUser	DEMO-SRV01\Administrator	JKsdfsjsdf!1!&8
DEMO-SRV02 Administrator	WindowsLocalUser	DEMO-SRV02\Administrator	JLksdff87!jhkdfgvcbnBV
DEMO-SRV03 Administrator	WindowsLocalUser	DEMO-SRV03\Administrator	qTeytJHdfsg!5^7*

Import Passwords

Racks

Rack [items](#) represent physical racks, typically within a data center [room](#) and must be [created manually](#). Racks can contain physical [items](#) such as [Windows machines](#) and [Unix systems](#).

Resources

A resource allows any external file to be stored within [XIA Configuration Server](#) - for example an image, [Microsoft Word](#) document or [Visio](#) diagram.

The subject and title of [Microsoft Office XML format](#) documents such as docx and xlsx will be extracted automatically, the same is true of JPEG images.

To create a new resource see [manually creating items](#).

Resource Storage

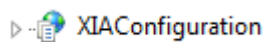
The actual resource files (for example a PNG image) are stored within the [XIA Configuration Server](#) database in the Resources table (ResourceData field) in binary format. This makes image resources accessible to the [reporting system](#).

Storing RDP Files

It is possible to store [Remote Desktop Connection](#) (.rdp) files within resources, double clicking these files allows you to easily connect to a remote Windows Server or PC from within the [XIA Configuration Server](#) interface.

However, by default, [Microsoft IIS](#) does not serve [RDP](#) files, and the following changes must be made to the [IIS](#) configuration:

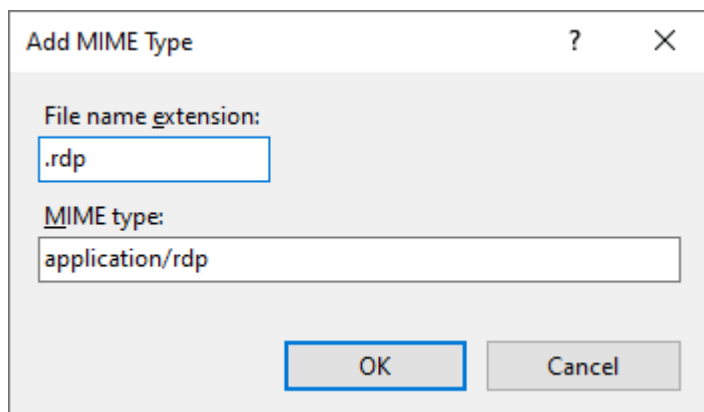
- Open the IIS Manager Application
- Browse to the [XIA Configuration Server](#) virtual directory



- In the right-hand pane double click MIME Types



- Right click within the right-hand pane and click "Add..."
- Enter ".rdp" for the file name extension
- Enter "application/rdp" for the MIME type



- Click OK

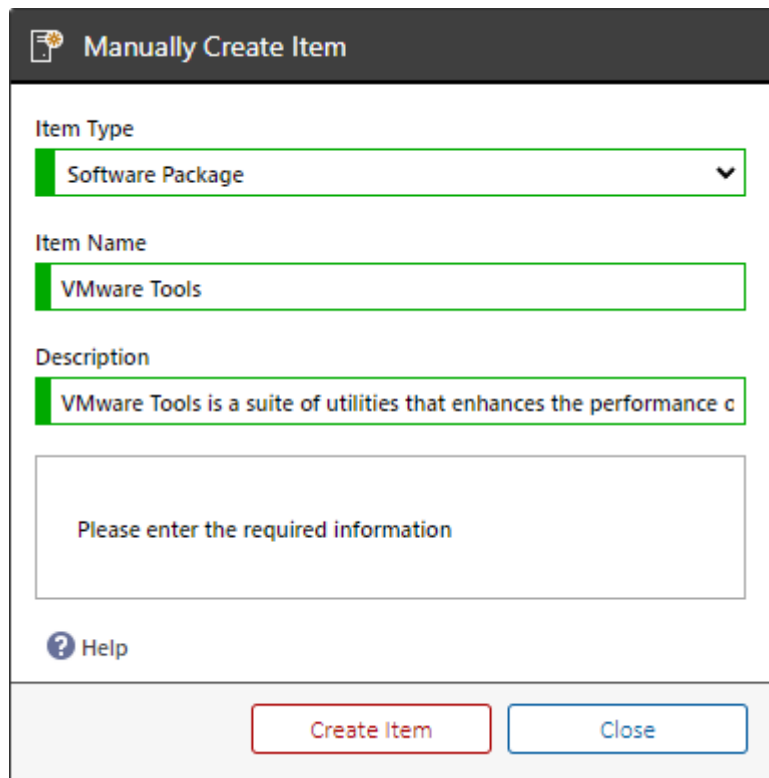
Rooms

Room [items](#) represent physical rooms within a [location](#) and must be [created manually](#). Rooms can contain racks as well as other physical [items](#).

Software Packages

Software package items allow the collation of information about a given software package including manufacturer, web site and version. Software packages can be extended with [custom attributes](#) and [lifecycle](#) information.

All software package items must be [created manually](#) using the [new item dialog](#).



The image shows a 'Manually Create Item' dialog box. It has a dark header with a gear icon and the title 'Manually Create Item'. Below the header, there are three input fields: 'Item Type' with a dropdown menu showing 'Software Package', 'Item Name' with the text 'VMware Tools', and 'Description' with the text 'VMware Tools is a suite of utilities that enhances the performance c'. Below these fields is a large empty text area with the placeholder text 'Please enter the required information'. At the bottom left is a 'Help' button with a question mark icon. At the bottom right are two buttons: 'Create Item' and 'Close'.

Manually Create Item

Item Type
Software Package

Item Name
VMware Tools

Description
VMware Tools is a suite of utilities that enhances the performance c

Please enter the required information

? Help

Create Item Close

Information can be entered in the editor for

- Manufacturer
- Web Site
- Version



VMware Tools

A software package within XIA Configuration stores information related to a software package including information about the manufacturer and version details.



Software Package Details

Manufacturer	VMware, Inc
Web Site	https://www.vmware.com/
Version	12.4.0

Software Lifecycle

The software lifecycle allows you to determine where the software package is installed on machines within the environment by assigning search parameters and the manufacturer assigned support and extended support end dates.

NOTE: Software lifecycle requires the use of SQL Server 2008 or above.



VMware Tools | Software Package | 40928

Software Lifecycle

Software lifecycle settings allows a software package to have a manufacturer support end date assigned and allows the system to locate machines on which this package has been deployed.

 Software Lifecycle

Enabled	☐ Software lifecycle enabled
---------	---

Enabled

Determines whether software lifecycle settings are enabled for this software package.



Software Lifecycle

Software lifecycle settings allows a software package to have a manufacturer support end date assigned and allows the system to locate machines on which this package has been deployed.

Software Lifecycle

Enabled	☒ Software lifecycle enabled
---------	--

Match Settings

Publisher Search Strings	VMware VMware, Inc
Product Search Strings	tools-windows
Version Search Strings	12.4.0

Support Periods

Release Date	10/09/2024
Support Expiry	10/09/2025
Extended Support Expiry	10/09/2026

Publishers

A list of values to match for the name of the publisher. These can include any characters valid in a T-SQL [LIKE](#) statement.

Products

A list of values to match for the name of the product. These can include any characters valid in a T-SQL [LIKE](#) statement.

Version

A list of values to match for the version of the product. These can include any characters valid in a T-SQL [LIKE](#) statement.

Release Date

The date on which the product was released by the manufacturer (optional).

Support Expiry

The date on which the manufacturer's primary support expires for the product.

Extended Support Expiry

The date on which the manufacturer's extended support expires for the product (optional).

Software Lifecycle Reports

There are several reports related to [software lifecycle](#) which can be found in the Unmanaged Item Reports > Software Lifecycle Reports [report folder](#).

Software Packages

Provides details of software packages including whether [software lifecycle](#) is enabled for this [software package](#).

Software Lifecycle Summary

Provides summary information about the [software lifecycle](#) settings for each [software package](#). If [software lifecycle](#) is not enabled for a [software package](#), it is not displayed in this report.



Software Lifecycle Summary

Provides summary information about the software lifecycle configuration in the environment.

Modify ReportExecute Report

1 Results

Name	Support Status	Release Date	Support Expiry Date	Extended Support Expiry Date
 VMware Tools	Supported	10 September 2024	10 September 2025	10 September 2026

Software Package Deployment

Displays information about the systems on which the [software package](#) has been deployed. Unlike the **Software Package Component Deployment**, only one result is returned per software package detected on each system.

 **Software Package Deployment**

Report against the container or customer

>  Demonstration Inc

Software Package

VMware Tools

▼

Report output format

Screen

▼

Execute

Close

Software Package Component Deployment

The package component deployment report provides additional information including exactly what product was detected as being part of the [software package](#). Multiple results can be returned for an individual item if several applications match the [software package](#).

SQL Instances

The [SQL Instance agent](#) is able to document both [Microsoft SQL Server](#) on-premises installations and Microsoft Azure SQL databases.

Support Provision

Support provision [items](#) can represent support contracts such as technical support agreements, warranties, or hardware maintenance agreements.

Support Hours

The hours on which support is available.

Reference Number

The reference number for the support provision.

Self Service Web Site

The URL of a self service web site for the support provision.

Email Address

The email address for the support provision.

Telephone Number

The telephone number for the support provision.

Start Date

The date on which the support provision became active.

Expiry Date

The date on which the support provision expires.

Tape Libraries

A tape library is a storage device which contains:

- One or more tape drives
- A number of slots to hold tape cartridges
- A method to identify tape cartridges
- An automated method for loading tapes

The system supports the [manual creation](#) of tape libraries and can store information relating to:

- Manufacturer
- Model
- Serial Number
- Asset Tag
- Location
- Support and Maintenance

Hardware items can be automatically detected and a representative image displayed by configuring a [hardware definition](#) for the tape libraries in the system.



Terminal Servers

A Terminal Server (known as Remote Desktop Session Host (RD Session Host) server on Windows 2008 and above) is a server that hosts Windows-based programs or the full Windows desktop for Remote Desktop Services clients.

Users can connect to a Terminal Server to run programs, to save files, and to use network resources on that server.

Users can access an RD Session Host server by using Remote Desktop Connection or on Windows 2008 and above by using RemoteApp.

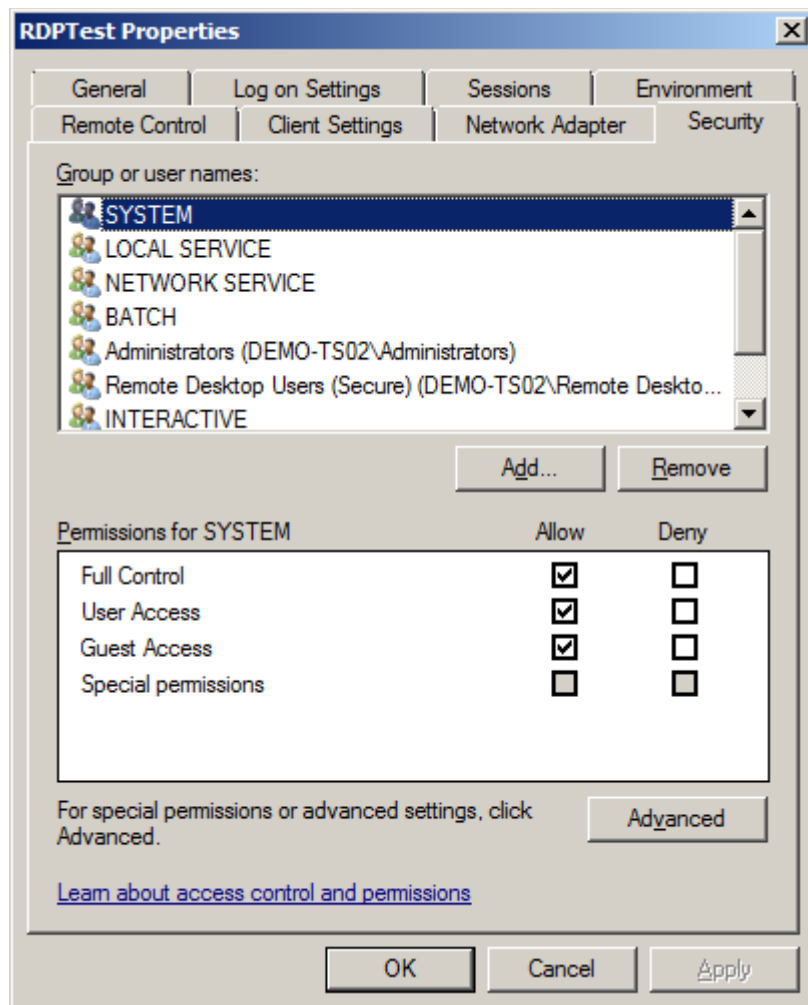
XIA Configuration can automatically detect the following information:

- Connection (Session) Broker settings
- Connection settings including
- General Settings
- Logon Settings
- Client Settings
- Environment Settings
- Session Settings
- Remote Control Settings
- Client Settings
- Network Settings
- Security Permissions (Windows 2008 and above)
- RemoteApp application configuration

Terminal Security Permissions

Each terminal can be configured with individual security permissions in the form of an ACL (Access Control List) on the Security tab of the terminal's property window.

For this information to be collected by the XIA Configuration Client, **both** the machine running the XIA Configuration Client and the Remote Desktop Session Host server must be running Windows Server 2008 or above.



Unix Systems

XIA Configuration Server is able to document Unix and Linux based systems including:

- Interface Configuration
- Platform type
- Installed packages
- Routing table
- Running processes
- Logical drives
- Processors

For more information about data collection using the [XIA Configuration Client](#) see the [Unix System](#) scan tasks.

Connected Disk Shelves

[Disk shelves](#) can be linked to [Unix Systems](#) by using the **Connected Disk Shelf** [relationship](#).

When connected, they are shown within the hardware section, under the disk shelves section. As the [disk shelves](#) are stored as a separate item, the user must have read access to both the item and the [disk shelf](#) to view the information.

For more information see the [Connecting Disk Shelves](#) section.

Connected Tape Libraries

[Tape libraries](#) can be linked to [Unix Systems](#) by using the **Connected Tape Library** [relationship](#).

When connected, they are shown within the hardware section, under the tape libraries section. As the [tape libraries](#) are stored as a separate item, the user must have read access to both the item and the [tape library](#) to view the information.

For more information see the [Connecting Tape Libraries](#) section.

Manually Entered IP Addresses

When a Unix system has been [manually created](#), it is possible to assign IP addresses within the networking section.

- Select the **Networking** section.
- Click the edit button on the [toolbar](#) to [edit](#) the item.
- Enter the IP addresses with or without the subnet mask, one per line.
- To include a subnet mask, enter the address and subnet mask separated by a space or forward slash - for example "192.168.10.10 / 255.255.255.0"

 **DEMO-UNIX01 | Unix System | 42014**

Network Configuration

Provides basic networking information for a manually created machine. For additional information please scan the Unix system using the XIA Configuration Client.

 **Networking Information**

IP Addresses	192.168.1.1 10.200.20.5
---------------------	----------------------------

VMware Physical ESX Hosts

Typically [VMware systems](#) are managed by a [vCenter server](#) which provides centralized management and all host systems appear within this management context.

In addition to [VMware Systems](#) items [XIA Configuration Server](#) creates individual [items](#) for the VMware physical ESX hosts.

Whilst these items contain minimal they provide the ability to assign the following to each individual host

- A physical location
- Support and Maintenance information
- Custom attributes

Whilst [XIA Configuration Server](#) will automatically create VMware physical ESX host [items](#) when data is imported by the [VMware system agent](#) these items may also be [created manually](#).

[XIA Configuration Server](#) will automatically link the VMware physical ESX hosts with their parent [VMware system](#) in the [relationship map](#).

VMware Systems

The [VMware system agent](#) is able to document both VMware standalone hosts and entire vCenter systems.

The data located by these tasks includes the following information types:

- Clusters
- Datastores
- Datastore Clusters
- Distributed Switches
- Host Systems
- Virtual Machines
- Resource Pools
- vCenter Configuration
- Security Permissions

Windows Machines

[XIA Configuration Server](#) is capable of documenting both Windows servers and Windows desktop operating systems.

.NET Framework Detection

The [XIA Configuration Client](#) is able to automatically detect the following versions of the [.NET Framework](#) installed on a [Windows machine](#):

- Microsoft .NET Framework 1.0
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 2.0 Service Pack 1
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.0
- Microsoft .NET Framework 3.0 Service Pack 1
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 4.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6
- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.7
- Microsoft .NET Framework 4.7.1
- Microsoft .NET Framework 4.7.2
- Microsoft .NET Framework 4.8

Connected Disk Shelves

[Disk shelves](#) can be linked to [Windows machines](#) by using the **connected disk shelf relationship**.

When connected, they are shown within the hardware section, under the disk shelves section. As the [disk shelves](#) are stored as a separate item, the user must have read access to both the item and the [disk shelf](#) to view the information.

For more information see the [connecting disk shelves](#) section.

Connected Tape Libraries

[Tape libraries](#) can be linked to [Windows machines](#) by using the **connected tape library relationship**.

When connected, they are shown within the hardware section, under the tape libraries section. As the [tape libraries](#) are stored as a separate item, the user must have read access to both the item and the [tape library](#) to view the information.

For more information see the [connecting tape libraries](#) section.

Connected Network Storage Devices

[Network Storage Devices](#) can be linked to [Windows machines](#) by using the **connected network storage device relationship**.

Unlike [tape libraries](#) and [disk shelves](#), network storage devices are only shown within the [relationships](#) section and not within the main user interface of the Windows machine. This is because network storage devices are typically configured and controlled completely independently of the Windows machine.

For more information see the [connecting network storage devices](#) section.

Manually Entered IP Addresses

When a [Windows machine](#) has been [manually created](#), it is possible to assign IP addresses within the networking section.

- Select the **networking** section.
- Click the edit button on the [toolbar](#) to [edit](#) the item.
- Enter the IP addresses with or without the subnet mask, one per line.
- To include a subnet mask, enter the address and subnet mask separated by a space or forward slash - for example "192.168.10.10 / 255.255.255.0"

 **DEMO-SRV01 | Windows Server | 42015**

Networking Information

Provides basic networking information for a manually created machine. For additional information please scan the machine using the XIA Configuration Client.

 **Networking Information**

IP Addresses	192.168.1.1 10.200.25.4
---------------------	----------------------------

Security

Security Audit Information

When scanning Windows machines, it is possible to document the security configuration of these machines including:

- Local users and groups
- Local account policy
- Local password policy
- Local security options
- User rights assignment

SSL Certificates

The XIA Configuration Client is able to obtain SSL certificate information from the following **Machine** certificate stores:

- Personal
- Intermediate Certification Authorities
- Trusted Root Certificate Authorities
- Trusted 3rd Party Root Certificate Authorities
- Trusted Publishers
- Trusted People

NOTE: Information that is displayed in the user interface for the "Trusted Root Certificate Authorities" also includes the certificates stored in the "Trusted 3rd Party Root Certificate Authorities" store. This behaviour mirrors that of the certificates Microsoft Management Console.

Local Account and Password Policies

The following [account and password policies](#) are read for [Windows machines](#).

Account Lockout Policy

 Policy	Policy Setting	Configuration Source
 Account lockout duration	Not Applicable	Configured Locally
 Account lockout threshold	0 invalid login attempt(s)	Default Domain Policy
 Reset account lockout counter after	Not Applicable	Configured Locally

Password Policy

 Policy	Policy Setting	Configuration Source
 Enforce password history	24 passwords remembered	Default Domain Policy
 Maximum password age	42 days	Default Domain Policy
 Minimum password age	1 days	Default Domain Policy
 Minimum password length	7	Default Domain Policy
 Password must meet complexity requirements	True	Default Domain Policy
 Relax minimum password length limits	Not Configured	Not Defined
 Store passwords using reversible encryption	False	Default Domain Policy

- Account Lockout Duration
- Account Lockout Threshold
- Reset Account Lockout
- Enforce Password History
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password must meet complexity requirements *
- Store passwords using reversible encryption *

* Due to the nature of these settings, these properties can only be read if the setting is configured using a domain [Group Policy](#).

Security Options

The following [security options](#) are read for [Windows machines](#).

NOTE: Not all security options apply to all [Windows](#) versions.

- Accounts: Administrator account status
- Accounts: Block Microsoft accounts
- Accounts: Guest account status
- Accounts: Limit local account use of blank passwords to console logon only
- Accounts: Rename administrator account
- Accounts: Rename guest account
- App Runtime: Allow Microsoft accounts to be optional
- Audit Process Creation: Include command line in process creation events
- Audit: Audit the access of global system objects
- Audit: Audit the use of Backup and Restore privilege
- Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.
- Audit: Shut down system immediately if unable to log security audits
- AutoPlay Policies: Disallow Autoplay for non-volume devices
- AutoPlay Policies: Set the default behavior for AutoRun
- AutoPlay Policies: Turn off Autoplay
- Biometrics: Configure enhanced anti-spoofing
- Cloud Content: Turn off Microsoft consumer experiences
- Connect: Require pin for pairing
- Credential User Interface: Do not display the password reveal button
- Credential User Interface: Enumerate administrator accounts on elevation
- Credentials Delegation: Encryption Oracle Remediation
- Credentials Delegation: Remote host allows delegation of non-exportable credentials
- Data Collection and Preview Builds: Allow Diagnostics Data
- Data Collection and Preview Builds: Allow Telemetry
- Data Collection and Preview Builds: Do not show feedback notifications
- Data Collection and Preview Builds: Toggle user control over Insider builds
- DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
- DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
- Devices: Allow undock without having to log on
- Devices: Allowed to format and eject removable media
- Devices: Prevent users from installing printer drivers
- Devices: Restrict CD-ROM access to locally logged-on user only
- Devices: Restrict floppy access to locally logged-on user only
- DNS Client: Turn off multicast name resolution
- Domain controller: Allow server operators to schedule tasks
- Domain controller: LDAP server signing requirements
- Domain controller: Refuse machine account password changes
- Domain member: Digitally encrypt or sign secure channel data (always)
- Domain member: Digitally encrypt secure channel data (when possible)
- Domain member: Digitally sign secure channel data (when possible)
- Domain member: Disable machine account password changes

- Domain member: Maximum machine account password age
- Domain member: Require strong (Windows 2000 or later) session key
- Early Launch Antimalware: Boot-Start Driver Initialization Policy
- EMET: Default Action and Mitigation Settings: Anti Detours
- EMET: Default Action and Mitigation Settings: Banned Functions
- EMET: Default Action and Mitigation Settings: Deep Hooks
- EMET: Default Action and Mitigation Settings: Exploit Action
- EMET: System ASLR
- EMET: System DEP
- EMET: System SEHOP
- Event Log: Application: Control Event Log behavior when the log file reaches its maximum size
- Event Log: Application: Specify the maximum log file size (KB)
- Event Log: Security: Control Event Log behavior when the log file reaches its maximum size
- Event Log: Security: Specify the maximum log file size (KB)
- Event Log: Setup: Control Event Log behavior when the log file reaches its maximum size
- Event Log: Setup: Specify the maximum log file size (KB)
- Event Log: System: Control Event Log behavior when the log file reaches its maximum size
- Event Log: System: Specify the maximum log file size (KB)
- File Explorer: Configure Windows SmartScreen
- File Explorer: Enable Microsoft Defender SmartScreen
- File Explorer: Microsoft Defender SmartScreen Level
- File Explorer: Turn off Data Execution Prevention for Explorer
- File Explorer: Turn off heap termination on corruption
- File Explorer: Turn off shell protocol protected mode
- Group Policy: Continue experiences on this device
- Group Policy: Registry policy processing: Do not apply during periodic background processing
- Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed
- Group Policy: Turn off background refresh of Group Policy
- Interactive logon: Display user information when the session is locked
- Interactive logon: Don't display last signed-in
- Interactive logon: Do not require CTRL+ALT+DEL
- Interactive logon: Machine account lockout threshold
- Interactive logon: Machine inactivity limit
- Interactive logon: Message text for users attempting to log on
- Interactive logon: Message title for users attempting to log on
- Interactive logon: Number of previous logons to cache (in case domain controller is not available)
- Interactive logon: Prompt user to change password before expiration
- Interactive logon: Require Domain Controller authentication to unlock workstation
- Interactive logon: Require smart card
- Interactive logon: Smart card removal behavior
- Internet Communication settings: Turn off access to the Store
- Internet Communication Settings: Turn off downloading of print drivers over HTTP
- Internet Communication Settings: Turn off handwriting personalization data sharing
- Internet Communication Settings: Turn off handwriting recognition error reporting
- Internet Communication Settings: Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com

- Internet Communication Settings: Turn off Internet download for Web publishing and online ordering wizards
- Internet Communication Settings: Turn off printing over HTTP
- Internet Communication Settings: Turn off Registration if URL connection is referring to Microsoft.com
- Internet Communication Settings: Turn off Search Companion content file updates
- Internet Communication Settings: Turn off the "Order Prints" picture task
- Internet Communication Settings: Turn off the "Publish to Web" task for files and folders
- Internet Communication Settings: Turn off the Windows Messenger Customer Experience Improvement Program
- Internet Communication Settings: Turn off Windows Customer Experience Improvement Program
- Internet Communication Settings: Turn off Windows Error Reporting
- Internet Explorer: Disable Internet Explorer as a stand alone browser
- Internet Explorer: Prevent downloading of enclosures
- IPv6: Disabled Components
- Lanman Workstation: Enable insecure guest logons
- Locale Services: Disallow copying of user input methods to the system account for sign-in
- Location and Sensors: Turn off location
- Logon: Block user from showing account details on sign-in
- Logon: Do not display network selection UI
- Logon: Do not enumerate connected users on domain-joined computers
- Logon: Enumerate local users on domain-joined computers
- Logon: Turn off app notifications on the lock screen
- Logon: Turn off picture password sign-in
- Logon: Turn on convenience PIN sign-in
- Microsoft Accounts: Block all consumer Microsoft account user authentication
- Microsoft Defender Antivirus: Configure detection for potentially unwanted applications
- Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS
- Microsoft Defender Antivirus: Configure Watson events
- Microsoft Defender Antivirus: Join Microsoft MAPS
- Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites
- Microsoft Defender Antivirus: Scan removable drives
- Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus
- Microsoft Defender Antivirus: Turn on behavior monitoring
- Microsoft Defender Antivirus: Turn on e-mail scanning
- Microsoft network client: Digitally sign communications (always)
- Microsoft network client: Digitally sign communications (if server agrees)
- Microsoft network client: Enable SMB version 1 protocol
- Microsoft network client: Send unencrypted password to connect to third-party SMB servers
- Microsoft network server: Amount of idle time required before suspending a session
- Microsoft network server: Attempt S4U2Self to obtain claim information
- Microsoft network server: Digitally sign communications (always)
- Microsoft network server: Digitally sign communications (if client agrees)
- Microsoft network server: Disconnect clients when logon hours expire
- Microsoft network server: Enable SMB version 1 protocol
- Microsoft network server: Enable SMB version 2 protocol
- Microsoft network server: Server SPN target name validation level

- Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider
- MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
- MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)
- MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)
- MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
- MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds
- MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers
- MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)
- MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
- MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)
- MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted
- MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted
- MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning
- Network access: Allow anonymous SID/Name translation
- Network access: Do not allow anonymous enumeration of SAM accounts
- Network access: Do not allow anonymous enumeration of SAM accounts and shares
- Network access: Do not allow storage of passwords and credentials for network authentication
- Network access: Let Everyone permissions apply to anonymous users
- Network access: Named pipes that can be accessed anonymously
- Network access: Remotely accessible registry paths
- Network access: Remotely accessible registry paths and subpaths
- Network access: Restrict anonymous access to Named Pipes and Shares
- Network access: Restrict clients allowed to make remote calls to SAM
- Network access: Shares that can be accessed anonymously
- Network access: Sharing and security model for local accounts
- Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network
- Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network
- Network Connections: Require domain users to elevate when setting a network's location
- Network Provider: Hardened UNC Paths
- Network security: Allow Local System to use computer identity for NTLM
- Network security: Allow LocalSystem NULL session fallback
- Network security: Allow PKU2U authentication requests to this computer to use online identities.
- Network security: Configure encryption types allowed for Kerberos
- Network security: Do not store LAN Manager hash value on next password change
- Network security: Force logoff when logon hours expire
- Network security: LAN Manager authentication level
- Network security: LDAP client signing requirements
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
- Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
- Network security: Restrict NTLM: Add server exceptions in this domain
- Network security: Restrict NTLM: Audit Incoming NTLM Traffic
- Network security: Restrict NTLM: Audit NTLM authentication in this domain
- Network security: Restrict NTLM: Incoming NTLM traffic
- Network security: Restrict NTLM: NTLM authentication in this domain
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
- Not Defined
- OneDrive: Prevent the usage of OneDrive for file storage
- Personalization: Prevent enabling lock screen camera
- Personalization: Prevent enabling lock screen slide show
- Recovery console: Allow automatic administrative logon
- Recovery console: Allow floppy copy and access to all drives and all folders
- Regional and Language Options: Allow users to enable online speech recognition services
- Remote Assistance: Allow Offer Remote Assistance
- Remote Assistance: Allow Solicited Remote Assistance
- Remote Desktop Connection Client: Do not allow passwords to be saved
- Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication
- Remote Procedure Call: Restrict Unauthenticated RPC clients
- Search: Allow Cloud Search
- Search: Allow indexing of encrypted files
- Secure Channel: Enable SSL 3.0 (Client)
- Secure Channel: Enable SSL 3.0 (Server)
- Secure Channel: Enable TLS 1.0 (Client)
- Secure Channel: Enable TLS 1.0 (Server)
- Secure Channel: Enable TLS 1.1 (Client)
- Secure Channel: Enable TLS 1.1 (Server)
- Secure Channel: Enable TLS 1.2 (Client)
- Secure Channel: Enable TLS 1.2 (Server)
- Security Providers: WDigest Authentication
- Shutdown: Allow system to be shut down without having to log on
- Shutdown: Clear virtual memory pagefile
- Sleep Settings: Require a password when a computer wakes (on battery)
- Sleep Settings: Require a password when a computer wakes (plugged in)
- System Cryptography: Force strong key protection for user keys stored on the computer
- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
- System objects: Require case insensitivity for non-Windows subsystems
- System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
- System settings: Optional subsystems
- System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
- TCP/IP: NetBT NodeType
- Turn off Microsoft Peer-to-Peer Networking Services
- Turn on Mapper I/O (LLTDIO) driver
- Turn on Responder (RSPNDR) driver
- User Account Control: Admin Approval Mode for the built-in Administrator account
- User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop

- User Account Control: Apply UAC restrictions to local accounts on network logons
- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
- User Account Control: Behavior of the elevation prompt for standard users
- User Account Control: Detect application installations and prompt for elevation
- User Account Control: Only elevate executables that are signed and validated
- User Account Control: Only elevate UIAccess applications that are installed in secure locations
- User Account Control: Run all administrators in Admin approval mode
- User Account Control: Switch to the secure desktop when prompting for elevation
- User Account Control: Virtualize file and registry write failures to per-user locations
- Windows Connect Now: Configuration of wireless settings using Windows Connect Now
- Windows Connect Now: Prohibit access of the Windows Connect Now wizards
- Windows Connection Manager: Minimize the number of simultaneous connections to the Internet or a Windows Domain
- Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network
- Windows Ink Workspace: Allow Windows Ink Workspace
- Windows Installer: Allow user control over installs
- Windows Installer: Always install with elevated privileges
- Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts
- Windows Logon Options: Sign-in and lock last interactive user automatically after a restart
- Windows Performance PerfTrack: Enable/Disable PerfTrack
- Windows PowerShell: Turn on PowerShell Script Block Logging
- Windows PowerShell: Turn on PowerShell Transcription
- Windows Security: App and browser protection: Prevent users from modifying settings
- Windows Update: Defer feature updates
- Windows Update: Manage preview builds
- Windows Update: Manage preview builds (Branch Readiness Level)

The following settings are only read by the [XIA Configuration Client](#) when they are configured in a group policy object. If they are configured locally they are not displayed, though information about the Administrator and Guest account can also be viewed in the "Local User Accounts" section.

- Accounts: Administrator account status
- Accounts: Guest account status
- Accounts: Rename administrator account
- Accounts: Rename guest account
- Network access: Allow anonymous SID/Name translation
- Network security: Force logoff when logon hours expire

Server Functions

[XIA Configuration Server](#) displays information about the functions being performed by a [Windows Server](#), this information can be used to identify servers which are running multiple functions.

 Server Functions			
 Name	Enabled	Active	Instance Identifier
 DHCP Server	True	True	
 DNS Server	True	True	
 Domain Controller	True	True	
 IIS FTP Server	True	True	
 IIS Web Server	True	True	
 SQL Instance	True	True	

The information includes

- Function name such as "DHCP Server".
- Enabled, which determines whether the role is enabled - for example whether the Windows service is enabled or disabled.
- Active, determines whether the function is active - for example whether the Windows service was running at the time of the scan.
- Instance identifier which determines the name of the instance for functions that can be installed multiple times such as SQL Server instances.

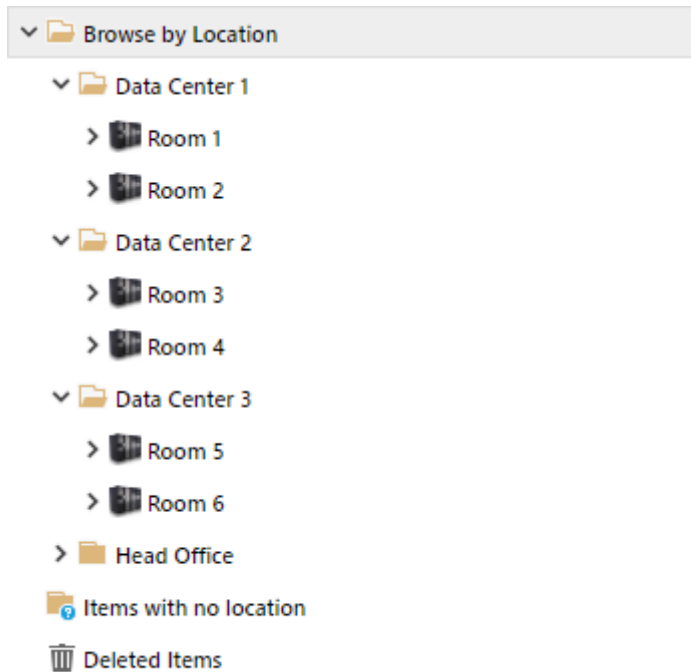
The [XIA Configuration Client](#) is able to automatically detect the following functions

- Citrix XenApp Farm Server
- Citrix XenDesktop Site Server
- DHCP Server
- DNS Server
- Domain Controller
- Hyper-V Server
- IIS FTP Server

- IIS Web Server
- Remote Desktop Session Host
- SQL Instance
- vCenter Server
- WINS Server

Location Hierarchy

The system allows users to browse and [search](#) for [items](#) based on their physical location.

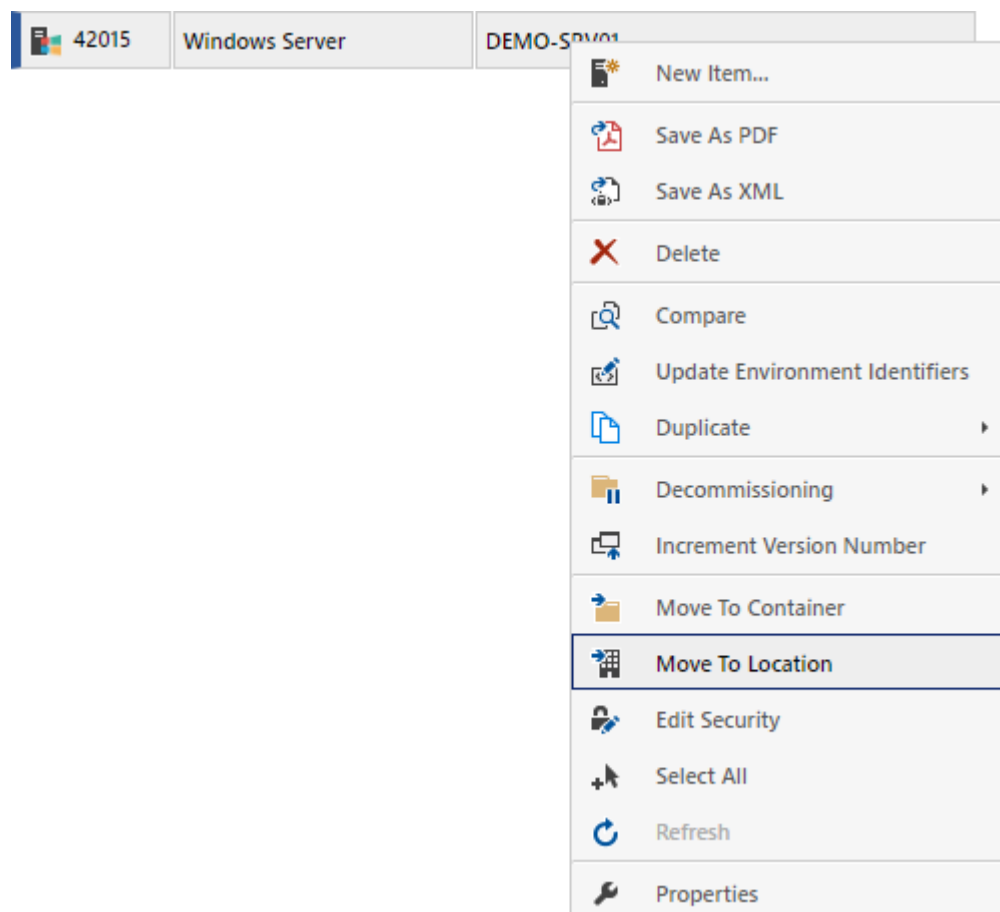


- [Locations](#) are the top level of the hierarchy and can contain only [rooms](#).
- [Rooms](#) can contain [racks](#) as well as other physical [items](#).
- [Racks](#) can contain physical [items](#) that are not [rooms](#), or [locations](#).

Assigning Locations

Rooms and racks can be dragged and dropped in the [location hierarchy](#).

Other [items](#) can be assigned to a [location](#), [room](#), or [rack](#) by selecting right clicking the [item](#), and selecting move to location.



The location can be selected from the move to location dialog.

 Move To Location

Location

▼

Locations

▼

Data Center 1

>

 Room 1

>

 Room 2

>

Data Center 2

>

Data Center 3

>

Head Office

Refresh

Please select the destination location

Move

Close

Page 343 of 1553

XIA Configuration Administrator's Guide

Main Page

The main [XIA Configuration Server](#) user interface provides the following:

- The ability to [search](#) the CMDB.
- Information about the logged-on user and version numbers of the product.
- A welcome title and description which can be configured by an administrator in the [general settings](#).

The following four main views are available

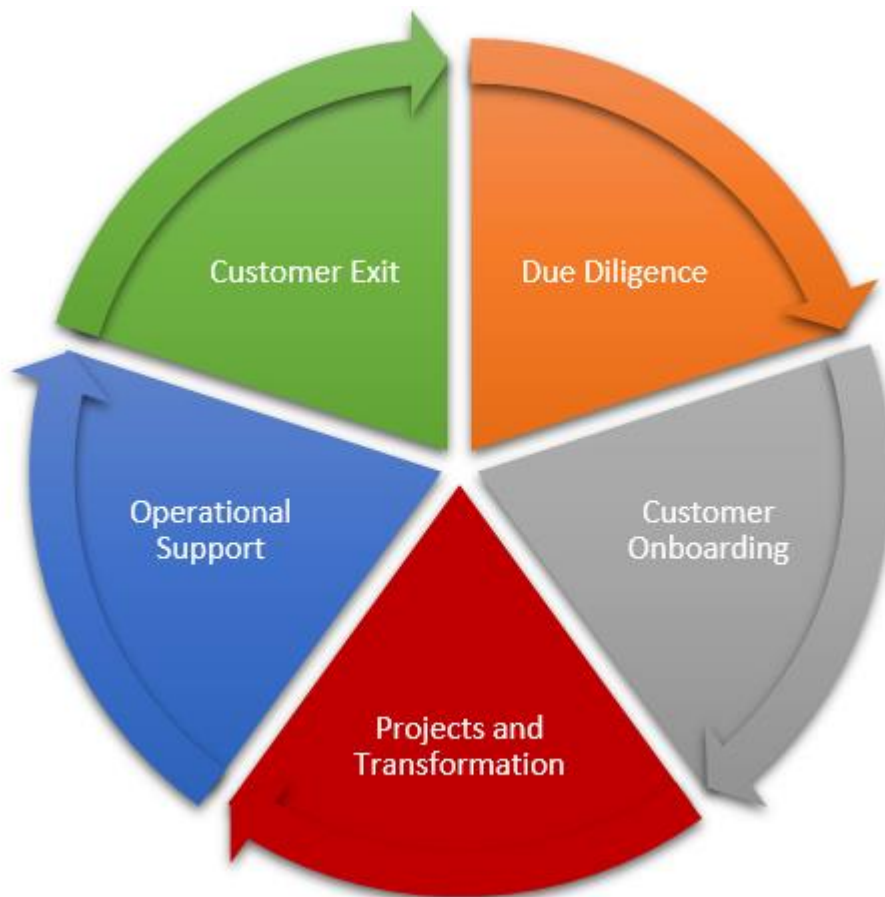
- The [organizational hierarchy](#) of [customers](#) and [containers](#).
- The [items](#) grouped by [item type](#).
- The [location hierarchy](#).
- The [reporting](#) section containing [reports](#) and [report binders](#).

The permissions to view the [items by type](#) and the [location hierarchy](#) can be configured by a [system administrator](#) in the [security settings](#).

Managed Service Providers

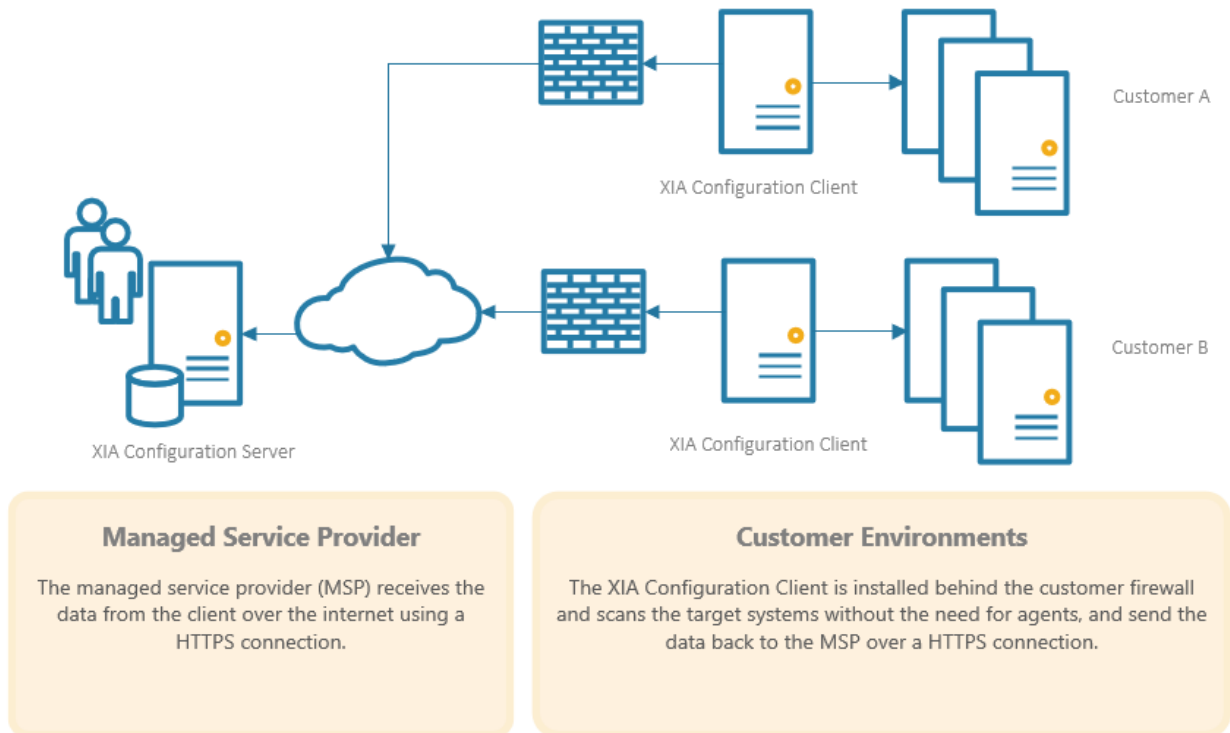
[XIA Configuration](#) helps Managed Support Providers (MSPs), from large to small, to automate technical documentation at each phase of the MSP lifecycle.

For more information see the [MSP Configuration Guidelines](#).



MSP Deployment Topology

XIA Configuration Server provides flexible options for deployment. For [Managed Support Providers \(MSPs\)](#) the following architecture is recommended



- [XIA Configuration Server](#) is [installed](#) on a dedicated virtual or physical machine within the [Managed Support Providers \(MSPs\)](#) network.
- The [SQL database](#) can be installed on the same machine as [XIA Configuration Server](#), or a different machine can be used.
- An SSL certificate is installed on the [XIA Configuration Server](#) machine.
- A copy of the [XIA Configuration Client](#) is [installed](#) on a machine in each [customer](#) environment with [service account credentials](#) appropriate for each [customer](#).
- Data is sent from each [XIA Configuration Client](#) to the [XIA Configuration Server](#) over a HTTPS connection configured in the [server settings](#).

MSP Configuration Guidelines

The following provides guidelines to be used by [Managed Service Providers](#) supporting multiple customers.

Server Installation

- Follow the [XIA Configuration Server installation guide](#) to install the product on the [Managed Service Provider's](#) network.
- Ensure that the server is accessible to the customers, either over the Internet or via dedicated network links.
- Configure the Internet Information Services (IIS) server to [use SSL encryption](#).
- [Rename](#) the root container to the [Managed Service Provider's](#) company name.
- Ensure that the "Hide containers from users that do not have permissions to view them" setting is configured in [Security Settings](#).

Default Item Creation

- [Create](#) a container called "New Items" and configure the [security](#) so that only Administrators can view these items.
- Configure the [item creation rules](#) so that new items are, by default, created in this container.

Customer Preparation

Perform the following steps for each customer. To assist with this process, see the [creating managed customers](#) PowerShell example.

- Create a new user account for each customer in Active Directory.
- [Grant access](#) to the new user account.
- [Create](#) a [customer](#) container for each customer.
- Configure the [security](#) for the newly created customer so that the customer has [write](#) access to this container.
- Configure the [item creation rules](#) so that new items for this customer are created in this [customer](#) container.
- [Install](#) the [XIA Configuration Client](#) on a supported machine in each customer environment using credentials suitable for that environment.

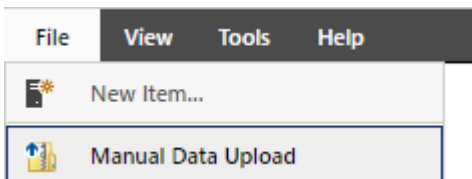
- Configure the [Server Upload](#) tab of the [Scan Profile](#)
 - a) Configure the URL to use the [Managed Service Provider's](#) externally facing [XIA Configuration Server](#) address - for example
`https://documentation.yourmsp.com/XIAConfiguration`
 - b) Configure the credentials to use the credentials created for the customer on the [Managed Service Provider's](#) network.
- Perform a scan of the customer's network and ensure the new items are created correctly in the appropriate [customer](#) container.

Manual Data Upload

Typically, [items](#) that are scanned by the [XIA Configuration Client](#) are automatically [uploaded](#) to [XIA Configuration Server](#) directly over a HTTP or HTTPS connection.

In the event that a direct connection between the [XIA Configuration Client](#) and the [XIA Configuration Server](#) is not possible, or desirable, the [XIA Configuration Client](#) can [output](#) the scan data to XML or Zip files which can be [imported using the scheduler service](#), or manually imported using the web interface.

Select *Manual Data Upload* from the file menu.



This displays the *Manual Data Upload* user interface.

Manual Data Upload - Work - Microsoft Edge

localhost/XIAConfiguration/ManualDataUpload.aspx



Manual Data Upload

Provides the ability to manually upload data created by the XIA Configuration Client as either a Zip or XML file format.

XML or Zip File



Browse

Zip Password

 Item Creation Method

☐ Use item creation rules

☒ Create new items in the following container

> CONTOSO MSP

Back

Start

Data File

Click the Browse button to locate the XML or Zip file that was [output](#) by the [XIA Configuration Client](#), alternatively you can drop the file onto the drop zone.



Zip Password

Optionally enter the Zip password if configured for the [output](#) by the [XIA Configuration Client](#). The control is disabled if the file uploaded is an XML file or is a Zip file that is not encrypted.

Use item creation rules

Any new [items](#) will be created in the [container](#) or [customer](#) that is determined by the [item creation rules](#). This setting has no effect when updating existing [items](#).

Create new items in the following container

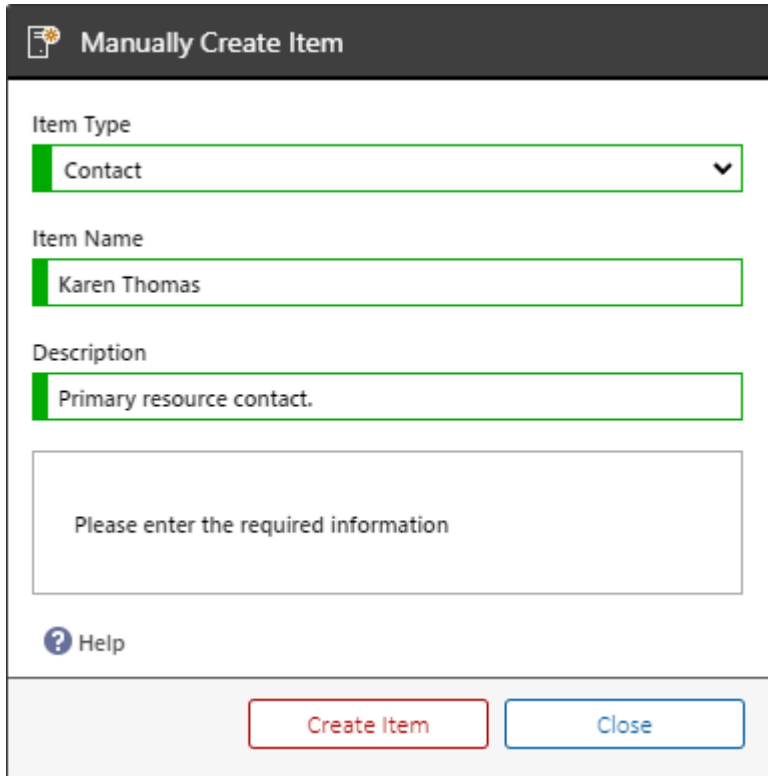
Any new [items](#) will be created in the specified [container](#) or [customer](#). This setting has no effect when updating existing [items](#).

Manually Creating Items

Many [items](#) are automatically detected, created and updated by the [XIA Configuration Client](#). Other [items](#) such as locations and password lists must be created manually.

To manually create a new item:

- Select File > New Item from the drop down menu.



Manually Create Item

Item Type
Contact

Item Name
Karen Thomas

Description
Primary resource contact.

Please enter the required information

? Help

Create Item Close

- Select the relevant [item](#) type from the drop down list. Note: the [items](#) in this list can be configured in the [manual item creation](#) settings.
- Enter a valid name that meets the [item naming](#) settings.
NOTE: This setting does not apply to [knowledge base articles](#) as these are named automatically.
- Enter a description for the [item](#).
- For [resource item](#) types, you must browse to a resource file to assign.

 Manually Create Item

Item Type

Resource

Item Name

Sample Image

Description

This is a sample image.

Resource File



Browse...

Please enter the required information

 Help

Create Item

Close

- For [external hyperlink item](#) types, you must enter the URL to assign.

 **Manually Create Item**

Item Type

External Hyperlink

Item Name

Entra Directory Web Site

Description

The Microsoft Entra Directory web site.

Link URL

https://www.microsoft.com/en-gb/security/business/identity-acces:

Please enter the required information

 Help

Create Item

Close

- Click the create item button to create the [item](#).

Mobile Support

[XIA Configuration Server](#) is capable of rendering a simplified version of the user interface for mobile users. The system automatically detects mobile devices and redirects them to the mobile section found at */mobile*.

The mobile site provides simplified functionality including:

- Search
- Item view
- PDF export

Organization Hierarchy

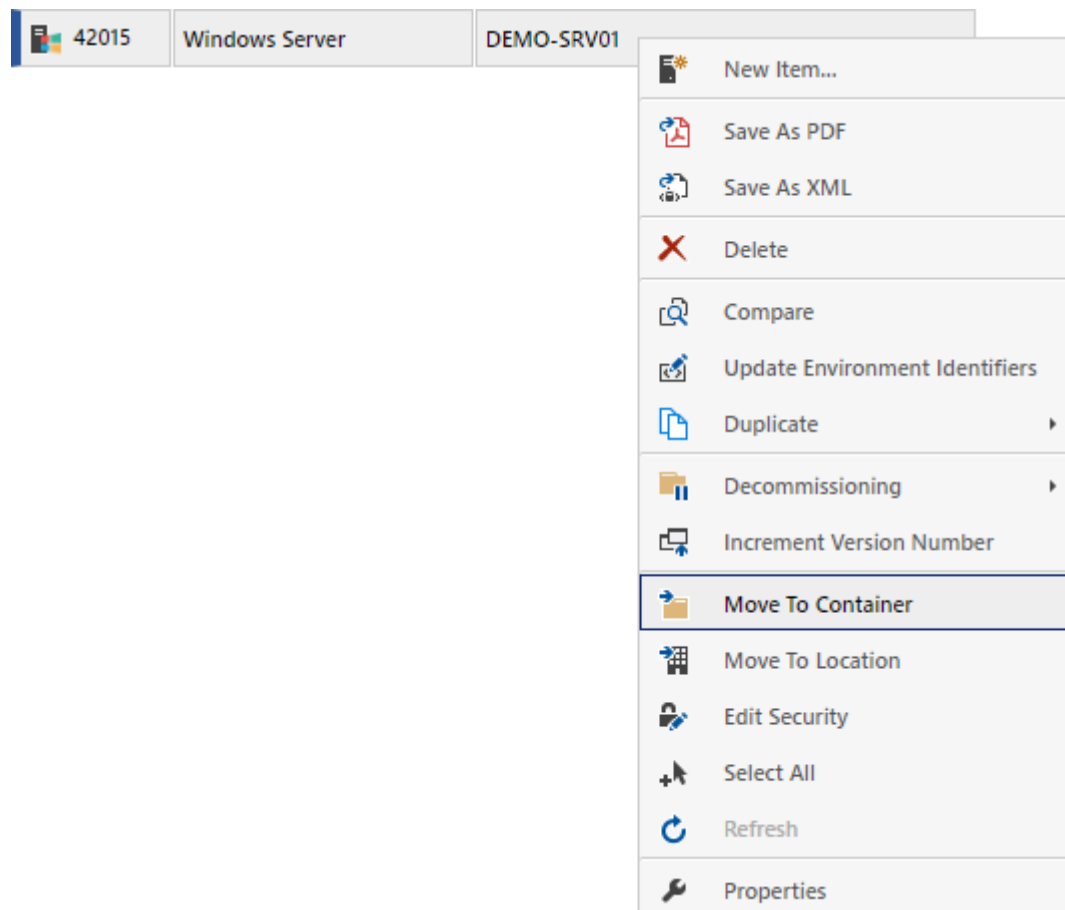
The organizational hierarchy allows items to be arranged within [containers](#) and [customers](#).

Unlike the [location hierarchy](#) which represents the physical locations of items, the organizational hierarchy allows items to be arranged in any way that meets the business requirements.

Both [containers](#) and [customers](#) allow nesting and [security descriptors](#) to be applied and inherited to child [items](#).

Assigning Parent Containers

Containers and customers can be dragged and dropped in the organization hierarchy. Other items can be assigned to a parent container or customer by right clicking the item, and selecting move to container.



The target container or customer can be selected from the move to container dialog.

 Move To Container

Container

▼  Demonstration Inc

▼  Managed Customers

 Customer 1

>  Customer 2

>  Customer 3

>  Customer 4

>  Lost and Found

Refresh

Please select the destination container

Move

Close

Reporting

XIA Configuration Server includes a reporting user interface that supports the ability to create and execute [reports](#) across all [items](#) within the configuration database.



Active Directory Domains Summary

Provides a summary of the Active Directory domains found within the environment.

Modify Report

Execute Report

2 Results

Domain Name	NetBIOS Name	Domain Functional Level	Forest Functional Level
 europe.demo2022.int	EUROPE	Windows Server 2016	Windows Server 2016
 demoxcs2022.int	DEMOXCS2022	Windows Server 2016	Windows Server 2016

The [installation](#) includes a number of built-in [reports](#) and additional reports can be created manually.

To view the reporting interface, select *browse reports* from the [main page](#).

 Organisation

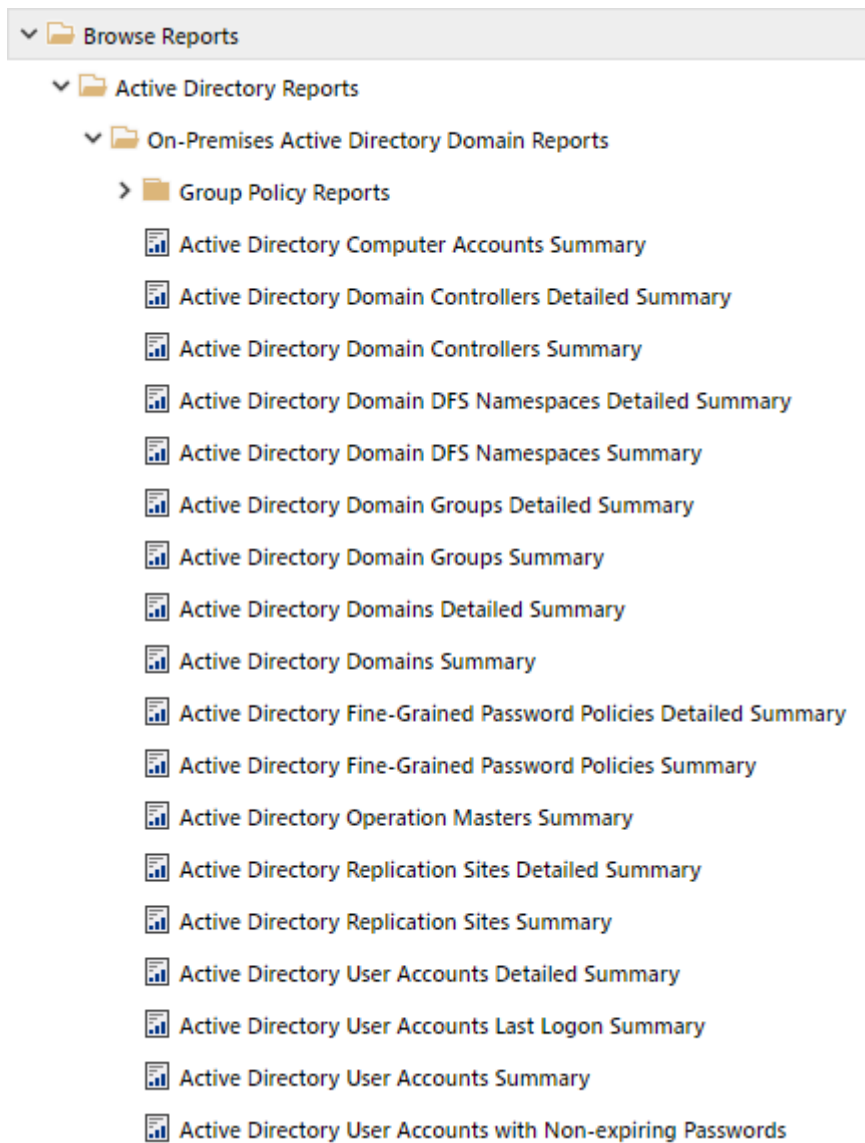
 Item Type

 Location

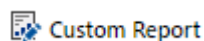
 Browse Reports

Reports

Reports provide the ability to query and display information within the [XIA Configuration Server](#) system.

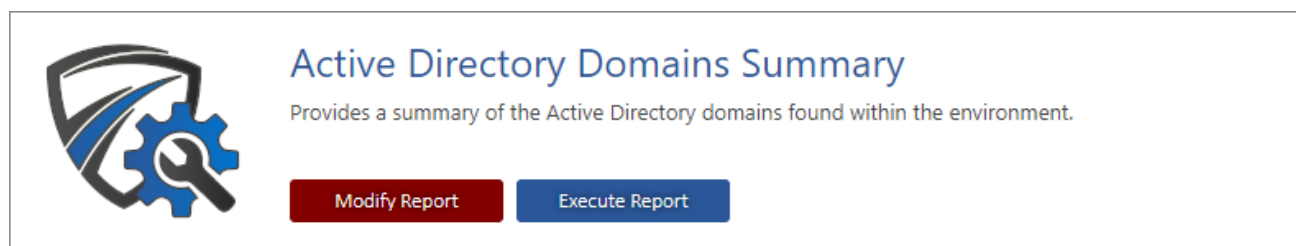


The [installation](#) includes a number of built-in reports and additional reports can be created by [system administrators](#). Custom reports can be identified by the pencil icon overlay.



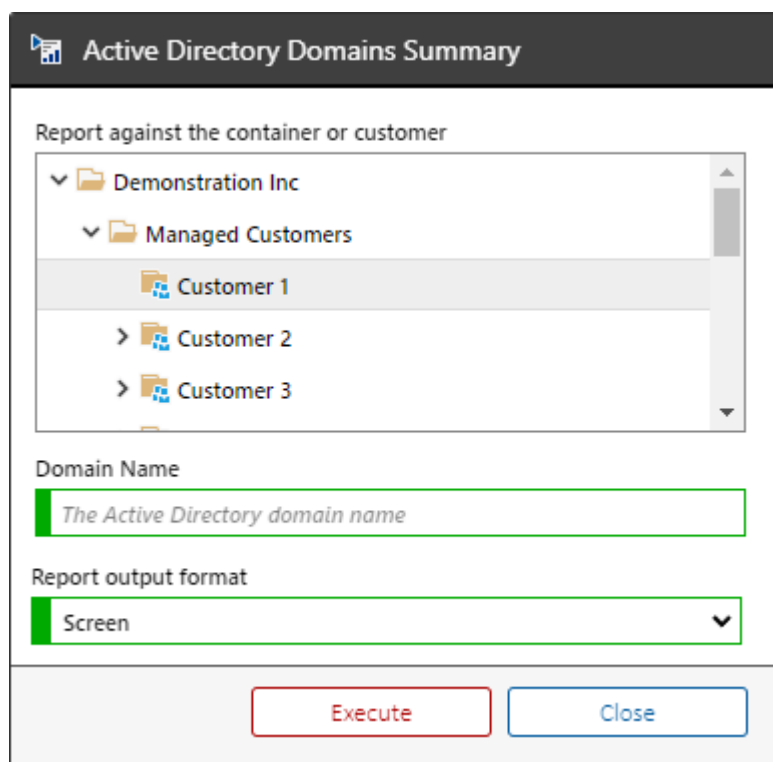
Executing Reports

To execute a [report](#) select the report to display the report information and click the *Execute Report* button.



Alternatively right click the report and click the *Execute* context menu item.

The following dialog will be shown.



If the option is available for the [report](#), select the [container](#) or [customer](#) against which to execute the [report](#).

If available for the [report](#) enter the [parameter values](#) as required.

Click the Execute button to execute the report and display the results.



Active Directory Domains Summary

Provides a summary of the Active Directory domains found within the environment.

[Modify Report](#)[Execute Report](#)

 2 Results

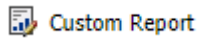
Domain Name	NetBIOS Name	Domain Functional Level	Forest Functional Level
 europe.demo2022.int	EUROPE	Windows Server 2016	Windows Server 2016
 demoxcs2022.int	DEMOXCS2022	Windows Server 2016	Windows Server 2016

Creating Reports

Whilst the [installation](#) includes a number of built-in [reports](#) additional reports can be created.

NOTE: Only [system administrators](#) can create [reports](#).

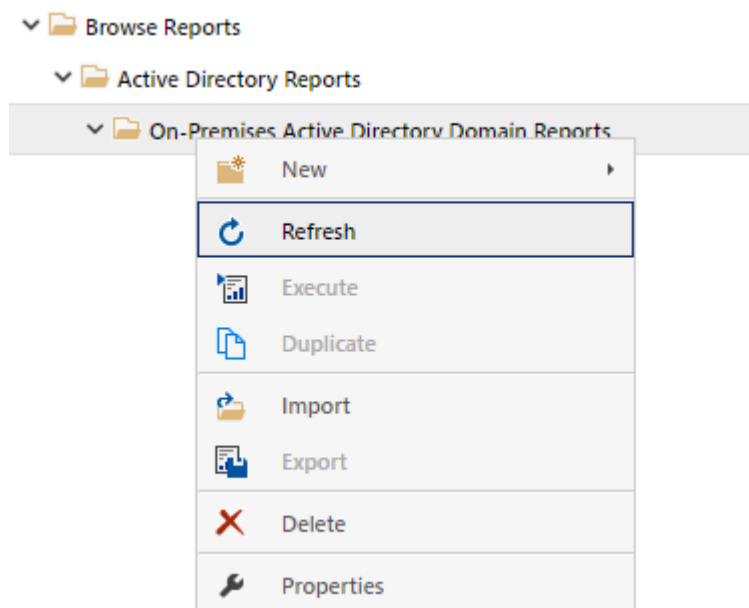
Custom reports can be identified by the pencil icon overlay.



To create a custom [report](#) right click a [report folder](#) or the [root report folder](#) in which to create the [report](#), and select *New, New Report*.

Complete the settings for the report and click *Save Report*.

Once complete right click the [report folder](#) in which the [report](#) was created and click *Refresh*.



Deleting Reports

To delete a [report](#) right click the [report](#) and click *Delete*.

Alternatively see the [delete report](#) PowerShell reporting sample.

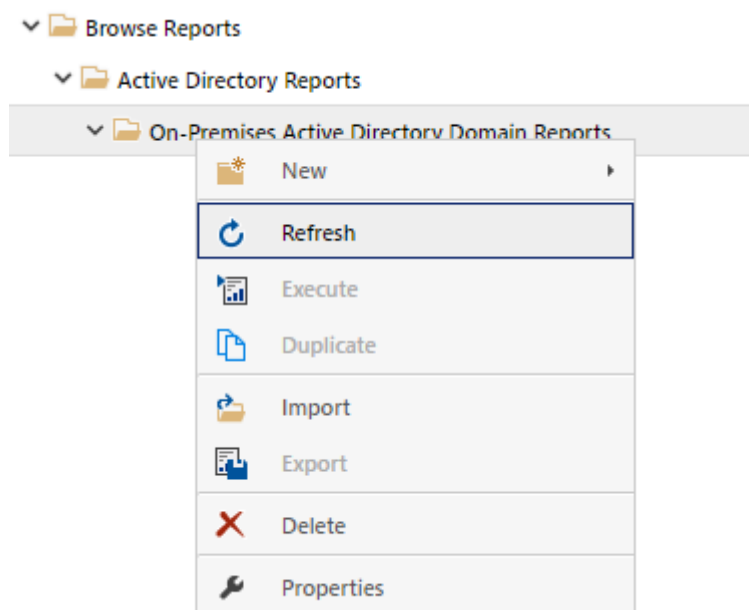
Duplicating Reports

To duplicate a [report](#) right click the [report](#) and click *Duplicate*.

A new [report](#) is created called "Copy of *original report name*" in the same [report folder](#) as the original [report](#), and the general properties are automatically displayed.

[Modify the settings](#) for the [report](#) as required and click *Save Report*.

If the name of the [report](#) has been changed right click the [report folder](#) in which the [report](#) was duplicated and click *Refresh* to display the new report name.



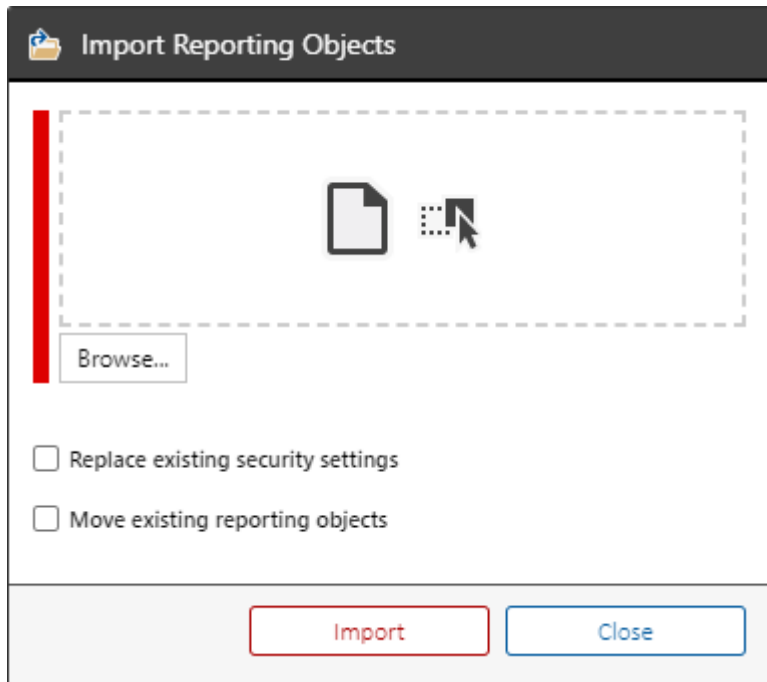
Exporting Reports

To export a [report](#) right click the [report](#) and click *Export*.

The [report](#) is downloaded to the browser in XML format.

Importing Reports

To import a [report](#) from XML right click the [report folder](#) into which you want to import the [report](#) and click *Import*.



Import File

Browse to the [report](#) file in XML format, or drop the file on the drop zone.

Replace existing security settings

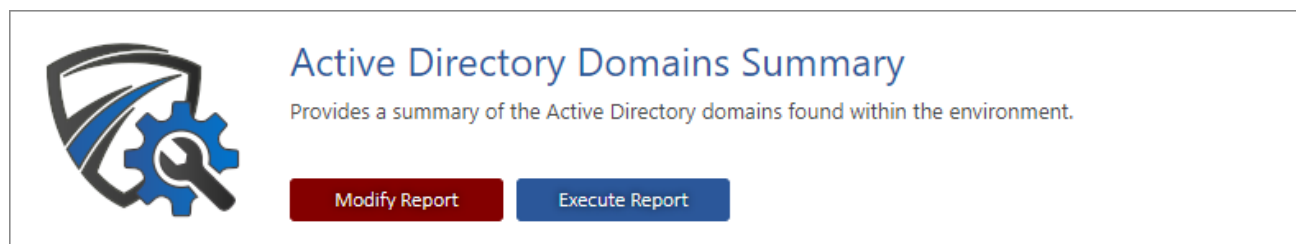
Determines whether, if the [report](#) already exists, that the [security settings](#) should be overwritten by the import.

Move existing reporting objects

Determines whether, if the [report](#) already exists, that the [report](#) should be [moved](#) to the currently selected [report folder](#).

Modifying Reports

To modify a [report](#) select the [report](#) and click the *Modify Report* button.



Alternatively, right click the [report](#) and click *Properties*.

This displays the [general settings](#) for the [report](#).

NOTE: It is not recommended that built in [reports](#) are modified as these may be overwritten by future versions of [XIA Configuration Server](#). Instead it is recommended that [reports](#) be [duplicated](#) before being modified. These built in [reports](#) will display a "This is a system managed report" warning.

This is a system managed report.

General Settings

Report Identifier

The unique identifier of the [report](#) in GUID format. This property cannot be modified.

Display Name

The display name for the [report](#).

Creation Date

The date and time that the [report](#) was created. This property cannot be modified.

Last Modified

The date and time that the [report](#) was last modified. This property cannot be modified.

Parent Folder

The name of the [report folder](#) in which this [report](#) resides. This property cannot be modified.

Description

The description of the [report](#).

SQL Statement

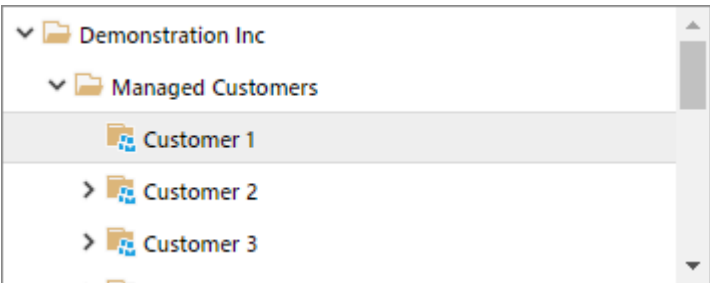
SQL Statement

All [reports](#) within [XIA Configuration Server](#) are written using the [Microsoft Transact-SQL \(TSQL\)](#) language with a small number of non-standard tokens described below. The [SQL statement](#) can be modified using the [SQL Code Editor](#).

Allow the user to select a container or customer against which to run the report

Determines whether the user can select a container or customer against which to run the report. If this check box is enabled the `[FILTERTOCONTAINER]` token must be found within the [WHERE](#) clause of the [SQL statement](#).

This displays the organization browser to the user when they [execute the report](#).



Allow the user to sort the results

Determines whether the user can sort the results. If this check box is enabled the `[SORTCOLUMN]` token must be found as part of the [ORDER BY](#) clause of the [SQL statement](#). When this option is enabled users can click the column headers of the [report](#) to sort by that column.

 2 Results

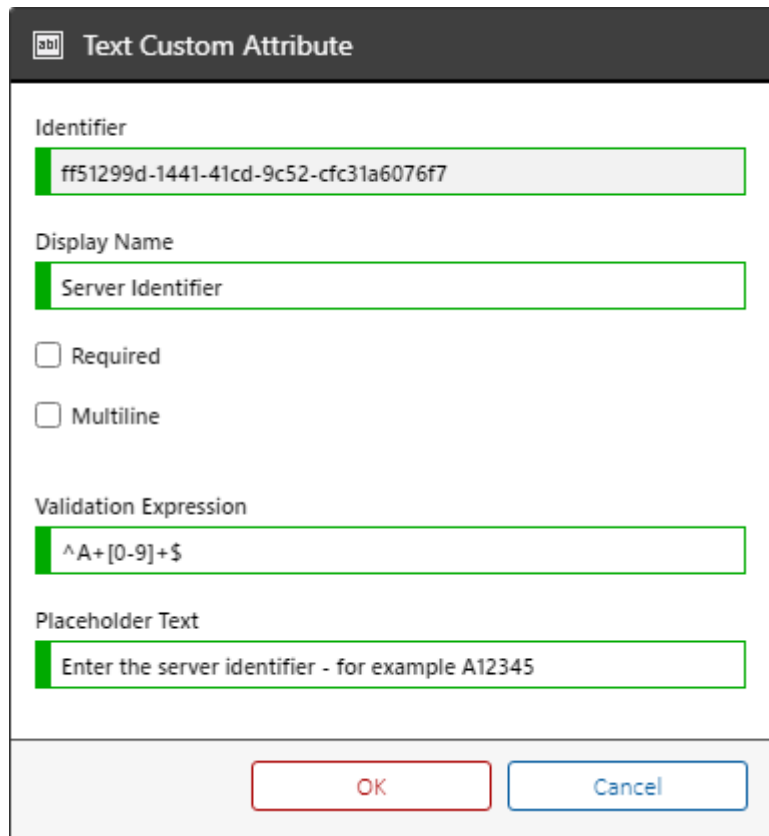
 Domain Name	NetBIOS Name	Domain Functional Level	Forest Functional Level
 europe.demo2022.int	EUROPE	Windows Server 2016	Windows Server 2016
 demoxcs2022.int	DEMOXCS2022	Windows Server 2016	Windows Server 2016

WARNING: Creating or modifying [reports](#) can expose information in the entire [XIA Configuration Server database](#). Ensure that all custom [reports](#) are validated before being used in a production environment.

Custom Attributes

Information stored for [items](#) can be extended using [custom sections and attributes](#).

To access the display value of a [custom attribute](#) in a [report](#), view the configuration of the [custom attribute](#) and note the identifier.



The screenshot shows a dialog box titled "Text Custom Attribute" with a dark header bar containing a small icon and the title. The dialog has several input fields and checkboxes. The "Identifier" field contains the value "ff51299d-1441-41cd-9c52-cfc31a6076f7". The "Display Name" field contains "Server Identifier". There are two unchecked checkboxes: "Required" and "Multiline". The "Validation Expression" field contains the regex "^A+[0-9]+\$". The "Placeholder Text" field contains "Enter the server identifier - for example A12345". At the bottom, there are "OK" and "Cancel" buttons.

Field	Value
Identifier	ff51299d-1441-41cd-9c52-cfc31a6076f7
Display Name	Server Identifier
Required	☐
Multiline	☐
Validation Expression	^A+[0-9]+\$
Placeholder Text	Enter the server identifier - for example A12345

To access the display value of the [custom attribute](#) the **GetCustomAttribute** function can be used, for example

SELECT

```
[dbo].[ItemCore].[ItemID] AS [ItemID],  
[dbo].[ItemCore].[Name] AS [Name],  
[dbo].[GetCustomAttribute] ([dbo].[ItemCore].[ItemID], '5e6d074d-d7e704f9e-b0ee-  
eff73bde89b8') AS [Server Identifier]
```

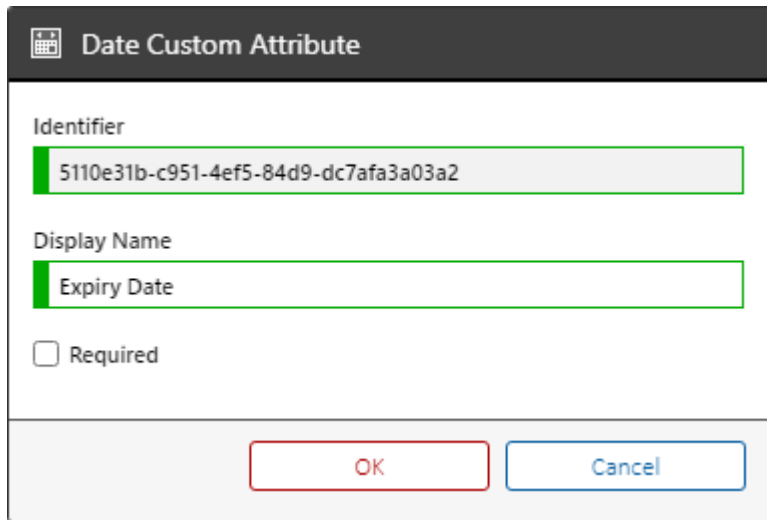
FROM [dbo].[ItemCore]

WHERE

```
[dbo].[ItemCore].[ItemDeletedDate] IS NULL
```

Date Custom Attributes

To access the `System.DateTime` value of a [date custom attribute](#) view the [configuration](#) and note the identifier.



The image shows a dialog box titled "Date Custom Attribute". It has a dark header bar with a calendar icon and the title. Below the header, there are three input fields: "Identifier" with the value "5110e31b-c951-4ef5-84d9-dc7afa3a03a2", "Display Name" with the value "Expiry Date", and a "Required" checkbox which is unchecked. At the bottom, there are two buttons: "OK" and "Cancel".

To access the value of the [custom attribute](#) the `GetCustomAttributeDateTime` function can be used, this will return a [T-SQL DATETIME2](#) value, or `NULL` if the [custom attribute](#) is not defined.

SELECT

```
[dbo].[ItemCore].[ItemID] AS [ItemID],  
[dbo].[ItemCore].[Name] AS [Name],  
[dbo].[GetCustomAttributeDateTime] ([dbo].[ItemCore].[ItemID], '87e69d55-6b59-42ff-b525-  
800daf18a0e3') AS [Operating System Expiry]
```

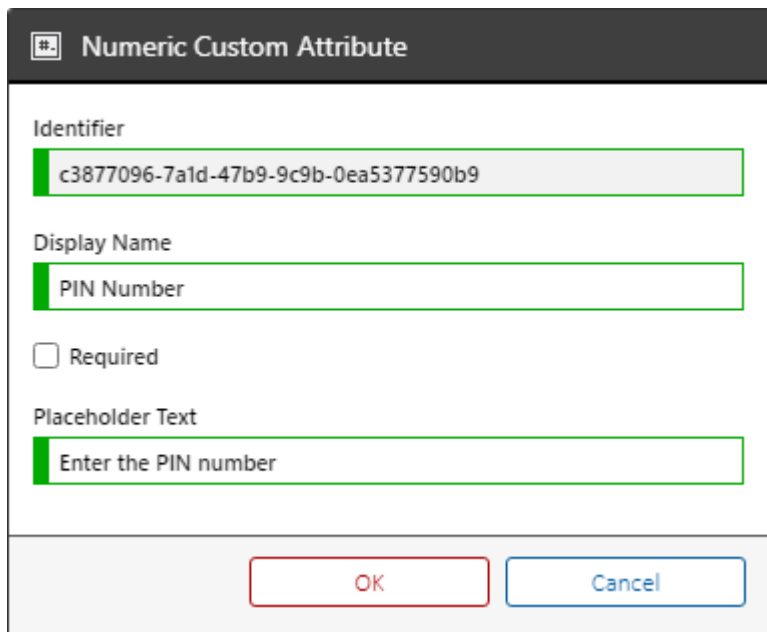
FROM [dbo].[ItemCore]

WHERE

```
[dbo].[ItemCore].[ItemDeletedDate] IS NULL
```

Numeric Custom Attributes

To access the `System.Int64` value of a [numeric custom attribute](#) view the [configuration](#) and note the identifier.



The screenshot shows a dialog box titled "Numeric Custom Attribute". It contains the following fields and controls:

- Identifier:** A text box containing the GUID "c3877096-7a1d-47b9-9c9b-0ea5377590b9".
- Display Name:** A text box containing "PIN Number".
- Required:** An unchecked checkbox.
- Placeholder Text:** A text box containing "Enter the PIN number".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

To access the value of the [custom attribute](#) the **GetCustomAttributeInteger** [function](#) can be used, this will return a [T-SQL BIGINT](#) value, or `NULL` if the [custom attribute](#) is not defined.

```
SELECT
    [dbo].[ItemCore].[ItemID] AS [ItemID],
    [dbo].[ItemCore].[Name] AS [Name],
    [dbo].[GetCustomAttributeInteger] ([dbo].[ItemCore].[ItemID], '17b4e771-2e02-4c97-8b2f-
eb77b97a4e80') AS [PIN number]
FROM [dbo].[ItemCore]
WHERE
    [dbo].[ItemCore].[ItemDeletedDate] IS NULL
```

Images



Windows Machine Summary

Provides general information about a Windows Server including operating system name, manufacturer and model number.

Modify ReportExecute Report

1 Results

Name	Manufacturer	Model	Domain Role	OS Name
 DEMO-XCS-2022	VMware, Inc.	VMware7,1	Domain Controller (PDC emulator)	Microsoft Windows Server 2022 Standard

To include an image for each result simply return the [ImageUrl] column with the path to the image.
`'~/images/grid/WindowsServer.png' AS [ImageUrl]`

For an `item` you can return the image for that `item` by calling the `GetTypeNameInternal`
`dbo.GetImageForType([ItemCore].[Type]) AS [ImageUrl]`

When the display each result in a new table `output and charting` setting is enabled for the `report` the image will be displayed in the title of the result.

 DEMO-XCS-2022

Name	DEMO-XCS-2022
Manufacturer	VMware, Inc.
Model	VMware7,1
Serial Number	VMware-56 4d 15 09 c7 22 13 00-4c 19 5c f1 85 44 54 22
Build Number	20348
Domain Role	Domain Controller (PDC emulator)
OS Name	Microsoft Windows Server 2022 Standard
Service Pack	[None Installed]
Server Core	False
Domain Name	demoxcs2022.int

Item Management

To enable the ability to manage [items](#) directly from the [report](#) ensure that the [report](#) returns the [ItemCore].[ItemID] column.

 1 Results

Name	Manufacturer	Model
 DEMO-XCS-2022	VMware, Inc.	VMware7,1

 New Item...

 Save As PDF

 Save As XML

 Delete

 Compare

 Update Environment Identifiers

 Duplicate

 Decommissioning

 Increment Version Number

 Move To Container

 Move To Location

 Edit Security

 Select All

 Refresh

 Properties

If the [item](#) identifier is required to be displayed in the [report](#) return this with a different column name for example

```
[ItemCore].[ItemID] AS [Item ID]
[ItemCore].[ItemID] AS [Item Identifier]
```

Location Information

The unique identifier of the parent location of an item can be found by querying the `LocationParentItemID` property within the `ItemCore` table.

However, this only provides information about the immediate parent location which may be a room, rack, or location.

The **`GetItemLocationInformation`** function provides the following additional information about the immediate parent and items within the location hierarchy:

```
[Parent] INT
[ParentType] INT
[ParentTypeName] NVARCHAR(200)
[GrandParent] INT
[GrandParentType] INT
[GrandParentTypeName] NVARCHAR(200)
[GreatGrandParent] INT
[GreatGrandParentType] INT
[GreatGrandParentTypeName] NVARCHAR(200)
[Rack] INT
[RackName] NVARCHAR(200)
[Room] INT
[RoomName] NVARCHAR(200)
[Location] INT
[LocationName] NVARCHAR(200)
```

For example:

```
SELECT
Name AS [Name],
LocationInformation.LocationName AS [Location]
FROM ItemCore
OUTER APPLY [dbo].GetItemLocationInformation (ItemCore.ItemID) LocationInformation
```

Override Strings

Certain information within [XIA Configuration Server](#) is stored as override strings. These allow the [XIA Configuration Client](#) to read a value from a [target system](#) such as the description of a [Windows Server](#) and display it in the user interface whilst allowing the user to manually override and edit this value.

Description	Demonstration DHCP server. 
-------------	--

As this information is stored as XML, executing the following query will display XML only
`<OverrideString Value="" AgentValue="" Overridden="false" />`

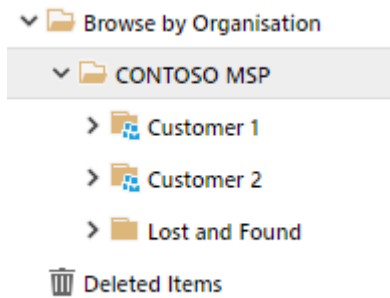
```
SELECT
    [ItemCore].[ItemID] AS [Item ID],
    [ItemCore].[Name] AS [Item Name],
    [ItemCore].[Description] AS [Description]
FROM
    ItemCore
WHERE
    ItemDeletedDate IS NULL
```

The **GetXValue** [function](#) returns only the value displayed to the user.

```
SELECT
    [ItemCore].[ItemID] AS [Item ID],
    [ItemCore].[Name] AS [Item Name],
    dbo.GetXValue([Description]) AS [Description]
FROM
    ItemCore
WHERE
    ItemDeletedDate IS NULL
```

Parent Customers

Within [XIA Configuration Server](#), it is possible to store [items](#) within [customers](#) which behave in a similar way to a standard [container](#).



To determine which [customer](#) an item belongs to, the **GetItemParentCustomerName** and **GetItemParentCustomerID** [functions](#) can be used.

- If multiple [customers](#) are nested within each other, the most immediate [customer](#) in the hierarchy is returned.
- When running GetItemParentCustomerID, if the [item](#) has no parent [customer](#), zero is returned.
- When running GetItemParentCustomerName, if the item has no parent [customer](#), an empty string is returned.

The following example returns the unique identifier and name of each [item](#)'s parent [customer](#) where a parent [customer](#) is available

SELECT

```
[dbo].[ItemCore].[ItemID] AS [Item ID],  
[dbo].[ItemCore].[Name] AS [Item Name],  
[dbo].[ItemCore].[Description] AS [Description],  
[dbo].GetItemParentCustomerID(ItemID) AS [Parent Customer ID],  
[dbo].GetItemParentCustomerName(ItemID) AS [Parent Customer Name]
```

FROM

```
[dbo].[ItemCore]
```

WHERE

```
[dbo].[ItemCore].[ItemDeletedDate] IS NULL  
AND  
[dbo].GetItemParentCustomerID([ItemCore].[ItemID]) <> 0
```

SQL Code Editor

```
1 -----
2 --
3 --      XIA Configuration Server
4 --      Copyright © CENTREL Solutions 2024
5 --
6 --      Name: Report Template
7 --      Date: 10 September 2024
8 --      Author: CENTREL-WS01\demouser
9 --
10 --      Description:
11 --      This is a XIA Configuration Server report template, please configure to your requirements.
12 --
13 --      Version History:
14 --      1.0.0 - 10 September 2024 - Initial Version
15 --
16 -----
17
18 SELECT
19     [ItemCore].[ItemID] AS [ItemID],
20     [ItemCore].[Name] AS [Name]
21 FROM
22     [ItemCore]
23 WHERE
24     [ItemCore].[ItemID] = 1000
25     AND [FILTERTOCONTAINER]
26 ORDER BY [SORTCOLUMN]
27
```

System administrators can use the SQL Code Editor to modify the [Microsoft Transact-SQL \(TSQL\)](#) of reports.

XML Data

[XIA Configuration Server](#) stores information collected by the [XIA Configuration Client](#) within the [database](#) as XML data.

For example the following displays abbreviated information collected by the [IIS server agent](#) relating to application pools.

```
<ApplicationPools>
  <ApplicationPool AutoStart="True" ManagedPipelineMode="Integrated"
ManagedRuntimeVersion="v4.0" Name="ASP.NET v4.0" QueueLength="1000">
    </ApplicationPool>
</ApplicationPools>
```

The following example shows how to read each application pool using CROSS APPLY and the [T-SQL XML value](#) method.

```
SELECT
  [dbo].[ItemCore].[ItemID] AS [ItemID],
  [dbo].[ItemCore].[Name] AS [IIS Server],
  [ApplicationPool].value('@Name[1]', 'NVARCHAR(200)') AS [Application Pool Name],
  [ApplicationPool].value('@ManagedRuntimeVersion[1]', 'NVARCHAR(200)') AS [Managed Runtime
Version]
FROM IIS Servers
INNER JOIN [dbo].[ItemCore] ON ItemCore.ItemID = IIS Servers.ItemID
CROSS APPLY [ApplicationPools].nodes('/ApplicationPools/ApplicationPool') AS
T(ApplicationPool)
WHERE
  [dbo].[ItemCore].[ItemDeletedDate] IS NULL
```

Using FLWOR

Certain data may be stored in multiple XML elements; however, you may wish to display these within a single row within a [report](#). This can be accomplished using [FLWOR](#).

In the following example, the names of the subnets assigned to an [Active Directory site](#) are stored in individual XML elements.

```
<Replication>
  <Sites Status="Complete">
    <Site>
      <SubnetNames>
        <SubnetName>10.1.0.0/24</SubnetName>
      </SubnetNames>
    </Site>
  </Sites>
</Replication>
```

To obtain this information, use [FLWOR](#) to read each **SubnetName** in **SubnetNames** and concatenate these values with a semicolon:

```
SELECT
  [dbo].[ItemCore].[ItemID] AS [ItemID],
  [dbo].[ItemCore].[Name] AS [Domain Name],
  '~/images/tables/ActiveDirectoryDomain/ReplicationSite.png' AS [ImageUrl],
  [dbo].[GetItemParentCustomerName]([dbo].[ItemCore].[ItemID]) AS [CustomerName],
  [ReplicationSite].value('@Name', 'NVARCHAR(200)') AS [Site Name],
  CAST([ReplicationSite].query('for $SubnetName in (SubnetNames/SubnetName) return
concat(data($SubnetName), ";")') AS NVARCHAR(MAX)) AS [Subnet Names]
FROM [dbo].[ActiveDirectoryDomains]
INNER JOIN [dbo].[ItemCore] ON [dbo].[ItemCore].[ItemID] =
[dbo].[ActiveDirectoryDomains].[ItemID]
CROSS APPLY [ActiveDirectoryDomains].[Replication].nodes('/Replication/Sites/Site') AS
R(ReplicationSite)
WHERE
  [dbo].[ItemCore].[ItemDeletedDate] IS NULL
AND [dbo].[ItemCore].[DecommissionDate] IS NULL
```

The [reporting system](#) automatically interprets these as a list and removes the semicolons, and displays each value on a new line within the subnets column of the report

Domain Name	Site Name	Subnet Names
 europe.demo2022.int	BranchOffice	
 europe.demo2022.int	Europe	
 europe.demo2022.int	HQ	10.1.0.0/24

Output and Charting

Enable chart

Determines whether to display a [chart](#) for the [report](#).

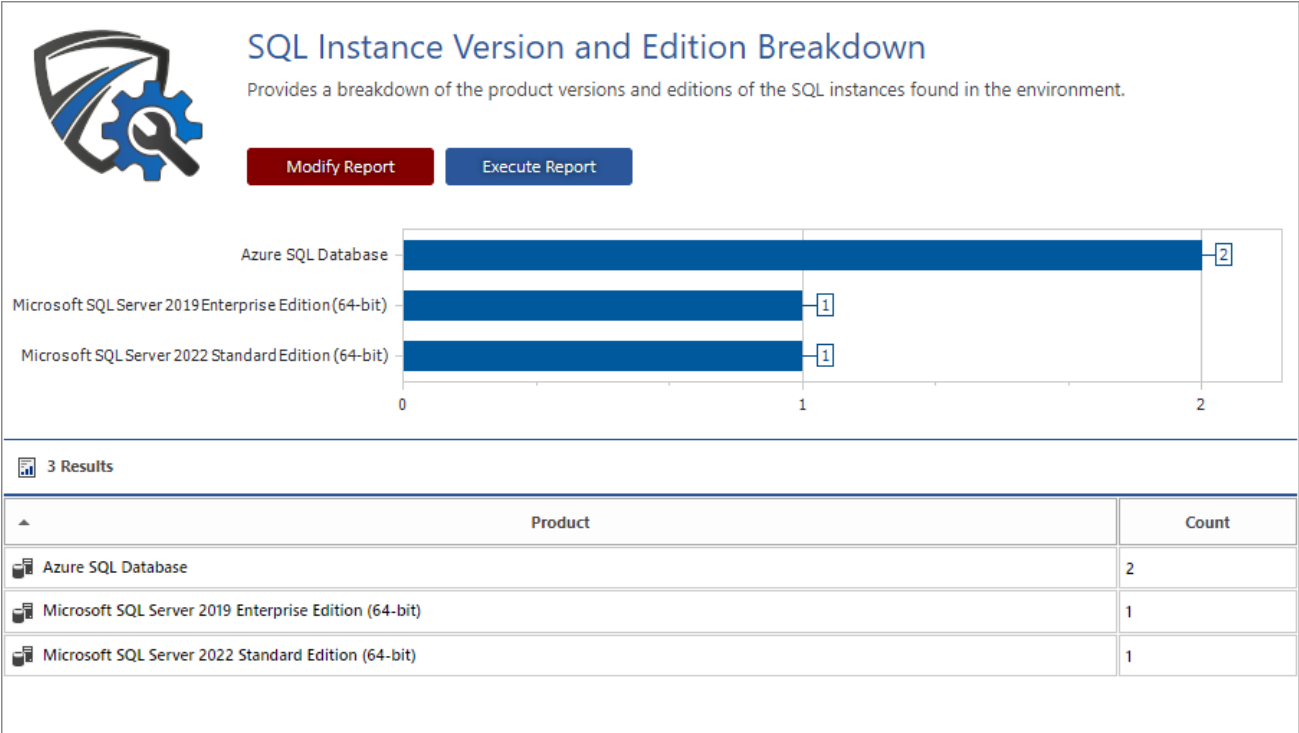
Display each result in a new table

Determines whether each result in the [report](#) should be [displayed in its own table](#).

Use landscape orientation for PDF output

Determines whether the [report](#) should use landscape orientation when the [report](#) is exported to a PDF document. It is possible to mix [reports](#) that use both portrait and landscape in the same [report binder](#).

Charts



The chart option should be used with reports that return a text value and a numeric field.

Display each result in a new table

 DEMO-XCS-2022	
Name	DEMO-XCS-2022
Manufacturer	VMware, Inc.
Model	VMware7,1
Serial Number	VMware-56 4d 15 09 c7 22 13 00-4c 19 5c f1 85 44 54 22
Build Number	20348
Domain Role	Domain Controller (PDC emulator)
OS Name	Microsoft Windows Server 2022 Standard
Service Pack	[None Installed]
Server Core	False
Domain Name	demoxcs2022.int

When enabled this option displays each result in its own table, allowing more information to be displayed for each result.

To render a title for each result return a [Title] of type NVARCHAR.

When displaying the [parent customer](#) name use the column header [CustomerName]. This interacts with the **Show Customer Names** option in the [reporting settings](#).

To render an image next to the title use the column header [ImageUrl] as described in the [images](#) section.

To render a full sized image use the column header [Image]. The data returned should be an image object in byte[] array format.

To render XHTML data use the column header [XHTML]. Note that the data will be cleaned and only valid HTML elements and attributes will be rendered to the page.

Report Parameters

Report parameters allow the user to supply information to the report being executed.



Report Parameters

Report parameters define the values that can be specified by the user and are passed to the report.

 3 Report Parameters

Display Name	Name	Type
 Service Name	ServiceName	Text
 Machine Name	MachineName	Text
 Service Display Name	ServiceDisplayName	Text

New Report Parameter

Several types of report parameters are available, all of which include a display name and parameter name.

 Text Report Parameter

Parameter Name

ServiceName

Display Name

Service Name

Placeholder Text

The service name e.g. Spooler

Default Value

☐ Hidden

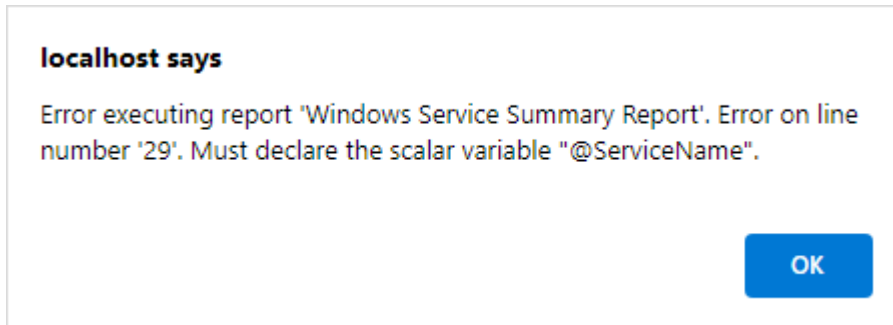
OK

Cancel

To use the report parameter within the [report](#) simply reference the parameter name within the [SQL statement](#), for example

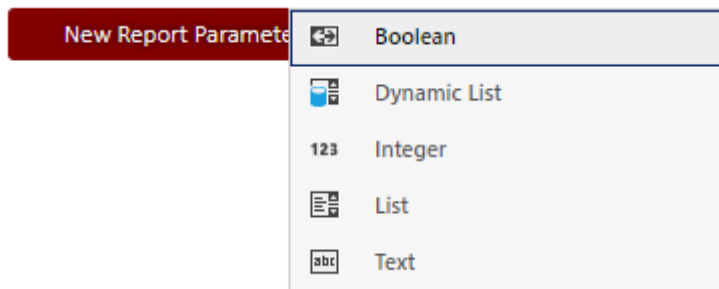
```
WHERE ([ItemCore].[Name] LIKE @ServerName)
```

If the [SQL statement](#) of the report contains a parameter that has not been defined as a [report parameter](#) an error similar to the following will be displayed to the user



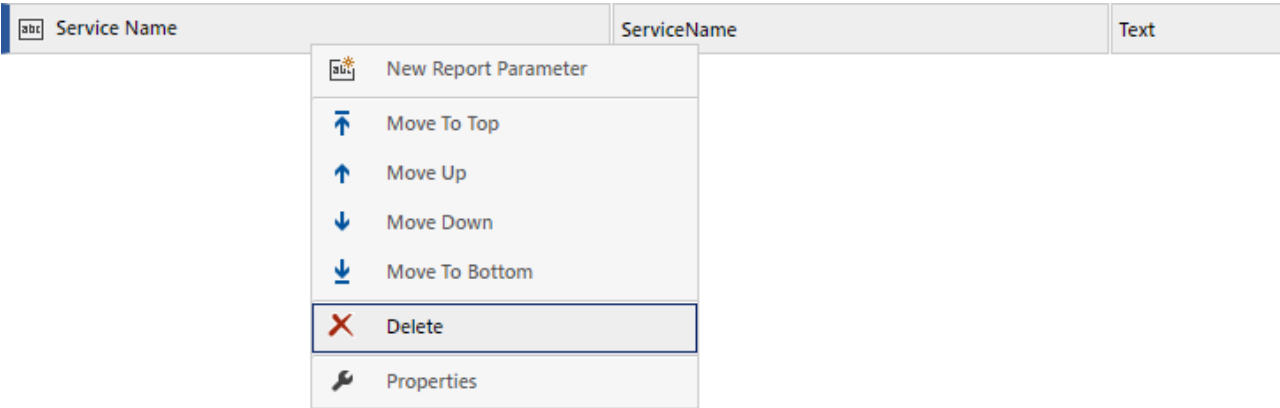
Creating Report Parameters

To add a new [report parameter](#) click the *New Report Parameter* button and select the required [report parameter type](#).



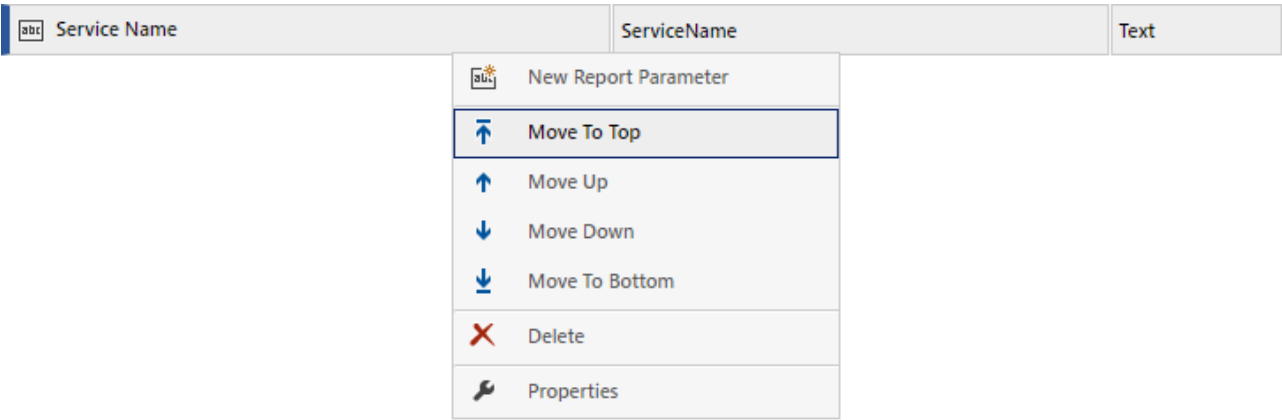
Deleting Report Parameters

To delete a [report parameter](#) right click the [report parameter](#) and click *Delete*.



Ordering Report Parameters

The order that the [report parameters](#) are [displayed to the user](#) can be modified by right clicking the [report parameter](#) and selecting to move up, move down, move to top, or move to bottom.



Report Parameter Types

The following [report parameter](#) types are available

Boolean Report Parameter

The boolean report parameter displays a check box to the user when collecting the [report parameter values](#).

Dynamic List Report Parameter

The dynamic list report parameter displays a drop down list to the user when collecting the [report parameter values](#).

Integer Report Parameter

The integer report parameter displays a text box to the user when collecting the [report parameter values](#) that allows the user to enter a numeric value between 0 and 999999999.

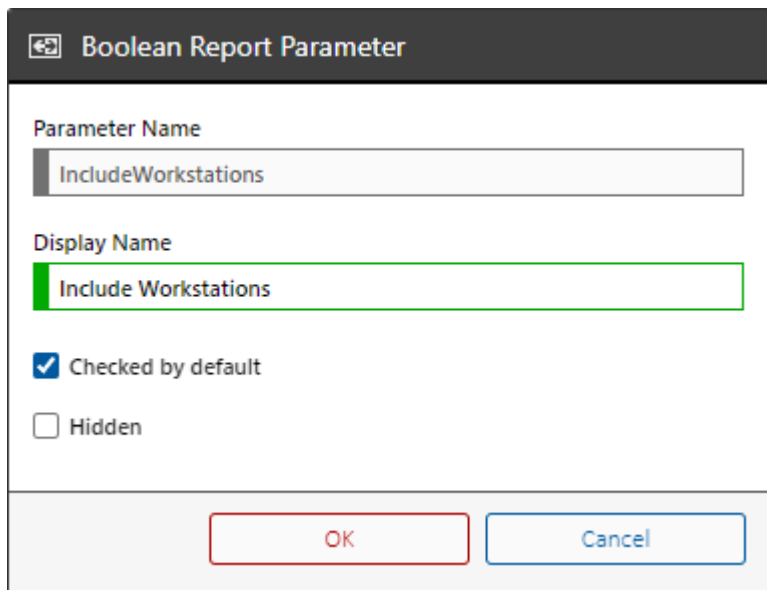
List Report Parameter

The list report parameter displays a drop down list to the user when collecting the [report parameter values](#).

Text Report Parameter

The text report parameter displays a text box to the user when collecting the [report parameter values](#) that allows the user to enter a text value.

Boolean Report Parameter



The screenshot shows a dialog box titled "Boolean Report Parameter". It contains two text input fields: "Parameter Name" with the value "IncludeWorkstations" and "Display Name" with the value "Include Workstations". Below these fields are two checkboxes: "Checked by default" which is checked, and "Hidden" which is unchecked. At the bottom of the dialog are two buttons: "OK" and "Cancel".

The boolean report parameter displays a check box to the user when collecting the [report parameter values](#).

Parameter Name

The name of the parameter available to the [SQL statement](#) as a [BIT value](#).

Display Name

The display name of the parameter displayed to the user when executing the [report](#).

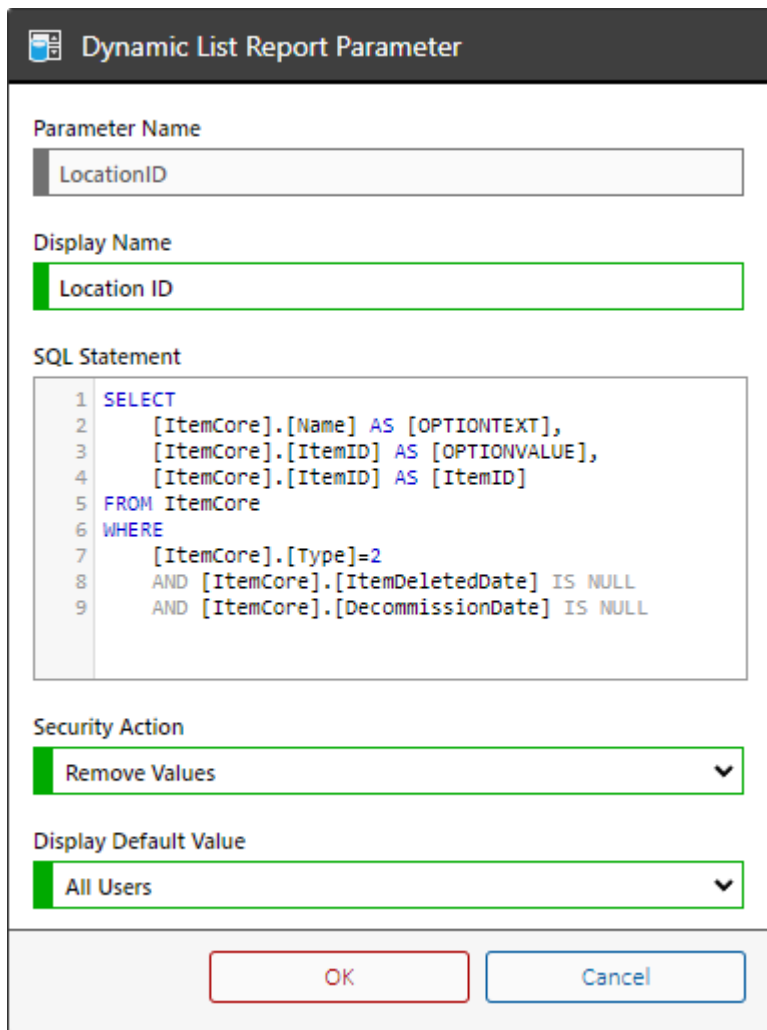
Checked by default

Determines whether the parameter is disabled as checked by default.

Hidden

Determines whether the report parameter is hidden from the user interface, the parameter is still available to the [reporting web services API](#).

Dynamic List Report Parameter



The screenshot shows a configuration window titled "Dynamic List Report Parameter". It contains several fields and buttons:

- Parameter Name:** A text box containing "LocationID".
- Display Name:** A text box containing "Location ID".
- SQL Statement:** A text area containing a SQL query:

```
1 SELECT
2     [ItemCore].[Name] AS [OPTIONTEXT],
3     [ItemCore].[ItemID] AS [OPTIONVALUE],
4     [ItemCore].[ItemID] AS [ItemID]
5 FROM ItemCore
6 WHERE
7     [ItemCore].[Type]=2
8     AND [ItemCore].[ItemDeletedDate] IS NULL
9     AND [ItemCore].[DecommissionDate] IS NULL
```
- Security Action:** A dropdown menu with "Remove Values" selected.
- Display Default Value:** A dropdown menu with "All Users" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

The dynamic list report parameter displays a drop down list to the user when collecting the [report parameter values](#).

Display Name

The display name of the parameter displayed to the user when executing the [report](#).

Parameter Name

The name of the parameter available to the [SQL statement](#) as an [NVARCHAR](#) value.

SQL Statement

The SQL statement to execute to obtain the values to display to the user which can be edited in the [SQL Code Editor](#).

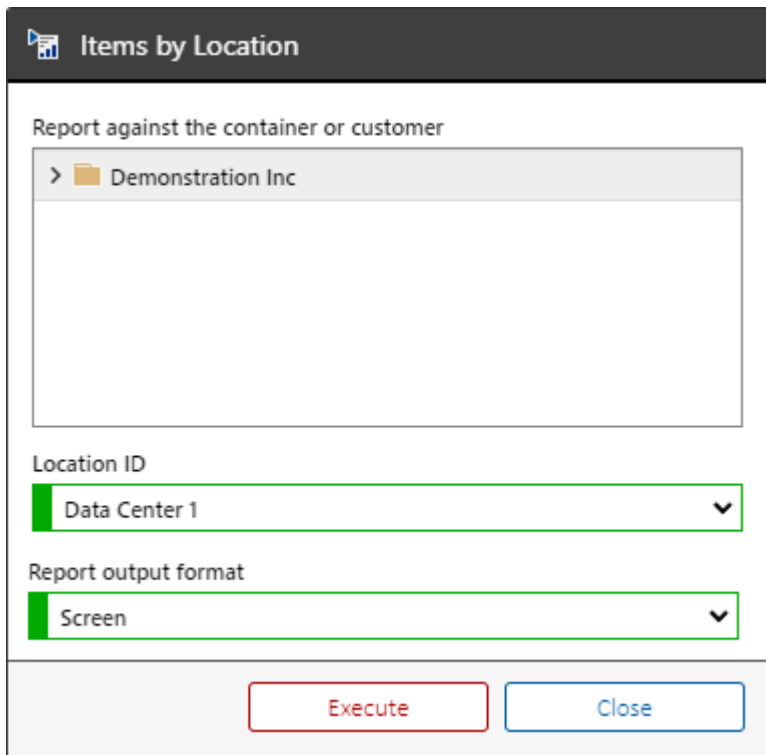
- The statement should return an [OPTIONTEXT] column that is the text to display in the drop down list.
- The statement should return an [OPTIONVALUE] column that is the value used for the parameter in the [SQL statement](#) of the [report](#), this may be the same as the [OPTIONTEXT]

Security Action

Determines whether the values should only be displayed in the drop down list for [items](#) that the user has read [permissions](#). When set to *remove values* the SQL statement must return an [ItemID] column.

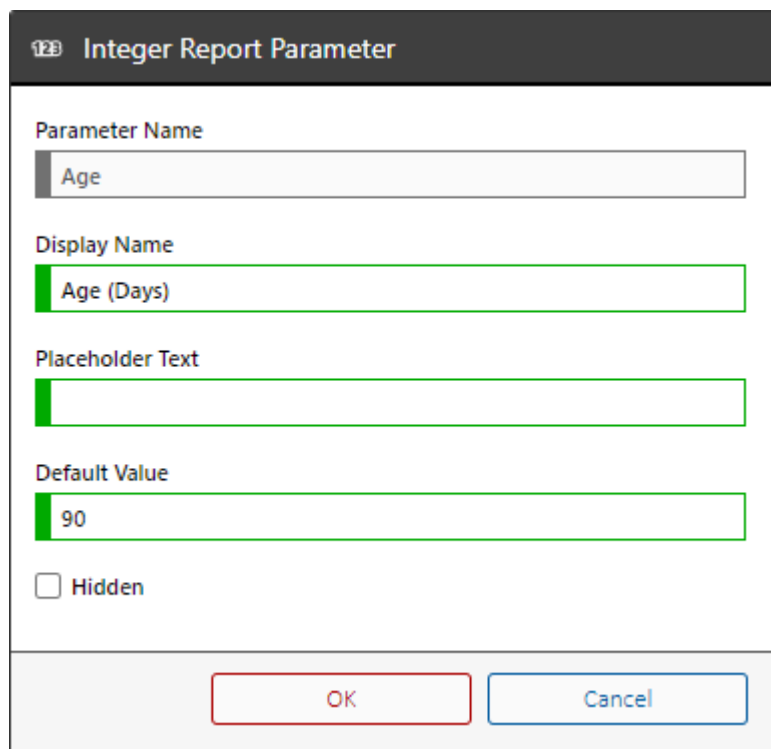
Display Default Value

Determines whether the report parameter should display an [Any Value] option in the drop down list for [system administrators](#), or any user.



The screenshot shows a window titled "Items by Location" with a dark header bar. Below the header, the text "Report against the container or customer" is displayed. A tree view shows a folder icon and the text "Demonstration Inc". Below this is a large empty rectangular area. Further down, there are two dropdown menus. The first is labeled "Location ID" and has "Data Center 1" selected. The second is labeled "Report output format" and has "Screen" selected. At the bottom of the window, there are two buttons: "Execute" (with a red border) and "Close" (with a blue border).

Integer Report Parameter



Integer Report Parameter

Parameter Name
Age

Display Name
Age (Days)

Placeholder Text

Default Value
90

☐ Hidden

OK Cancel

The integer report parameter displays a text box to the user when collecting the [report parameter values](#) that allows the user to enter a numeric value between 0 and 999999999.

Display Name

The display name of the parameter displayed to the user when executing the [report](#).

Parameter Name

The name of the parameter available to the [SQL statement](#) as an [INT value](#).

Placeholder Text

Determines whether placeholder text is displayed in the text box when no value is entered.

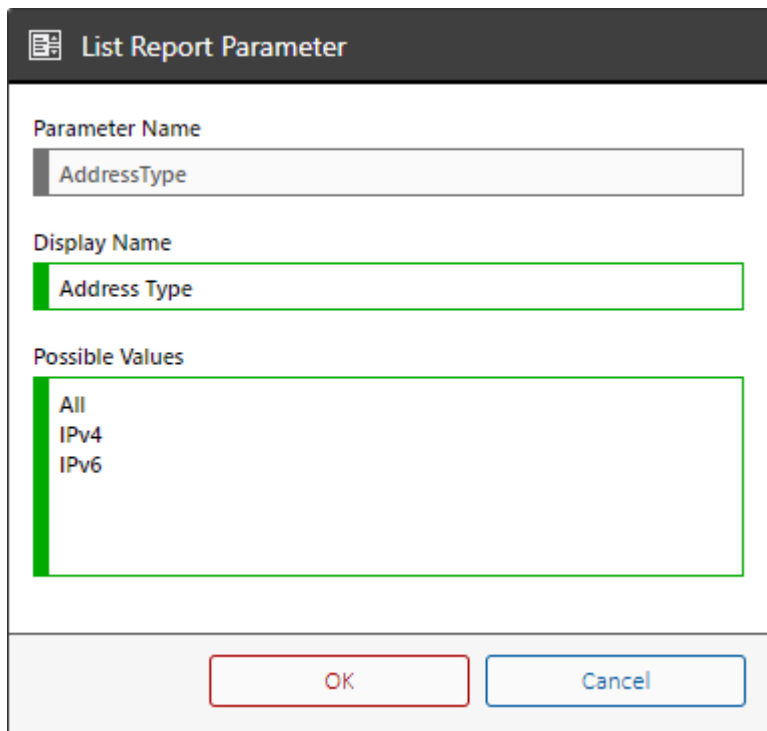
Default Value

The default numeric value to use when executing the [report](#).

Hidden

Determines whether the report parameter is hidden from the user interface, the parameter is still available to the [reporting web services API](#).

List Report Parameter



List Report Parameter

Parameter Name
AddressType

Display Name
Address Type

Possible Values
All
IPv4
IPv6

OK Cancel

The list report parameter displays a drop down list to the user when collecting the [report parameter values](#).

Display Name

The display name of the parameter displayed to the user when executing the [report](#).

Parameter Name

The name of the parameter available to the [SQL statement](#) as an [NVARCHAR](#) value.

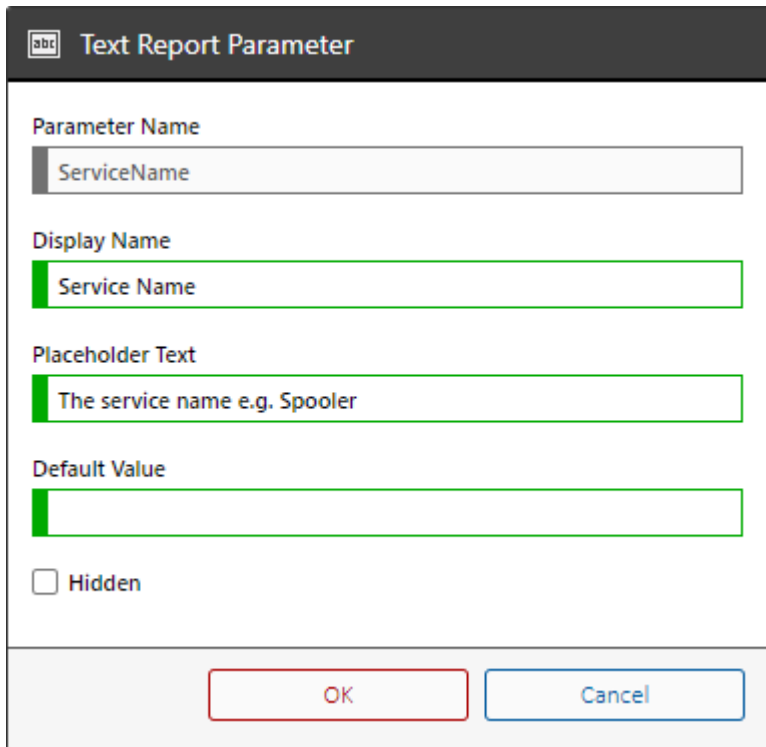
Possible Values

Determines the values that are available to the user in the following format, one per line.

Display Text, Value

If the comma is omitted and only the display text is entered this is used for both the display text and the value.

Text Report Parameter



Text Report Parameter

Parameter Name
ServiceName

Display Name
Service Name

Placeholder Text
The service name e.g. Spooler

Default Value

☐ Hidden

OK Cancel

The text report parameter displays a text box to the user when collecting the [report parameter values](#) that allows the user to enter a text value.

Display Name

The display name of the parameter displayed to the user when executing the [report](#).

Parameter Name

The name of the parameter available to the [SQL statement](#) as an [NVARCHAR](#) value.

Placeholder Text

Determines whether placeholder text is displayed in the text box when no value is entered.

Default Value

The default text value to use when executing the [report](#).

Hidden

Determines whether the report parameter is hidden from the user interface, the parameter is still available to the [reporting web services API](#).



Security

This section determines the security to apply to the report. When configured to inherit the security of the parent report folder is applied.

- ☒ Inherit security from the parent report folder
- ☐ Only system administrators can execute this report
- ☐ Evaluate the security on each result in the report
 - ☐ Prevent the user from running the report if they do not have permissions to any result
- ☐ The specified accounts can execute the report

Inherit security from the parent report folder

The security settings for this [report](#) will be inherited from the parent [report folder](#).

Only system administrators can execute this report

Only [system administrators](#) will be able to execute this [report](#).

Evaluate the security on each result in the report

Users will be able to execute the [report](#) however users will only see results to which they have [read permissions](#). The [report](#) must return the item identifier as [ItemID] for this security option to be valid. Optionally an additional item identifier can also be validated as [SecondaryItemID].

Prevent the user from running the report if they do not have permissions to any result

Users will be able to execute the [report](#) only if they have have [read permissions](#) to all returned results. The [report](#) must return the item identifier as [ItemID] for this security option to be valid. Optionally an additional item identifier can also be validated as [SecondaryItemID].

The specified accounts can execute the report

Only [system administrators](#) and the specified user accounts will be able to execute the [report](#).

Effective Security

This section determines the [security](#) which is effective for this [report](#).

This is helpful in determining where the [security settings](#) have been inherited from.

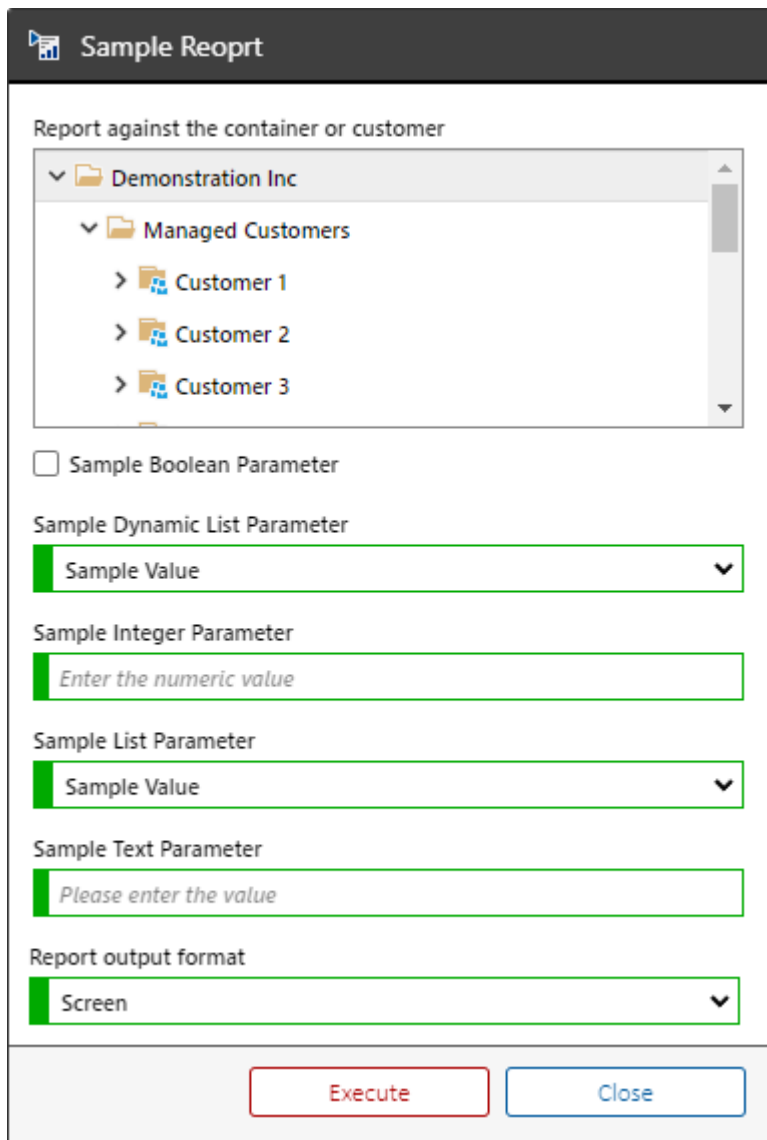
Moving Reports

To move a [report](#) simply drag and drop the report to the new [report folder](#) as a [system administrator](#).

NOTE: The ability to drag and drop reporting objects can be disabled in the [reporting settings](#).

Alternatively see the [move report](#) PowerShell sample.

Report Parameter Values



Sample Report

Report against the container or customer

- ▼ Demonstration Inc
 - ▼ Managed Customers
 - > Customer 1
 - > Customer 2
 - > Customer 3

☐ Sample Boolean Parameter

Sample Dynamic List Parameter

Sample Value ▼

Sample Integer Parameter

Enter the numeric value

Sample List Parameter

Sample Value ▼

Sample Text Parameter

Please enter the value

Report output format

Screen ▼

Execute Close

Boolean Parameter

Allows the user to select a value of checked or unchecked.

Dynamic List Parameter

Allows the user to select from a drop down list of values obtained dynamically from the database.

Integer Parameter

Allows the user to enter a [signed integer](#) value between 0 and 2147483647.

List Parameter

Allows the user to select from a drop down list of values.

Text Parameter

Allows the user to enter a text value.

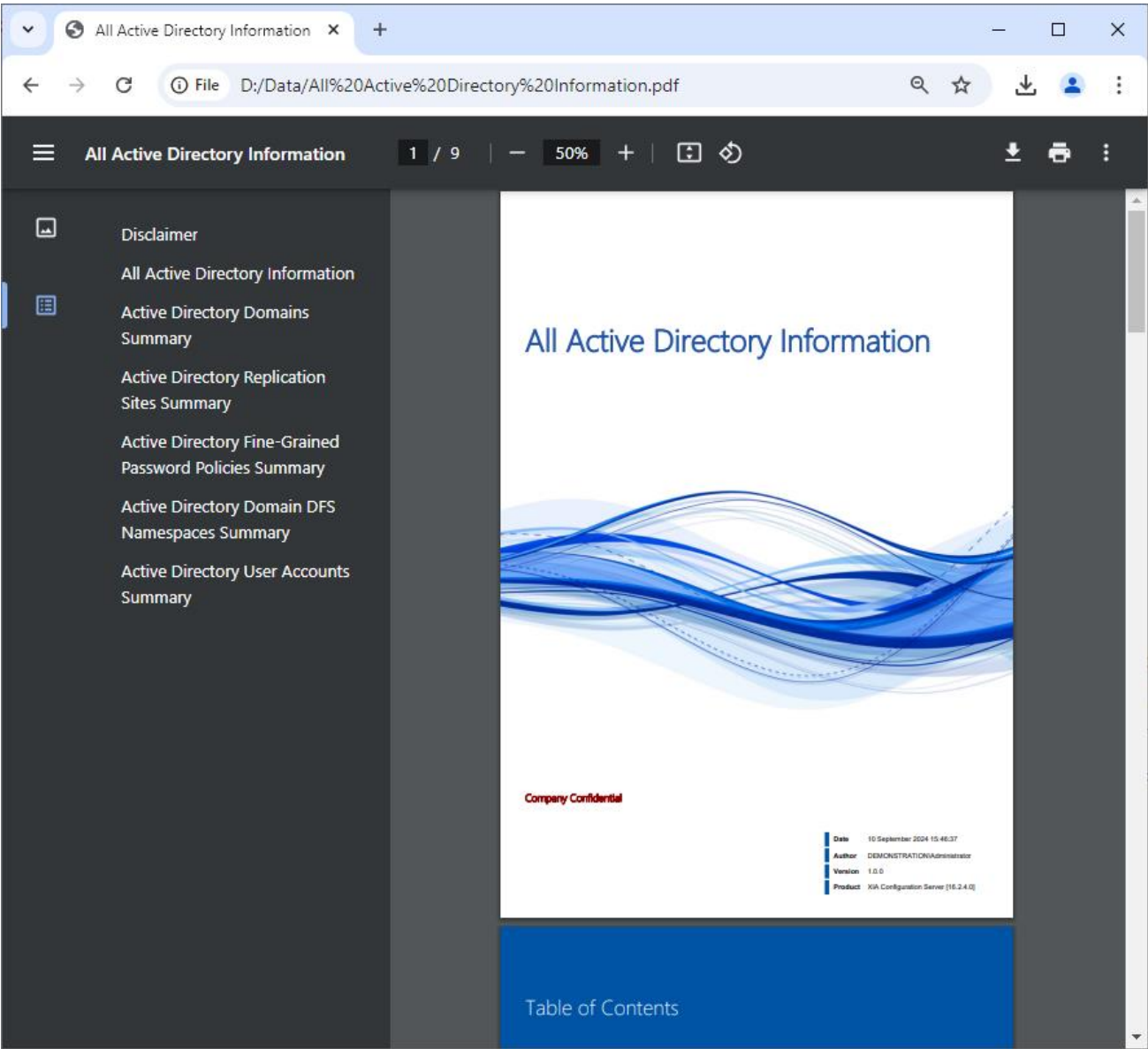
Scheduling Reports

To execute a [report](#) on a schedule you can either

- Create a [report execution scheduled task](#) within the [configuration settings](#).
- Create a [PowerShell script](#) to execute the [report](#) using the [reporting SDK](#) and schedule the execution manually.

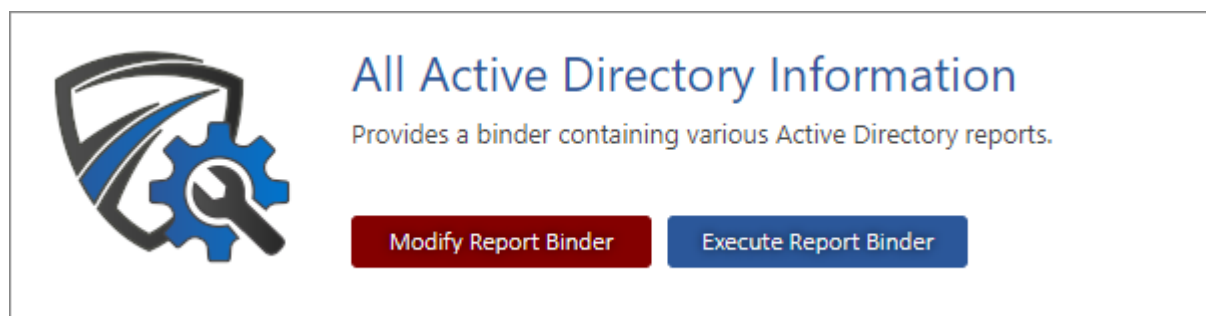
Report Binders

Report binders allow reports within XIA Configuration Server to be combined into a single PDF document.



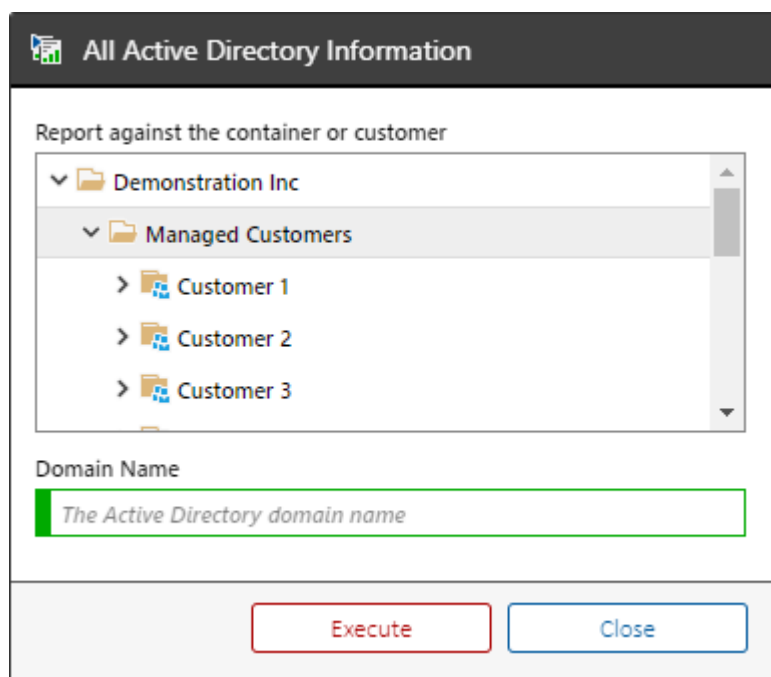
Executing Report Binders

To execute a [report binder](#) select the [report binder](#) to display the [report binder](#) information and click the *Execute Report Binder* button.



Alternatively right click the [report binder](#) and click the *Execute* context menu item.

The following dialog will be shown.



If the option is available for the [report binder](#), select the [container](#) or [customer](#) against which to execute the [report binder](#).

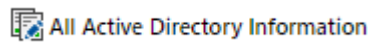
If available for the [report binder](#) enter the [parameter values](#) as required.

Click the Execute button to execute the [report binder](#) and download the PDF document.

Creating Report Binders

NOTE: Only [system administrators](#) can create [report binders](#).

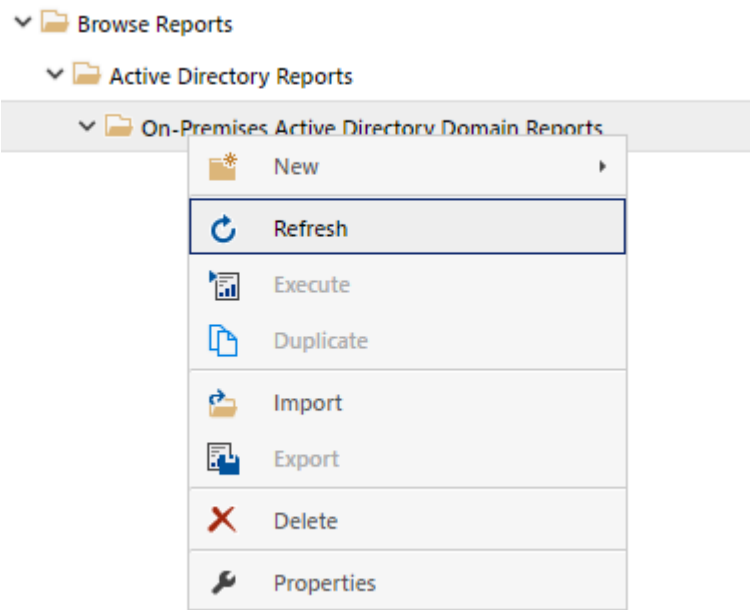
Custom [report binders](#) can be identified by the pencil icon overlay.



To create a [report binder](#) right click a [report folder](#) or the [root report folder](#) in which to create the [report binder](#), and select *New, New Report Binder*.

Complete the settings for the [report binder](#) and click *Save Report Binder*.

If the name of the [report binder](#) was changed right click the [report folder](#) in which the [report binder](#) was created and click *Refresh*.



Deleting Report Binders

To delete a [report binder](#) right click the [report binder](#) and click *Delete*.

Alternatively see the [delete report binder](#) PowerShell reporting sample.

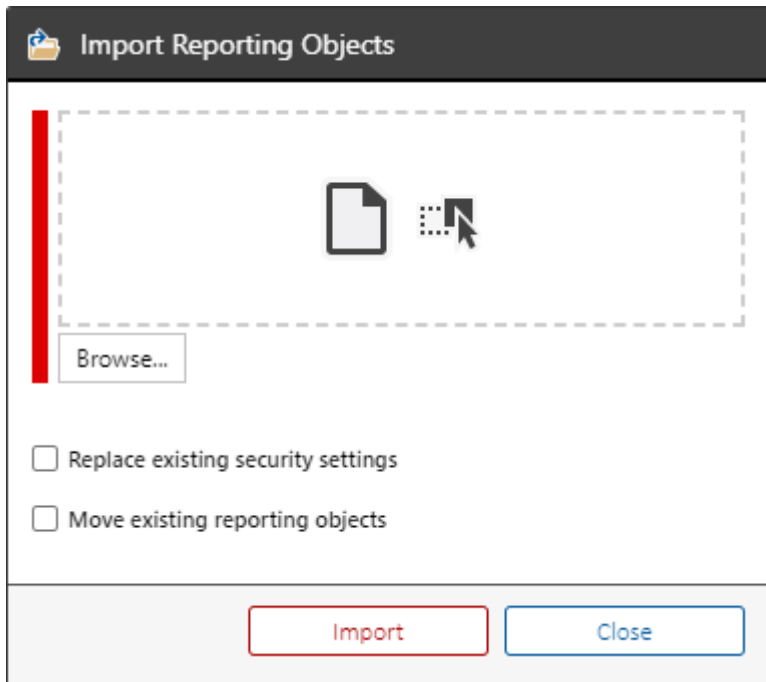
Exporting Report Binders

To export a [report binder](#) right click the [report binder](#) and click *Export*.

The [report binder](#) is downloaded to the browser in XML format.

Importing Report Binders

To import a [report binder](#) from XML right click the [report folder](#) into which you want to import the [report binder](#) and click *Import*.



Browse

Browse to the [report binder](#) file in XML format, or drop the file in the drop zone.

Replace existing security settings

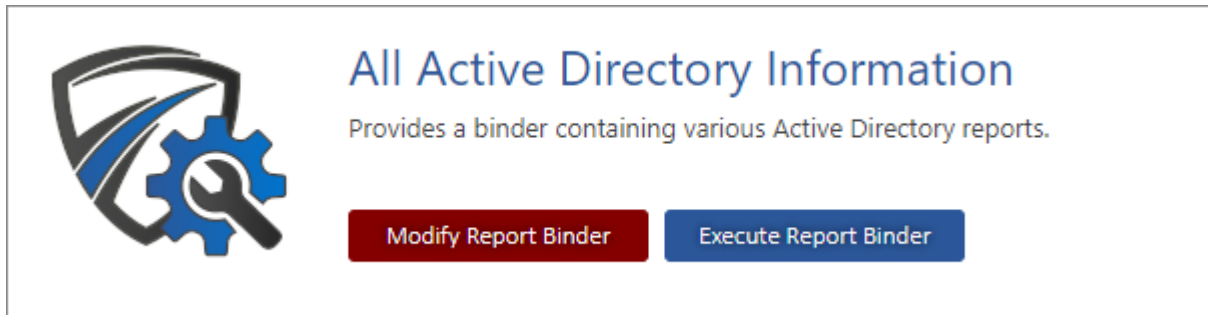
Determines whether, if the [report binder](#) already exists, that the [security settings](#) should be overwritten by the import.

Move existing reporting objects

Determines whether, if the [report binder](#) already exists, that the [report binder](#) should be [moved](#) to the currently selected [report folder](#).

Modifying Report Binders

To modify a [report binder](#) select the [report binder](#) and click the *Modify Report Binder* button.



Alternatively, right click the [report binder](#) and click *Properties*.

This displays the [general settings](#) for the [report binder](#).

General Settings

Display Name

The display name for the [report binder](#).

Report Identifier

The unique identifier of the [report binder](#) in GUID format. This property cannot be modified.

Creation Date

The date and time that the [report binder](#) was created. This property cannot be modified.

Last Modified

The date and time that the [report binder](#) was last modified. This property cannot be modified.

Parent Folder

The name of the [report folder](#) in which this [report binder](#) resides. This property cannot be modified.

Description

The description of the [report binder](#).

Reports

Reports

This determines which [reports](#) are included in the [report binder](#) including their name and unique identifier. To add a [report](#) select it from the drop down list and click the *Add Report* button.

Allow the user to select a container or customer against which to run the reports in the binder

Determines whether the user is able to select the [container](#) or [customer](#) against which to run the [reports](#) in this [report binder](#).

Report Parameters

Report Parameters

Report parameters allow the user to supply information to the **reports** being executed within the **report binder**. To automatically detect and add the **report parameters** in each of the **reports** in the **report binder** click the *Import Parameters* button.

Output

Show table of contents

Determines whether the table of contents should be shown for the [report binder](#).

Security

Inherit security from the parent report folder

The security settings for this [report binder](#) will be inherited from the parent [report folder](#).

Only system administrators can execute this report binder

Only [system administrators](#) will be able to execute the [report binder](#).

The specified accounts can execute this report binder

Only [system administrators](#) and the specified user accounts will be able to execute the [report binder](#). In addition the users must have [permissions](#) to execute each [report](#) within the [report binder](#).

Effective Security

This section determines the [security](#) which is effective for this [report binder](#).

This is helpful in determining where the [security settings](#) have been inherited from.

Moving Report Binders

To move a [report binder](#) simply drag and drop the [report binder](#) to the new [report folder](#) as a [system administrator](#).

NOTE: The ability to drag and drop reporting objects can be disabled in the [reporting settings](#).

Alternatively see the [move report binder](#) PowerShell sample.

Scheduling Report Binders

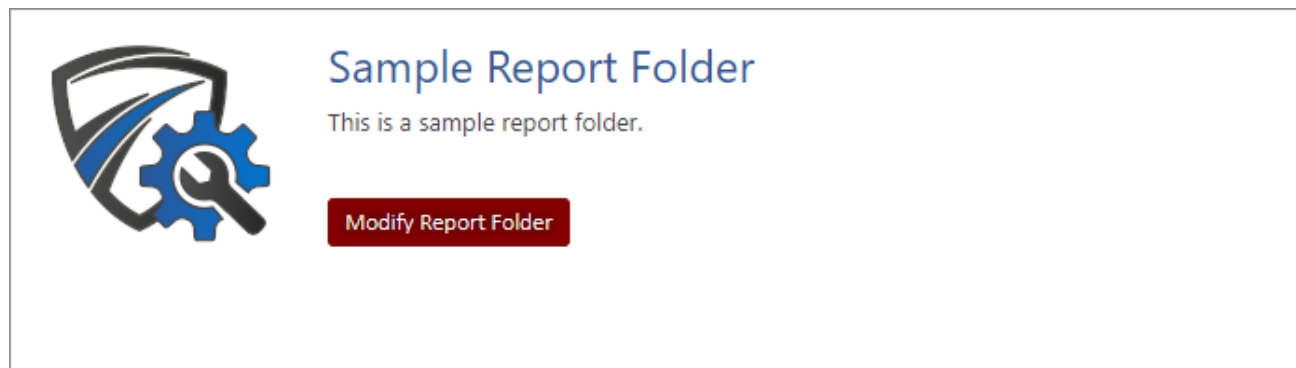
To execute a [report binder](#) on a schedule you can either

- Create a [report binder execution scheduled task](#) within the [configuration settings](#).
- Create a [PowerShell script](#) to execute the [report binder](#) using the [reporting SDK](#) and schedule the execution manually.

Report Folders

Within the [reporting system](#), [reports](#) can be organized into report folders.

Selecting a report folder displays the name and a description of the folder.



The *Modify Report Folder* button is only visible to [system administrators](#).

The [installation](#) includes a number of built-in report folders and additional report folders can be created by [system administrators](#). Custom report folders can be identified by the pencil icon overlay.

>  Sample Report Folder

Creating Report Folders

Whilst the [installation](#) includes a number of built-in [report folders](#) additional [report folders](#) can be created.

NOTE: Only [system administrators](#) can create [report folders](#).

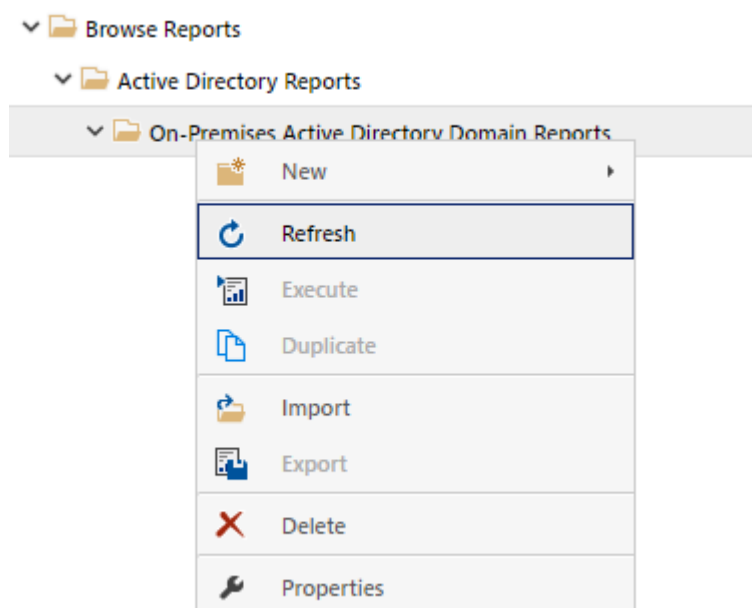
Custom [report folders](#) can be identified by the pencil icon overlay.

>  Sample Report Folder

To create a [report folder](#) right click a [report folder](#) or the [root report folder](#) in which to create the [report folder](#), and select *New, New Report Folder*.

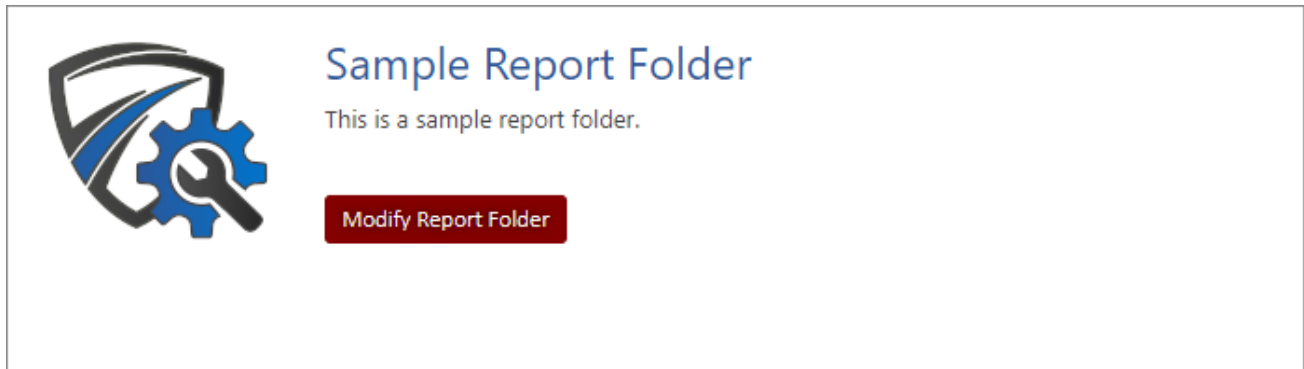
Complete the settings for the [report folder](#) and click *Save Report Folder*.

If the name of the [report folder](#) was changed right click the [report folder](#) in which the [report folder](#) was created and click *Refresh*.



Modifying Report Folders

To modify a [report folder](#) select the [report folder](#) and click the *Modify Report Folder* button.



Alternatively, right click the report folder and click *Properties*.

This displays the [general settings](#) for the [report folder](#).

General Settings

Display Name

The display name for the [report folder](#).

Report Folder Identifier

The unique identifier of the [report folder](#) in GUID format. This property cannot be modified.

Creation Date

The date and time that the [report folder](#) was created. This property cannot be modified.

Last Modified

The date and time that the [report folder](#) was last modified. This property cannot be modified.

Parent Folder

The name of the [report folder](#) in which this [report folder](#) resides. This property cannot be modified.

Description

The description of the [report folder](#).

Security

Inherit security from the parent report folder

The security settings for this [report folder](#) will be inherited from the parent [report folder](#). This setting does not apply to the [root report folder](#).

Only system administrators can execute reports and report binders in this folder

Only system administrators will be able to execute the [reports](#) and [report binders](#) in this [report folder](#), and child [report folders](#) that inherit from this [report folder](#).

Evaluate the security on each result for reports in this folder

Users will be able to execute [reports](#) in this [report folder](#), and child [report folders](#) that inherit from this [report folder](#), however users will only see results to which they have [read permissions](#). The [reports](#) must return the item identifier for this security option to be valid.

Prevent the user from running the report if they do not have permissions to any result

Users will be able to execute [reports](#) in this [report folder](#), and child [report folders](#) that inherit from this [report folder](#) only if they have [read permissions](#) to all returned results. The [reports](#) must return the item identifier for this security option to be valid.

The specified accounts can execute reports and report binders in this folder

Only [system administrators](#) and the specified user accounts will be able to execute the [reports](#) and [report binders](#) in this [report folder](#), and child [report folders](#) that inherit from this [report folder](#).

Effective Security

This section determines the [security](#) which is effective for this [report folder](#).

This is helpful in determining where the [security settings](#) have been inherited from.

Root Report Folder

The root report folder is a [report folder](#) in which all other reporting objects reside.

The root report folder has the well-known report identifier of '3f836181-2109-4f5b-a1cf-b7aa8d14c212'.

To view the properties of the root report folder, right click the *Browse Reports* item and click properties. This will display the [general settings](#). Only the [security settings](#) of the root report folder can be modified.

Moving Report Folders

To move a [report folder](#) simply drag and drop the [report folder](#) to the new [report folder](#) as a [system administrator](#). All [reports](#), [report binders](#), and [report folders](#) contained within the report folder are also moved.

NOTE: The ability to drag and drop reporting objects can be disabled in the [reporting settings](#).

Alternatively see the [move report folder](#) PowerShell sample.

Deleting Report Folders

To delete a [report folder](#) right click the [report folder](#) and click *Delete*.

NOTE: When a [report folder](#) is deleted all the [reports](#), [report binders](#), and [report folders](#) contained within it are also deleted.

Alternatively see the [delete report folder PowerShell reporting sample](#).

Scheduler Service

The scheduler service is a Windows service that polls the scheduler web service and allows the automated execution of [scheduled tasks](#) and the [import of data files](#) on the [XIA Configuration Server](#).

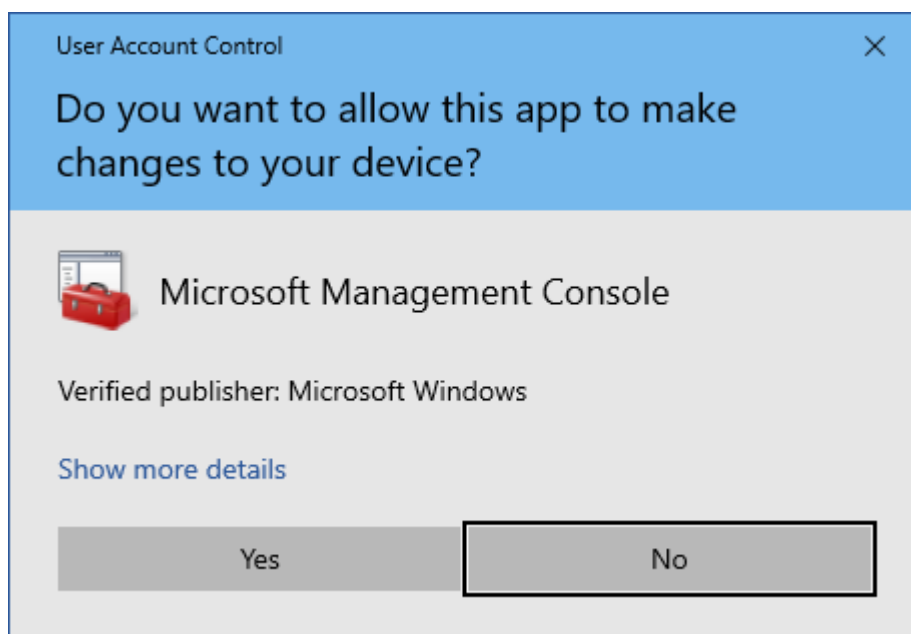
The scheduler service checks for tasks to execute every 60 seconds and can be configured with the [scheduler configuration tool](#).

Configuring Client Certificates

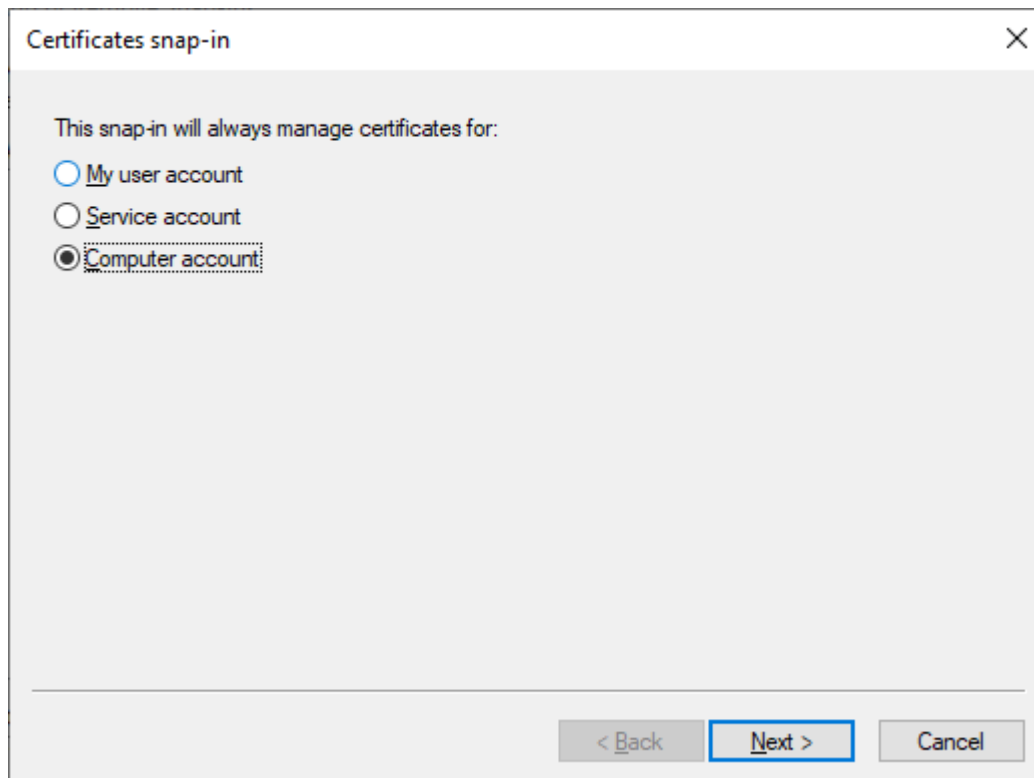
When using client certificate authentication, the [scheduler service](#) requires additional configuration. The [scheduler service](#) permits only local connections and it is possible to disable client certificate authentication for the scheduler web service only.

To enable the [scheduler service](#) to use client certificate authentication perform the following steps:

- Ensure that the server URL uses a secure (HTTPS) connection in the [scheduler registry keys](#).
- Ensure that the **Connect to server** setting on the [server settings](#) or [server upload](#) uses the appropriate HTTPS address of the server.
- Login as an **administrator** and run mmc.exe.
- Accept the user account control (UAC) prompt if required.



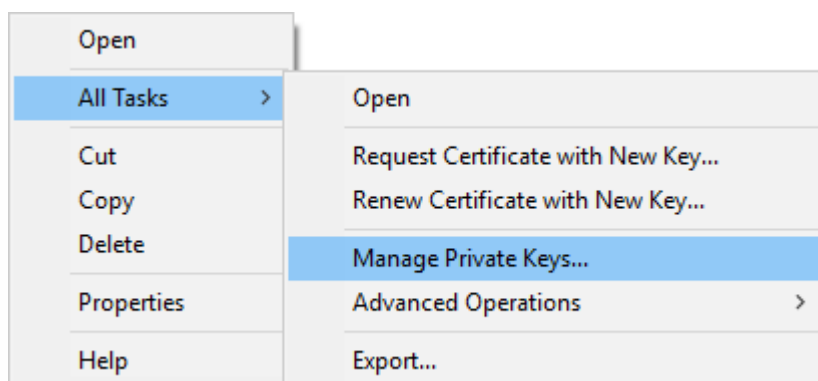
- Add the **Certificates** snap-in and ensure that **Computer account** is selected (using the Server account option is not supported)



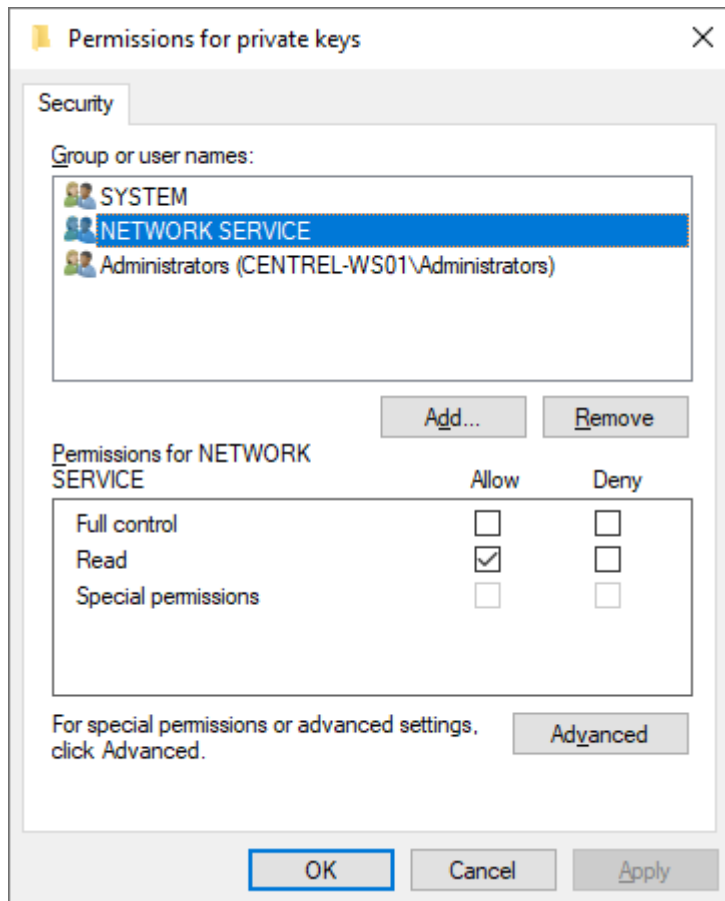
- Import the client certificate into the **Personal** folder for the computer account.
- When imported ensure that the client certificate is within the expiration date and that **Client Authentication** is one of the intended purposes

Issued To	Issued By	Expiration Date	Intended Purposes
 ClientCert	MyPersonalCA	01/01/2018	Client Authentication

- Right click the certificate and select **Manage Private Keys**



- Ensure that the [scheduler service](#) account has permissions to **Read** the key.



- Enter the key thumbprint in the **ClientCertificateThumbprint** value of the [scheduler registry keys](#), or using the [scheduler configuration tool](#).

Importing Data

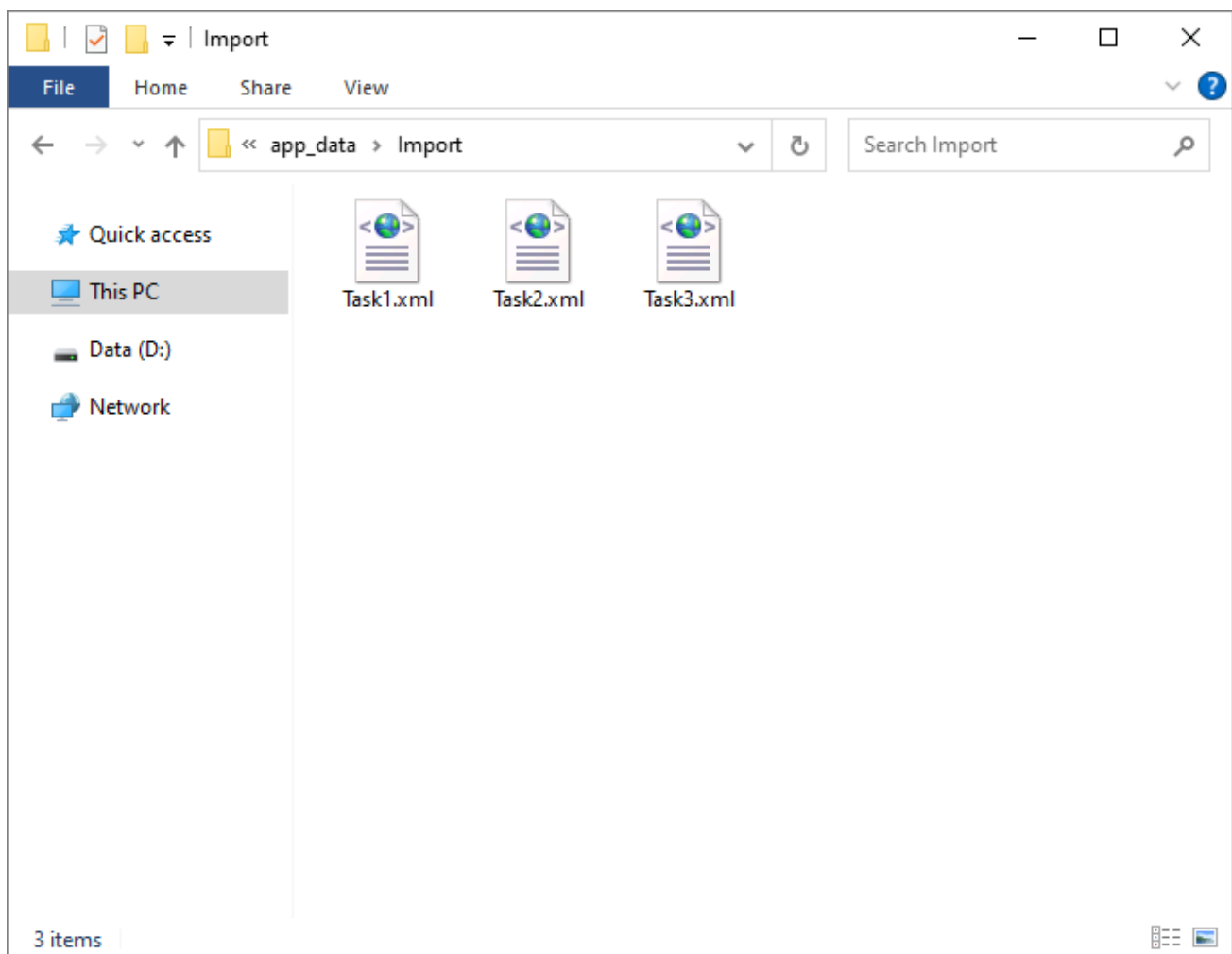
The [scheduler](#) can be configured to automatically import data from XML or ZIP files found in the import directory. These files are generated by the [XIA Configuration Client](#) when configured on the [file output](#) tab of the [scan profile](#) settings.

This functionality can be useful when the [XIA Configuration Client](#) cannot send data directly to the [XIA Configuration Server](#) because of firewalls, or other security constraints.

The [automatically import data files found in the import directory](#) setting must be enabled in the [import engine settings](#).

The import directory can be found by default at the following location:

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Server\app_data\Import



When importing data where the ZIP file has been encrypted, ensure that the correct ZIP password has been entered in the [import engine settings](#). Otherwise, the [scheduler](#) will fail and an event log error message will be logged to the [event log](#).

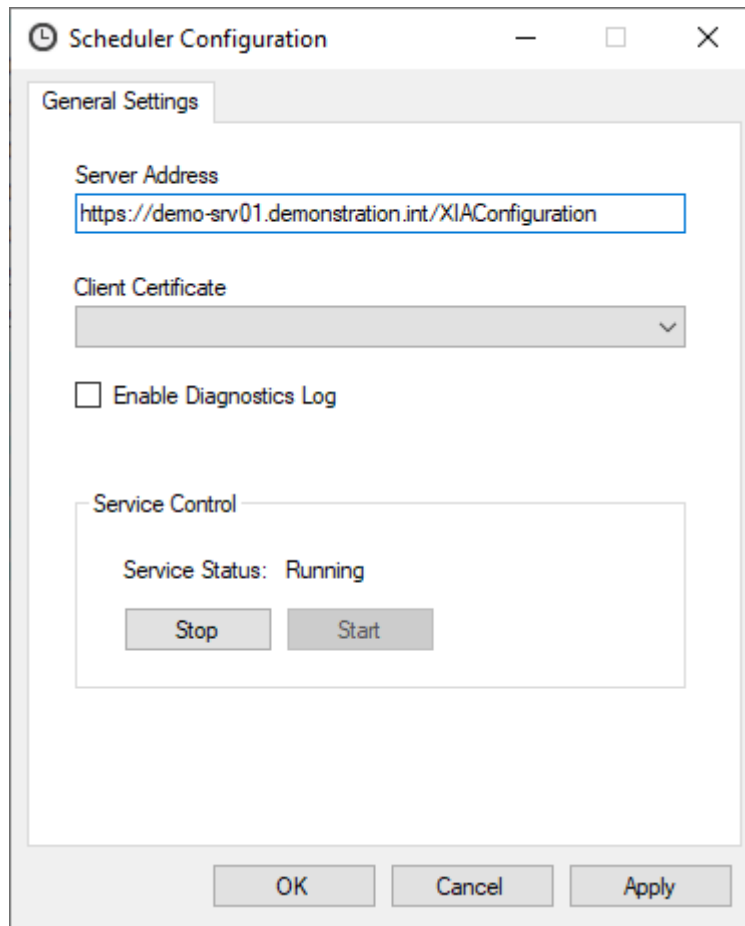
NOTE: Both data files and ZIP files must be in the root of the import directory as subdirectories will not be read.

Scheduler Configuration Tool

The scheduler configuration tool allows for the simple configuration of the [scheduler service](#).

Installation Directory\XIA Configuration

Scheduler\CENTREL.XIA.Configuration.Server.SchedulerUI.exe



Server Address

The address of the XIA Configuration Server installation.

Client Certificate

Determines which client certificate to use for client certificate authentication, if required. Only certificates that support client authentication and have the private key available will be listed. For more information see the [configuring client certificates](#) section.

Enable Diagnostics Log

Determines whether the diagnostics log should be enabled for the scheduler.

Service Control

Provides information about the state of the [service](#), and allows the service to be stopped and started.

Scheduler Registry Keys

The following registry keys are used by the [scheduler service](#) and are provided for reference only. Please use the [scheduler configuration tool](#) to configure the [scheduler service](#).

URL

This stores the URL used by the scheduler to access XIA Configuration server. By default, this is `http://localhost/xiaconfiguration`, however, it can be modified if the server is installed at a different URL.

`HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Server\Setup\URL`

ClientCertificateThumbprint

The thumbprint of the client authentication to use when connecting to the XIA Configuration Server. For more information see the [configuring client certificates](#) section.

`HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Scheduler`

EnableTrace

This value determines whether trace logging should be enabled by the scheduler service. When set to zero, trace is disabled. When set to "1", trace is enabled.

`HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Scheduler\EnableTrace`

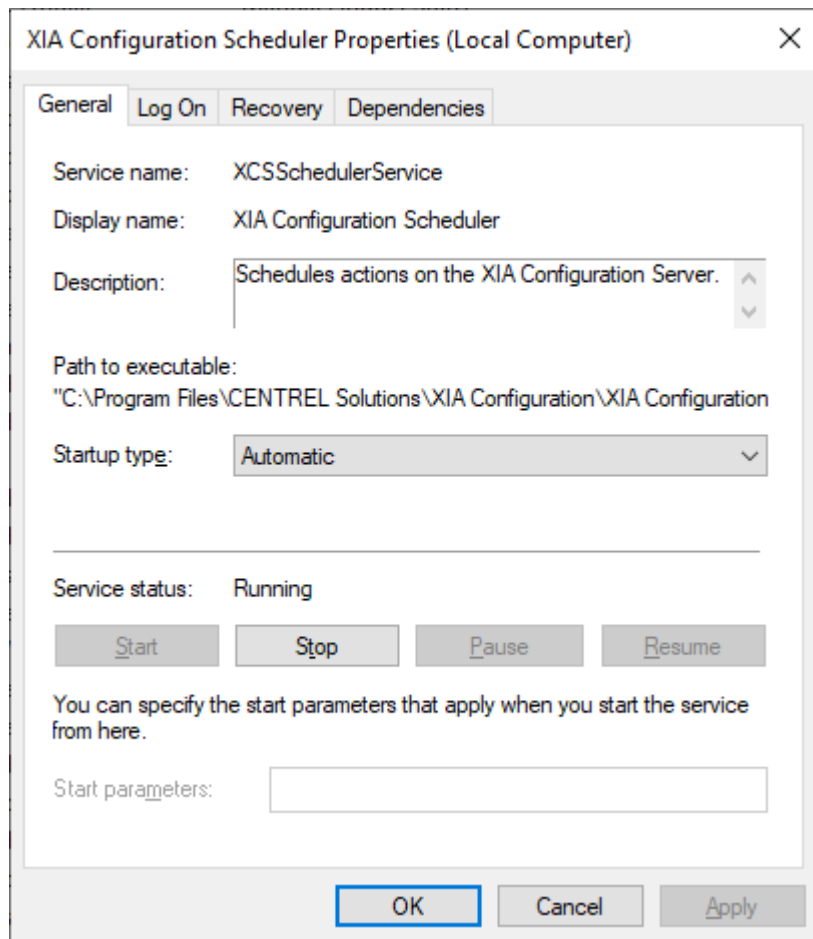
InstallDirectory

This value determines the installation directory of the scheduler service.

`HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Scheduler\InstallDirectory`

Scheduler Service Details

The service can be accessed through the Windows services management console.



- The service runs as the same account used to host the [XIA Configuration Server](#) - by default, this is the [Network Service](#) account.
- The service polls the scheduler access web service at `/webservice/scheduler/scheduleraccess.asmx`, this web service is for internal use and can only be accessed locally.

SDK

XIA Configuration supports the ability to extend the system using the following SDKs.

Server Development

[Web Services API](#)

Client Development

[Dynamic Agent Plugins](#)

Web Services SDK

The following development environments are supported:

- Microsoft [Visual Studio](#) 2010 and above. using [C#.NET](#) or [VB.NET](#) languages.
- Microsoft [PowerShell](#) or [PowerShell Integrated Scripting Environment \(ISE\)](#).

The following web services are integrated into [XIA Configuration Server](#).

Administration Web Service

The [administration web service](#) provides functions such as access to the [event log](#), and [configuration settings](#).

Client Access Web Service

The client access web service is used by the [XIA Configuration Client](#) to upload data and for [automatic updates](#). This web service is for **internal use** only and should not be accessed by the SDK.

Configuration Web Service

The [configuration web service](#) provides the ability to access and update [items](#).

Reporting Web Service

The [reporting web service](#) provides access to the [reporting system](#) including the ability to access, update, and delete [reports](#), [report folders](#), and [report binders](#).

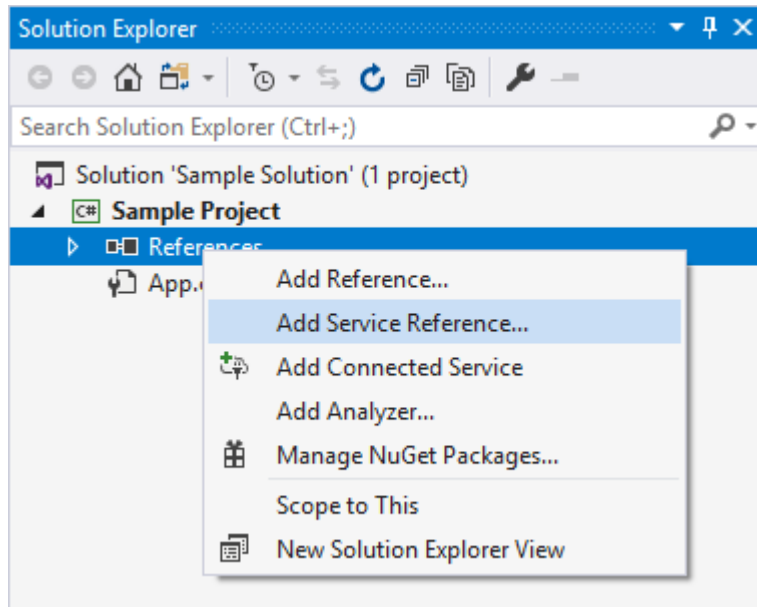
Scheduler Access Web Service

The scheduler access web service is used by the [scheduler service](#) to perform automated actions such as [importing data](#). This web service is for **internal use** only and should not be accessed by the SDK.

Using Visual Studio

To access the [web services SDK](#) from Microsoft [Visual Studio](#) perform the following steps

- Create a new project in [Visual Studio](#).
- Within the solution explorer, right click the project and click *Add Service Reference*.



- Enter the address for the web service - for example <http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx>. For more information see the [web service settings](#) configuration section.

Add Service Reference ? X

To see a list of available services on a specific server, enter a service URL and click Go. To browse for available services, click Discover.

Address:

Services: **Operations:**

Namespace:

- Enter the namespace - for example "XiaWebService", and click OK.
- Within the application the follow configures the end point address, and uses integrated Windows authentication for the connection.

```

EndpointAddress remoteAddress = new
EndpointAddress("http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx");
BasicHttpBinding binding = new
BasicHttpBinding(BasicHttpSecurityMode.TransportCredentialOnly);
binding.Security.Transport.ClientCredentialType = HttpClientCredentialType.Windows;
binding.MaxReceivedMessageSize = 10485760;
XiaWebService.XiaConfigurationWebServiceSoapClient service = new
XiaWebService.XiaConfigurationWebServiceSoapClient(binding, remoteAddress);
string username = (service.GET_AuthenticatedUserName());

```

Using Windows PowerShell

[Windows PowerShell](#) is a command-line shell and scripting language designed especially for system administration. The following describes how to access [XIA Configuration Server](#) from [PowerShell](#).

Configuration Web Service

The [configuration web service](#) provides the ability to access and update [items](#) and related information.

Administration Web Service

The [administration web service](#) provides functions such as access to the [event log](#), and [configuration settings](#).

Reporting Web Service

The [reporting web service](#) provides access to the [reporting](#) system including the ability to [modify](#) and [execute reports](#) and [report binders](#).

Configuration Web Service

The configuration [web service](#) provides the ability to access and update [items](#).

```
# Connect to the configuration web service.
Clear-Host;
$url = "http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx";
Write-Host "Connecting to standard web service at" $url;
$xia = New-WebServiceProxy -UseDefaultCredential -Uri $url;
Write-Host "Connected as" $xia.GET_AuthenticatedUserName();

# To use specific credentials use the Get-Credential cmdlet.
$creds = Get-Credential;
$xia = New-WebServiceProxy -Uri $url -Credential $creds;
```

Accessing Items

[Items](#) can be created, accessed, and updated with the [configuration web service](#).

Create Item

Typically new [items](#) are created automatically by the [XIA Configuration Client](#), however it is also possible to [manually create](#) new [items](#).

- Connect to the [configuration web service](#).
- Specify the name of the item to create.
- Specify the [type](#) of [item](#) to create.
- Specify the identifier of the [container](#) or [customer](#) in which to create the [item](#).
- The user must have [write permissions](#) to the [container](#) or [customer](#) in which the item is being created.

Code Sample

```
# Create the new item.  
$itemID = $xia.DO_CreateItem("DEMO-PC01", "WindowsPC", 1000);  
Write-Host "Created item $($itemID)";
```

Get Item

Get an existing [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the required [item](#).
- Specific code can be written based on the [item](#) type.
- The user must have [read permissions](#) to the [item](#).

Code Sample

```
# Get the item.
$item = $xia.GET_Item(1234, 0);
Write-Host $item.Name;
Write-Host $item.TypeDisplayName;

# windows server specific example.
if ($item.Type -ne "WindowsServer") { return; }
foreach($service in $item.WindowsServices.WindowsService)
{
    Write-Host "$($service.Name) [$($service.StateString)]";
}
```

Move Item

Moves an existing [item](#) to a different [container](#) or [customer](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) to move.
- Specify the unique identifier of the [container](#) or [customer](#) to which the item is to be moved.
- The user must have [write permissions](#) to the [item](#) and the destination [container](#) or [customer](#).

Code Sample

```
# Move the item to a different customer or container.  
$xia.DO_MoveItem(1234, 5678);
```

Move Item Location

Moves an existing [item](#) to a different room, rack, or location.

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) to move.
- Specify the unique identifier of the room, rack, or location which the item is to be moved.
- The [item](#) must support locations, and the destination must be of an appropriate [item](#) type.
- The user must have [write permissions](#) to the [item](#) and the destination room, rack, or location.

Code Sample

```
# Move the item to a new location.  
$xia.DO_MoveItemLocation(1234, 5678);
```

Update Item

Update an existing [item](#).

- Connect to the [configuration web service](#).
- Set the unique identifier of the required [item](#).
- Specific code can be written based on the [item](#) type.
- The item must be [checked out](#) and [checked back in](#).
- The user must have [write permissions](#) to the [item](#).

Code Sample

```
# Get the existing item.
$item = $xia.GET_Item(1234, 0);

# Check out the item.
$xia.DO_CheckOutItem($item.ItemID);

# Modify the item.
$item.AssetTag.Overridden = $true;
$item.AssetTag.Value = "A12345";

# Update the item.
$item.VersionDescription = "Updated the asset tag";
$xia.SET_Item($item);

# Check in the item back in.
$xia.DO_CheckInItem($item.ItemID);
```

Valid Item Types

When performing actions such as [creating items](#) it is necessary to supply the [item type](#), the following code displays how to determine the valid [item types](#) supported by the system.

- Connect to the [configuration web service](#).

Code Sample

```
# Get the valid item types.
$itemTypes = $xia.GET_ValidItemTypes();
foreach ($itemType in $itemTypes)
{
    Write-Host $itemType;
}
```

Check Out (Users)

When [items](#) are edited by a user, they are automatically [checked out](#) so that they cannot be edited by other users.

The information in this section refers to code that can be executed by all users. Additional methods can be accessed by [system administrators](#), more information can be found in the [check out \(system administrators\)](#) section.

Check In Item

Once an [item](#) has been checked out and updated, it should be [checked in](#) again.

- Connect to the [configuration web service](#).
- Set the unique identifier of the required [item](#).

Code Sample

```
# Check in the item.  
$itemIdentifier = 1234;  
$xia.DO_CheckInItem($itemIdentifier);
```

Check Out Item

An [item](#) must be [checked out](#) before it can be modified.

- Connect to the [configuration web service](#).

Code Sample

```
# Check out the item.  
$itemIdentifier = 1234;  
$xia.DO_CheckOutItem($itemIdentifier);
```

Get Check Out Information

The following example gets the [check out](#) information for the specified [item](#).

- Connect to the [configuration web service](#).

Code Sample

```
# Get the check out information for the specified item.
$itemIdentifier = 1234;
$checkOutInformation = $xia.GET_CheckOutInformation($itemIdentifier);
if ($checkOutInformation.IsCheckedOut -eq $false) { Write-Host "The item is not checked out."; return; }
Write-Host "The item was checked out on $($checkOutInformation.CheckOutDate) by $($checkOutInformation.Username).";
```

Get Checked Out Items

The following example gets the unique identifiers of the [items](#) that are currently [checked out](#) by the current user.

- Connect to the [configuration web service](#).

Code Sample

```
# Gets the identifiers of the items that are checked out by the current user.
$identifiers = $xia.GET_CheckedOutItemIdentifiers();
foreach ($identifier in $identifiers)
{
    Write-Host $identifier;
}
```

Comparison

This allows the comparison of any two [items](#) of the same [type](#), or two [versions](#) of the same [item](#), and displays the differences.

Compare Items

This allows the comparison of any two [items](#) of the same [type](#), or two [versions](#) of the same [item](#), and displays the differences in a PDF document.

- Connect to the [configuration web service](#).
- Get the appropriate version of the required item.

Code Sample

```
# Get the source and destination items.
$source = $xia.GET_Item(1234, 0);
$destination = $xia.GET_Item(1234, 0);

# Perform the comparison.
Write-Host "Performing comparison";
$data = $xia.Get_ItemComparisonPdf($source, $destination);

# Write the PDF to a file
Write-Host "Saving PDF file";
$filename = "$env:temp\sample.pdf";
[IO.File]::WriteAllBytes($filename, $data);
[System.Diagnostics.Process]::Start($filename);
```

Custom Attributes

Custom attributes store additional information for [items](#), and are displayed in [custom sections](#).

Get Custom Attributes

Custom attributes are stored as part of an [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the required [item](#).
- The user must have [read permissions](#) to the [item](#).

Code Sample

```
# Get the item.
$item = $xia.GET_Item(1234, 0);

# Display the custom attributes.
foreach ($customAttribute in $item.CustomAttributes.CustomAttribute)
{
    Write-Host $customAttribute.DisplayName;
    Write-Host $customAttribute.Identifier;
    Write-Host $customAttribute.DisplayValue;
}
```

Modify Custom Attributes

Custom attributes are stored as part of an [item](#).

- Connect to the [configuration web service](#).
- Set the unique identifiers of the required [item](#), [custom attribute](#), and the new values to assign.
- The example uses the AddCustomAttribute helper method to automatically create and add the custom attribute of the appropriate type, or update the existing custom attribute with the specified identifier.
- The item must be [checked out](#) and [checked back in](#).
- The user must have [write permissions](#) to the [item](#).

Code Sample

```
# Set the variables.
$itemID = 1234;

# Get the item.
$item = $xia.GET_Item($itemID, 0);

# Get the custom attributes.
$customAttributes = $item.CustomAttributes;

# Check out the item.
$xia.DO_CheckOutItem($itemID);

# Add or update the specified custom attribute.
$xia.DO_AddCustomAttribute([ref]$customAttributes, [GUID]"00b0c5f6-800a-4866-be2a-75927c50fe53", "Enhanced");
$xia.DO_AddCustomAttribute([ref]$customAttributes, [GUID]"a85b928e-bad3-4a09-84ab-ad2ff625faf2", "A12345");

# Update the item.
$item.CustomAttributes = $customAttributes;
$item.VersionDescription = "Updated custom attributes";
$xia.SET_Item($item);

# Check in the item back in.
$xia.DO_CheckInItem($itemID);
```

Decommissioning

All [items](#) support the ability to be [decommissioned](#) which allows you to maintain information about systems that are no longer in use within your organization.

Decommission Item

Decommission an **item** that is no longer is no longer in use within your organization.

- Connect to the [configuration web service](#).
- Set the unique identifier of the **item** to **decommission**.
- Set the description of the **decommissioning** action. This will be recorded in the [event log](#), and displayed in the **item**.
- The **item** must not be **checked out**.

Code Sample

```
# Decommission the item.  
$xia.DO-DecommissionItem(2685, "Change record 12345");
```

Recommission Item

Recommission an [item](#) that has previously been [decommissioned](#).

- Connect to the [configuration web service](#).
- Set the unique identifier of the [item](#) to [recommission](#).
- Set the description of the [recommissioning](#) action. This will be recorded in the [event log](#).

Code Sample

```
# Recommission the item.  
$xia.DO_RecommissionItem(2685, "Change record 12345");
```

Get Decommissioning Information

To determine if and when an [item](#) has been [decommissioned](#) get the [decommissioning information](#) for that [item](#).

- Connect to the [configuration web service](#).
- Set the unique identifier of the [item](#) for which to obtain the [decommissioning information](#).

Code Sample

```
# Get the decommissioning information.
$information = $xia.GET_DecommissioningInformation(1234);

# Display the decommissioning information.
write-Host "Decommissioned: $($information.IsDecommissioned)";
if (!$information.IsDecommissioned) { return; }
write-Host " Date: $($information.DecommissionDate)";
write-Host " By: $($information.DecommissionAccountName)";
write-Host " Reason: $($information.DecommissionDescription)";
```

Deleted Items

When [items](#) are deleted they are moved to the [deleted items](#) folder. [System administrators](#) are able to restore [deleted items](#), or permanently delete them.

Delete Item

Delete an [item](#) that is no longer is no longer required.

When [items](#) are deleted they are moved to the [deleted items](#) folder.

- Connect to the [configuration web service](#).
- Set the unique identifier of the [item](#) to be [deleted](#).
- The user must have the [delete permission](#) for the [item](#).
- If the [item](#) is a [container](#) or [customer](#) all child [item](#) are also deleted.

Code Sample

```
# Delete the item.  
$xia.DO_DeleteItem(1234);
```

Find Deleted Items

System administrators are able to find deleted item.

- Connect to the [configuration web service](#).
- This functionality is also available using the [advanced search](#).

Code Sample

```
# Find deleted items.
$results = $xia.DO_FindDeletedItems();
foreach ($result in $results.SearchResult)
{
    Write-Host "$($result.name) [$($result.ItemID)]";
}
```

Permanently Delete Item

System administrators are able to permanently delete a [deleted item](#) that is no longer required.

- Connect to the [configuration web service](#).
- Set the unique identifier of the [deleted item](#) to be permanently deleted.
- The item must already be deleted before it can be permanently deleted.
- This action cannot be undone.

Code Sample

```
# Permanently deletes the deleted item.  
$xia.DO_PermanentlyDeleteItem(37584);
```

Restore Item

System administrators are able to restore deleted items.

- Connect to the [configuration web service](#).
- Set the unique identifier of the [deleted item](#) to restore.

Code Sample

```
# Restores the deleted item.  
$xia.DO_RestoreItem(1234);
```

Documentation Output

All [items](#) can be [written to PDF documents](#) which can be read using [Adobe Acrobat Reader](#), or other compatible products.

There are two SDK methods that can be used to [generate PDF documents](#)

- [Generate PDF Basic](#)
- [Generate PDF Advanced](#)

All [items](#) can be [written to XML](#). This can be achieved using the following SDK method.

- [Generate XML Output](#)

Generate PDF Basic

The basic method allows the current version of the specified [item](#) to be written to a PDF using the default options.

- Connect to the [configuration web service](#).
- Specify the identifier of the [item](#).

Code Sample

```
# Generate the PDF as a byte array.
$data = $xia.GET_PdfOutputBasic(1234);

# Write the PDF to a file.
write-Host "Saving PDF file...";
$filename = "$env:temp\sample.pdf";
[IO.File]::WriteAllBytes($filename, $data);

# Display the file.
[System.Diagnostics.Process]::Start($filename);
```

Generate PDF Advanced

The advanced method allows the [version](#) of the [item](#) to be specified, as well as the PDF output options.

- Connect to the [configuration web service](#).
- Configure the options as required.
- Specify the identifier of the [item](#).
- Specify the [version](#) of the [item](#).

Code Sample

```
# Get the current default options.
$pdfOptions = $xia.GET_CurrentPdfOptions();

# Configure the options.
$pdfOptions.ShowRelationships = $false;
$pdfOptions.Author = "Sample Author";

# Set a password.
$encryptedPassword = $xia.GET_EncryptedPassword("password");
$pdfOptions.Password.EncryptedPassword = $encryptedPassword;

# Generate the current version of the item PDF as a byte array.
$data = $xia.GET_PdfOutput(1000, 0, $pdfOptions);

# Write the PDF to a file.
Write-Host "Saving PDF file...";
$filename = "$env:temp\sample.pdf";
[IO.File]::WriteAllBytes($filename, $data);

# Display the file.
[System.Diagnostics.Process]::Start($filename);
```

Generate XML Output

The method allows the generation of XML for the [version](#) of the [item](#) specified.

- Connect to the [configuration web service](#).
- Specify the identifier and [version](#) of the [item](#).

Code Sample

```
# Get the XML for the item.
$xml = $xia.GET_XmlOutput(1234,0);

# Write the XML to a file.
write-Host "Saving XML file...";
$filename = "$env:temp\sample.xml";
[IO.File]::WriteAllText($filename, $xml);

# Open the file.
[System.Diagnostics.Process]::Start($filename);
```

Password Lists

Password lists can be created, accessed, and updated with the [configuration web service](#).

Get Password List

Get an existing [password list item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the required [password list](#).
- The user must have [read permissions](#) to the [item](#), the user must also have the [decrypt password lists server permission](#).

Code Sample

```
# Get the item.
$item = $xia.GET_Item(1234, 0);

# Display the password entries.
foreach($passwordEntry in $item.PasswordEntries.PasswordEntry)
{
    Write-Host $passwordEntry.DisplayName;
    Write-Host "Description: $($passwordEntry.Description)";
    Write-Host "Entry Type: $($passwordEntry.EntryTypeString)";
    Write-Host "Account Name: $($passwordEntry.AccountName)";
    Write-Host "Password: $($passwordEntry.PasswordPlainText)";
    Write-Host;
}
```

Custom Password List Entry Types

When using [custom password list entry types](#) the entry type above will be displayed as "Custom". To display the full display name of the custom type replace this line with the following.

```
Write-Host "Entry Type: $($xia.GET_PasswordListEntryTypeDisplayName($passwordEntry))";
```

Update Password List

Update an existing [password list](#).

- Connect to the [configuration web service](#).
- Set the unique identifier of the required [password list](#).
- Add a new password entry to the [password list](#).
- The item must be [checked out](#) and [checked back in](#).
- The user must have [write permissions](#) to the [item](#).
- The password should be set using the PasswordPlainText property. The system will automatically encrypt the password.

Code Sample

```
# Get the existing item.
$item = $xia.GET_Item(1234, 0);

# Check out the item.
$xia.DO_CheckOutItem($item.ItemID);

# Create a new password entry entry.
$passwordEntry = New-Object "$($xia.GetType().Namespace).PasswordListEntry";
$passwordEntry.DisplayName = "Sample Password Entry";
$passwordEntry.Description = "This is a sample password entry.";
$passwordEntry.EntryType = "windowsLocalUser";
$passwordEntry.AccountName = "DEMO-SRV01\Administrator";
$passwordEntry.PasswordPlainText = "Passw0rd!!&";
$item.PasswordEntries.PasswordEntry += $passwordEntry;

# Update the item.
$xia.SET_Item($item);

# Check in the item back in.
$xia.DO_CheckInItem($item.ItemID);
```

Custom Password List Entry Types

When using [custom password list entry types](#) the entry type should be set to "Custom", and the definition identifier set to that configured for the desired [custom password list entry types](#).

```
$passwordEntry.EntryType = "Custom";
$passwordEntry.DefinitionIdentifier = "3d9fa8c1-17cc-4f55-a1a1-fce065710e0d";
```

Relationships

Relationships are either automatically detected, or manually created, between an [item](#) and other [items](#) within the system.

Get Manual Relationships

The method gets the manual [relationships](#) between an [item](#) and other [items](#) within the system.

- Connect to the [configuration web service](#).
- Specify the identifier of the [item](#).

Code Sample

```
# Get the manual relationships.
$manualRelationships = $xia.GET_ManualRelationships(1234);

# Display manual relationship information.
foreach ($manualRelationship in $manualRelationships.ManualRelationship)
{
    Write-Host $manualRelationship.TargetItemID;
    Write-Host $manualRelationship.RelationshipType;
}
```

Get Relationships

The method gets the [relationships](#) between an [item](#) and other [items](#) within the system.

- Connect to the [configuration web service](#).
- Specify the identifier of the [item](#).

Code Sample

```
# Get the relationships.
$relationships = $xia.GET_Relationships(1234);

# Display relationship information.
foreach ($relationship in $relationships.Relationship)
{
    Write-Host "$($relationship.TargetName) [$($relationship.TargetItemID)]";
    Write-Host $relationship.DirectionString;
    Write-Host $relationship.RelationshipTypeString;
    Write-Host;
}
```

Get Relationship Type Referenced

The method determines whether the [custom relationship type](#) with the specified identifier has been referenced by any [items](#).

- Connect to the [configuration web service](#).
- Specify the identifier of the [custom relationship type](#).

Code Sample

```
# The unique identifier of the custom relationship type.  
$definitionIdentifier = "f707b4a9-ce3c-447a-921a-b1d72769be14";  
  
# Update the relationships.  
$isReferenced = $xia.GET_IsRelationshipTypeReferenced($definitionIdentifier);  
Write-Host $isReferenced;
```

Update Manual Relationships (Custom Relationships)

The method updates the manually created [relationships](#) between an [item](#) and other [items](#), adding a new [custom relationship](#).

- Connect to the [configuration web service](#).
- Specify the identifier of the [item](#).
- Specify the identifier of the target [item](#).
- Specify the identifier of the [custom relationship type definition identifier](#).

Code Sample

```
# Set the variables.
$itemID = 1234;
$targetItemID = 5678;
$relationshipDefinitionIdentifier = "f707b4a9-ce3c-447a-921a-b1d72769be14";

# Get the manual relationships.
$manualRelationships = $xia.GET_ManualRelationships($itemID);

# Create a new relationship.
$manualRelationship = New-Object "($xia.GetType().Namespace).ManualRelationship";
$manualRelationship.CreateInboundConnection = $false;
$manualRelationship.DefinitionIdentifier = $relationshipDefinitionIdentifier;
$manualRelationship.RelationshipType = "Custom";
$manualRelationship.TargetItemID = $targetItemID;

# Add the manual relationship to the collection.
$manualRelationships.ManualRelationship += $manualRelationship;

# Update the relationships.
$xia.SET_ManualRelationships($itemID, $manualRelationships);
```

Update Manual Relationships (System Relationships)

The method updates the manually created [relationships](#) between an [item](#) and other [items](#), adding a new [system managed relationship](#).

- Connect to the [configuration web service](#).
- Specify the identifier of the [item](#).
- Specify the identifier of the target [item](#).
- Specify a valid [system relationship type](#).

Code Sample

```
# Set the variables.
$itemID = 1234;
$targetItemID = 5678;
$relationshipType = "IsSupportedBy";

# Get the manual relationships.
$manualRelationships = $xia.GET_ManualRelationships($itemID);

# Create a new relationship.
$manualRelationship = New-Object "$($xia.GetType().Namespace).ManualRelationship";
$manualRelationship.CreateInboundConnection = $false;
$manualRelationship.RelationshipType = $relationshipType;
$manualRelationship.TargetItemID = $targetItemID;

# Add the manual relationship to the collection.
$manualRelationships.ManualRelationship += $manualRelationship;

# Update the relationships.
$xia.SET_ManualRelationships($itemID, $manualRelationships);
```

Valid System Relationship Types

The following code displays how to determine the valid system managed [relationship types](#) supported by the system.

- Connect to the [configuration web service](#).

Code Sample

```
# Get the valid system managed relationship types.
$relationshipTypes = $xia.GET_ValidSystemRelationshipTypes();
foreach ($relationshipType in $relationshipTypes)
{
    Write-Host $relationshipType;
}
```

Search

Items can be found by using [search](#).

There are two SDK methods that can be used to [search](#)

- [Basic Search](#)
- [Advanced Search](#)

Basic Search

The basic search allows [items](#) to be found using a simple syntax.

- Connect to the [configuration web service](#).

Code Sample

```
# Perform a basic search.
$searchResults = $xia.DO_PerformBasicSearch("DEMO-DHCP*");
foreach ($searchResult in $searchResults.SearchResult)
{
    Write-Host "Located $($searchResult.Name) [$($searchResult.ItemID)"]";
}
```

Advanced Search

The advanced search allows [items](#) to be found using detailed search criteria.

Searching by Item Type

The example uses the advanced search to find [items](#) of the specified [item type](#).

- Connect to the [configuration web service](#).

Code Sample

```
# Get the default search criteria.
$criteria = $xia.GET_DefaultSearchCriteria();

# Configure the criteria.
$criteria.SearchString = "*";
$criteria.Filters.Type = "WindowsServer";

# Perform the search.
$searchResults = $xia.DO_PerformSearch($criteria)
foreach ($searchResult in $searchResults.SearchResult)
{
    Write-Host "Located $($searchResult.Name) [$(($searchResult.ItemID))>";
}
```

Searching by Parent Customer

The example uses the advanced search to find [items](#) of the specified parent [customer](#).

- Connect to the [configuration web service](#).

Code Sample

```
# Get the default search criteria.
$criteria = $xia.GET_DefaultSearchCriteria();

# Configure the criteria.
$criteria.SearchString = "*";
$criteria.Filters.ParentCustomerID = 35169;

# Perform the search.
$searchResults = $xia.DO_PerformSearch($criteria)
foreach ($searchResult in $searchResults.SearchResult)
{
    Write-Host "Located $($searchResult.Name) [$(($searchResult.ItemID))>";
}
```

Security Descriptors

The web service allows the [security descriptor](#) to be viewed and modified for [items](#).

Get Effective Permissions

The following example gets the [effective permissions](#) for an [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) for which the [effective permissions](#) are to be returned.

Code Sample

```
# Set the item identifier of the item for which the effective permissions to be returned.
$itemID = 1000;

# Read the effective permissions.
$effectivePermissions = $xia.GET_EffectivePermissions($itemID);
Write-Host $effectivePermissions.AccountName;
Write-Host "Full control:" $effectivePermissions.FullControl;
Write-Host "Rename:" $effectivePermissions.Rename;
Write-Host "Read:" $effectivePermissions.Read;
Write-Host "Write:" $effectivePermissions.Write;
Write-Host "Decommission:" $effectivePermissions.Decommission;
Write-Host "Delete:" $effectivePermissions.Delete;
Write-Host "Delete history:" $effectivePermissions.DeleteHistory;
Write-Host "Modify security:" $effectivePermissions.ModifySecurity;
```

Get Security Descriptor

The following example gets the [security descriptor](#) for an [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) for which the [security descriptor](#) is to be returned.
- The user must have at least [read permissions](#) to the [item](#) to execute this command.

Code Sample

```
# Set the item identifier of the item for which the security descriptor is to be returned.
$itemID = 1000;

# Read the security descriptor and enumerate the security entries.
$securityDescriptor = $xia.GET_SecurityDescriptor($itemID);
Write-Host "Inherited: " $securityDescriptor.Inherit;
foreach ($securityEntry in $securityDescriptor.SecurityEntries)
{
    Write-Host "Security Entry:";
    Write-Host $securityEntry.AccountName;
    Write-Host "Full Control: " $securityEntry.FullControl;
    Write-Host "Read: "$securityEntry.Read;
    Write-Host "Write: "$securityEntry.Write;
}
```

Replace Owner

The following example updates the owner of an [item](#) by removing the existing [security descriptor](#), and assigning the specified user account [full control](#) to the item and all child [items](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) for which the [security descriptor](#) is to be replaced.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Set the item identifier of the item for which the security descriptor is to be replaced.
$itemID = 37423;

# Set the name of the user or group account to take ownership of the item.
$accountName = "CENTREL-WS01\Managers";

# Replaces the ownership of the specified item.
$xia.DO_ReplaceOwnership($itemID, $accountName);
```

Update Security Descriptor

The following example modifies the [security descriptor](#) for an [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) for which the [security descriptor](#) is to be updated.
- The user must have at least [modify security permissions](#) to the [item](#) to execute this command.

Code Sample

```
# Set the item identifier of the item for which the security descriptor is to be updated.
$itemID = 37423;

# Set the account name to add to the security descriptor.
$accountName = "CENTREL-WS01\Managers";

# Read the existing descriptor.
$securityDescriptor = $xia.GET_SecurityDescriptor($itemID);

# Create a new security entry.
$securityEntry = New-Object "$($xia.GetType().Namespace).SecurityEntry";
$securityEntry.FullControl = $true;
$securityEntry.AccountName = $accountName;

# Ensure that the security descriptor does not inherit from the parent, and add the new
security entry.
$securityDescriptor.Inherit = $false;
$securityDescriptor.SecurityEntries += $securityEntry;

# Update the security descriptor.
$xia.SET_SecurityDescriptor($itemID, $securityDescriptor, $true);
```

ServiceNow Integration (Users)

XIA Configuration Server is able to integrate with a [ServiceNow](#) instance using the [ServiceNow Connector](#).

The information in this section refers to code that can be executed by all users. Additional methods can be accessed by [system administrators](#), more information can be found in the [ServiceNow integration \(system administrators\)](#) section.

Get Item Synchronization Information

The following example gets information about the synchronization of the [item](#) between the [XIA Configuration Server](#) and a [ServiceNow instance](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) for which the information is to be returned.
- The [item](#) type must [support synchronization](#).
- The user must have [read permissions](#) to the [item](#).

Code Sample

```
# Gets the ServiceNow synchronization information for the item with the specified item  
identifier.  
$information = $xia.GET_ServiceNowItemSynchronizationInformation(38709);  
$information;
```

Synchronize Item

The following example synchronizes an [item](#) with the [ServiceNow](#) instance.

- Connect to the [configuration web service](#).
- The user must have both [write permissions](#) to the [item](#) and the [manage ServiceNow item synchronization](#) or [synchronize items with ServiceNow server permission](#).
- To synchronize all [items](#) with the [ServiceNow](#) instance see the [synchronize items](#) code example.

Code Sample

```
# Manually synchronizes the item with the specified item identifier with the ServiceNow instance.  
$result = $xia.DO_SynchronizeServiceNowItem(40939);  
$result;
```

Update Item Synchronization Settings

The following example updates the [ServiceNow](#) synchronization settings for the [item](#).

- Connect to the [configuration web service](#).
- Get the current [ServiceNow](#) synchronization settings for the [item](#).
- Modify and commit the [ServiceNow](#) synchronization settings for the [item](#).
- The [item](#) type must [support synchronization](#).
- The user must have both [write permissions](#) to the [item](#) and the [manage ServiceNow item synchronization server permission](#).

Code Sample

```
# Gets the current ServiceNow synchronization settings for the item with the specified
item identifier.
$settings = $xia.GET_ServiceNowItemSynchronizationSettings(37663);

# Modify the settings.
$settings.Enabled = $true;
$settings.ServiceNowIdentifier = [System.Guid]::Parse("82e0ca66-42cb-4c0e-a2c1-
c7d0709761cf");

# Commit the changes to the ServiceNow synchronization settings.
$xia.SET_ServiceNowItemSynchronizationSettings($settings);
```

Support Provisions

[Support provisions](#) can be created, accessed, and updated with the [configuration web service](#).

Assign Support Provision

Assign a [support provision](#) to an [item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the [item](#) to which the [support provision](#) is to be assigned.
- Specify the unique identifier of the [support provision](#) to assign.
- Specify the relationship type, either "IsSupportedBy" for technical support, or "IsMaintainedBy" for hardware support or maintenance.
- Determine whether to overwrite all relationships of this relationship type.
- This method is a helper function to the underlying [relationships](#) methods.

Code Sample

```
# Set the identifier of the item and the support provision.
$itemID = 12345;
$supportProvisionID = 123456;
$relationshipType = "IsSupportedBy";
$createInboundConnection = $false;
$overwriteExisting = $true;

# Perform the action.
$xia.DO_AssignManualRelationship($itemID, $supportProvisionID, $relationshipType,
$createInboundConnection, $overwriteExisting);
```

Get Support Provision

Get an existing [support provision item](#).

- Connect to the [configuration web service](#).
- Specify the unique identifier of the required [support provision](#).
- The user must have [read permissions](#) to the [support provision](#).

Code Sample

```
# Get the item.
$item = $xia.GET_Item(1234, 0);

# Display the information.
Write-Host $item.Name;
Write-Host "-----";
Write-Host $item.Hours;
Write-Host $item.ReferenceNumber;
Write-Host $item.SelfServiceWeb;
Write-Host $item.Email;
Write-Host $item.TelephoneNumber;
if ($item.StartDate -ne [datetime]::MinValue) { Write-Host $item.StartDate; }
if ($item.ExpiryDate -ne [datetime]::MinValue) { Write-Host $item.ExpiryDate; }
```

Update Support Provision

Update an existing [support provision](#).

- Connect to the [configuration web service](#).
- Set the unique identifier of the [support provision](#).
- The item must be [checked out](#) and [checked back in](#).
- The user must have [write permissions](#) to the [item](#).

Code Sample

```
# Get the existing item.
$item = $xia.GET_Item(1234, 0);

# Check out the item.
$xia.DO_CheckOutItem($item.ItemID);

# Update the properties.
$item.Hours = "Monday to Friday, 8am to 5pm";

# Update the item.
$xia.SET_Item($item);

# Check in the item back in.
$xia.DO_CheckInItem($item.ItemID);
```

Version Control (Users)

Version control automatically creates new, numbered versions of [items](#) when they are modified by a user or updated by the [XIA Configuration Client](#).

The information in this section refers to code that can be executed by all users. Additional methods can be accessed by [system administrators](#), more information can be found in the [version control \(system administrators\)](#) section.

Get Version History

Gets the [version history](#) for an [item](#).

- Connect to the [configuration web service](#).

Code Sample

```
# Get the version history.
$itemIdentifier = 1000;
$versionHistory = $xia.GET_VersionHistory($itemIdentifier);
foreach ($versionRecord in $versionHistory.VersionRecord)
{
    Write-Host "Version $($versionRecord.VersionIdentifier)";
    Write-Host " Created: $($versionRecord.CreationDate)";
    Write-Host " Description: $($versionRecord.Description)";
    Write-Host " Username: $($versionRecord.Username)";
}
```

Delete Previous Version

Deletes a [previous version](#) for an [item](#).

- Connect to the [configuration web service](#).
- The user must have the [delete previous versions](#) permission to the [item](#).

Code Sample

```
# Delete the specified previous version.  
$itemIdentifier = 1000;  
$versionIdentifier = 1.00;  
$xia.DO_DeletePreviousVersion($itemIdentifier, $versionIdentifier);
```

Increment Major Version Number

Creates a [previous version](#) for an [item](#) if versioning is enabled in the [version control settings](#), and then increments the version number of the [item](#) to the next major version.

- Connect to the [configuration web service](#).
- The user must have the [write previous versions](#) permission to the [item](#).
- Specify the identifier of the [item](#).
- Specify the version description.

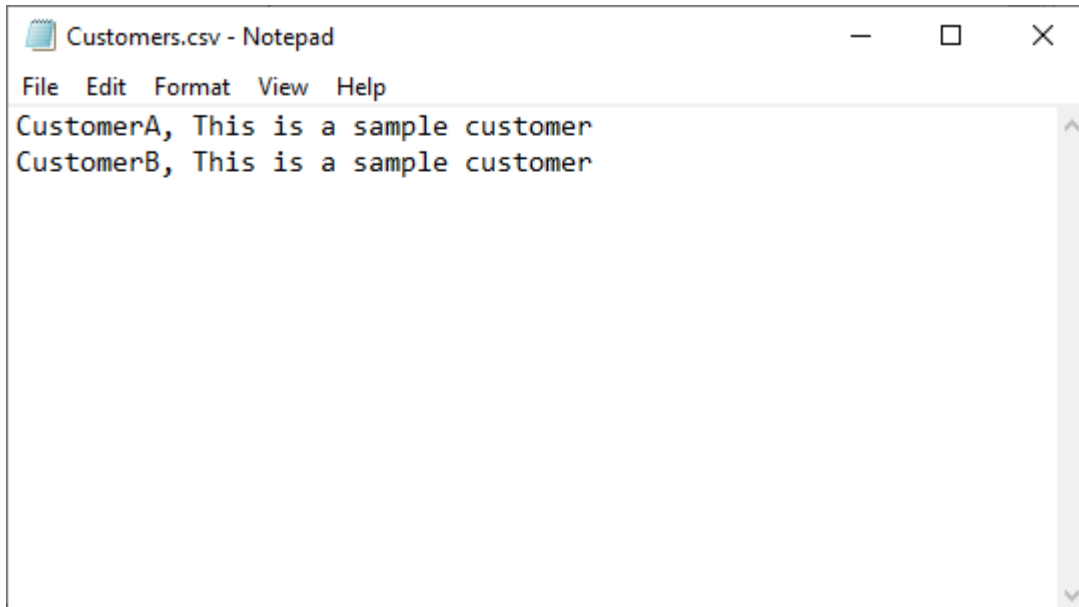
Code Sample

```
# Increment the major version of the item.  
$itemIdentifier = 1526;  
$versionDescription = "Repurposed the item as a test server.";  
$xia.DO_IncrementMajorVersionNumber($itemIdentifier, $versionDescription);
```

Creating Items from CSV

The following example creates **Customer** items from a CSV file:

- The CSV file in the example resides in "c:\temp\customers.csv" and contains the following simplistic data:



- The item is created in the default container "1000", however, this can be changed to any valid container.
- The item must be [checked out](#) before modifying.
- The **Description** field is an [OverrideString](#) which must be configured as Overridden.

Code Sample

```
# Read each line of the CSV.
$csvFilename = "c:\temp\customers.csv";
$csv = Import-Csv $csvFilename -Header @"(Name","Description)";
foreach ($line in $csv) {

    # Create the customer.
    Write-Host "Creating customer: $($line.Name)";
    $NewItemID = $xia.DO_CreateItem($line.Name, "Customer", "1000");
    Write-Host "Created new item" $NewItemID;
    Write-Host "";

    # Set the item description.
    $xia.DO_CheckOutItem($NewItemID);
    $newCustomer = $xia.GET_Customer($NewItemID, 0);
    $newCustomer.Description.Overridden = "True";
    $newCustomer.Description.Value = $line.Description;
    $xia.SET_Customer($newCustomer);
    $xia.DO_CheckInItem($NewItemID);

}
```


Output

```
Connecting to XIA Server at http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx  
Creating customer CustomerA  
Created new item 4787  
  
Creating customer CustomerB  
Created new item 4788
```

Creating Managed Customers

The following example can be used by managed service providers (MSPs) to create new [customers](#) and assign the appropriate security permissions and [item creation rules](#):

- The variables must be completed before running the script.
- Configure the `$serverUrl` variable with the base URL of the server.
- Configure the `$customerName` variable with the name of the customer. This must meet the configured customer [item naming](#) setting. This is used as the name of the [customer](#) in the user interface and in the [item creation rule](#).
- Configure the `$customerAccountName` variable with the Windows account name that will be assigned full permissions to this [customer](#). This account must already exist and be in the format DOMAIN\Username.
- Configure the `$customerClientMachineName` variable with the name of the computer running the [XIA Configuration Client](#) at the customer site. This is used by the [item creation rule](#) to ensure that items belonging to this [customer](#) are created in the correct [customer](#) container.

Code Sample

```
# Set the variables.
$serverUrl = "http://localhost/xiaconfiguration";
$customerName = "NewCustomer";
$customerAccountName = "DEMONSTRATION\Administrator";
$customerClientMachineName = "CORP-SRV01";

# Connect to the server, both the configuration and administration web services are
# required.
Clear-Host;
Write-Host "Connecting to server $($serverUrl)";
$xiaUrl = $serverUrl + "/webservice/xiaconfiguration.asmx";
$administrationUrl = $serverUrl + "/webservice/administration.asmx";
$xia = New-WebServiceProxy -UseDefaultCredential -Uri $xiaUrl;
$administration = New-WebServiceProxy -UseDefaultCredential -Uri $administrationUrl;
Write-Host "Connected as" $xia.GET_AuthenticatedUserName();

# Create the customer container.
$newCustomerID = $xia.DO_CreateItem($customerName, "Customer", 1000);
Write-Host "Created customer with identifier" $newCustomerID;

# Set security on the container.
$xia.DO_ReplaceOwnership($newCustomerID, $customerAccountName);

# Add a new item creation rule.
$administration.DO_CreateComputerBasedItemCreationRule($customerName, $newCustomerID,
$customerClientMachineName);
Write-Host "Created item creation rule" $customerName;
```

Administration Web Service (System Administrators)

The administration [web service](#) provides functions such as access to the [event log](#), and [configuration settings](#).

```
# Connect to the administration web service.
Clear-Host;
$url = "http://localhost/xiaconfiguration/webService/administration.asmx";
Write-Host "Connecting to administration web service at" $url;
$administration = New-WebServiceProxy -UseDefaultCredential -Uri $url;
Write-Host "Connected as" $administration.GET_AuthenticatedUserName();

# To use specific credentials use the Get-Credential cmdlet.
$creds = Get-Credential;
$administration = New-WebServiceProxy -Uri $url -Credential $creds;
```

NOTE: Only [system administrators](#) can access this web service.

Check Out (System Administrators)

When [items](#) are edited by a user, they are automatically [checked out](#) so that they cannot be edited by other users.

The information in this section refers to code that can be executed by [system administrators](#). Additional methods can be accessed by all users - more information can be found in the [check out \(users\)](#) section.

Get Checked Out Items

The following example gets the unique identifiers of the [items](#) that are currently [checked out](#).

- Connect to the [administration web service](#).

Code Sample

```
# Set the username, or an empty string for all users.
$username = "";

# Gets the identifiers of the items that are currently checked out.
$identifiers = $administration.GET_CheckedOutItemIdentifiers($username);
foreach ($identifier in $identifiers)
{
    write-host $identifier;
}
```

Check In Items

The following example checks in [items](#) that are currently [checked out](#).

WARNING: Changes to items currently being edited may be lost.

- Connect to the [administration web service](#).

Code Sample

```
# Checks in the items that have been checked out for 20 minutes or longer.  
$minutes = 20;  
$administration.DO_CheckInItems($minutes);
```

Event Log

The [event log](#) allows [system administrators](#) to view the history of actions performed on the [system](#).

Get Events

The following example gets the [event log](#) events that match the criteria.

- Connect to the [administration web service](#).
- Get the default event log [filter criteria](#), and configure if required.

Code Sample

```
# Gets the events that match the specified criteria.
$criteria = $administration.GET_DefaultEventLogCriteria();

# Optionally configure the required criteria.
$criteria.Username = "*Administrator*";
$criteria.MaximumResultCount = 100;

# Get the event log entries, and optional attributes.
$entries = $administration.GET_EventLogEntries($criteria);
foreach ($entry in $entries.Event)
{
    Write-Host "----- Entry -----";
    Write-Host $entry.CreationDate;
    Write-Host $entry.EntryCodeString;
    Write-Host $entry.Message;
    Write-Host $entry.EntryCode;
    foreach ($attribute in $entry.Attributes.Attribute)
    {
        Write-Host "$($attribute.InformationTypeDisplayName): $($attribute.value)";
    }
}
```

Clear Event Log

The following example clears the [event log](#).

- Connect to the [administration web service](#).

Code Sample

```
# clear the event log.  
$administration.DO_ClearEventLog();
```

Hardware Definitions

Hardware definitions allow information such as a description and image to be automatically detected for any hardware **items**.

Create Hardware Definition

The following example creates a new [hardware definition](#).

- Connect to the [administration web service](#).

Code Sample

```
# Creates a new hardware definition.  
$identifier = $administration.DO_CreateHardwareDefinition();  
Write-Host $identifier;
```

Delete Hardware Definition

The following example deletes the specified [hardware definition](#).

- Connect to the [administration web service](#).

Code Sample

```
# Deletes the specified hardware definition.  
$administration.DO_DeleteHardwareDefinition("e1fa7db7-6f47-423e-befa-efb32875e193");
```

Get Hardware Definitions

The following examples get the configured [hardware definitions](#).

- Connect to the [administration web service](#).

Code Sample

```
# Gets all hardware definitions.
$hardwareDefinitions = $administration.GET_HardwareDefinitions();
foreach ($hardwareDefinition in $hardwareDefinitions.HardwareDefinition)
{
    Write-Host $hardwareDefinition.DisplayName;
    Write-Host $hardwareDefinition.Identifiers.Manufacturers;
    Write-Host $hardwareDefinition.Identifiers.Models;
    Write-Host
}

# Get the hardware definition with the specified identifier.
$hardwareDefinition = $administration.GET_HardwareDefinition("e1fa7db7-6f47-423e-befa-efb32875e193");
Write-Host $hardwareDefinition.DisplayName;
Write-Host $hardwareDefinition.Identifiers.Manufacturers;
Write-Host $hardwareDefinition.Identifiers.Models;
Write-Host

# Get the hardware definition for the specified manufacturer and model.
$hardwareDefinition = $administration.GET_HardwareDefinitionByIdentifiers("Hewlett-Packard", "D6000");
if ($hardwareDefinition -eq $null) { Write-Host "No definition was found"; }
else
{
    Write-Host $hardwareDefinition.DisplayName;
    Write-Host $hardwareDefinition.Identifiers.Manufacturers;
    Write-Host $hardwareDefinition.Identifiers.Models;
    Write-Host
}

# Get the image for the hardware definition.
$binaryData = $administration.GET_HardwareDefinitionImage("e1fa7db7-6f47-423e-befa-efb32875e193");
[System.IO.File]::WriteAllBytes("C:\temp\image.png", $binaryData);
```

Update Hardware Definition

The following examples update the specified [hardware definition](#), and its associated image.

- Connect to the [administration web service](#).

Code Sample

```
# Update the hardware definition.
$hardwareDefinition = $administration.GET_HardwareDefinition("1f2bf8bb-ed73-4db7-bd4e-f063068bdde1");
$hardwareDefinition.DisplayName = "Updated Display Name";
$hardwareDefinition.Description = "Updated Description";
$administration.SET_HardwareDefinition($hardwareDefinition);

# Update the image for the hardware definition.
$binaryData = [System.IO.File]::ReadAllBytes("C:\temp\UpdatedImage.png");
$administration.SET_HardwareDefinitionImage("1f2bf8bb-ed73-4db7-bd4e-f063068bdde1",
$binaryData);
```

Scheduler

The scheduler allows the automated execution of [scheduled tasks](#) and the [import of data files](#) on the [XIA Configuration Server](#).

Get Scheduler Status

The following example gets the status of the scheduler.

- Connect to the [administration web service](#).

Code Sample

```
# Gets the status of the scheduler service.  
$administration.GET_SchedulerStatus();
```

Scheduled Tasks

The [administration web service](#) can be used to [create](#), [access](#), [delete](#), and [update](#) scheduled tasks.

Create Scheduled Task

The following example creates a new [scheduled task](#).

- Connect to the [administration web service](#).
- Specify the scheduled task type as one of the following values

[ReportExecution](#)

[ReportBinderExecution](#)

Code Sample

```
# Creates a new scheduled report execution task.
```

```
$identifier = $administration.DO_CreateScheduledTask("ReportExecution");
```

```
# Creates a new scheduled report binder execution task.
```

```
$identifier = $administration.DO_CreateScheduledTask("ReportBinderExecution");
```

Delete Scheduled Task

The following example deletes an existing [scheduled task](#).

- Connect to the [administration web service](#).
- Specify the unique identifier of the [scheduled task](#) to delete in [GUID](#) format.

Code Sample

```
# Deletes the scheduled task with the specified identifier.  
$administration.DO_DeleteScheduledTask("e2283abb-b844-4c6f-b6c3-a555dd5d47c5");
```

Get Scheduled Tasks

The following example gets information about the configured [scheduled tasks](#).

- Connect to the [administration web service](#).
- The unique identifiers specified are in [GUID](#) format.

Code Sample

```
# Lists basic information about each scheduled task.
$tasks = $administration.GET_ScheduledTasks();
foreach ($task in $tasks)
{
    Write-Host $task.DisplayName;
    Write-Host $task.Identifier;
    Write-Host $task.TaskType;
    Write-Host
}

# Gets the full details of the scheduled task with the specified identifier.
$task = $administration.GET_ScheduledTask("22176cac-8f38-49ea-aca4-6a579d333853");

# Gets the unique identifiers of the scheduled tasks that are due to execute.
$administration.GET_ScheduledTasksToExecute();
```

Update Report Execution Scheduled Task

The following example updates an existing [report execution scheduled task](#).

- Connect to the [administration web service](#).
- Specify the unique identifier of the [scheduled task](#) in [GUID](#) format.

Code Sample

```
# Updates the scheduled report execution task with the specified identifier.  
$task = $administration.GET_ScheduledTask("22176cac-8f38-49ea-aca4-6a579d333853");  
$task.DisplayName = "Updated Report Execution Scheduled Task";  
$administration.SET_ScheduledReportExecutionTask($task);
```

Update Report Binder Execution Scheduled Task

The following example updates an existing [report binder execution scheduled task](#).

- Connect to the [administration web service](#).
- Specify the unique identifier of the [scheduled task](#) in [GUID](#) format.

Code Sample

```
# Updates the scheduled report binder execution task with the specified identifier.  
$task = $administration.GET_ScheduledTask("1f1ef16c-b3dd-44d2-b15a-64883249b3c8");  
$task.DisplayName = "Updated Report Binder Execution Scheduled Task";  
$administration.SET_ScheduledReportBinderExecutionTask($task);
```

Task Output Targets

The [administration web service](#) can be used to create, access, delete, and update [task output targets](#).

Create Task Output Target

The following example creates a new [task output target](#).

- Connect to the [administration web service](#).
- Specify the task output target type as one of the following values

[FileSystem](#)
[Smtp](#)

Code Sample

```
# Creates a new file system task output target.  
$identifier = $administration.DO_CreateTaskOutputTarget("FileSystem");  
  
# Creates a new SMTP task output target.  
$identifier = $administration.DO_CreateTaskOutputTarget("Smtp");
```

Delete Task Output Target

The following example deletes an existing [task output target](#).

- Connect to the [administration web service](#).
- A [task output target](#) cannot be deleted whist it is [referenced](#) by other objects.
- Specify the unique identifier of the [task output target](#) to delete in [GUID](#) format.

Code Sample

```
# Deletes the task output target with the specified identifier.  
$administration.DO_DeleteTaskOutputTarget("ad65ad4a-7ca0-4538-99eb-249bdc34498a");
```

Get Task Output Targets

The following example gets information about the configured [task output targets](#).

- Connect to the [administration web service](#).
- The unique identifiers specified are in [GUID](#) format.

Code Sample

```
# Lists basic information about each task output target.
$targets = $administration.GET_TaskOutputTargets();
foreach ($target in $targets)
{
    Write-Host $target.DisplayName;
    Write-Host $target.Identifier;
    Write-Host $target.TargetType;
    Write-Host
}

# Gets the full details of the task output target with the specified identifier.
$target = $administration.GET_TaskOutputTarget("3f718566-19e9-45a9-8a0a-0f1a9f9c2c58");
```

Get Task Output Target References

The following example gets information about the objects such as [report execution scheduled tasks](#) and [report binder execution scheduled tasks](#) that reference a [task output target](#).

- Connect to the [administration web service](#).
- A [task output target](#) cannot be [deleted](#) whilst it is referenced by other objects.
- The unique identifiers specified are in [GUID](#) format.

Code Sample

```
# Gets information about the objects that reference the specified task output target.
$references = $administration.GET_TaskOutputTargetReferences("26b9ad46-e799-4f22-a1fc-
e49083c522ec");
foreach ($reference in $references)
{
    Write-Host $reference.DisplayName;
    Write-Host $reference.Identifier;
    Write-Host $reference.ReferenceType;
    Write-Host
}
```

Update File System Task Output Target

The following example updates an existing [file system task output target](#).

- Connect to the [administration web service](#).
- Specify the unique identifier of the [task output target](#) in [GUID](#) format.
- Specify the path for the [file system task output target](#).

Code Sample

```
# Updates the file system task output target with the specified identifier.  
$target = $administration.GET_TaskOutputTarget("ef2523e2-b305-4915-a679-f191be790d5d");  
$target.DisplayName = "Updated File System Task Output Target";  
$target.Path = "D:\Data\TaskOutput";  
$administration.SET_TaskOutputFileSystemTarget($target);
```

Update SMTP Task Output Target

The following example updates an existing [SMTP task output target](#).

- Connect to the [administration web service](#).
- Specify the unique identifier of the [task output target](#) in [GUID](#) format.
- Specify the SMTP address to set for the [SMTP task output target](#).

Code Sample

```
# Updates the SMTP task output target with the specified identifier.  
$target = $administration.GET_TaskOutputTarget("3f718566-19e9-45a9-8a0a-0f1a9f9c2c58");  
$target.DisplayName = "Updated SMTP Task Output Target";  
$target.Addresses.ToAddresses.Clear();  
$target.Addresses.ToAddresses += "administrator@demonstration.int";  
$administration.SET_TaskOutputSmtpTarget($target);
```

ServiceNow Integration (System Administrators)

[XIA Configuration Server](#) is able to integrate with a [ServiceNow](#) instance using the [ServiceNow Connector](#).

The information in this section refers to code that can be executed by [system administrators](#). Additional methods can be accessed by all users - more information can be found in the [ServiceNow integration \(users\)](#) section.

Abort Synchronization

The following example aborts the synchronization between [XIA Configuration Server](#) and a [ServiceNow](#) instance.

- Connect to the [administration web service](#).
- The abort method is effective for both synchronization and synchronization simulations.
- If the synchronization is not running an [exception](#) is thrown.

Code Sample

```
# Aborts the synchronization with the ServiceNow instance.  
$administration.DO_AbortServiceNowSynchronization();
```

Get Synchronization Status

The following example gets the synchronization status of the [ServiceNow connector](#).

- Connect to the [administration web service](#).

Code Sample

```
# Gets the current synchronization status of the ServiceNow connector.  
$status = $administration.GET_ServiceNowItemSynchronizationStatus();  
$status | SELECT *;
```

Get Synchronization Results

The following example gets the synchronization results of the [ServiceNow connector](#).

- Connect to the [administration web service](#).
- The command cannot be run when a synchronization is in progress - to determine the current synchronization status see the [get synchronization status](#) section.

Code Sample

```
# Gets the results of the ServiceNow item synchronization in CSV format.  
$csv=$administration.GET_ServiceNowItemSynchronizationResultsCsv();  
write-Host $csv;
```

Simulate Synchronization

The following example simulates the synchronization between [XIA Configuration Server](#) and a [ServiceNow](#) instance using the [ServiceNow connector](#).

- Connect to the [administration web service](#).
- To force a resynchronization of items that are currently synchronized set the parameter to `$true`.
- To view the synchronization status see the [get ServiceNow item synchronization status](#) example.

Code Sample

```
# Performs a simulation of the synchronization of all items that currently require  
synchronization asynchronously.  
$administration.DO_SimulateServiceNowSynchronization($false);
```

Synchronize Items

The following example starts the synchronization between [XIA Configuration Server](#) and a [ServiceNow](#) instance using the [ServiceNow connector](#).

- Connect to the [administration web service](#).
- To simulate forcing a resynchronization of items that are currently synchronized set the parameter to `$true`.
- To view the synchronization simulation status see the [get ServiceNow item synchronization status](#) example.

Code Sample

```
# Synchronizes all items that currently require synchronization asynchronously.  
$administration.DO_SynchronizeServiceNow($false);
```

Usage and Diagnostics Data

The [administration web service](#) can be used to [enable](#) or [disable usage and diagnostics data](#), and well as [obtaining the current settings](#).

Enable Usage and Diagnostics Data

The following example enables [usage and diagnostics data](#), creating the required [scheduled task](#) and [task output target](#).

- Connect to the [administration web service](#).
- If [usage and diagnostics data](#) is already enabled an exception will be thrown.

Code Sample

```
# Enable diagnostics and usage data.  
$administration.DO_EnableUsageDiagnosticsData();
```

Disable Usage and Diagnostics Data

The following example disables [usage and diagnostics data](#), removing the [scheduled task](#) and [task output target](#).

- Connect to the [administration web service](#).

Code Sample

```
# Disables diagnostics and usage data.  
$administration.DO_DisableUsageDiagnosticsData();
```

Get Usage and Diagnostics Data Settings

The following example gets the current [usage and diagnostics data](#) settings.

- Connect to the [administration web service](#).
- If [usage and diagnostics data](#) is misconfigured an exception will be thrown.

Code Sample

```
# Get diagnostics and usage data settings.
$settings = $administration.GET_UsageDiagnosticsDataSettings();

# Write enabled setting.
Write-Host "Enabled: $($settings.Enabled)";
if (!$settings.Enabled) { return ;}

# If enabled, write all settings.
Write-Host "To Addresses: $($settings.ToAddresses)";
Write-Host "CC Addresses: $($settings.CcAddresses)";
Write-Host "Information Level: $($settings.InformationLevel)";
Write-Host "Schedule: $($settings.Schedule.Summary)";
```

Version Control (System Administrators)

Version control automatically creates new, numbered versions of [items](#) when they are modified by a user or updated by the [XIA Configuration Client](#).

The information in this section refers to code that can be executed by [system administrators](#). Additional methods can be accessed by all users - more information can be found in the [version control \(users\)](#) section.

Clear Previous Versions

The example deletes all previous versions for all [items](#), and resets the version identifier for all [items](#) to "1.00".

- Connect to the [administration web service](#).
- **WARNING:** This action cannot be undone.

Code Sample

```
# Delete all previous versions for all items, and resets the version identifier for all  
items to "1.00".  
$administration.DO_ClearPreviousVersions();
```

Delete Previous Versions

The following example deletes the [version history](#) for [items](#) based on the criteria.

- Connect to the [administration web service](#).
- Set the minimum [date](#) is the from which previous versions should be deleted.
- Setting the [item type](#) to 'Unknown' deletes previous versions for all [item type](#).
- View the [event log](#), or [get previous versions storage information](#) for information about the number of records deleted.

Code Sample

```
# Delete the previous versions that are older than 3 years, for all items.  
$minimumDate = (Get-Date).AddYears(-3);  
$administration.DO_DeletePreviousVersions('Unknown', $minimumDate);
```

Get Previous Versions Storage Information

The following example gets the storage used by the previous versions created by [version control](#) for all [items](#).

- Connect to the [administration web service](#).

Code Sample

```
# Get the previous version storage information.
$information = $administration.GET_PreviousVersionsStorageInformation();
Write-Host "$($information.PreviousVersionsCount) previous versions";
Write-Host "Storage used: $($information.UsedSpace)KB";
```

Reporting Web Service

The [reporting web service](#) provides access to the [reporting](#) system including the ability to [modify](#) and [execute reports](#) and [report binders](#).

```
# Connect to the reporting web service.
Clear-Host;
$url = "http://localhost/xiaconfiguration/webservice/reporting.asmx";
Write-Host "Connecting to reporting web service at" $url;
$reporting = New-WebServiceProxy -UseDefaultCredential -Uri $url;
Write-Host "Connected as" $reporting.GET_AuthenticatedUserName();

# To use specific credentials use the Get-Credential cmdlet.
$creds = Get-Credential;
$reporting = New-WebServiceProxy -Uri $url -Credential $creds;
```

Create Report

The following example creates a new [report](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) where the [report](#) is to be created in GUID format. To create the [report](#) in the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Creates a new report in the report folder with the specified identifier and displays the  
# identifier of the newly created report.  
$newIdentifier = $reporting.DO_CreateReport("e5cf10bc-a9e0-446e-b049-e06937213615");  
Write-Host $newIdentifier;
```

Create Report Binder

The following example creates a new [report binder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) where the [report binder](#) is to be created in GUID format. To create the [report binder](#) in the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Creates a new report binder in the report folder with the specified identifier and  
# displays the identifier of the newly created report binder.  
$newIdentifier = $reporting.DO_CreateReportBinder("e5cf10bc-a9e0-446e-b049-e06937213615");  
Write-Host $newIdentifier;
```

Create Report Folder

The following example creates a new [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) where the [report folder](#) is to be created in GUID format. To create the [report folder](#) in the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Creates a new report folder in the report folder with the specified identifier and  
# displays the identifier of the newly created report folder.  
$newIdentifier = $reporting.DO_CreateReportFolder("e5cf10bc-a9e0-446e-b049-e06937213615");  
Write-Host $newIdentifier;
```

Delete Report

The following example deletes a [report](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) to delete.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Deletes the report with the specified identifier.  
$reporting.DO_DeleteReport("891b670a-87d4-4630-a812-3bafd280e6b8");
```

Delete Report Binder

The following example deletes a [report binder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) to delete.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Deletes the report binder with the specified identifier.  
$reporting.DO_DeleteReportBinder("4105841f-9776-4283-8cba-08de4e9fbc3f");
```

Delete Report Folder

The following example deletes a [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) to delete.
- The user must be a [system administrator](#) to execute this command.
- The [root report folder](#) itself cannot be deleted.

Code Sample

```
# Deletes the report folder with the specified identifier. The report folder must be empty  
to run this command.  
$reporting.DO_DeleteReportFolder("dcc28043-6292-4473-830a-a6f40832bd96");
```

- or -

```
# WARNING: Deletes the report folder with the specified identifier AND all child objects.  
$reporting.DO_DeleteReportFolderRecursive("dcc28043-6292-4473-830a-a6f40832bd96");
```

Duplicate Report

The following example duplicates an existing [report](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) to duplicate in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Duplicates the report with the specified identifier and displays the identifier of the  
newly created report.  
$newIdentifier = $reporting.DO_DuplicateReport("5d1ae1a7-6625-4c2c-baf9-b08f6b6f87f1");  
Write-Host $newIdentifier;
```

Duplicate Report Binder

The following example duplicates an existing [report binder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) to duplicate in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Duplicates the report binder with the specified identifier and displays the identifier  
of the newly created report binder.  
$newIdentifier = $reporting.DO_DuplicateReportBinder("48340e7b-952a-4713-b3a4-  
c4d943b7cd7d");  
Write-Host $newIdentifier;
```

Execute a Report to PDF

The following example executes a [report](#), saves the output as a PDF document and opens the file in the default PDF document viewer.

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) to execute in GUID format.
- Specify the [customer](#) or [container](#) against which to execute the [report](#), by default this is the root container with identifier 1000.
- Set the sort order to "Ascending" or "Descending", and the sort column as a numeric value starting at 1. This has no effect if the report does not support sorting.
- Optionally set the report parameter values.
- The user must have permissions to execute this report.

Code Sample

```
# Executes the report and saves the output as a PDF file in the user's temp directory.
$filename = "$env:TEMP\ReportOutput.pdf"
$reportIdentifier = [Guid]"5413a609-80da-490b-ad76-104aa8d4021f";
$parameterValues = $reporting.GET_DefaultReportParameterValues($reportIdentifier);
$output = $reporting.DO_ExecuteReportPdf($reportIdentifier, $parameterValues, 1000,
"Ascending", 1);
[IO.File]::WriteAllBytes($filename, $output);
[System.Diagnostics.Process]::Start($filename);
```

To configure the parameters for the report use the SET_ReportParameterValue method. For example to set the "ServerName" parameter to "DEMO-SRV01" and the "Age" parameter to 31 use the following commands.

```
$reporting.SET_ReportParameterValue([ref]$parameterValues, "ServerName", "DEMO-SRV01");
$reporting.SET_ReportParameterValue([ref]$parameterValues, "Age", 31);
```

Execute a Report to CSV

The following example executes a [report](#), saves the output as a CSV file and opens the file in the default CSV document viewer.

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) to execute in GUID format.
- Specify the [customer](#) or [container](#) against which to execute the [report](#), by default this is the root container with identifier 1000.
- Set the sort order to "Ascending" or "Descending", and the sort column. This has no effect if the report does not support sorting.
- The user must have permissions to execute this report.

Code Sample

```
# Executes the report and saves the output as a CSV file in the user's temp directory.
$filename = "$env:TEMP\ReportOutput.csv"
$reportIdentifier = [Guid]"5413a609-80da-490b-ad76-104aa8d4021f";
$parameterValues = $reporting.GET_DefaultReportParameterValues($reportIdentifier);
$output = $reporting.DO_ExecuteReportCsv($reportIdentifier, $parameterValues, 1000,
"Ascending", 1)
[IO.File]::WriteAllText($filename, $output)
[System.Diagnostics.Process]::Start($filename)
```

For information about setting report parameters see the [Execute a Report to PDF](#) example.

Execute a Report Binder to PDF

The following example executes a [report binder](#), saves the output as a PDF document and opens the file in the default PDF document viewer.

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) to execute in GUID format.
- Specify the [customer](#) or [container](#) against which to execute the [report binder](#), by default this is the root container with identifier 1000.
- Optionally set the [report binder](#) parameter values.
- The user must have permissions to execute this [report binder](#).

Code Sample

```
# Executes the report binder and saves the output as a PDF file in the user's temp
directory.
$filename = "$env:TEMP\ReportBinderOutput.pdf"
$reportBinderIdentifier = [Guid]"7993bda0-6085-423f-8b03-80b196cde299";
$parameterValues =
$reporting.GET_DefaultReportBinderParameterValues($reportBinderIdentifier);
$output = $reporting.DO_ExecuteReportBinderPdf($reportBinderIdentifier, $parameterValues,
1000);
[IO.File]::WriteAllBytes($filename, $output);
[System.Diagnostics.Process]::Start($filename);
```

For information about setting report parameters see the [Execute a Report to PDF](#) example.

Get Reporting Objects

The following example gets the reporting objects in the specified [report folder](#).

- Connect to [the reporting web service](#).
- The identifier "e5cf10bc-a9e0-446e-b049-e06937213615" refers to the unique identifier of the [report folder](#) from which the reporting objects are to be displayed.
- Alternatively the unique identifier "3F836181-2109-4F5B-A1CF-B7AA8D14C212" can be used which is the well-known identifier of the [root report folder](#).
- The boolean parameter determines whether the system should recurse child [report folders](#).
- This method is affected by the "Hide reports and report binders from users who do not have permissions to execute them" [reporting settings](#).

Code Sample

```
# Gets the reporting objects in the specified report folder and child report folders, and
# displays the reporting object name and object type.
$reportingObjects = $reporting.GET_ReportingObjects("e5cf10bc-a9e0-446e-b049-
e06937213615", $true);
foreach ($reportingObject in $reportingObjects.ReportingObject)
{
    Write-Host $reportingObject.DisplayName "-" $reportingObject.ObjectTypeString;
}
```

Get Report Configuration

The following example gets the configuration of a [report](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Gets the report with the specified unique identifier and displays the report's display  
name and description.  
$report = $reporting.GET_Report("5d1ae1a7-6625-4c2c-baf9-b08f6b6f87f1");  
Write-Host $report.DisplayName;  
Write-Host $report.SqlStatement;
```

Get Report Binder Configuration

The following example gets the configuration of a [report binder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Gets the report binder with the specified unique identifier and displays the name and
description.
$reportBinder = $reporting.GET_ReportBinder("34d7de3c-ea46-4a66-9cf1-f877605d6cd3");
Write-Host $reportBinder.DisplayName
Write-Host $reportBinder.Description
```

Get Report Folder Configuration

The following example gets the configuration of a [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Gets the report folder with the specified unique identifier and displays the name and
description.
$reportFolder = $reporting.GET_ReportFolder("e5cf10bc-a9e0-446e-b049-e06937213615");
Write-Host $reportFolder.DisplayName
Write-Host $reportFolder.Description
```

Move Report

The following example moves a [report](#) to a different [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) to move in GUID format.
- Specify the unique identifier of the [report folder](#) where the [report](#) is to be moved in GUID format. To move the [report](#) to the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Moves the specified report to a different report folder.  
$report = $reporting.GET_Report("5d1ae1a7-6625-4c2c-baf9-b08f6b6f87f1");  
$report.ParentFolderIdentifier = "3f836181-2109-4f5b-a1cf-b7aa8d14c212";  
$reporting.SET_Report($report);
```

Move Report Binder

The following example moves a [report binder](#) to a different [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) to move in GUID format.
- Specify the unique identifier of the [report folder](#) where the [report binder](#) is to be moved in GUID format. To move the [report binder](#) to the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Moves the specified report binder to a different report folder.
$reportBinder = $reporting.GET_ReportBinder("34d7de3c-ea46-4a66-9cf1-f877605d6cd3");
$reportBinder.ParentFolderIdentifier = "3f836181-2109-4f5b-a1cf-b7aa8d14c212";
$reporting.SET_ReportBinder($reportBinder);
```

Move Report Folder

The following example moves a [report folder](#) to a different [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) to move in GUID format.
- Specify the unique identifier of the [report folder](#) where the [report folder](#) is to be moved in GUID format. To move the [report folder](#) to the [root report folder](#) use the well known identifier of the [root report folder](#) "3f836181-2109-4f5b-a1cf-b7aa8d14c212".
- The [root report folder](#) itself cannot be moved.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Moves the specified report folder to a different report folder.  
$reportFolder = $reporting.GET_ReportFolder("1ca8f7bd-c306-4eb9-b2f5-1d1eac6481c9");  
$reportFolder.ParentFolderIdentifier = "3f836181-2109-4f5b-a1cf-b7aa8d14c212";  
$reporting.SET_ReportFolder($reportFolder);
```

Update Report Configuration

The following example updates the configuration of a [report](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Updates the report with the specified unique identifier, changing the display name of  
the report.  
$report = $reporting.GET_Report("5d1ae1a7-6625-4c2c-baf9-b08f6b6f87f1");  
$report.DisplayName = "Updated Name";  
$reporting.SET_Report($report);
```

Update Report Binder Configuration

The following example updates the configuration of a [report binder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report binder](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.

Code Sample

```
# Updates the report binder with the specified unique identifier changing the display name  
of the report binder.  
$reportBinder = $reporting.GET_ReportBinder("34d7de3c-ea46-4a66-9cf1-f877605d6cd3");  
$reportBinder.DisplayName = "Updated Report Binder";  
$reporting.SET_ReportBinder($reportBinder);
```

Update Report Folder Configuration

The following example updates the configuration of a [report folder](#).

- Connect to [the reporting web service](#).
- Specify the unique identifier of the [report folder](#) in GUID format.
- The user must be a [system administrator](#) to execute this command.
- Changes to any of the settings of the [root report folder](#) other than the [security settings](#) will have no effect.

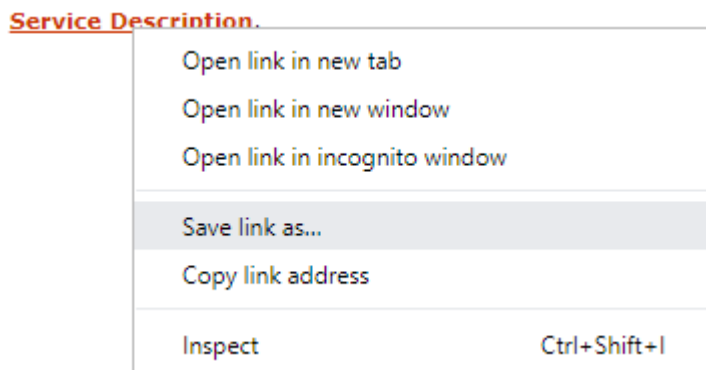
Code Sample

```
# Updates the report folder with the specified unique identifier changing the display name  
of the report folder.  
$reportFolder = $reporting.GET_ReportFolder("e5cf10bc-a9e0-446e-b049-e06937213615");  
$reportFolder.DisplayName = "Updated Report Folder";  
$reporting.SET_ReportFolder($reportFolder);
```

Using Windows PowerShell with Client Certificates

When using client certificates additional steps must be taken due to a limitation in the [New-WebServiceProxy](#) cmdlet which does not support client certificates.

- Open the [XIA Configuration Server](#) web service that you are trying to access - for example <http://localhost/xiaconfiguration/webservice/xiaconfiguration.asmx>
- Right click the service description link, and click save link as



- Save the WSDL document to a location accessible to the script - for example "C:\WebService\XiaConfiguration.wsdl"
- Use the following in a [PowerShell](#) script or the [PowerShell Integrated Scripting Environment \(ISE\)](#), replacing the highlighted text with appropriate values

```
Clear-Host
$xia = New-WebServiceProxy "file://C:\webService\filename.wsdl"
$certificate = Get-ChildItem Cert:\CurrentUser\My\{THUMBPRINT}
$xia.ClientCertificates.Add($certificate)
$xia.UseDefaultCredentials = $true
$xia.Url = {URL}
Write-Host $xia.GET_AuthenticatedUserName()
```

NOTE: When [XIA Configuration Server](#) is upgraded the steps to generate the WSDL file must be repeated.

NOTE: The client certificate can be installed in the local machine certificate store and the script updated accordingly.

Search

XIA Configuration includes the ability to search for items found within the configuration database.



To search, enter the search terms in the search field and press *Enter* or click the search button.

For information about which fields are searched, please see the [default search fields](#) section. To search additional fields, see the [advanced search menu](#) section.

The following wildcards can be used:

- % Any string of zero or more characters.
- * Any string of zero or more characters.
- _ Any single character.

Default Search Fields

The following fields are searched by default:

Item Name

The name of the item in the database.

Description

The description of an item.

Serial Number

The serial number of a physical device such as a server or network switch or virtual machine.

Component Serial Number

The serial number of a component of a physical device such as a switch in switch stack.

MAC Address

The MAC address of a device such as a server or network switch.

NOTE: the full MAC address must be entered. To enter a partial MAC address, the appropriate option must be selected on the [Advanced Search Menu](#).

Valid formats for the MAC address include:

BA-78-2E-84-E8-39

BA:78:2E:84:E8:39

BA.78.2E.84.E8.39

Connected MAC Address

The MAC address of a device connected to a network device such as a network switch.

NOTE: the full MAC address must be entered. To enter a partial MAC address, the appropriate option must be selected on the [Advanced Search Menu](#).

IP Address

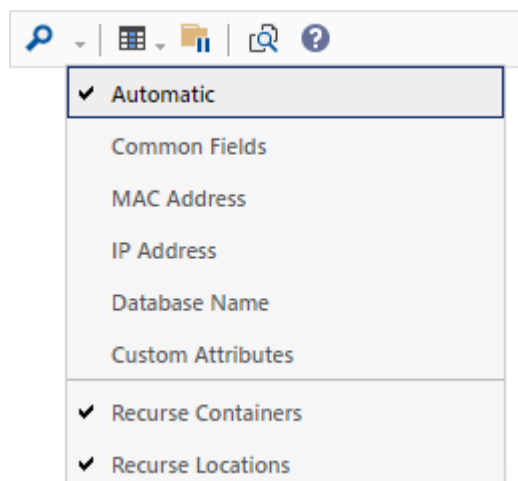
The IPv4 or IPv6 address of a networked device such as a windows server or workstation, network switch or Unix system.

NOTE: the full IP address must be entered. To enter a partial IP address such as "192.168.*", the *IP Address* option must be selected on the [Advanced Search Menu](#).

Item ID

The unique ID of any item in the system - for example 1024.

Advanced Search Menu



Click the advanced search menu to make the following available for selection:

Automatic

The system will use the best search possible given the search text provided, for example, if a MAC address is entered, the system will search only MAC address fields.

Common Fields

The system will search the common fields as described in the [Default Search Fields](#) section.

MAC Address

The system will search only MAC address fields and allows for partial MAC addresses to be entered - for example "AB:*".

IP Address

The system will search only IP address fields.

Database Name

The system will search for databases with the specified name in SQL instances.

Custom Attributes

The system will search the custom attributes assigned to items.

Recurse Containers

When the user is searching a container, this determines whether the system should search for items in child containers. It is enabled by default.

Recurse Locations

When the user is searching a location, this determines whether the system should search for items in child location. It is enabled by default.

Search by Container

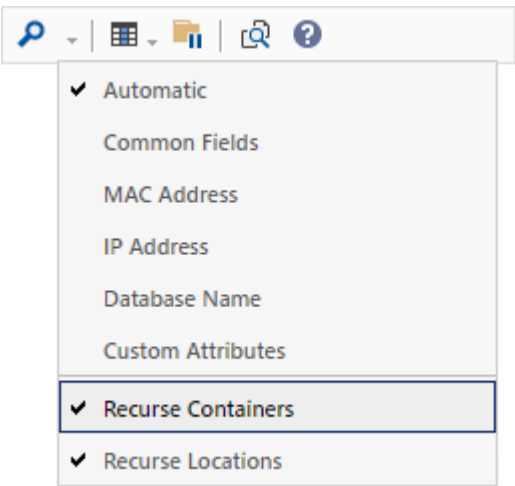
When the system is set to organization, the search filter is restricted to the [container](#) or [customer](#) which is currently selected.



The search field displays information about which [container](#) or [customer](#) will be searched, for example, here it will search the root container *"Demonstration Inc"*.



From the [advanced search menu](#), select recurse containers to determine whether the system should search for items in child [containers](#) and [customers](#).



Search by Type

When the system is set to item type, the search filter is restricted to the **type** of **item** which is currently selected.



The search field will display information about which **item** type will be searched, for example, here it will search for **Windows server** items:



Search by Location

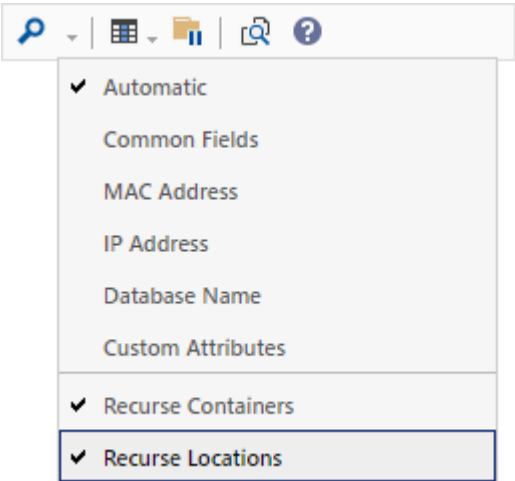
When the system is set to location, the search filter is restricted to the location which is currently selected.



The search field will display information about which location will be searched, for example, here it will search within the location "Room 1".



From the [Advanced Search Menu](#), select **Recurse Locations** to determine whether the system should search for items in child locations.



Security

This section provides information about the authentication and security within [XIA Configuration Server](#).

For information about the security configuration settings, see the [Security Settings](#) section.

Authentication

XIA Configuration utilises the authentication methods built into Windows Internet Information Services (IIS) and supported web browsers. The following methods are supported:

Basic Authentication

This authentication method is useful when hosting XIA Configuration for external customers. Users are prompted for credentials when they access the XIA Configuration site. An SSL certificate should be installed to ensure that the password is encrypted before being sent to the server.

Windows Integrated Authentication

This authentication method can utilise either NTLM or Kerberos and allows the user to be authenticated automatically without being prompted for a username or password. To enable this for use with the [Firefox web browser](#), please see how to [configure Firefox for integrated authentication](#).

Client Certificates

Client certificates can be used as a method of two factor authentication

- To configure the [XIA Configuration Client](#) to use client certificates see the [configuring client certificates](#) section.
- To configure the [XIA Configuration Scheduler](#) to use client certificates see the [configuring client certificates](#) section.
- To use client certificates with the [PowerShell API](#) see the [configuring client certificates](#) section.

Custom Login Page

If you're logging into XIA Configuration server remotely and Windows integrated authentication is not available, you are prompted with the standard authentication dialog window. The background to the browser window is empty or displays the last page that was loaded:

To implement a custom login page, perform the following steps:

1. Create a new **.htm** file on web space that allows **anonymous** access.
2. Open the .htm file in notepad or any suitable HTML editor and enter the following HTML:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <title>Welcome to XIA Configuration Server</title>
  <meta http-equiv="refresh" content="0;url=https://www.centrel-solutions.com/cloud">
  <link href="website.css" rel="stylesheet" type="text/css" />
</head>
<body>
  
  <h1>Authorised Access Only</h1>
  Please login with your network credentials. <br />
</body>
</html>
```

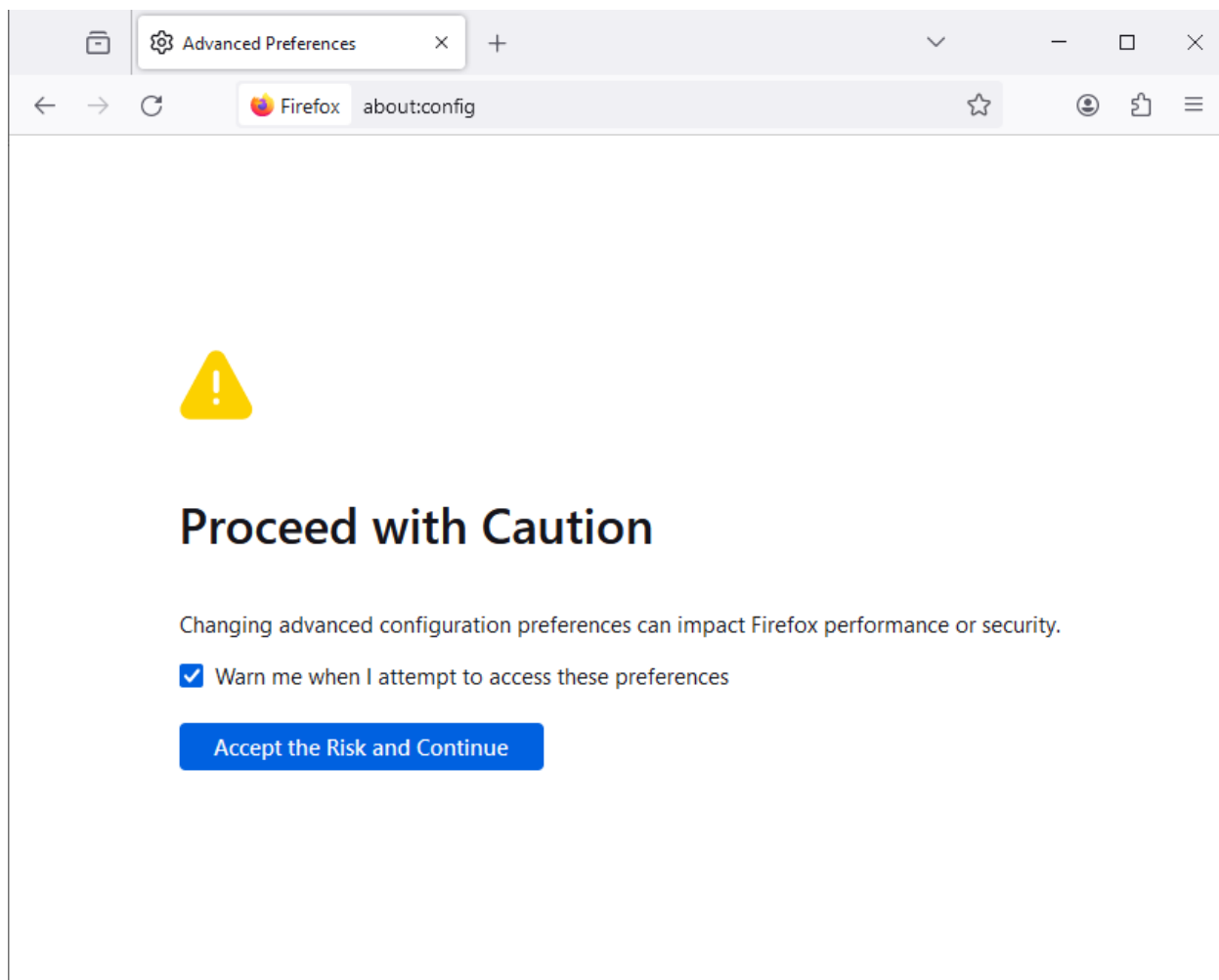
3. Customise the title found between the <title></title> tags to the title you wish to use.
4. Configure the URL to the full URL of XIA Configuration Server.
5. Upload any images and CSS files you require for the web site. The images and css displayed in the sample HTML are provided as an example only.
6. Provide access to users using the newly created .htm file. The web page should load and then immediately redirect to the secure site, prompting for credentials.

Configure Firefox for Integrated Authentication

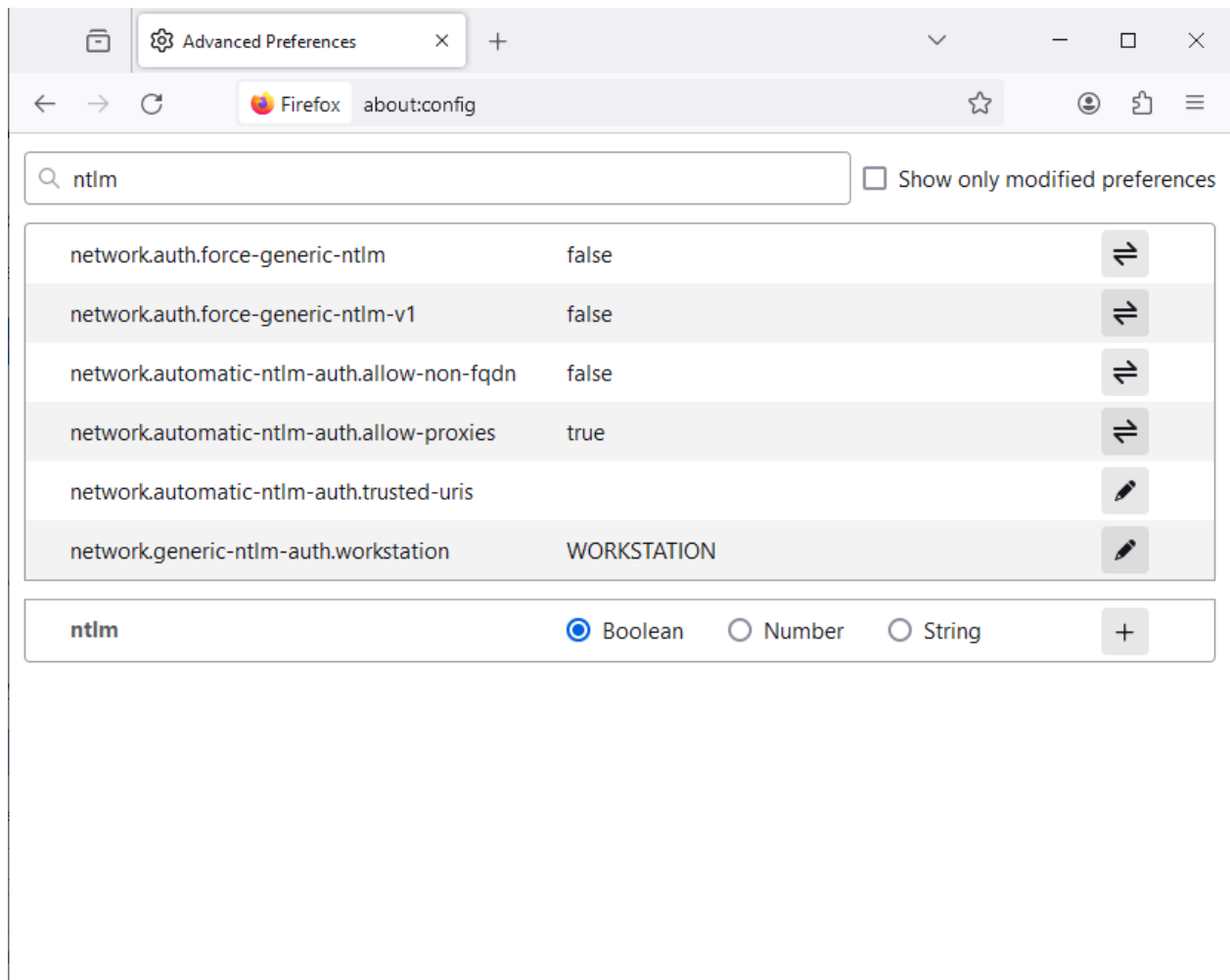
By default the [Firefox](#) web browser does not support *Integrated Authentication* and you are prompted for a password when accessing [XIA Configuration Server](#).

To enable *Integrated Authentication* complete the following steps

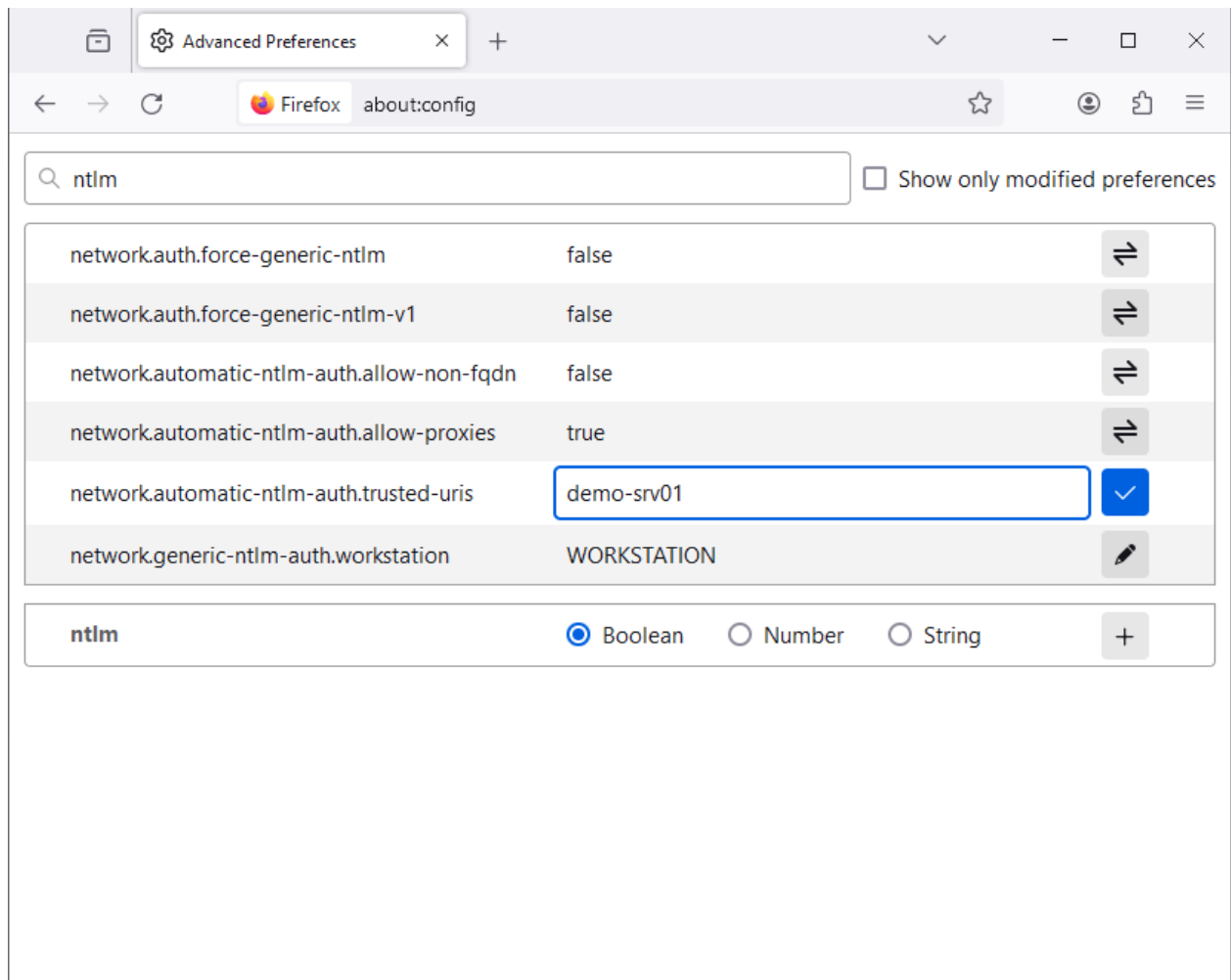
- Open the Firefox browser and enter **about:config** in the address bar.
- Carefully read any warnings and disclaimers and only proceed if you agree to them.



- Enter *ntlm* in the search field.



- Click the edit button next to the *network.automatic-ntlm-auth.trusted-uris* field and enter the [XIA Configuration Server](#) name or fully qualified domain name that is used to access [XIA Configuration Server](#) (**not** the full URL).



- Click the Save button.
- Restart the browser when ready.

Logging Out

As [XIA Configuration Server](#) does not handle authentication directly, the ability to log out of the system is handled by Internet Information Services and your web browser.

When using **Integrated Authentication**, it is not possible to log out of a session because opening the browser and connecting to XIA Configuration Server will perform an NTLM / Kerberos secure login again automatically.

When using **Basic Authentication**, it is possible to log out by:

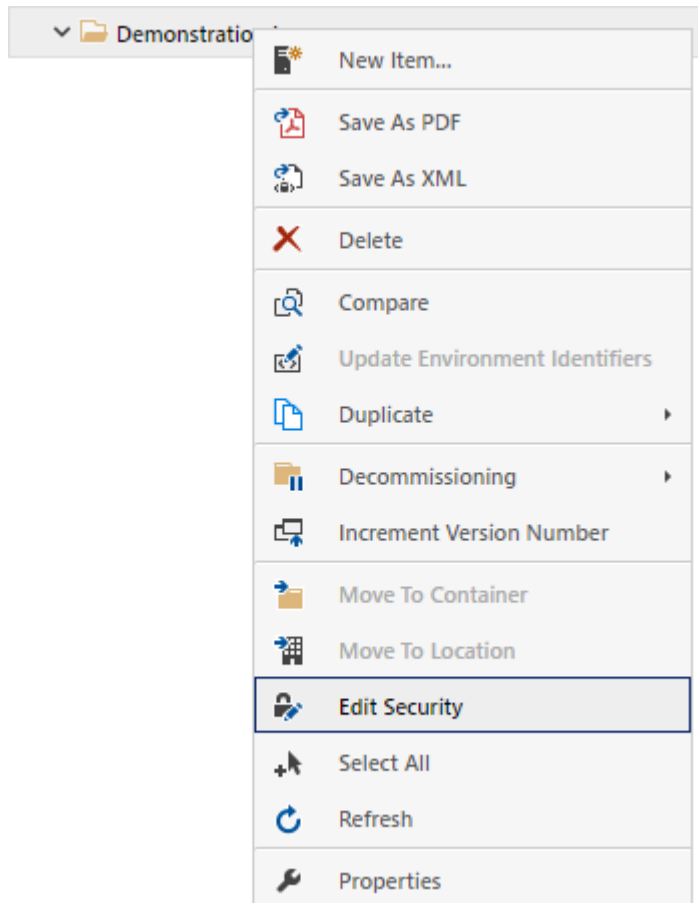
- Ensuring that you do not allow the web browser to save any passwords if prompted.
- Close **all** browser windows.

Attempting to access the [XIA Configuration Server](#) again will prompt for credentials. In a secure environment, it is recommended to ensure that users check that they are again being prompted for credentials before assuming their session is finished.

Granting Access

To grant a user access to the system, either make the user a [system administrator](#), or perform the following

- Access the [system](#) with a web browser as a [system administrator](#).
- Right click the [root container](#).



- Select the *edit security* menu option to display the [security descriptor](#) for the [root container](#).
- Click the *new security entry* button.

Security for Demonstration Inc [1000] - Work - Microsoft Edge
localhost/XIAConfiguration/itemsecurity.aspx?ItemID=1000



Security for Demonstration Inc [1000]

Determines the security that is to be applied to this item.

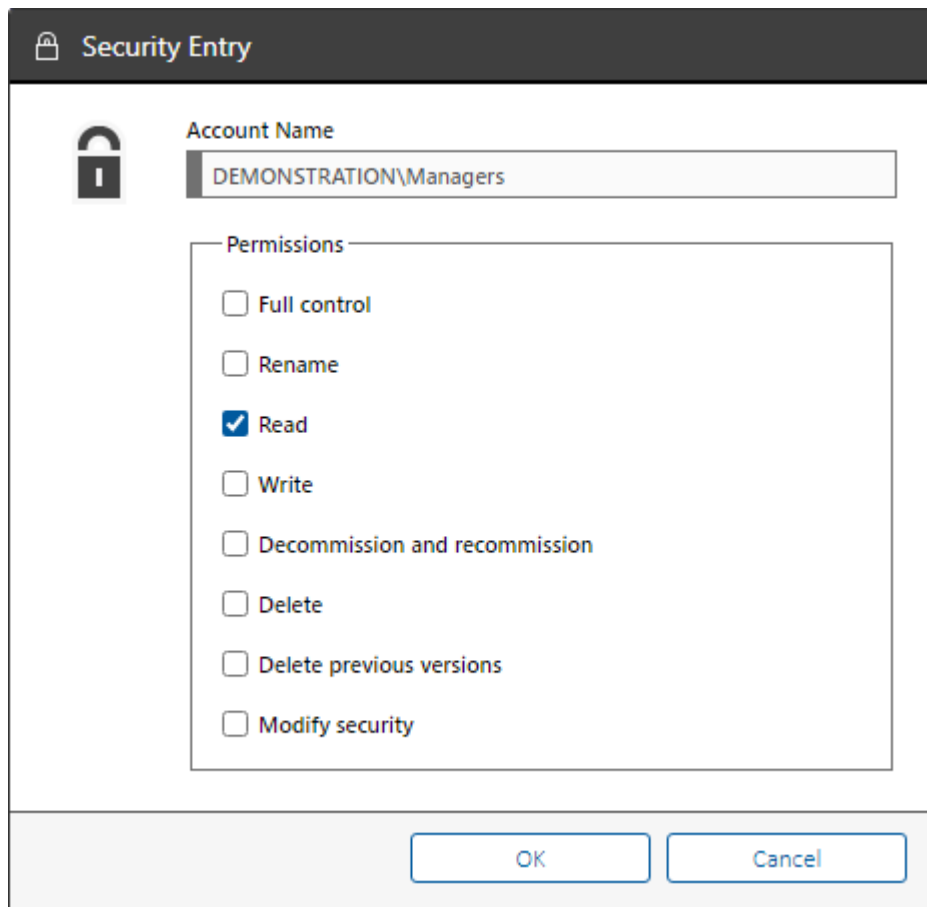
1 Security Entries (applied directly)

Account Name	Full	Rename	Read	Write	Decom.	Delete	Versions	Security
 DEMONSTRATION\Managers	False	False	True	False	False	False	False	False

☐ Replace security on all child objects to inherit from this object.

Enable Inheritance
New Security Entry
Apply Security

- Enter the account name of the user or group you wish to have access to the system and select the appropriate permissions. To access the system, the user must have at least **read** access to the root container.



- Click the *OK* button.
- Click the *apply security* button.

System Administrators

System administrators have full access to use and manage [XIA Configuration Server](#).

Users who are members of the [Administrators group](#) on the machine running [XIA Configuration Server](#) are automatically given system administrator rights, however additional users and groups can be configured within the [security settings](#) section of the [configuration settings](#).

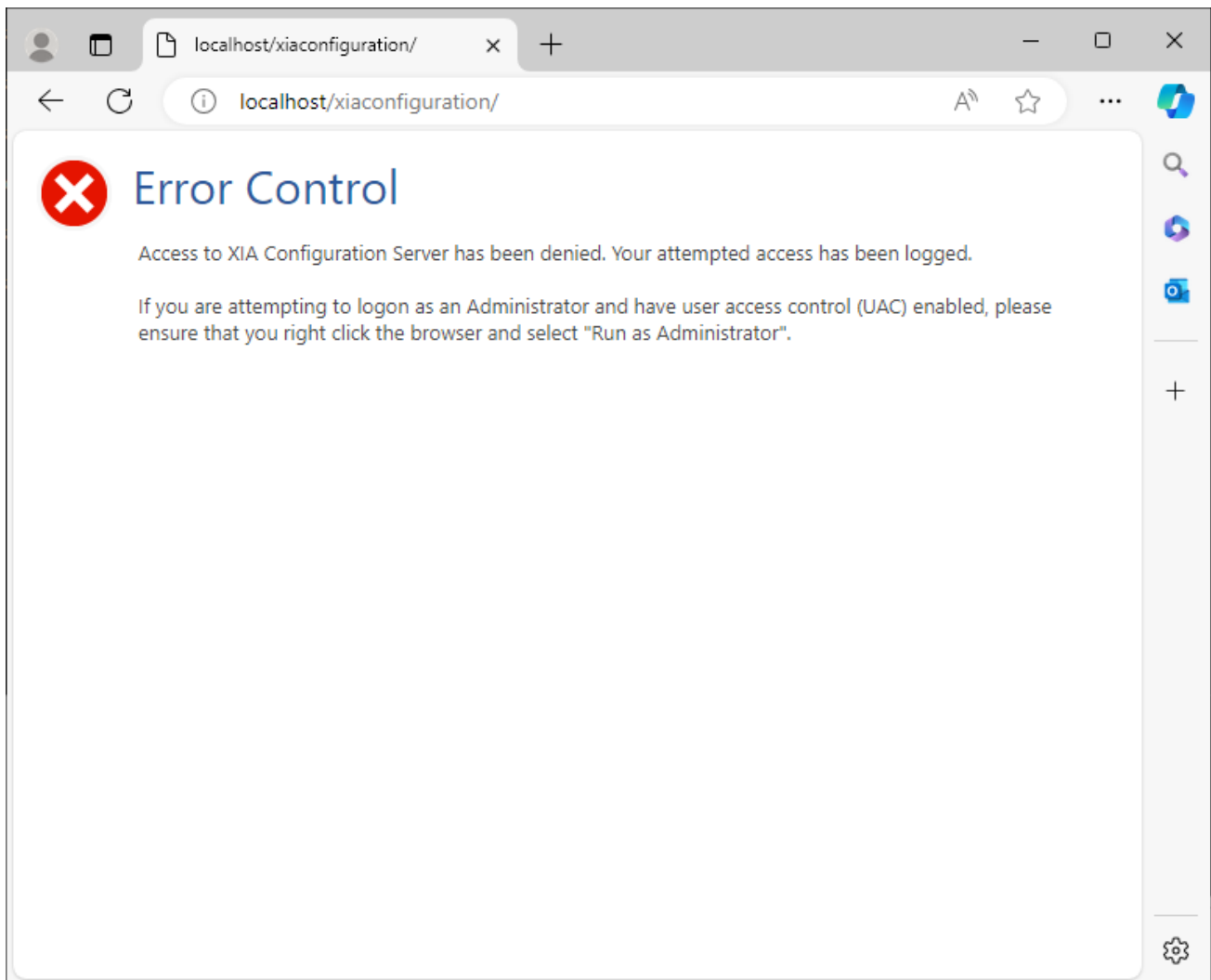
- By default the user who performed the [installation](#) is automatically added as a system administrator.
- Please note that [User Access Control \(UAC\)](#) may affect users being detected as members of the [Administrators group](#).

User Access Control (UAC)

User Access Control (UAC) is a Windows security feature designed to protect the operating system from unauthorized changes. When changes to the system require administrator-level permission, UAC notifies the user, giving the opportunity to approve or deny the change.

By default, all local server Administrators are [system administrators](#) of [XIA Configuration Server](#).

However, with [UAC](#) enabled, you may see the following message displayed.

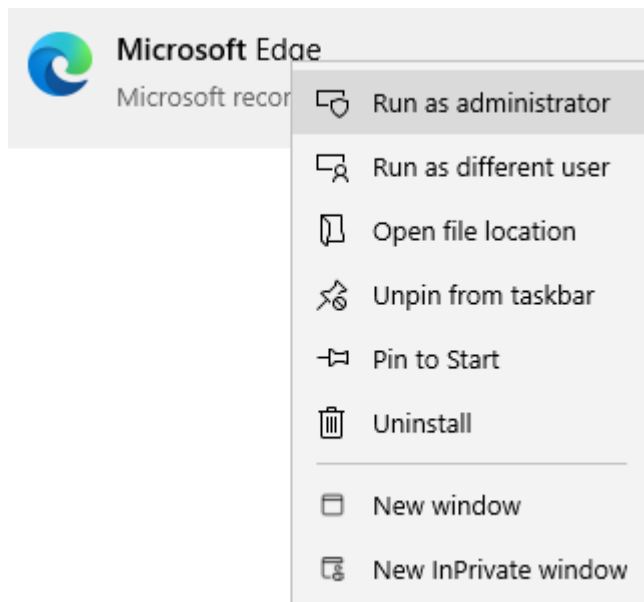


Resolution

To resolve this issue either:

- Start your web browser as an Administrator right click the browser and select "Run as administrator".

NOTE: For Microsoft Edge you may need to add the `--do-not-de-elevate` parameter to the command line.



- or -

- Log in as another user account that is already a [system administrator](#).

Update System Administrators

Once logged into the system as administrator it is possible to go to the security settings and assign your user account as a [system administrator](#), either explicitly or by specifying a group to which the account is a member. This will remove the need to run the browser as an administrator.

Tools > Configuration > Security Settings

 System Administrators

DEMONSTRATION\Managers

Validate Account Names

Server Troubleshooting

The following chapters cover the troubleshooting of [XIA Configuration Server](#), for issues with troubleshooting the [installation](#) see the [server installation troubleshooting](#) section.

Also see the [diagnostics](#) section.

[401.2 - You are not authorized to view this page due to invalid authentication headers](#)

[500.19 - This configuration section cannot be used at this path](#)

[A blank page is displayed](#)

[Access to this XIA Configuration System has been denied by ACL](#)

[Could not execute the report with ID 'XXXX'. Timeout expired](#)

[Error decrypting string value](#)

[Uploading of data to the server fails](#)

[You are prompted for a password when you attempt to access the web interface](#)

A blank page is displayed

Symptoms

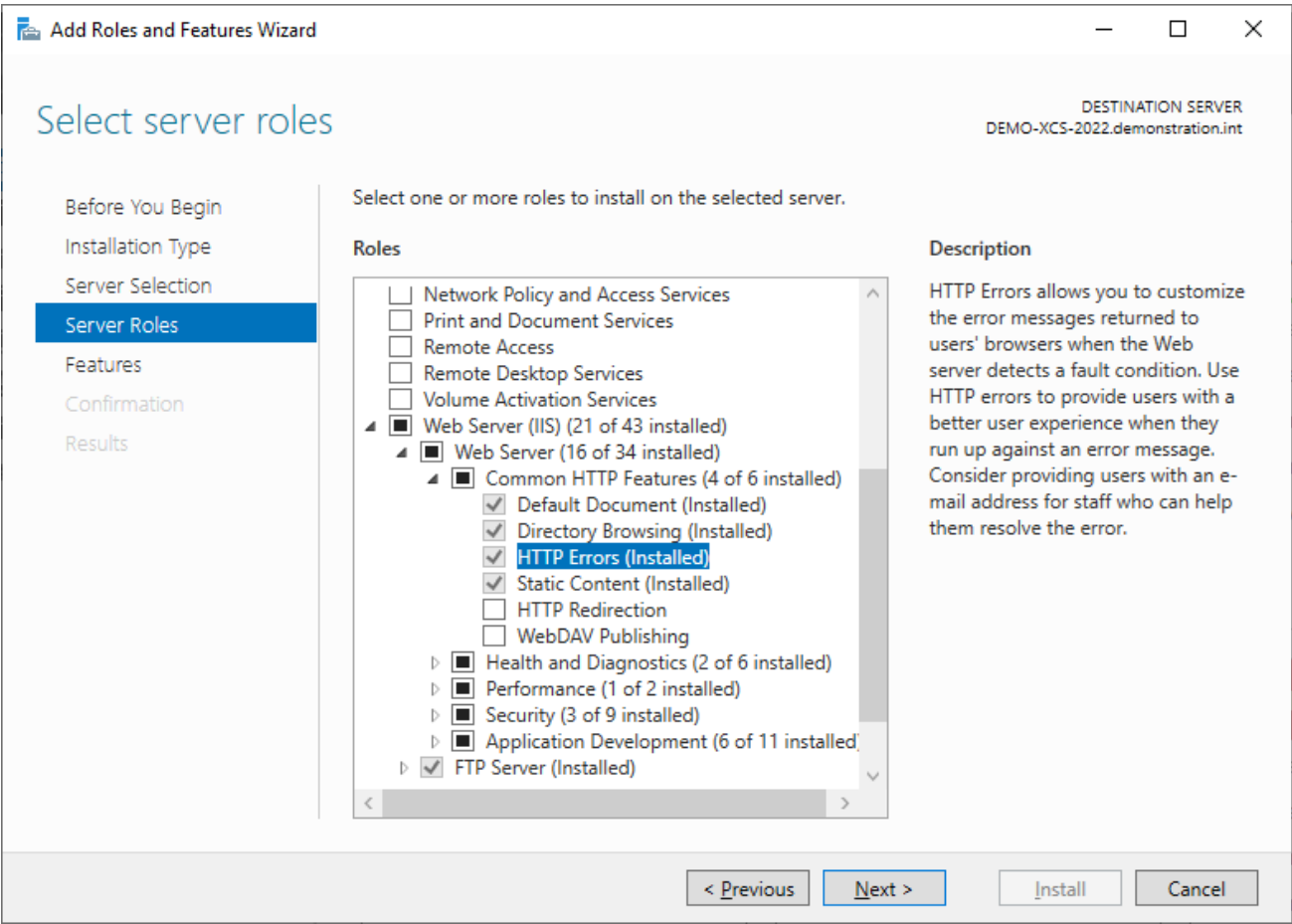
When you attempt to access [XIA Configuration Server](#) a blank page is displayed.

Cause

This is caused by an [Internet Information Server \(IIS\)](#) configuration issue, but the *HTTP Errors* role service is not installed.

Resolution

Ensure the the HTTP Errors role service is installed, and reload [XIA Configuration Server](#).



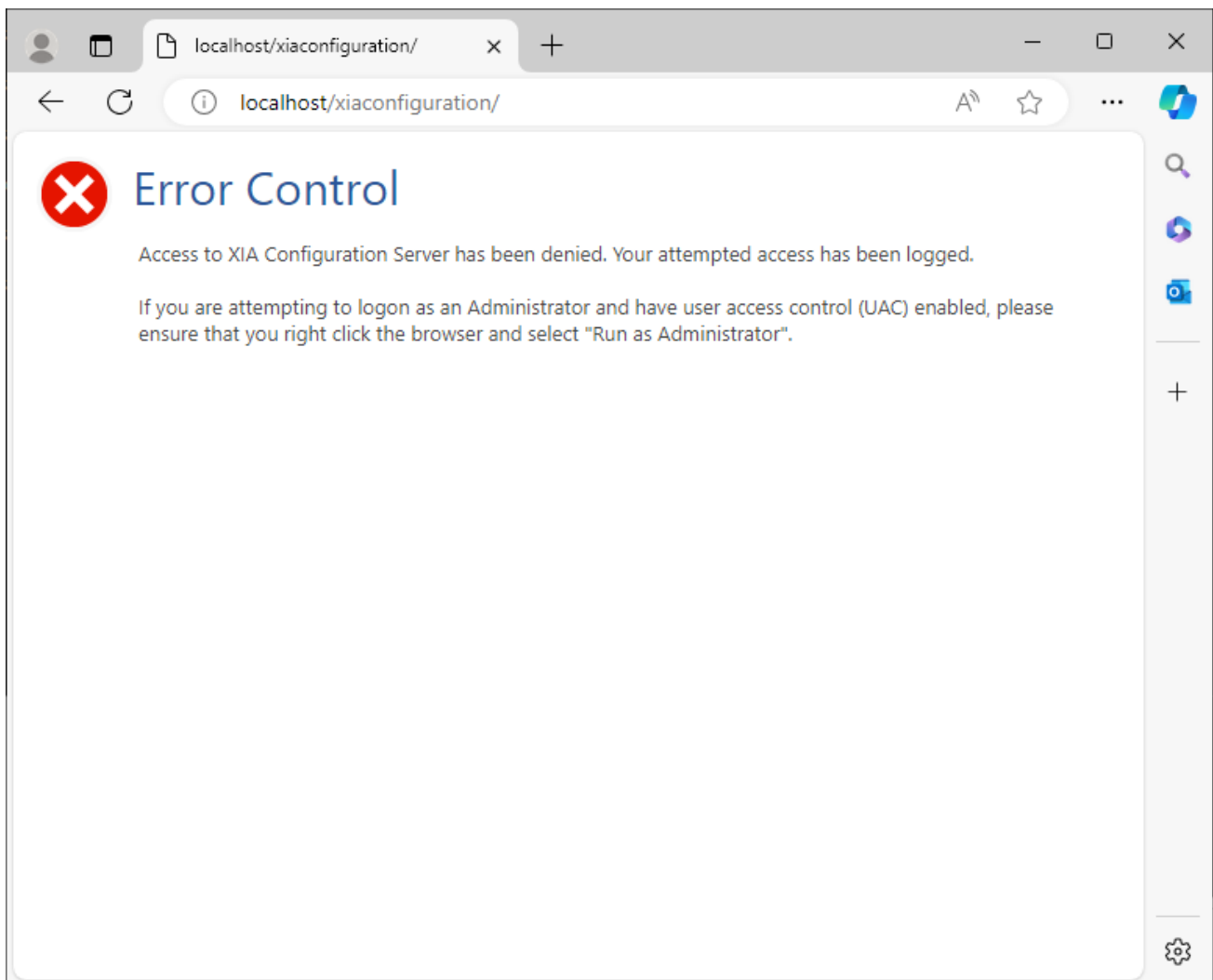
Access to this XIA Configuration System has been denied by ACL

Symptoms

When a user attempts to access the [XIA Configuration Server](#), they may see the following error message

Access to this XIA Configuration System has been denied by ACL. Your attempted access has been logged.

If you are attempting to log-on as an Administrator and have user access control (UAC) enabled, please ensure that you right click the browser and select "Run as Administrator".



Cause

- The user has not been granted permissions to access the [XIA Configuration Server](#).
- The user has been granted permissions to access the [XIA Configuration Server](#) however UAC is preventing access.

Resolution

Depending on the cause as listed above either:

- Follow the instructions in the [granting access](#) section.
- Follow the instructions in the [User Access Control \(UAC\)](#) section.

Could not execute the report with ID 'XXXX'. Timeout expired.

Symptoms

When executing a [report](#) on [XIA Configuration Server](#), you see the message:

"Could not execute the report with ID 'XXXX'. Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding."

where "XXXX" is the unique identifier of the report.

Cause

The report is taking longer to execute than the current reporting timeout.

Resolution

- If this is a [custom written](#) report, review the SQL query and optimize if possible.
- Open the [Configuration Settings](#)
- Increase the **Report Execution Timeout** setting within the [Database Connection Settings](#) section.

Error decrypting string value

Symptoms

When accessing a configuration page or viewing a [diagnostics log](#), you see the message:
"Error decrypting string value"

Cause

XIA Configuration uses encryption to store sensitive data. The error can be caused when:

- The [encryption keys](#) are deleted or replaced.
- A configuration file is copied from another machine where different [encryption keys](#) were used to perform the encryption.

Resolution

Ensure that the correct [encryption keys](#) are in place.

HTTP Error 401.1 - Unauthorized

Symptoms

When you attempt to access [XIA Configuration Server](#) you may see the following error message:
HTTP Error 401.1 - Unauthorized

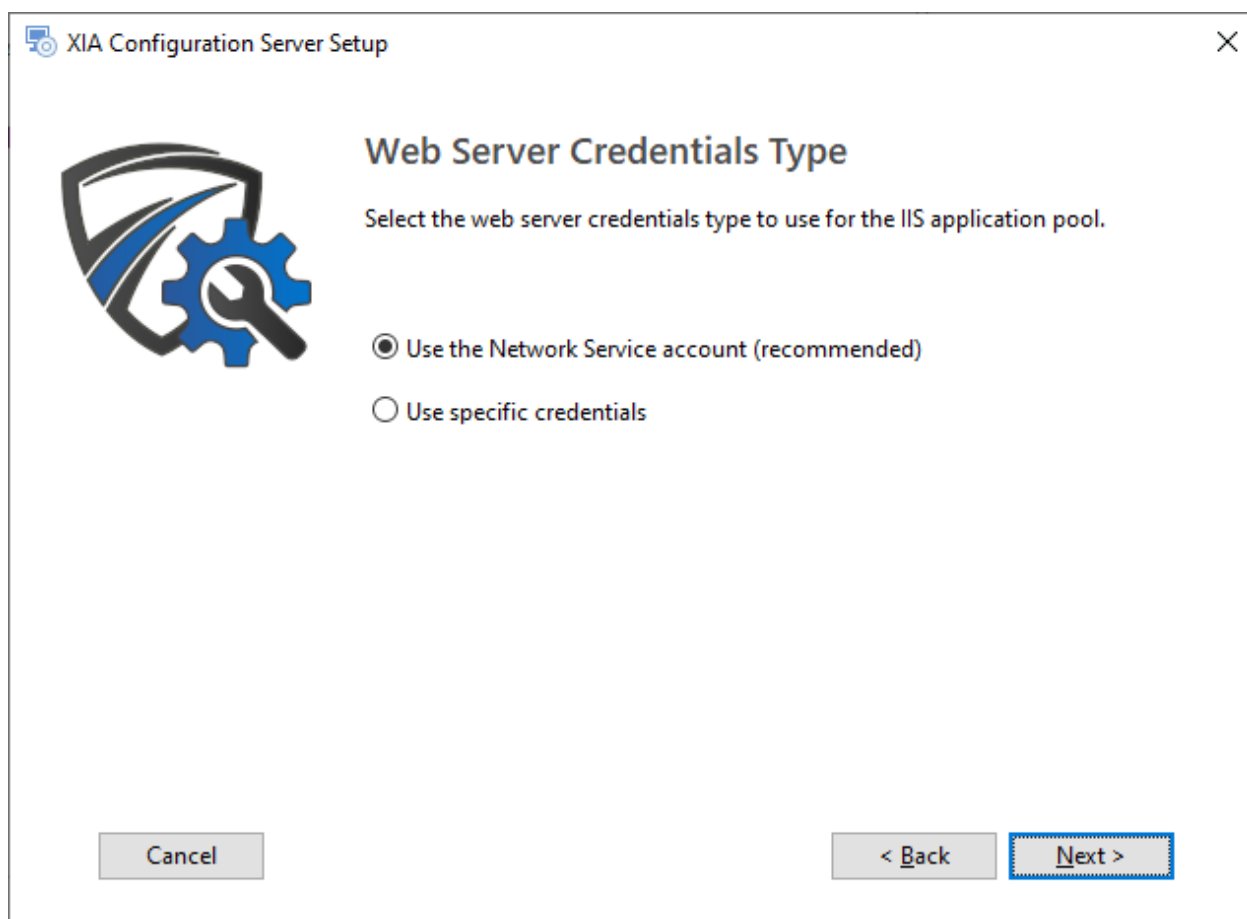
Cause

The issue can be caused if

- You are accessing [XIA Configuration Server](#) using a NetBIOS name or fully qualified domain name that is different from the server name - for example the server is *demo-srv01.demonstration.int* and you are using the address *inventory.demonstration.int*.

- and -

- You [installed XIA Configuration Server](#) using specific credentials instead of the default which is to use the [Network Service account](#). This sets the credentials used by the [XIA Configuration Server](#) application pool.



Resolution

To resolve the issue

- Access the server using the server's fully qualified domain name.
- or -
- When you [install XIA Configuration Server](#) select the option to use the [Network Service account](#).
- or -
- Register the SPN for the custom FQDN and specific credentials using the following Microsoft article [KB871179](#).

HTTP Error 401.1 - Unauthorized (locally only)

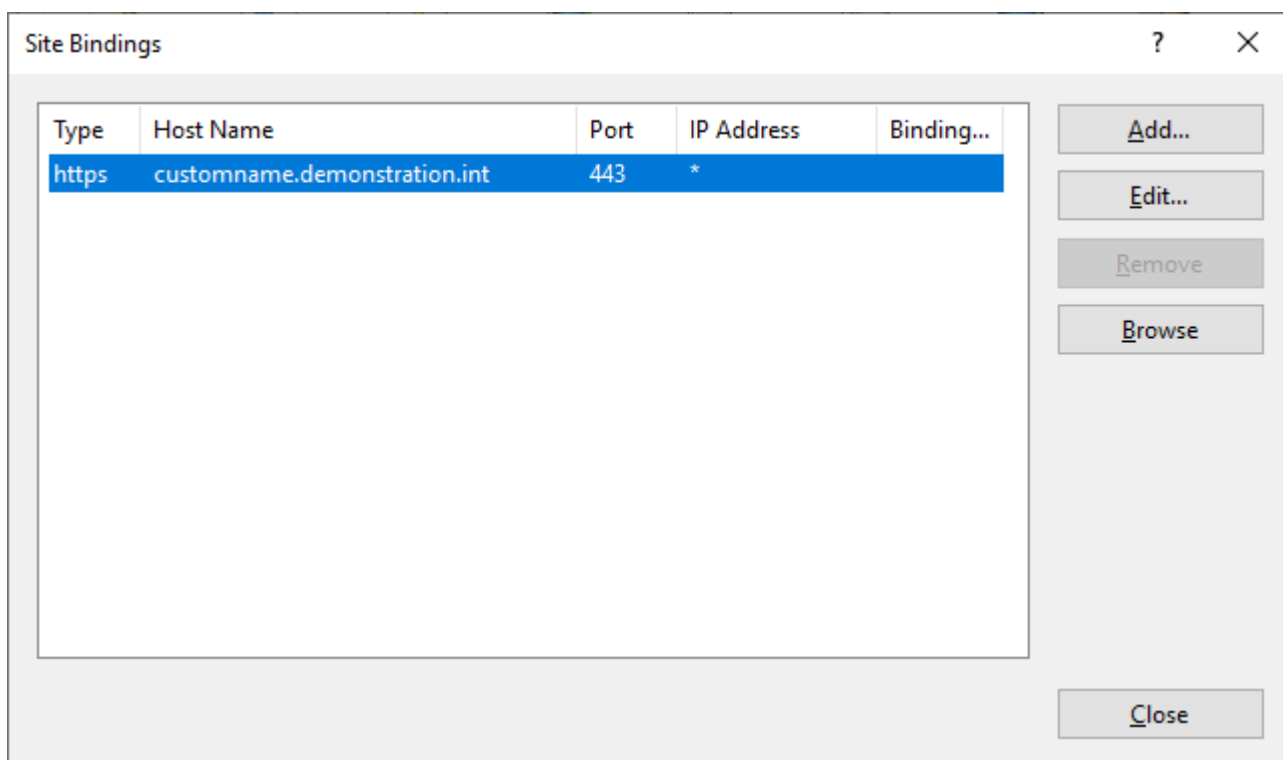
Symptoms

When you attempt to access [XIA Configuration Server](#) **locally** from the server where it is installed you may be prompted for credentials. Entering the credentials does not allow access even when the credentials are correct and the following error is displayed

HTTP Error 401.1 - Unauthorized

Cause

The issue can be caused if you are accessing the server locally using a custom server name or fully qualified domain name. Windows XP SP2, Windows Server 2003 SP1, and above include a loopback check security feature that is designed to help prevent reflection attacks on your computer. Therefore, authentication fails if the FQDN or the custom host header that you use does not match the local computer name. For more information see the [Microsoft article](#).



Resolution

- Access the server remotely.
- or -
- Configure the site bindings to allow the server to be accessed using its NetBIOS name or fully qualified domain name.
- or -

- Follow the instructions in the [Microsoft article](#).

HTTP Error 401.2 - You are not authorized to view this page due to invalid authentication headers

Symptoms

When you attempt to access [XIA Configuration Server](#) you receive the following message

HTTP Error 401.2 - Unauthorized

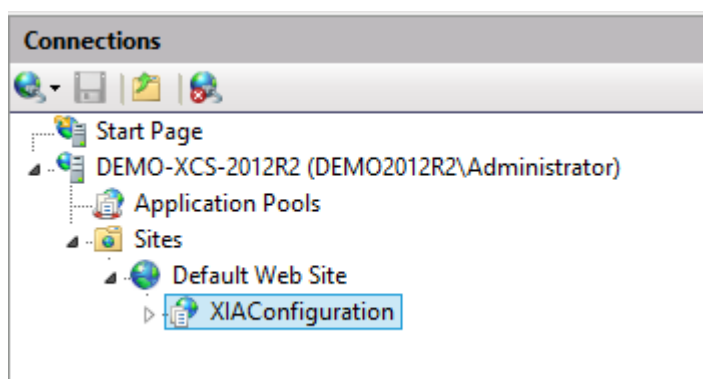
You are not authorized to view this page due to invalid authentication headers.

Cause

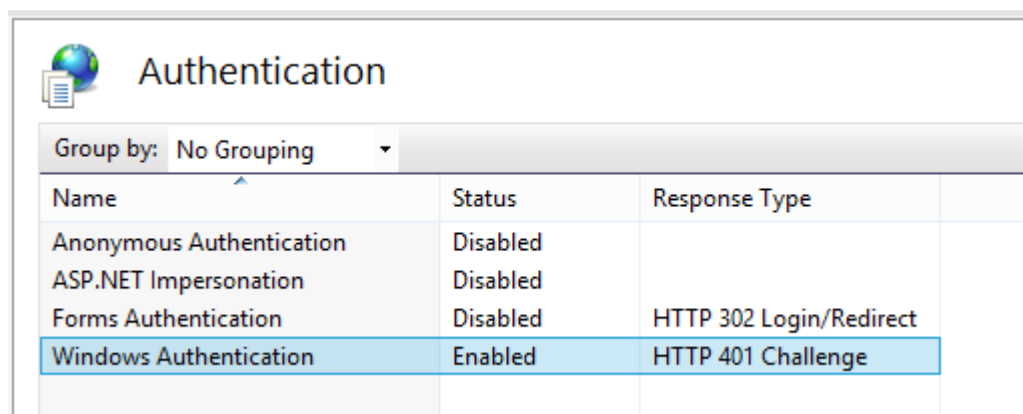
This is caused by the [Internet Information Server \(IIS\)](#) authentication settings being incorrectly configured.

Resolution

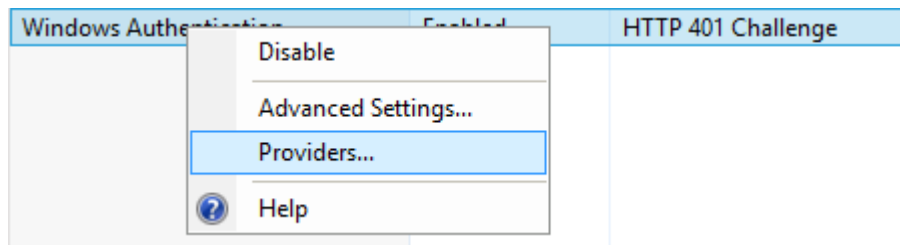
- Open the *Internet Information Services (IIS) Manager* from *Administrative Tools*.
- Browse to the [XIA Configuration Server](#) application, by default this is *XIAConfiguration*.



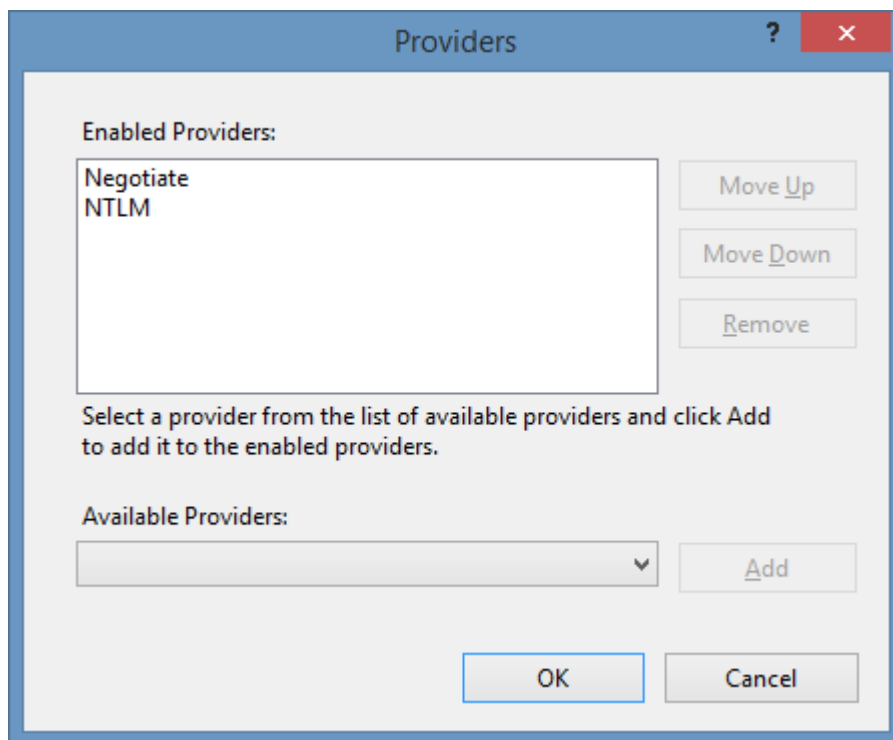
- Goto the *Authentication* section.
- Ensure that only *Windows Authentication* is *Enabled*.



- Right click *Windows Authentication* and select *Providers*.



- Ensure that the *Enabled Providers* is set to *Negotiate* and *NTLM*.



HTTP Error 500.0 - Internal Server Error

Symptoms

When you attempt to access [XIA Configuration Server](#) you may see the following error message:

HTTP Error 500.0 - Internal Server Error

The page cannot be displayed because an internal server error has occurred.

More Information

Accessing a specific page such as the following may cause the page to be displayed but with incorrect styling and images missing.

<https://DEMO-SRV01/XIAConfiguration/default.aspx>

Cause

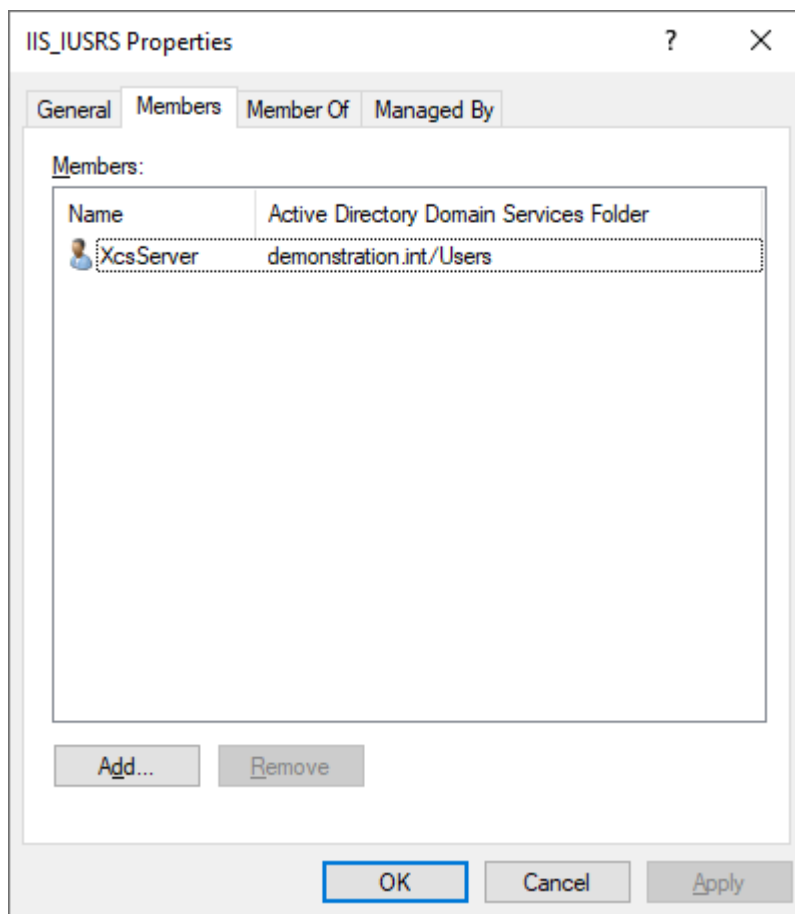
This error can occur if the [web server account](#) does not have the [impersonate a client after authentication](#) user right.

Typically the [Network Service](#) account has this right so the issue is normally only seen when [XIA Configuration Server](#) has been [installed](#) using a custom [web server account](#).

This error is normally only seen when specific security policies have been applied by your organization to the server where [XIA Configuration Server](#) is [installed](#).

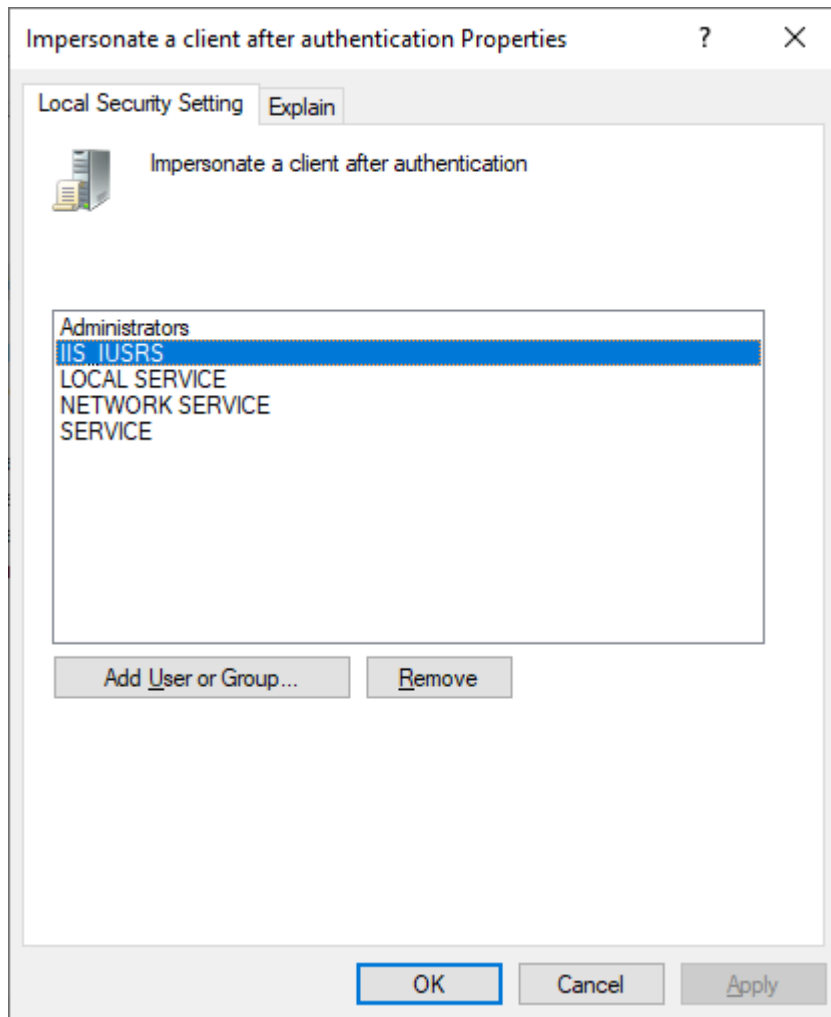
Resolution

- Check that the [web server account](#) is a member of the IIS_IUSRS local group.



- In the Local Security Policy (secpol.msc) select *Local Policies* then select *User Rights Assignment*.
- Open the [impersonate a client after authentication](#) user right.

- Ensure that the IIS_IUSRS group has this right



- or -

- [Reinstall XIA Configuration Server](#) using [Network Service](#) as the [web server account](#).

HTTP Error 500.19 - This configuration section cannot be used at this path

Symptoms

When you attempt to access [XIA Configuration Server](#) you may see the following error message:

HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

This configuration section cannot be used at this path. This happens when the section is locked at a parent level. Locking is either by default (overrideModeDefault="Deny"), or set explicitly by a location tag with overrideMode="Deny" or the legacy allowOverride="false".

Cause

- The required [roles and features](#) have not been installed on the machine running [XIA Configuration Server](#).

- or -

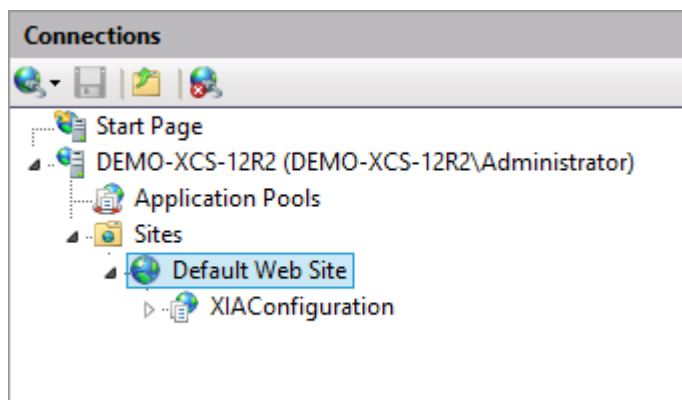
- A configuration section has been **locked** on the IIS server.

Resolution 1: Roles and Features

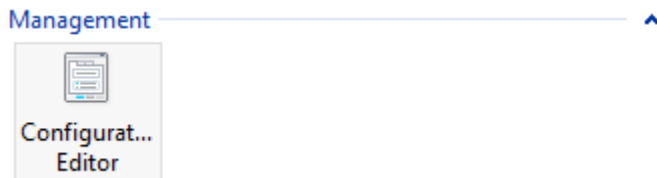
- Ensure that all [roles and features](#) have been installed.

Resolution 2: Check Configuration Section Locking

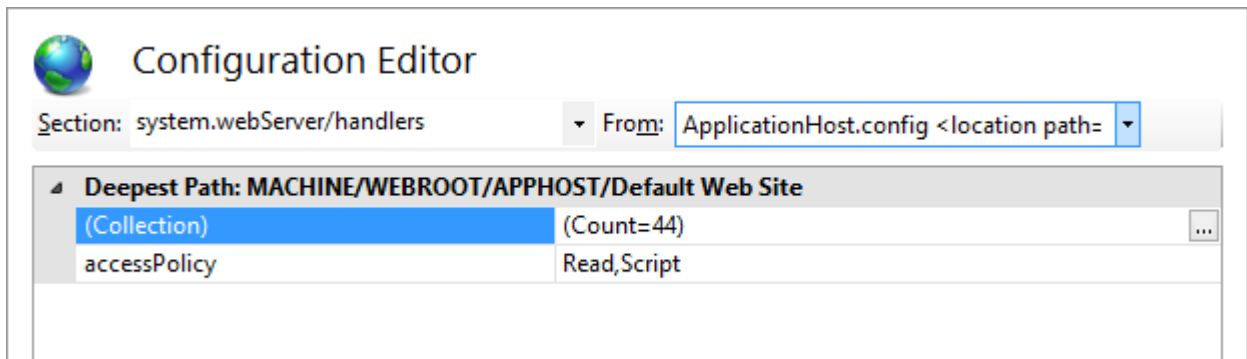
- Open IIS Manager and browse to the **Default Web Site**.



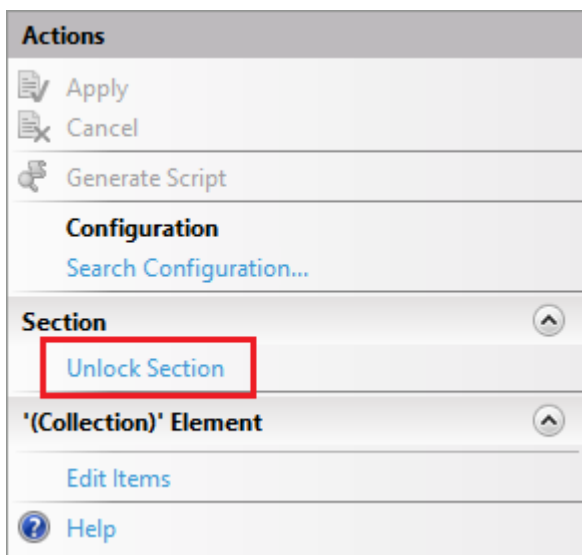
- Go to **Management > Configuration Editor**.



- Select "system.webServer/handlers" in the **Section** dropdown and "ApplicationHost.config" in the **From** dropdown.



- In the **Actions** pane click **Unlock Section**.



The 'PRIMARY' filegroup is full

Symptoms

When you attempt to update [XIA Configuration Server](#) you may see the following error message:

Could not allocate space for object 'table' in database 'XIAConfiguration' because the 'PRIMARY' filegroup is full. Create disk space by deleting unneeded files, dropping objects in the filegroup, adding additional files to the filegroup, or setting autogrowth on for existing files in the filegroup.

Cause

The issue can be seen if

- The [database](#) used by [XIA Configuration Server](#) is found on a drive that does not have sufficient disk space.

- or -
- The [database](#) used by [XIA Configuration Server](#) is hosted on [Microsoft SQL Server](#) Express Edition, and the [database](#) has reached the size limit imposed by Express Edition.

Resolution

To resolve the issue

- Ensure that drive on which the [XIA Configuration Server database](#) is found has sufficient disk space.

- or -
- Use the [previous versions management](#) tool to delete some of the [version history](#) of [items](#) that are no longer required.

- or -
- If the [database](#) used by [XIA Configuration Server](#) is hosted on [Microsoft SQL Server](#) Express Edition, upgrade the instance to an edition that does not have a database size limit.

This page can't be displayed

Symptoms

When a user attempts to access the [XIA Configuration Server](#), they may see one of the following error messages depending on the browser used.

- This page can't be displayed
- This site can't be reached

Cause

This issue can occur if HTTP redirect has been configured within IIS, and the redirect has been applied at both the web site and application level.



Resolution

- Confirm if HTTP Redirect has been enabled on the web site hosting the [XIA Configuration Server](#) application.



HTTP Redirect

Use this feature to specify rules for redirecting incoming requests to another file or URL.

☒ **R**edirect requests to this destination:

Example: <http://www.contoso.com/sales>

Redirect Behavior

☒ **R**edirect all requests to exact destination (instead of relative to destination)

☐ **O**nly redirect requests to content in this directory (not subdirectories)

Status code:

- If enabled, ensure that HTTP redirect has been configured with the correct address.
- Ensure that HTTP Redirect has been disabled on the [XIA Configuration Server](#) application.

Uploading of data to the server fails

Symptoms

When you are uploading data manually to [XIA Configuration Server](#) using the upload page, you may see the error.

The connection to the server was reset while the page was loading.

When uploading using the XIA Configuration Client, the following error may be shown in the results file:

The request failed with HTTP status 404: Not Found.

Cause

This error can be seen when the data file being uploaded exceeds the maximum request length configured by ASP.NET.

Resolution

The maximum size can be modified by opening the **web.config** file found in the XIA Configuration Server installation directory and modifying the **maxRequestLength** property of the **httpRuntime** section to be the same or greater than the size of the data file being uploaded.

```
<!--  
    The maxRequestLength in kilobytes determines the maximum file size that can be sent to XIA  
    Configuration  
    This can be extended to a higher amount if the Output from the XIA Configuration Client  
    exceeds this amount.  
-->  
<httpRuntime maxRequestLength ="30000" />
```

For IIS7 and above, the following must also be modified in the **system.webServer** configuration section which controls the request filtering settings for this platform:

```
<security>  
  <requestFiltering>  
    <requestLimits maxAllowedContentLength="35000000"/>  
  </requestFiltering>  
</security>
```

You are prompted for a password when you attempt to access the web interface

Symptoms

When you attempt to access [XIA Configuration Server](#) you are prompted for a password, clicking cancel displays an authorisation error.

Cause

This is caused by the [XIA Configuration Server](#) address not being in your Local Intranet Zone and therefore the browser is not passing your current credentials to the [XIA Configuration Server](#).

Resolution

Ensure that the [XIA Configuration Server](#) address is in the Local Intranet Zone and that the connection is not via a proxy server.

When using [Firefox](#) you may need to [configure Firefox for integrated authentication](#).

ServiceNow Integration

XIA Configuration Server is able to integrate with a [ServiceNow](#) instance using the [ServiceNow Connector](#).

Supported Item Types

The following [item types](#) support synchronization with a [ServiceNow instance](#).

Windows Servers

Windows Servers

[Windows server](#) items support synchronization with a [ServiceNow instance](#) including.

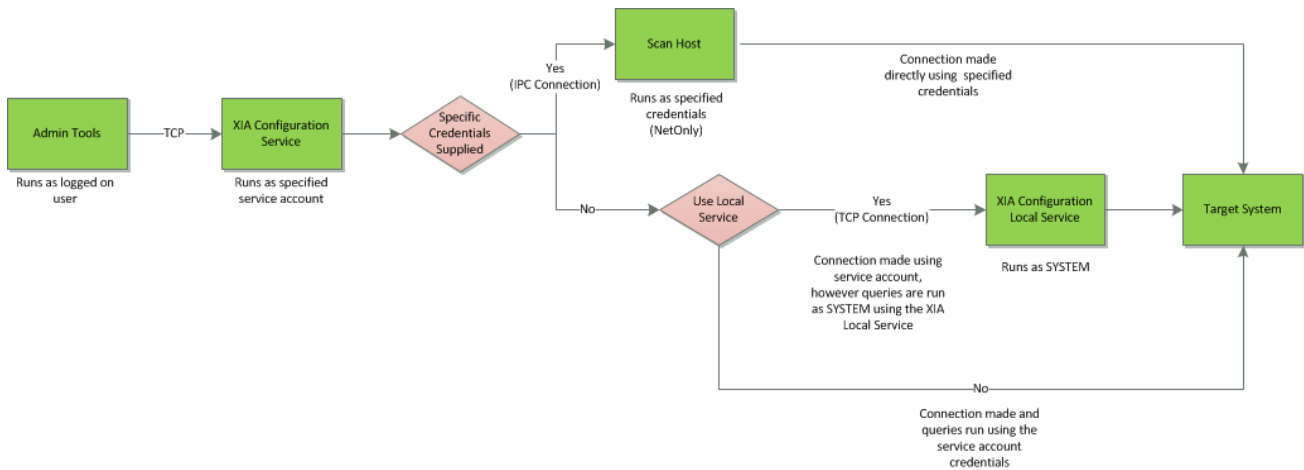
- CPU Count
- CPU Core Core
- CPU Manufacturer
- CPU Name
- CPU Type
- Manufacturer
- Total Disk Space
- Fully Qualified Domain Name
- Operating System Name
- Operating System Address Width
- Operating System Service Pack
- Total RAM
- Virtual / Physical

Technical Reference

This section provides a technical reference to the software.

Credentials and Security Contexts Overview

The following displays under what credentials and security contexts the XIA Configuration Client and associated services are run.



Admin Tools

The admin tools are a Windows forms based application that runs under the context of the interactive user. The tools connect to the XIA Configuration Service using (by default) the credentials of the interactive user however specific credentials can be provided within the user interface. The admin tools will raise a UAC prompt when executed if required.

XIA Configuration Service

The XIA Configuration Service runs with specific credentials configured in the services MMC. These credentials are typically required to have permissions to access and scan the systems on the network however this is not essential as alternative credentials can be supplied or the Local Service can be used.

Scan Host

When alternative credentials are supplied in the scan profile the XIA Configuration Service will start a scan host application using those credentials. As these credentials are NetOnly credentials it is possible to supply a username and password that can access resources on an untrusted Active Directory domain or workgroup.

Local Service

The local service is installed locally on Windows based target systems and uses the SYSTEM account. This simplifies credential management and security issues however does require that the client software be maintained on target systems. By default, the XIA Configuration Service connects to the Local Service using the Service Account credentials however alternative credentials can be supplied that are valid on the target system.

GUID

A [globally unique identifier \(GUID\)](#) is a 128-bit value consisting of one group of 8 hexadecimal digits, followed by three groups of 4 hexadecimal digits each, followed by one group of 12 hexadecimal digits.

GUIDs are the [Microsoft](#) implementation of the distributed computing environment (DCE) universally unique identifier (UUID).

The following is an example of a GUID

6B29FC40-CA47-1067-B31D-00DD010662DA

Viewing and Editing Items

When viewing an item, the following toolbar items are available:



 Displays the [generate documents dialog](#)

 Saves the item as [XML](#)

 Save changes to the current [item](#) (available only in [edit](#) mode)

 [Edits](#) the [item](#) (only available if you have write [permissions](#) to the item)

 Expands all items in the treeview

 Collapses all items in the treeview

 [Compares](#) this [item](#) to another [item](#)

 Shows the help

Checking Out Items

When [items](#) are edited by a user, they are automatically checked out so that they cannot be edited by other users.

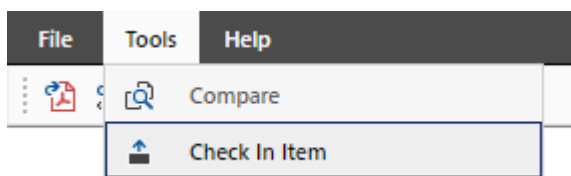
This checkout occurs when the edit button  is clicked on the toolbar.

NOTE: When an [item](#) is checked out, updates are also blocked from the [XIA Configuration Client](#).

When the user saves the changes  to an [item](#) or clicks the cancel edit button , the [item](#) is automatically checked in.

In addition [items](#) can be checked in using the following methods

- The user who has checked out an item, or a [system administrator](#) can select *check in item* from the tools menu.



- A [system administrator](#) can view and check in [item](#) using the [checked out items](#) user interface.
- The [scheduler](#) can automatically check in [items](#) that have been checked out for a specified number of minutes within the [check out](#) settings.

Custom Sections

[Custom sections](#) are created by [system administrators](#) to allow additional information to be collected for an [item](#).

General Information

The general information tab provides an overview of the [item](#).



DEMO-SRV01 | Windows Server | 40963

General Information

Provides general information for this item.

 General Information

Name	DEMO-SRV01
Description	Demonstration Windows server.
Primary Owner Name	IT Services Department
Primary Owner Contact	itservices@demonstration.int

 System Information

Item Path	Demonstration Inc > Managed Customers > Customer 1
Identifier	467d4bb4-7817-4c4a-8a93-4dca715219b5
Item ID	40963
Version ID	1.06
Check Out Status	Available

 HPE DL380 Gen 11



 Custom Item Details

This is a sample Windows server.

Item ID

The unique identifier of the [item](#).

Item Path

The location of the [item](#) in the organizational view.

Version

The currently viewed [version](#) of the [item](#).

Checkout Status

Determines whether the [item](#) is currently [checked-out](#) and being [edited](#). This field will display the username of the user that has [checked-out](#) the [item](#), or *Available* if the [item](#) is not currently [checked-out](#).

Name

The name of the [item](#).

Description

A description of the [item](#). Depending on the [item type](#), this field may have been populated automatically by the [XIA Configuration Client](#), but can also be manually updated.

Primary Owner Name

The name of the owner of the [item](#). Depending on the [item type](#), this field may have been populated automatically by the [XIA Configuration Client](#), but can also be manually updated.

Primary Owner Contact

The contact details of the owner of the [item](#). Depending on the [item type](#), this field may have been populated automatically by the [XIA Configuration Client](#), but can also be manually updated.

Hardware Image and Name

If the [item](#) is a hardware item and the manufacturer and model have been detected as a known [hardware definition](#) an image and details of the detected hardware will be displayed.

Custom Item Details

This field allows additional information to be added to the [item](#) using the [HTML editor](#) control.

Client Information

This section provides information about the [XIA Configuration Client](#) that scanned this [item](#).

This information is not displayed for manually created items.

Client Information

Provides information about the client that was used to generate the information and the data used by the client to uniquely identify this item.

 Item Identifiers	
Primary Identifier	DEMO-SRV01
Secondary Identifier	HPE12345
Tertiary Identifier	
Environment Identifier	
 Client Information	
Client Machine Name	CENTREL-WS01
Client Identifier	ccbf2b98-938d-4ab6-b29f-fd5f71d0e69c
Client IP Address	192.168.1.182
Client Scan Date	11 September 2024 11:19 (today)
Client Service Username	DEMONSTRATION\XiaConfigurationSvc
Client Version	16.2.8.0
 Scan Profile	
Target	DEMO-SRV01
Profile Name	Default Scan Profile
Profile Identifier	be3c53be-2624-4f5b-a964-c311d18dbf04

Item Identifiers

The [item identifiers](#) that are used to uniquely identify this [item](#).

Client Machine Name

The NetBIOS name of the computer running the [XIA Configuration Client](#).

Client Identifier

The unique identifier of the [XIA Configuration Client](#) in [GUID](#) format used when the [client registers](#)

and communicates with the [XIA Configuration Server](#).

Client IP Address

The IP address of the computer running the [XIA Configuration Client](#).

Client Scan Date

The date and time that the [item](#) was scanned.

Client Service Username

The name of the user account that performed the scan - this is either the [service account](#) or the [custom credentials](#) configured for the [scan profile](#).

Client Version

The version of the [XIA Configuration Client](#) software that performed the scan.

Target

The target of the [scan task](#) that performed the scan.

Profile Name

The name of the [scan profile](#) that documented the item.

Profile Identifier

The unique identifier of the [scan profile](#) that documented the item in [GUID](#) format.

Editing Items

To edit an [item](#), click the edit button  on the toolbar (this is only enabled if you have [write permissions](#) to the [item](#), and the [item](#) has not been [decommissioned](#)).

Whilst being edited, the [item](#) is [checked out](#) and cannot be modified by other users.

 Clicking the cancel edit button undoes any changes made to the [item](#) and returns to view mode.

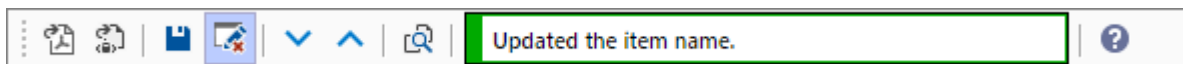
 Clicking the save button on the toolbar saves changes to the [item](#).

It is possible to enter a description of the changes that have been made, this is displayed on the [version history](#) for the [item](#).

This field can be made mandatory within the [configuration settings](#), which will cause the field to display in red and the user will be unable to save their changes until a [version description](#) has been entered:



When the [version description](#) has been entered, the field will display in green:



Effective Permissions

This section displays the user's effective [security descriptor](#) permissions for the currently viewed item.

Effective Permissions

Provides information about the effective permissions for the current user.

 DEMONSTRATION\tjackson	
Full control	True
Rename	True
Read	True
Write	True
Decommission and recommitment	True
Delete	True
Delete previous versions	True
Modify security	True

Location

Physical [items](#) can be [assigned a location](#) which dynamically generates the information visible in the location section.



DEMO-SRV01 | Windows Server | 40963

Location

Provides details of the physical location of this item.

 Data Center 1

Street	123 North Street
City	London
State, Province, or County	
ZIP or Postal Code	NW1 1AB
Country	United Kingdom

 Room

Name	Room 1
------	--------

 Rack

Name	Rack 1A
------	---------

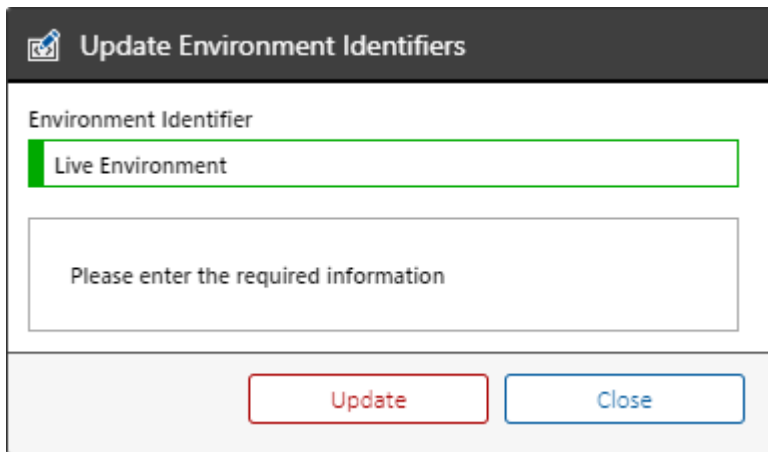
Manually Updating Environment Identifiers

When the [XIA Configuration Client](#) sends data to the [XIA Configuration Server](#), [item identifiers](#) are used to locate an existing [item](#) to be updated.

[Environment identifiers](#) are used to distinguish between multiple identical [items](#) where the primary, secondary, and tertiary identifiers are all identical.

To manually update the [environment identifiers](#) for multiple [items](#)

- Select the [items](#) in the user interface.
- Right click the [items](#) and click the update environment identifiers context menu item.
- This displays the update environment identifiers dialog.



The dialog box is titled "Update Environment Identifiers" with a small icon of a document and a pencil. It contains a text input field labeled "Environment Identifier" with the text "Live Environment" inside. Below the input field is a large rectangular box with the text "Please enter the required information". At the bottom of the dialog are two buttons: "Update" (with a red border) and "Close" (with a blue border).

- Enter the new [environment identifier](#) and click the update button.

Relationships

The relationships section displays the relationships between an [item](#) and other [items](#) within the system.

 **DEMO-SRV01 | Windows Server | 1007**

Relationships

Provides a summary of the relationships between this item and other items in the environment.

6 Relationships

Item ID	Direction	Managed	Name	Item Type	Relationship Type
1000	Outbound	True	Demonstration Inc	Container	Contained Within
1001	Outbound	True	demonstration.int	Active Directory Domain	Is Domain Controller
1004	Outbound	True	DEMO-SRV01	Microsoft DNS Server	Hosts Microsoft DNS Server
1005	Outbound	True	DEMO-SRV01		Hosts IIS Server
1006	Outbound	True	DEMO-SRV01	Microsoft WINS Service	Hosts WINS Service
1003	Outbound	True	DEMO-SRV01	Microsoft DHCP Server	Hosts Microsoft DHCP Server

View Item

Item ID

The unique identifier of the [item](#).

Direction

The direction of the [relationship](#).

Outbound

The [relationship](#) is from the [item](#) being viewed to another [item](#) within the system.

Inbound

The [relationship](#) is from another [item](#) within the system to the [item](#) being viewed.

Internal

An internal [relationship](#) between the [item](#) being viewed and a component of that [item](#).

Managed

Determines whether the [relationship](#) was dynamically generated by the system, or has been manually created.

Name

The name of the [item](#).

Item Type

The [type](#) of the [item](#).

Relationship Type

The type of relationship.

Right clicking a [relationship](#), and clicking view item opens the [item](#) in a new window.

Assigning Support Provisions

Many [items](#) support the ability to have one or more [support provisions](#) assigned through [relationships](#).

Open the [item](#) for [editing](#), and [modify the relationships](#) and select the [support provision](#) to assign.

Manual Item Relationship

Search

High*

Item Type

Support Provision

1 Results

Item ID	Name	Type
1158	High Availability Support	Support Provision

Relationship Type

Is Supported By

☐ Create Inbound Connection

OK

Cancel

Relationship Type

Select the Is "Is Maintained By" relationship type for hardware maintenance.
Select the Is "Is Supported By" relationship type for technical support.

Click OK, and save the [relationships](#).

Refresh the browser window to display the newly assigned [support provisions](#).

Connecting Disk Shelves

Items including [Windows machines](#) and [Unix systems](#) support the ability to have one or more [disk shelves](#) connected through [relationships](#).

Open the [item](#) for [editing](#), and [modify the relationships](#), and select the [disk shelf](#) to connect. Ensure to select "Connected Disk Shelf" as the relationship type.

Manual Item Relationship

Search

Item Type

CORP*

Disk Shelf

2 Results

Item ID	Name	Type
7881	CORP-SHELF-01	Disk Shelf
7882	CORP-SHELF-02	Disk Shelf

Relationship Type

Connected Disk Shelf

☐ Create Inbound Connection

OK

Cancel

Click OK, and save the [relationships](#).

Refresh the browser window to display the newly connected [disk shelves](#).

Connecting Network Storage Devices

Items including [Windows machines](#) and [Unix systems](#) support the ability to have one or more [network storage devices](#) connected through [relationships](#).

Open the [item](#) for [editing](#), and [modify the relationships](#), and select the [network storage device](#) to connect. Ensure to select "Connected Network Storage Device" as the relationship type.

Manual Item Relationship

Search

CORP*

Item Type

Network Storage Device

1 Results

Item ID	Name	Type
 9886	CORP-SAN01	Network Storage Device

Relationship Type

Connected Network Storage Device

☐ Create Inbound Connection

OK

Cancel

Click OK, and save the [relationships](#).

Refresh the browser window to display the newly connected [network storage devices](#).

Connecting Tape Libraries

Items including [Windows machines](#) and [Unix systems](#) support the ability to have one or more [tape libraries](#) connected through [relationships](#).

Open the [item](#) for [editing](#), and [modify the relationships](#), and select the [tape library](#) to connect. Ensure to select "Connected Tape Library" as the relationship type.

Manual Item Relationship

Search

Item Type

Tape*

Tape Library

1 Results

Item ID	Name	Type
 14112	TapeLibrary01	Tape Library

Relationship Type

Connected Tape Library

☐ Create Inbound Connection

OK

Cancel

Click OK, and save the [relationships](#).

Refresh the browser window to display the newly connected [tape libraries](#).

Modifying Relationships

To modify the [relationships](#) for an [item](#), open the [item](#) for editing by using the edit command button on the [toolbar](#).

As [relationships](#) relate to multiple [items](#), they are managed outside of the [version control](#) system and must be saved independently.

DEMO-SRV01 | Windows Server | 1007

Relationships

Provides a summary of the relationships between this item and other items in the environment.

6 Relationships

Item ID	Direction	Managed	Name	Item Type	Relationship Type
1000	Outbound	True	Demonstration Inc	Container	Contained Within
1001	Outbound	True	demonstration.int	Active Directory Domain	Is Domain Controller
1004	Outbound	False	DEMO-SRV01	Microsoft DNS Server	Hosts Microsoft DNS Server
1005	Outbound	True	DEMO-SRV01		Hosts IIS Server
1006	Outbound	True	DEMO-SRV01		Hosts WINS Service
1003	Outbound	True	DEMO-SRV01		Hosts Microsoft DHCP Server

Add Relationship

Delete Relationship

View Item

Properties

Right clicking a [relationship](#) displays the context menu.

Add Relationship

Displays the [relationship dialog](#) to allow the creation of a new [relationship](#) between this [item](#) and another [item](#).

Delete Relationship

Deletes the currently selected [relationship](#). This only applies to manually created [relationships](#).

View Item

Opens the [item](#) referenced by the [relationship](#) in a new window.

Properties

Displays the properties of the [relationship](#) in the [relationship dialog](#). This only applies to manually created [relationships](#).

Relationship Dialog

The relationship dialog allows a new [relationship](#) to be created or an existing [relationship](#) modified.

Manual Item Relationship

Search

Tape*

Item Type

Tape Library

1 Results

Item ID	Name	Type
14112	TapeLibrary01	Tape Library

Relationship Type

Connected Tape Library

Create Inbound Connection

OK

Cancel

Search

Allows you to [search](#) for the [item](#) to which to link with the [relationship](#).

Item Type

The type of [item](#) to [search](#) for.

Relationship Type

The type of [relationship](#) to establish between the [items](#). This may be a system managed [relationship](#) type or a user defined [relationship type definition](#).

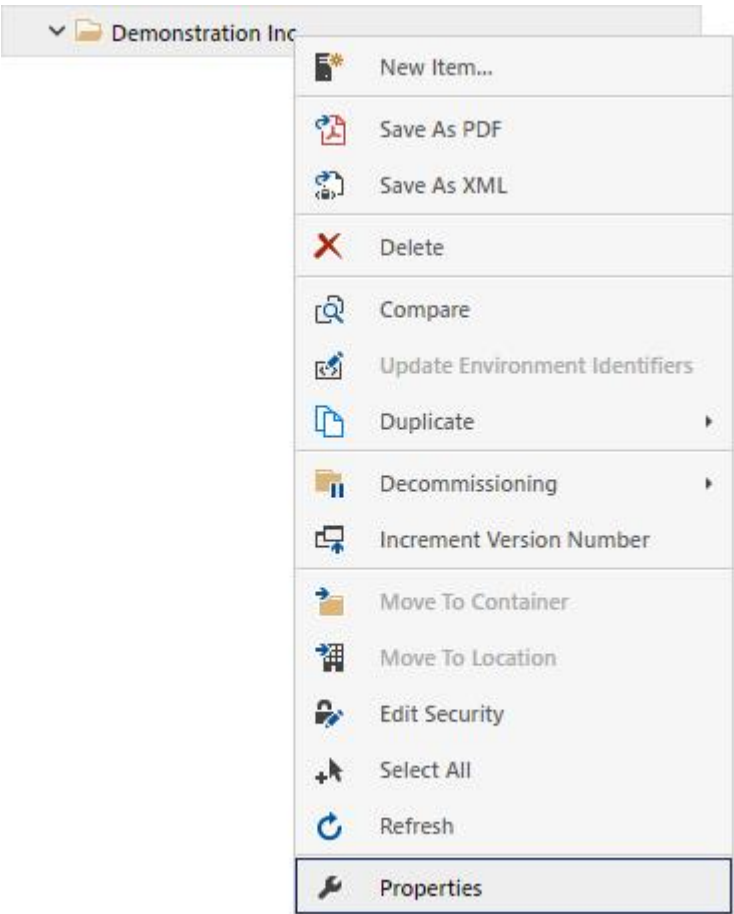
Create Inbound Connection

Determines whether the system should automatically create a reciprocal inbound [relationship](#) on the target [item](#). The [relationship type](#) may require or prevent an inbound [relationship](#).

Renaming Items

To change the **name** of an **item** (including the root container), perform the following steps:

- You must have write and rename **permissions** for the **item**.
- Right click the **item** and select properties.



- Click the edit button  on the toolbar.
- Enter a new name that conforms to the **item naming** rules.

General Information	
Name	Your Company

- Enter a version description if required, for example, "Renamed the item".

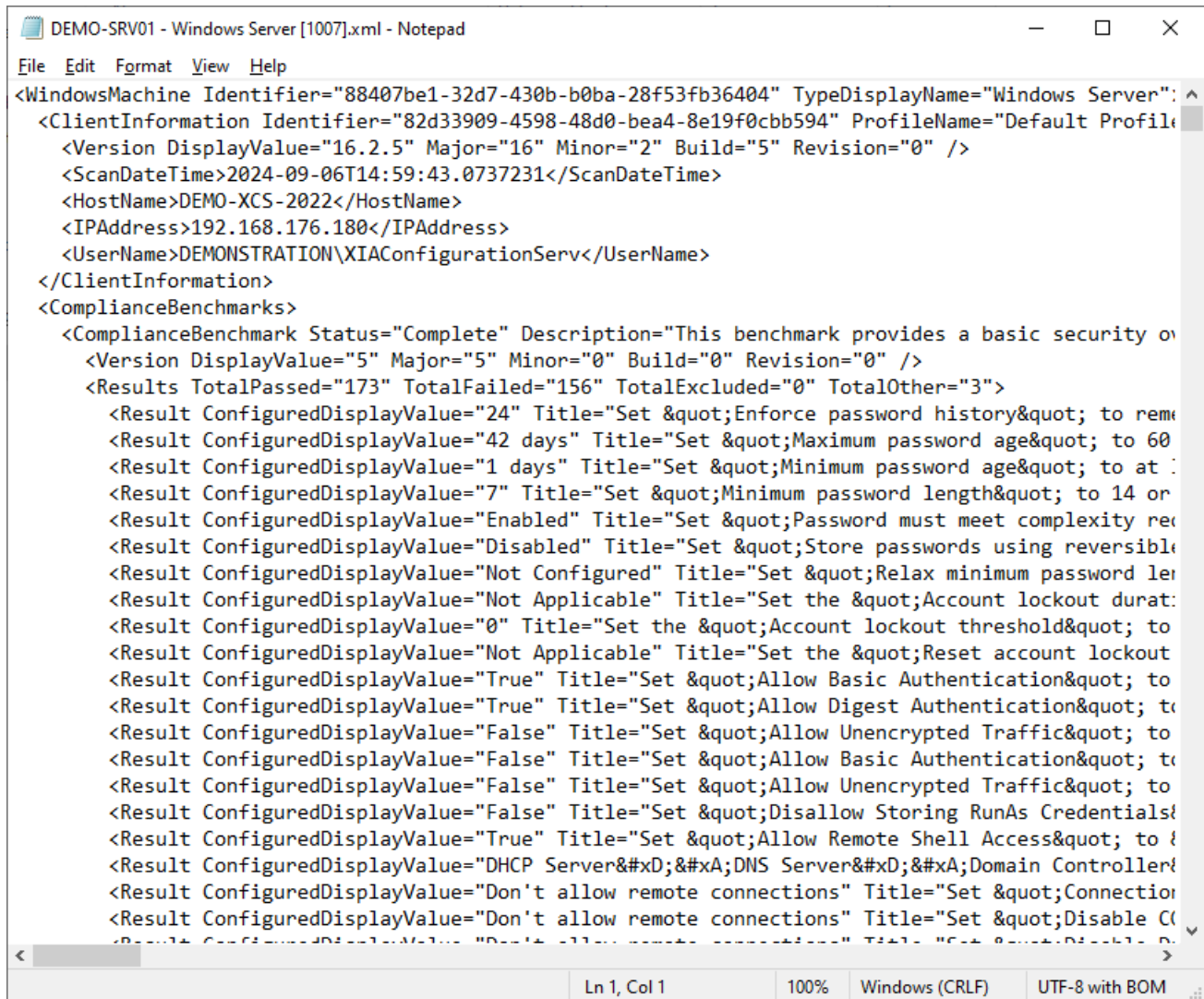


- Click the save button  on the toolbar.

Save as XML

Clicking the save as XML button  on the toolbar exports the currently viewed [version](#) of the item to an XML file.

Depending on the browser, when you press this button, you will be prompted to save or open the XML file.



```
DEMO-SRV01 - Windows Server [1007].xml - Notepad
File Edit Format View Help
<WindowsMachine Identifier="88407be1-32d7-430b-b0ba-28f53fb36404" TypeDisplayName="Windows Server":
  <ClientInformation Identifier="82d33909-4598-48d0-bea4-8e19f0cbb594" ProfileName="Default Profile
    <Version DisplayValue="16.2.5" Major="16" Minor="2" Build="5" Revision="0" />
    <ScanDateTime>2024-09-06T14:59:43.0737231</ScanDateTime>
    <HostName>DEMO-XCS-2022</HostName>
    <IPAddress>192.168.176.180</IPAddress>
    <UserName>DEMONSTRATION\XIAConfigurationServ</UserName>
  </ClientInformation>
  <ComplianceBenchmarks>
    <ComplianceBenchmark Status="Complete" Description="This benchmark provides a basic security on
      <Version DisplayValue="5" Major="5" Minor="0" Build="0" Revision="0" />
      <Results TotalPassed="173" TotalFailed="156" TotalExcluded="0" TotalOther="3">
        <Result ConfiguredDisplayValue="24" Title="Set "Enforce password history" to rem
        <Result ConfiguredDisplayValue="42 days" Title="Set "Maximum password age" to 60
        <Result ConfiguredDisplayValue="1 days" Title="Set "Minimum password age" to at
        <Result ConfiguredDisplayValue="7" Title="Set "Minimum password length" to 14 or
        <Result ConfiguredDisplayValue="Enabled" Title="Set "Password must meet complexity req
        <Result ConfiguredDisplayValue="Disabled" Title="Set "Store passwords using reversibl
        <Result ConfiguredDisplayValue="Not Configured" Title="Set "Relax minimum password ler
        <Result ConfiguredDisplayValue="Not Applicable" Title="Set the "Account lockout durat
        <Result ConfiguredDisplayValue="0" Title="Set the "Account lockout threshold" to
        <Result ConfiguredDisplayValue="Not Applicable" Title="Set the "Reset account lockout
        <Result ConfiguredDisplayValue="True" Title="Set "Allow Basic Authentication" to
        <Result ConfiguredDisplayValue="True" Title="Set "Allow Digest Authentication" to
        <Result ConfiguredDisplayValue="False" Title="Set "Allow Unencrypted Traffic" to
        <Result ConfiguredDisplayValue="False" Title="Set "Allow Basic Authentication" to
        <Result ConfiguredDisplayValue="False" Title="Set "Allow Unencrypted Traffic" to
        <Result ConfiguredDisplayValue="False" Title="Set "Disallow Storing RunAs Credentials
        <Result ConfiguredDisplayValue="True" Title="Set "Allow Remote Shell Access" to
        <Result ConfiguredDisplayValue="DHCP Server&#xD;&#xA;DNS Server&#xD;&#xA;Domain Controller
        <Result ConfiguredDisplayValue="Don't allow remote connections" Title="Set "Connection
        <Result ConfiguredDisplayValue="Don't allow remote connections" Title="Set "Disable C
      </Results>
    </ComplianceBenchmark>
  </ComplianceBenchmarks>
</WindowsMachine>
```

NOTE: For [password list](#) items the user must also have the [decrypt password lists](#) server permission.

Security Descriptor

Provides information about the security assigned to the [item](#).

The security settings can be applied directly to any [item](#), or inherited from the parent [container](#) or [customer](#).

Security

Determines the security that is to be applied to this item.

 2 Security Entries (applied directly)

Account Name	Full	Rename	Read	Write	Decom.	Delete	Versions	Security
 DEMONSTRATION\IT Support	True	True	True	True	True	True	True	True
 DEMONSTRATION\Managers	True	True	True	True	True	True	True	True

☐ Replace security on all child objects to inherit from this object.

Enable Inheritance

New Security Entry

Apply Security

Account Name

The user or group account that is assigned to the security entry.

Permissions

See the [security entry dialog](#) for details on the security permissions.

Replace security on all child objects to inherit from this object

Enables inheritance on all child [items](#), removing their explicitly set permissions, and inheriting the permissions from this item. This only applies when the item is a [container](#) or [customer](#).

Enable Inheritance

Enables inheritance, removing the explicitly set permissions from the [item](#), and inheriting the permissions from the parent [container](#) or [customer](#).

Disable Inheritance

Disables inheritance, converting the inherited permissions into explicit permissions on the [item](#).

New Security Entry

Displays the [security entry dialog](#).

Apply Security

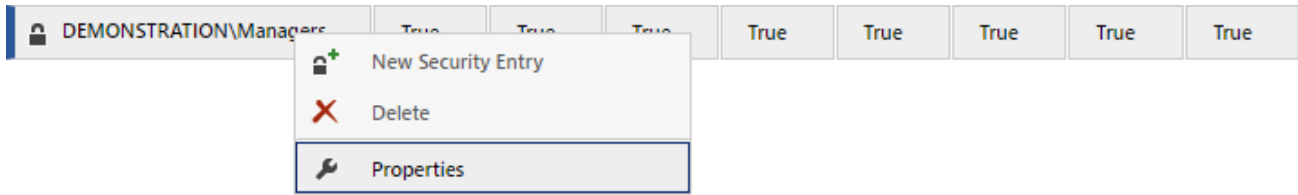
Applies the security to the [item](#).

Right clicking a security entry displays the [security entry context menu](#).

Double clicking a security entry displays the [security entry dialog](#).

Context Menu

Right clicking a security entry in the [security descriptor](#) user interface displays the context menu.



New Security Entry

Displays the [security entry dialog](#).

Delete

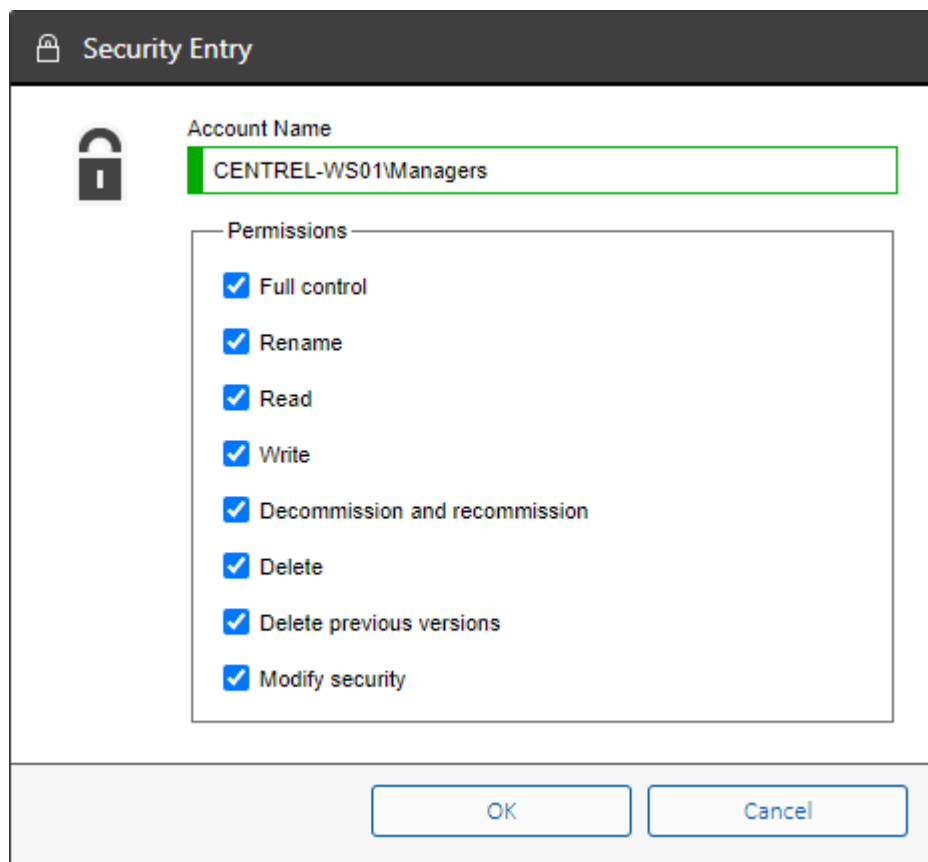
Deletes the currently selected security entry.

Properties

Displays the [security entry dialog](#) for the currently selected security entry.

Security Entry Dialog

The security entry dialog displays a security entry in the [security descriptor](#).

The image shows a 'Security Entry' dialog box. It has a dark title bar with a lock icon and the text 'Security Entry'. Inside, there's a light gray area with a lock icon on the left. To the right of the icon is a text field labeled 'Account Name' containing 'CENTREL-WS01\Managers'. Below this is a section titled 'Permissions' containing a list of permissions, each with a checked checkbox: 'Full control', 'Rename', 'Read', 'Write', 'Decommission and recommission', 'Delete', 'Delete previous versions', and 'Modify security'. At the bottom right are 'OK' and 'Cancel' buttons.

Account Name

The user or group account that is assigned to the security entry.

Full control

The user has full control over an [item](#).

Rename

The user is permitted to rename an [item](#) (the user must also have write permission to rename an [item](#)).

Read

The user is permitted to read and view this [item](#).

Write

The user is permitted to make changes to the [item](#).

Decommission and recommission

The user is permitted to [decommission](#) and [recommission](#) the [item](#).

Delete

The user is permitted to [delete](#) the [item](#).

Delete previous versions

The user is permitted to delete the previous versions found in the [version history](#) of the [item](#).

Modify security

The user is permitted to make changes to the security permissions of an [item](#).

If the security entry has no permissions assigned it is removed from the [security descriptor](#).

ServiceNow Synchronization

The section provides information about the synchronization of the [item](#) between the [XIA Configuration Server](#) and a [ServiceNow instance](#). This section is only visible if the [ServiceNow connector](#) is enabled, and the [item](#) type [supports synchronization](#).



DEMO-SRV01 | Windows Server | 40963

ServiceNow Synchronization

Provides details of the synchronization between the item and the ServiceNow instance.

 Synchronization Settings

Effective Enabled	Enabled (directly on the item)
ServiceNow Identifier	2c9a7c21231948c2b151c9952bbf2c2f

 Synchronization Status

Last Synchronization Attempt	11 September 2024 16:52:09
Last Synchronization Success	11 September 2024 16:52:03

Synchronize Now

Open ServiceNow Item

Effective Enabled

Determines whether synchronization with a [ServiceNow instance](#) is enabled for the [item](#).

ServiceNow Identifier

The unique identifier of the synchronized item in the [ServiceNow instance](#).

Last Synchronization Attempt

The date and time that the [XIA Configuration Server](#) attempted to synchronize the [item](#) with the [ServiceNow instance](#).

Last Synchronization Success

The date and time that the [XIA Configuration Server](#) successfully synchronized the [item](#) with the [ServiceNow instance](#).

Synchronize Now

Synchronizes the [item](#) with the [ServiceNow instance](#). The user must have both [write permissions](#) to the [item](#) and the [manage ServiceNow item synchronization](#) or [synchronize items with ServiceNow server permission](#).

Open ServiceNow Item

Launches a web browser to display the synchronized [item](#) in the [ServiceNow instance](#). This command is only available if the [item](#) has been matched with the [ServiceNow instance](#) and the ServiceNow identifier is available.

Modify ServiceNow Synchronization Settings

The section provides information about modifying the [ServiceNow](#) synchronization settings of the [item](#).

The user must have the "Manage ServiceNow Item Synchronization" [server permission](#) as well as [write access](#) to the [item](#) to be able to modify these settings.



DEMO-SRV01 | Windows Server | 40963

ServiceNow Synchronization

Provides details of the synchronization between the [item](#) and the [ServiceNow](#) instance.

 Synchronization Settings

Enabled	☒
ServiceNow Identifier	2c9a7c21231948c2b151c9952bbf2c2f

Save Synchronization Settings

Enabled

Determines whether [ServiceNow](#) synchronization is enabled for the [item](#). This setting is ignored if the the synchronization of the [item type](#) is disabled in the [ServiceNow connector settings](#).

ServiceNow Identifier

The unique identifier of the configuration item in the [ServiceNow instance](#) to which the [item](#) is matched. The identifier can be set manually to bypass the matching process, or cleared to reapply the matching process.

Support Provisions

Many [items](#) support the ability to have one or more [support provisions](#) assigned through [relationships](#).

[Support provision items](#) can represent support contracts such as technical support agreements, warranties, or hardware maintenance agreements.



DEMO-SRV01 | Windows Server | 40963

Support Provisions

Provides information about the support provisions assigned to this item.

 2 Support Provisions

▲	Name	Relationship Type	Hours	Start Date	Expiry Date
	High Availability Support	Technical Support	Monday to Friday 8am - 6pm	11 September 2024	11 September 2027
	HPE Warranty	Hardware Maintenance	Monday to Friday 8am - 6pm	11 September 2024	11 September 2027

Name

The name of the assigned [support provision](#).

Relationship Type

The [relationship](#) type, either technical support, or hardware maintenance.

Hours

The hours on which support is provided by the [support provision](#).

Start Date

The date that the [support provision](#) becomes active.

Expiry Date

The date on which the [support provision](#) expires.

To assign a support provision see the [assigning support provisions](#) section.

Version History

Version control automatically creates new, numbered versions of [items](#) when they are modified by a user or updated by the [XIA Configuration Client](#).

All new items are created as version 1.00 and version numbers can go as high as 999.99.

Version History

Displays the version history for the item.

 4 versions (all displayed)

Version	Username	Date	Time	Description
 1.03 (viewing)	DEMONSTRATION\Administrator	11/09/2024	17:00	Updated item details.
 1.02	DEMONSTRATION\Administrator	09/09/2024	16:47	Updated item description.
 1.01	DEMONSTRATION\Administrator	09/09/2024	11:12	Updated support contract.
 1.00	DEMONSTRATION\Administrator	06/09/2024	15:18	Item created.

Show All Versions

Delete All Versions

Version

The version number.

Username

The username of the user that created this version.

Date

The date on which the version was created.

Time

The date on which the version was created.

Description

The description of the version.

Show All Versions

By default only the most recent 10 versions are displayed, clicking the show all versions button displays all versions for the [item](#).

Delete All Versions

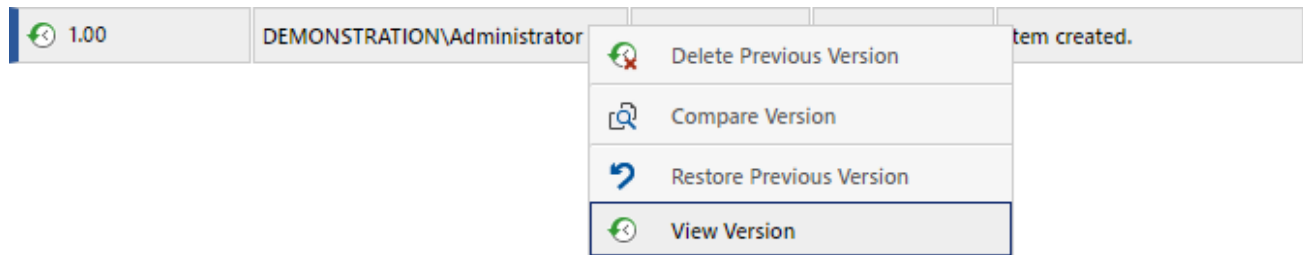
Deletes all previous versions of the [item](#). The user must have [delete previous version](#) permissions. This option is not available when viewing a previous version.

Right clicking a version record displays the [version history context menu](#).

Double clicking a version record displays that version of the [item](#).

Context Menu

Right clicking on a previous version in the [version history](#) user interface displays the context menu.



Delete Previous Version

Deletes the currently selected version of the [item](#). The user must have [delete previous version](#) permissions for the [item](#).

This option is not available for the current version, or the currently viewed version, of the [item](#).

Compare Version

Displays the [item comparison dialog](#) for the currently selected version of the [item](#). The user must have [write](#) permissions for the [item](#).

Restore Previous Version

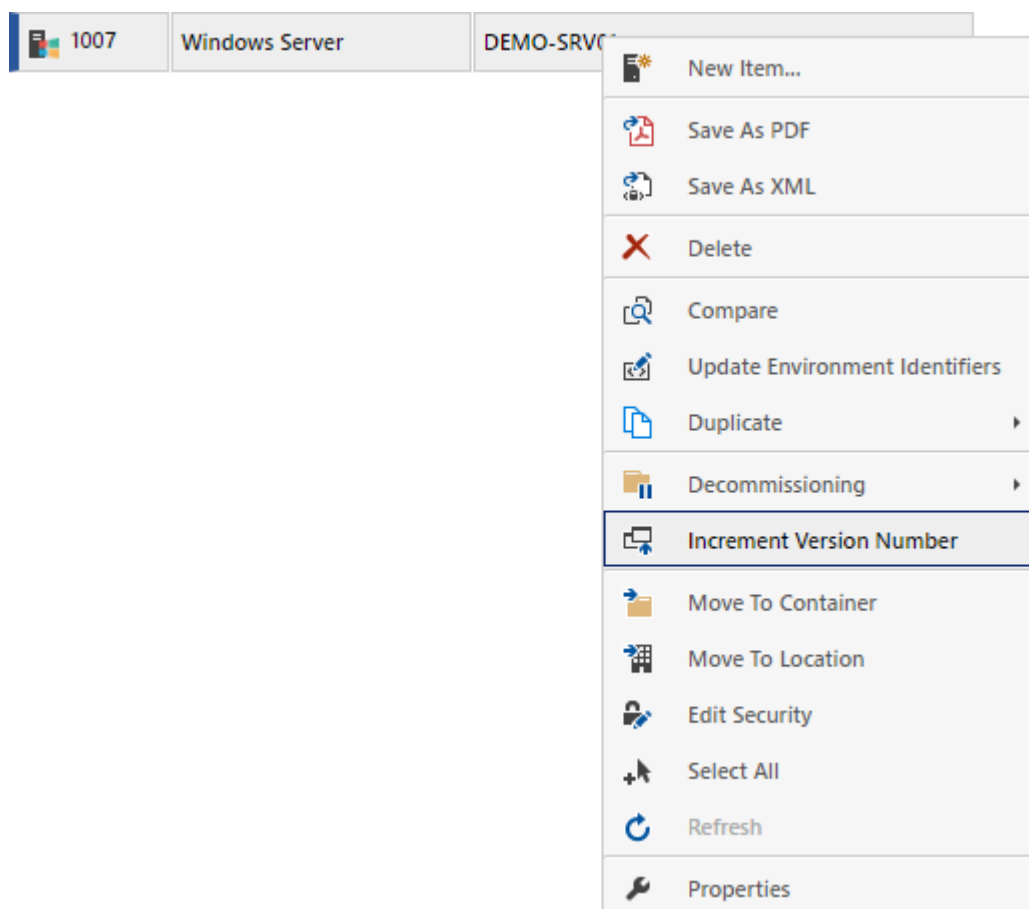
Restores the currently selected version as a new version of the [item](#).

View Version

Displays the selected version of the [item](#).

Incrementing Major Version Numbers

To increment the version number of the [item](#) to the next major version, right click the [item](#) or [items](#) and select increment version number.



Enter a description of the new major version if required, and click apply. The version description can be made mandatory within the [version control settings](#).

 **Increment Major Version**

Version Description

Server was repurposed under change request CR12345.

Please enter the version description.

Apply

Close

Web Controls

This section describes the web based controls in the product.

Advanced Upload Control

The [advanced upload control](#) allows files to be uploaded to the [XIA Configuration Server](#).

Date Picker

The [date picker](#) control allows the user to select a calendar date.

HTML Editor

The [HTML editor](#) allows the user to enter HTML data directly in a standard web browser.

Schedule

The [schedule](#) control allows the configuration of a schedule.

Advanced Upload Control

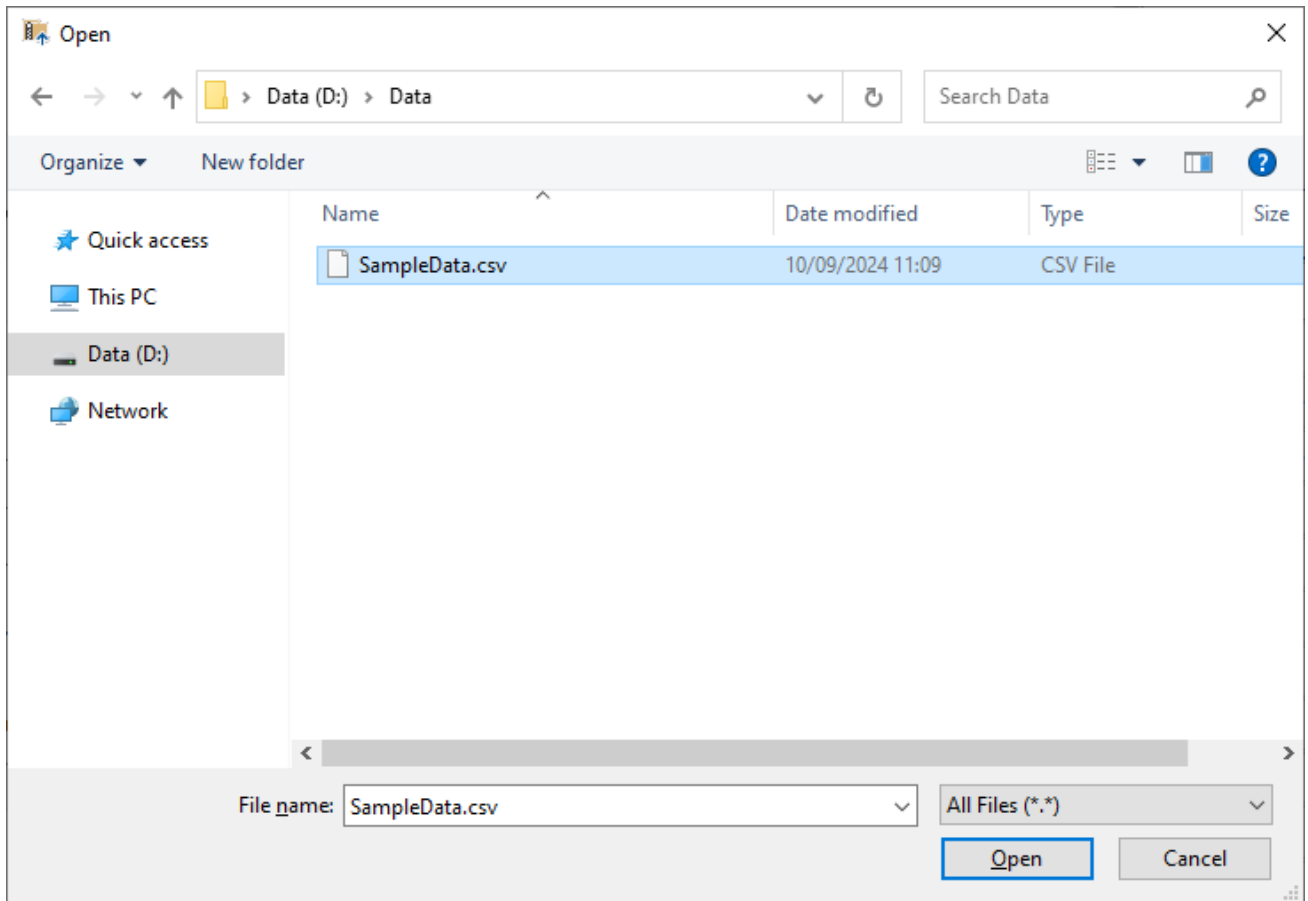
The advanced upload control allows files to be uploaded to the [XIA Configuration Server](#).



Files can be dropped directly into the drop zone shown with the dashed outline.



Clicking the button displays the file browse dialog.



When a file has been uploaded the success icon is displayed.



If the file uploaded is a valid image file, a thumbnail of that image is displayed.



Date Picker

The date picker control allows the selection of a date within a range of valid dates.



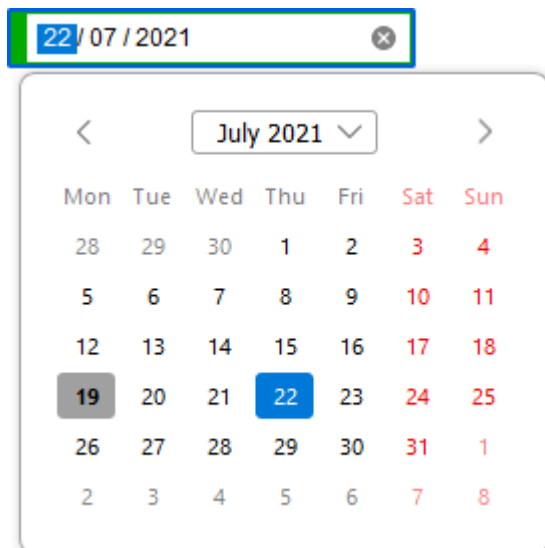
If the date is required but not set, or is not set within the range of valid dates the control displays with a red border.



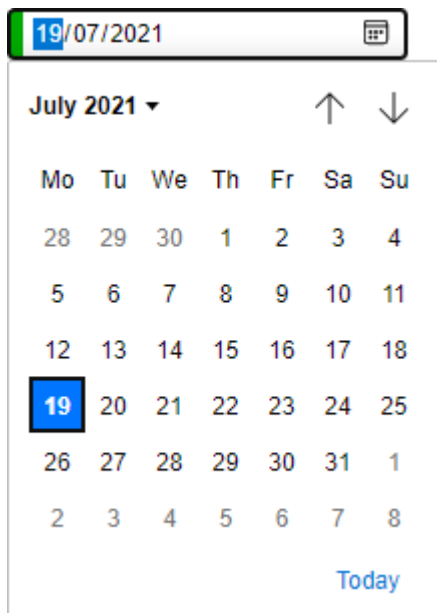
The control uses the [HTML 5 date input](#) control and the behaviour of this control varies between browsers.

The date can be entered by typing within the control or using the up and down arrows on the keyboard and is displayed in the short date format configured for the operating system.

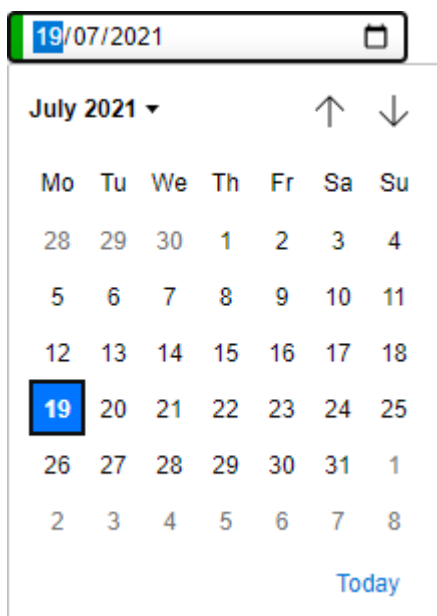
The control displayed in [Mozilla Firefox](#).



The control displayed in [Microsoft Edge](#).



The control displayed in [Google Chrome](#).



The control displayed in [Internet Explorer](#), the date must be entered manually in the format year-month-date.



HTML Editor

The editor allows the user to enter HTML data directly in a standard web browser, for example within the *Custom Item Details* section of an [item's general information](#) tab.



Design

HTML

Preview



 Displays the [Paste from Word](#) dialog.

 Undo the last action.

 Redo the last action.

 Clears the formatting from the selected region.

 Sets the selected text as superscript.

 Creates a numbered list.

 Creates a bullet list.

 Outdents the current selection.

 Indents the current selection.

 Inserts a [link](#)¹.

 Removes the [link](#)¹ in the current selection.

 Inserts an [image](#)¹.

 Inserts a [table](#)¹.

 Inserts a symbol.

 Displays the [find and replace](#) dialog.

 Displays the editor in full screen mode¹.

 Applies the specified CSS class to the current selection.

 Assigns the specified font to the current selection.

    Applies bold, italic, underline, and strike-through styles to the current selection.

   Left, centre, or right aligns the current selection.

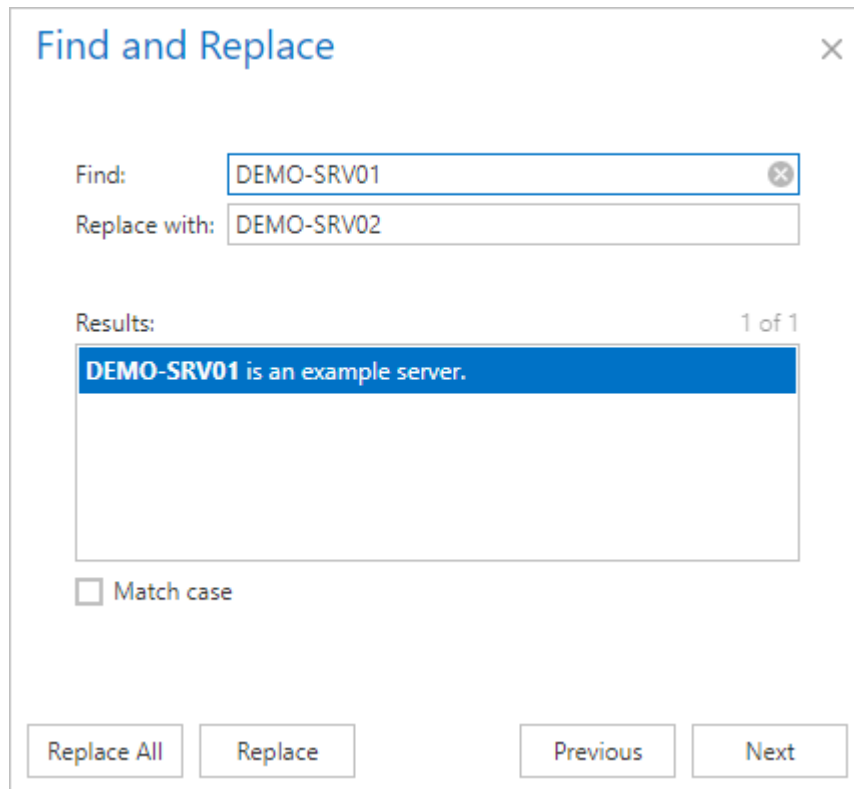
 Sets the background color for the current selection.

 Sets the font color for the current selection.

¹ The toolbar items can be removed within the [HTML editor settings](#).

Find and Replace

The find and replace dialog allows text within the [HTML editor](#) to be located and changed.



The image shows a 'Find and Replace' dialog box with a title bar and a close button. It contains two input fields: 'Find:' with the text 'DEMO-SRV01' and 'Replace with:' with the text 'DEMO-SRV02'. Below these is a 'Results:' section showing '1 of 1' results, with a list item 'DEMO-SRV01 is an example server.' highlighted in blue. A 'Match case' checkbox is present and unchecked. At the bottom are four buttons: 'Replace All', 'Replace', 'Previous', and 'Next'.

Find

The text to be located.

Replace with

The text to replace the selected text.

Results

Locations with the document where the selected text has been found. Clicking the item in the list will display it in the editor.

Match case

Determines whether the exact case must be found.

Replace All

Replaces all instances of the specified text.

Replace

Replaces the selected instance of the specified text.

Previous

Selects the previous instance of the specified text.

Next

Selects the next instance of the specified text.

HTML Tab

The HTML tab¹ displays the source HTML within the [HTML editor](#) allowing the HTML to be edited directly.

```
<table style="width: 100%; border-collapse: collapse;"><thead><tr><th style="width: 50%;" scope="col">Server Name</th><th style="width: 50%;" scope="col">Operating System</th></tr></thead><tbody><tr><td style="width: 50%;">DEMO-SRV01</td><td style="width: 50%;">Windows Server 2016</td></tr></tbody></table><br />
```

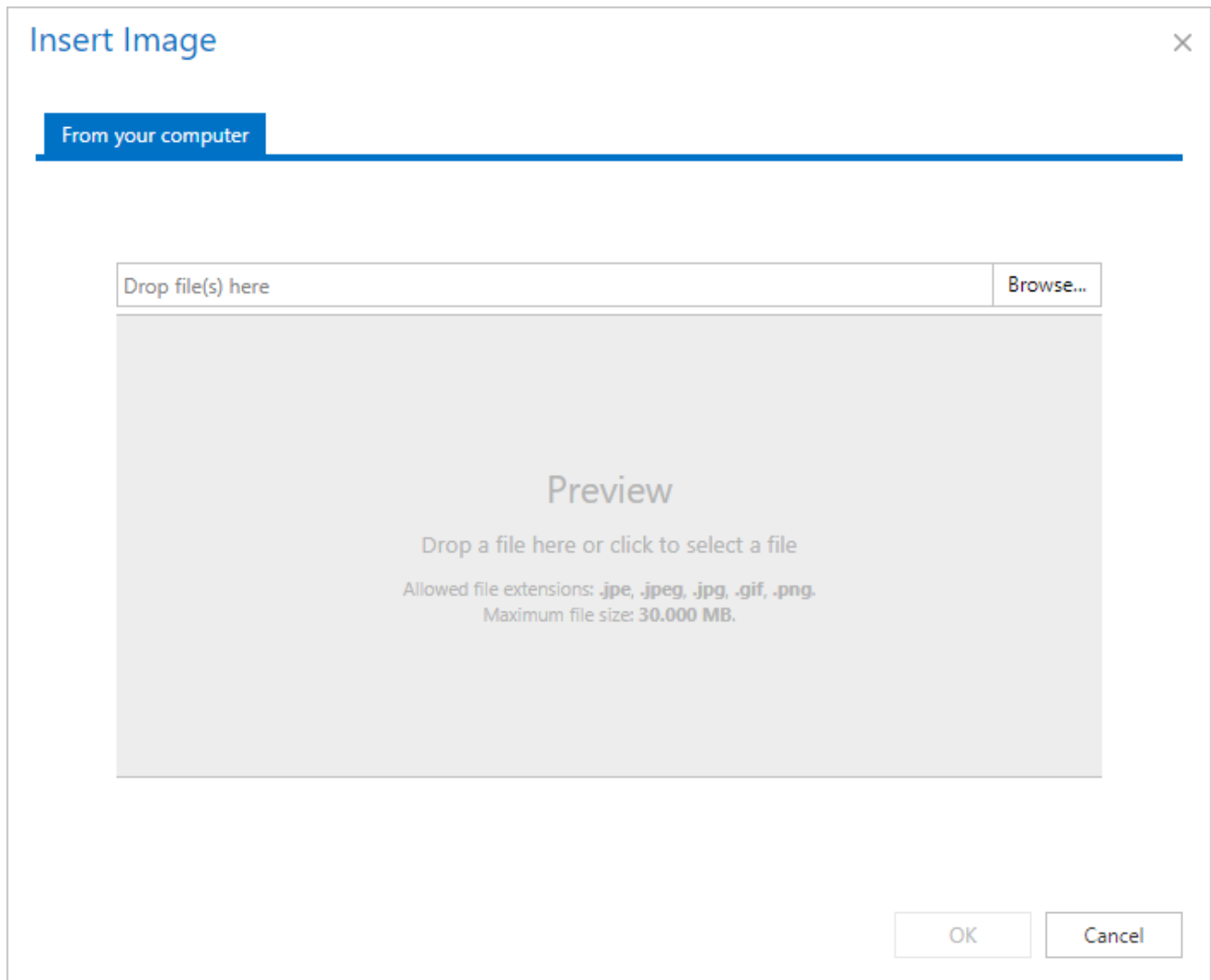


¹The user must be assigned permissions to access the HTML tab within the [HTML editor settings](#).

Images

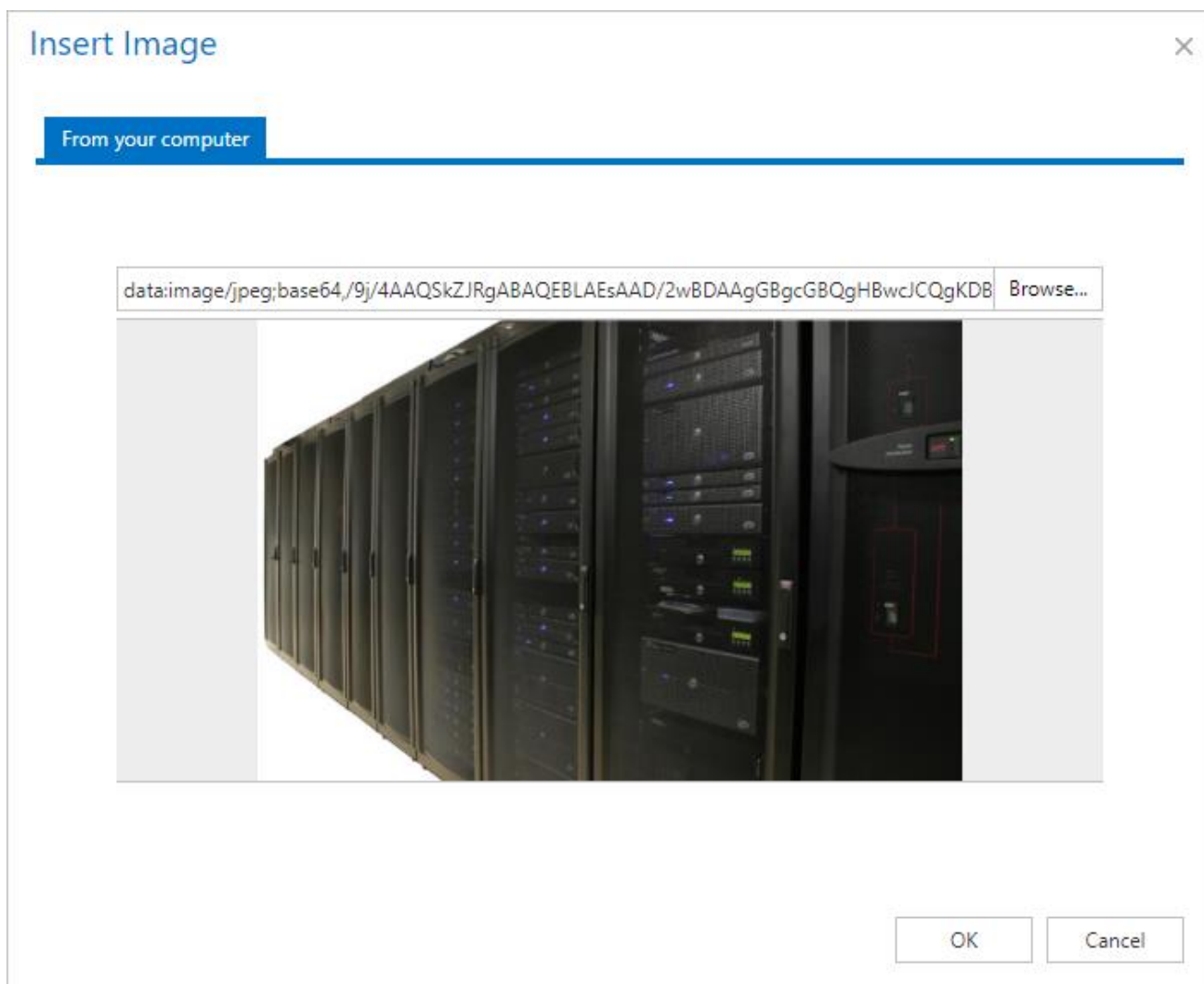
The [HTML editor](#) supports the ability to [insert](#) images within the content.

Clicking the image toolbar button¹  displays the insert image dialog.



An image can be added by dragging and dropping the image into the grey area, or by clicking the *Browse...* button.

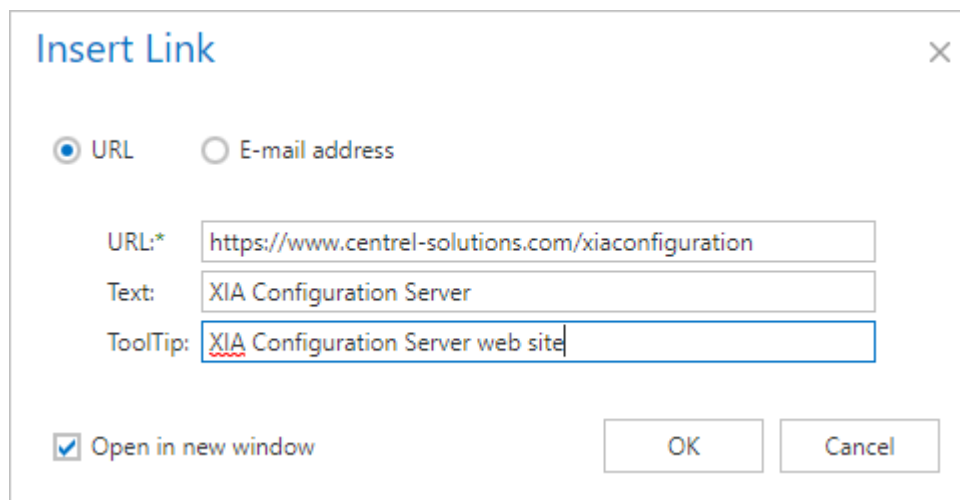
The image is automatically resized to a maximum size of 640 x 480 pixels, and converted to Base64 encoding.



¹ The toolbar items can be removed within the [HTML editor settings](#).

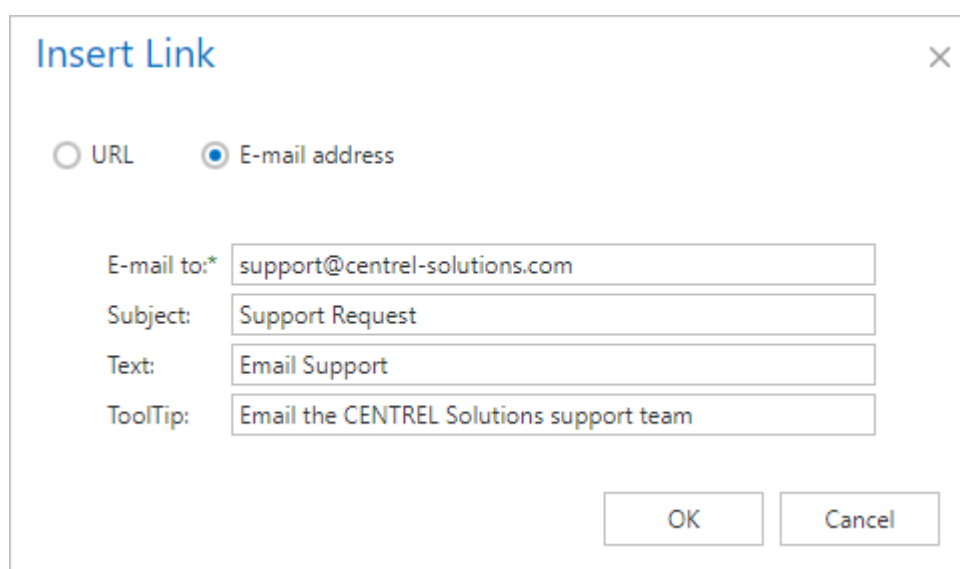
Links

Clicking the link toolbar button¹  displays the dialog to insert a link into the document. The options displayed depend on whether a link to a URL or email address is being inserted.



The 'Insert Link' dialog box is shown with the 'URL' radio button selected. It contains the following fields and options:

- URL:**
- Text:**
- ToolTip:**
- ☒ Open in new window
- Buttons:** OK, Cancel



The 'Insert Link' dialog box is shown with the 'E-mail address' radio button selected. It contains the following fields and options:

- E-mail to:**
- Subject:**
- Text:**
- ToolTip:**
- Buttons:** OK, Cancel

URL / E-mail address

Determines whether a link to a URL or email address should be inserted.

URL

The URL address of the link to insert.

E-mail to

The email address of the link to insert.

Subject

The subject of the email to send.

Text

The text to display for the link.

Tooltip

The tooltip to display when the mouse is hovered over the link.

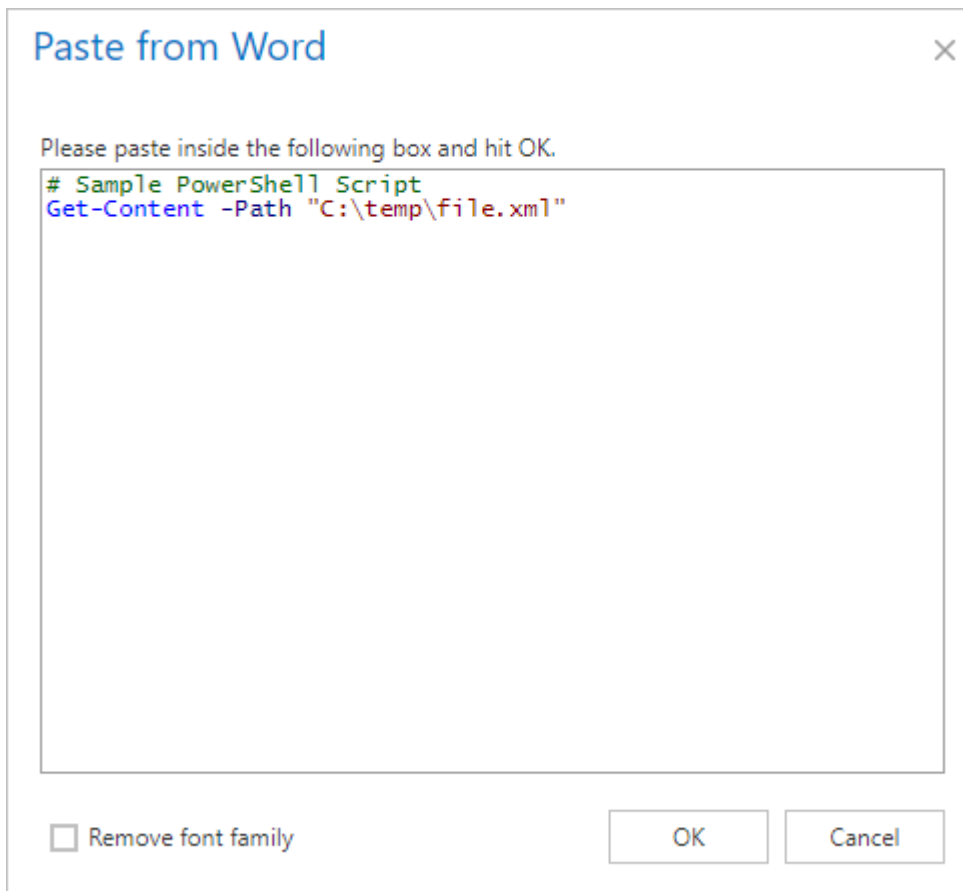
Open in a new window

Determines whether the link should be opened in a new window.

¹The toolbar items can be removed within the [HTML editor settings](#).

Paste from Word

The Paste from Word dialog allows formatted text from [Microsoft Word](#) to be safely pasted into the [HTML editor](#) as standard HTML.



Remove font family

Determines whether the font family should be removed from the pasted text.

Preview Tab

The preview tab¹ displays a preview of the HTML within the [HTML editor](#).

Server Name	Operating System
DEMO-SRV01	Windows Server 2016

Design

HTML

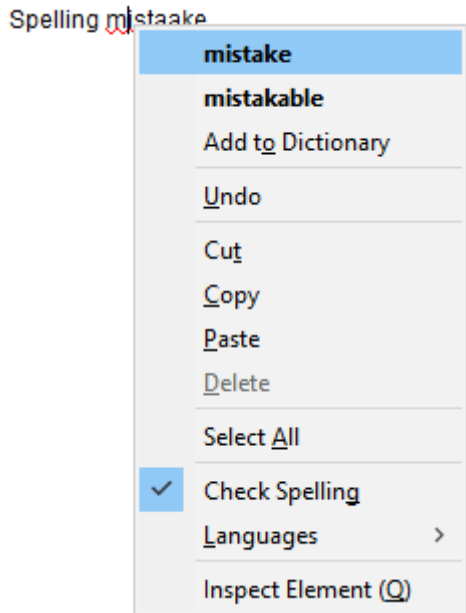
Preview



¹The preview tab can be removed within the [HTML editor settings](#).

Spell Checking

The spell check within the [HTML editor](#) is provided by the web browser. Whilst each browser provides spell checking differently this is typically provided as a red underline, and a right click context menu for spelling suggestions.



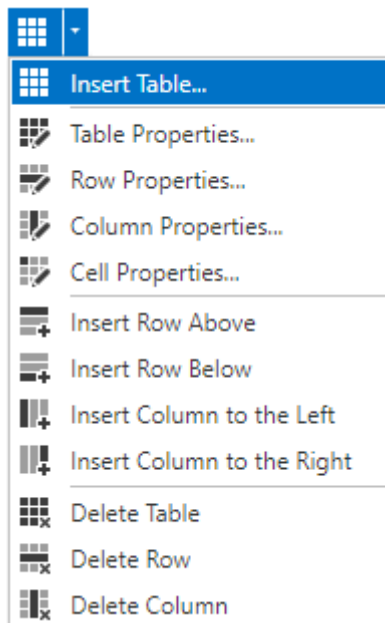
For more information please see the documentation for your specific web browser.

Tables

The [HTML editor](#) supports the ability to [insert](#) and modify tables within the content.

Server Name	Operating System
DEMO-SRV01	Microsoft Windows Server 2016 Standard
DEMO-SRV02	Microsoft Windows Server 2016 Standard

Clicking the arrow next to the table toolbar button¹  displays the table menu.



Insert Table

Displays the [insert table](#) dialog.

Table Properties

Displays the table properties dialog.

Row Properties

Displays the [row properties](#) dialog.

Column Properties

Displays the [column properties](#) dialog.

Cell Properties

Displays the [cell properties](#) dialog.

Insert Row Above

Inserts a new table row above the currently selected row.

Insert Row Below

Inserts a new table row below the currently selected row.

Insert Column to the Left

Inserts a new table column to the left of the currently selected column.

Insert Column to the Right

Inserts a new table column to the right of the currently selected column.

Delete Table

Deletes the currently selected table.

Delete Row

Deletes the currently selected row.

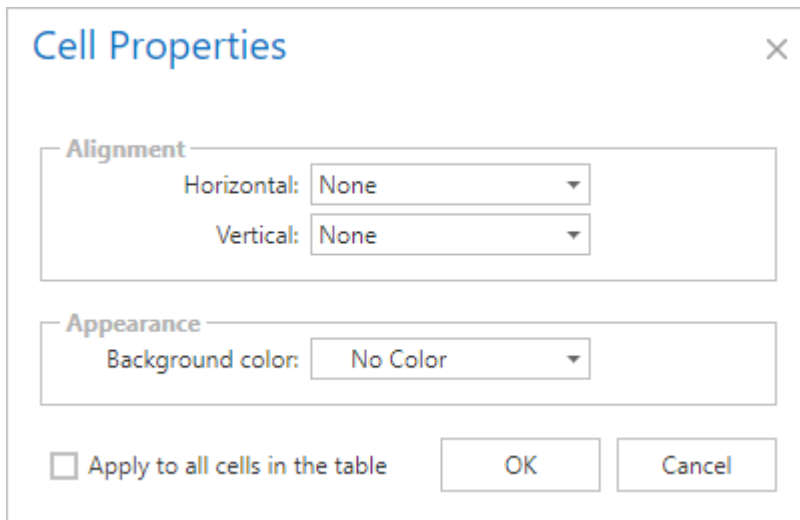
Delete Column

Deletes the currently selected column.

¹ The toolbar items can be removed within the [HTML editor settings](#).

Cell Properties

The cell properties dialog of the [HTML editor](#) allows you to modify the properties of a [table](#) cell.

The image shows a 'Cell Properties' dialog box with a title bar and a close button. It contains two sections: 'Alignment' and 'Appearance'. The 'Alignment' section has two dropdown menus: 'Horizontal' and 'Vertical', both currently set to 'None'. The 'Appearance' section has a dropdown menu for 'Background color' set to 'No Color'. At the bottom, there is a checkbox labeled 'Apply to all cells in the table' which is unchecked, and two buttons labeled 'OK' and 'Cancel'.

Horizontal

The horizontal alignment of the cell.

Vertical

The vertical alignment of the cell.

Background Color

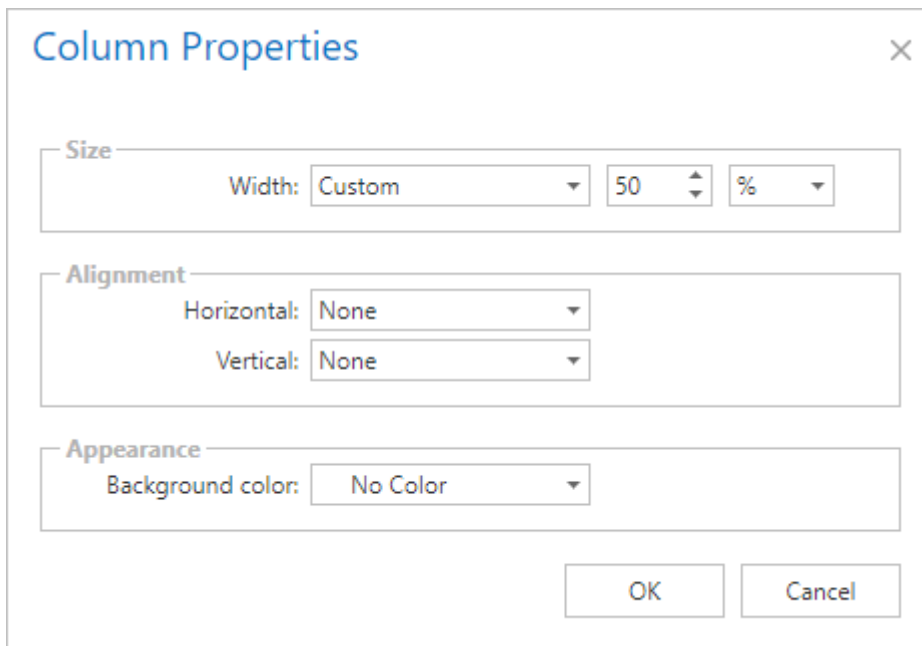
The background color to assign to the cell.

Apply to all cells in the table

Determines whether the settings in the dialog should be applied to all cells in the table.

Column Properties

The column properties dialog of the [HTML editor](#) allows you to modify the properties of a [table](#) column.



The screenshot shows a dialog box titled "Column Properties" with a close button (X) in the top right corner. The dialog is divided into three sections: "Size", "Alignment", and "Appearance".

- Size:** Contains a "Width:" label, a dropdown menu set to "Custom", a text input field containing "50", a small up/down arrow, and a unit dropdown menu set to "%".
- Alignment:** Contains two labels, "Horizontal:" and "Vertical:", each followed by a dropdown menu. Both dropdowns are currently set to "None".
- Appearance:** Contains a label "Background color:" followed by a dropdown menu set to "No Color".

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Width

The width of the column.

Horizontal

The horizontal alignment of the column.

Vertical

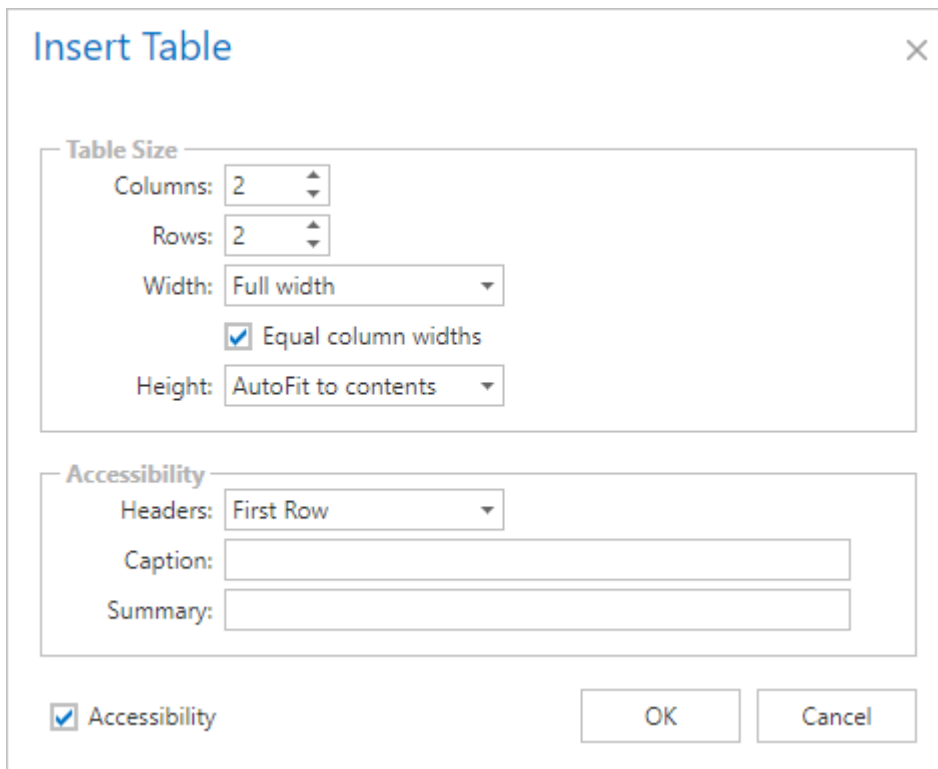
The vertical alignment of the column.

Background Color

The background color to assign to the column.

Inserting Tables

Clicking the table toolbar button¹  displays the dialog to insert a table into the document.



The "Insert Table" dialog box is shown with a close button (X) in the top right corner. It contains two main sections: "Table Size" and "Accessibility".

Table Size

- Columns: 2 (with up/down arrows)
- Rows: 2 (with up/down arrows)
- Width: Full width (dropdown menu)
- ☒ Equal column widths
- Height: AutoFit to contents (dropdown menu)

Accessibility

- Headers: First Row (dropdown menu)
- Caption: (text input field)
- Summary: (text input field)

At the bottom left, there is a checkbox labeled "Accessibility" which is checked. At the bottom right, there are "OK" and "Cancel" buttons.

Columns

Determines the number of columns that the created table should have.

Rows

The number of rows that the created table should have.

Width

The width of the table. By default this is the full width of the page.

Equal Column Widths

Determines whether the widths of the columns should be equal.

Height

Determines the height of the table. By default this is set to *AutoFit to contents*.

Headers

Determines whether a heading row, heading column, or both should be created for the table.

Row Heading 1	Row Heading 2
Sample Data	Sample Data
Sample Data	Sample Data

Column Heading 1	Sample Data
Column Heading 2	Sample Data

Caption

The caption for the table.

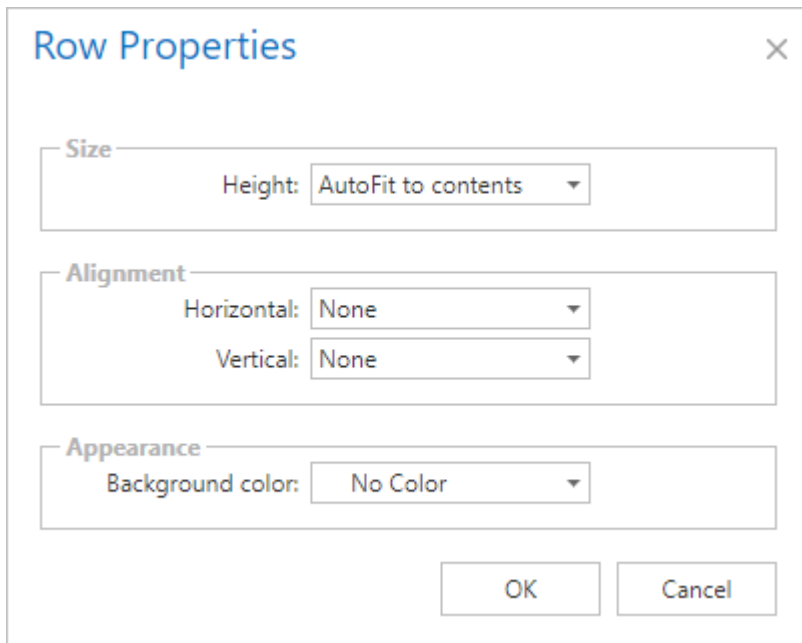
Summary

The summary for the table.

¹ The toolbar items can be removed within the [HTML editor settings](#).

Row Properties

The row properties dialog of the [HTML editor](#) allows you to modify the properties of a [table](#) row.

The image shows a 'Row Properties' dialog box with a close button (X) in the top right corner. It contains three sections: 'Size' with a 'Height' dropdown set to 'AutoFit to contents'; 'Alignment' with 'Horizontal' and 'Vertical' dropdowns both set to 'None'; and 'Appearance' with a 'Background color' dropdown set to 'No Color'. At the bottom are 'OK' and 'Cancel' buttons.

Row Properties X

Size

Height: AutoFit to contents ▼

Alignment

Horizontal: None ▼

Vertical: None ▼

Appearance

Background color: No Color ▼

OK Cancel

Height

The height of the row.

Horizontal

The horizontal alignment of the row.

Vertical

The vertical alignment of the row.

Background Color

The background color to assign to the row.

Schedule

The schedule control allows the configuration of a schedule.



☒ Once ☐ Weekly ☐ Monthly

☒ Enabled

Start Date

11/09/2024	20:00
------------	-------

Once

The [once schedule](#) is executed once at the specified date and time.

Weekly

The [weekly schedule](#) is executed at the specified time on each of the selected days of the week.

Monthly

The [monthly schedule](#) is executed at the specified time on each of the selected days of the specified months.

Once

The [schedule](#) will be executed once only at the specified date and time.



☒ Once ☐ Weekly ☐ Monthly

☒ Enabled

Start Date

11/09/2024		20:00	
------------	---	-------	---

Enabled

Determines whether the [schedule](#) is enabled.

Start Date

The date and time that the [schedule](#) will be executed.

Weekly

The [schedule](#) will be executed at the specified time on each of the selected days of the week.

☐ Once ☒ Weekly ☐ Monthly

☒ Enabled

Start Date

11/09/2024

20:00

☐ Expires

11/09/2025

17:09

Days Of Week

☒ Sunday

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

Enabled

Determines whether the [schedule](#) is enabled.

Start Date

The date on which the schedule becomes effective, and the time on which the [schedule](#) will be executed.

Expires

An optional date and time after which the [schedule](#) will no longer be effective.

Days of Week

The days of the week on which the [schedule](#) will be executed.

Monthly

The [schedule](#) will be executed at the specified time on each of the selected days of the specified months.

☐ Once ☐ Weekly ☒ Monthly

☒ Enabled

Start Date

11/09/2024

20:00

☐ Expires

11/09/2025

17:09

Months

Days

☒ January

☒ February

☒ March

☒ April

☒ May

☒ June

☒ July

☒ August

☒ September

☒ October

☒ November

☒ December

☒ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

☐ 11

☐ 12

☐ 13

☐ 14

☐ 15

☐ 16

☐ 17

☐ 18

☐ 19

☐ 20

☐ 21

☐ 22

☐ 23

☐ 24

☐ 25

☐ 26

☐ 27

☐ 28

☐ 29

☐ 30

☐ 31

Enabled

Determines whether the [schedule](#) is enabled.

Start Date

The date on which the [schedule](#) becomes effective, and the time on which the [schedule](#) will be executed.

Expires

An optional date and time after which the [schedule](#) will no longer be effective.

Months

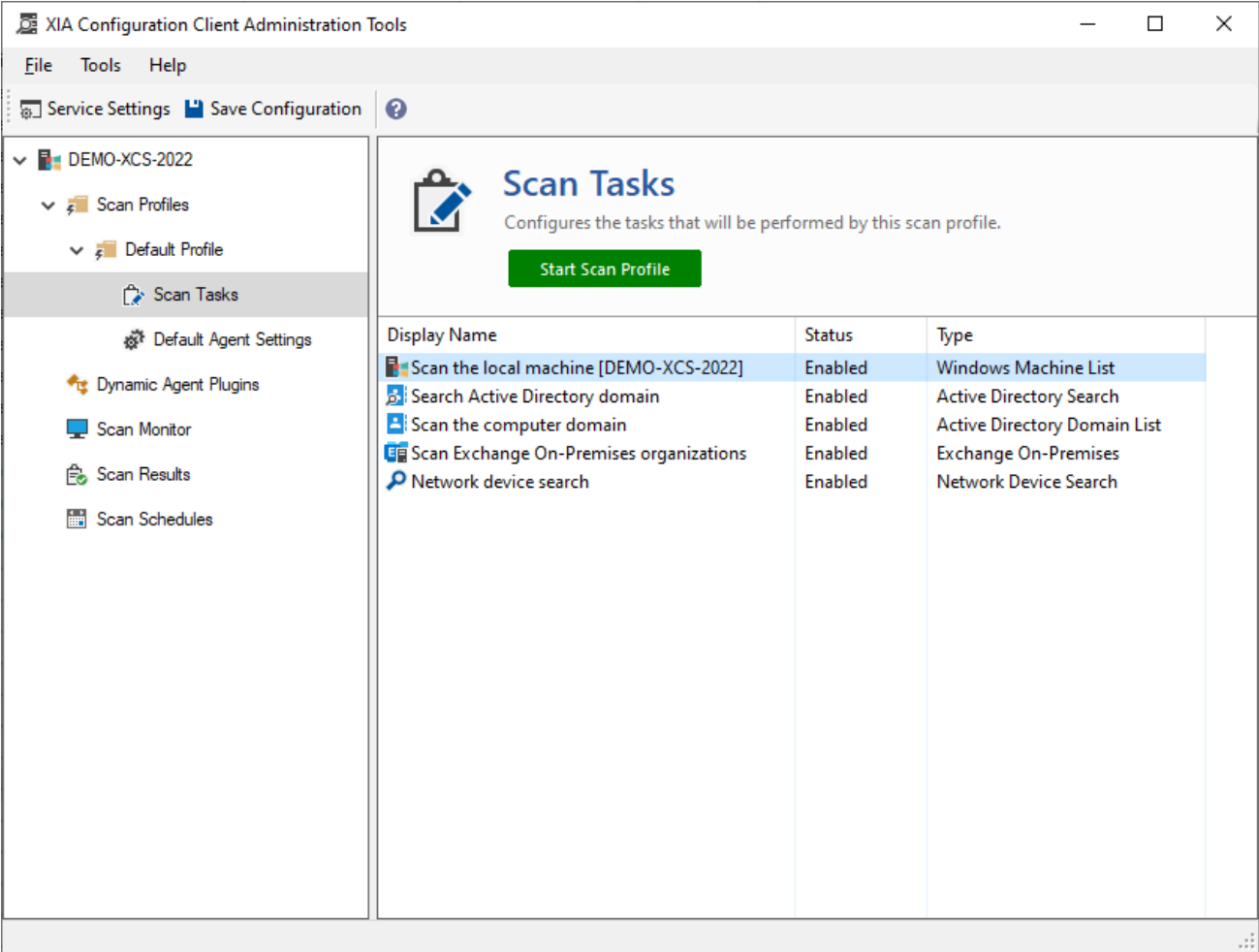
The months on which the [schedule](#) will be executed.

Days

The days of the month on which the [schedule](#) will be executed.

XIA Configuration Client

The XIA Configuration Client automates the collection of configuration information from [items](#) and provides that information to the [XIA Configuration Server](#).

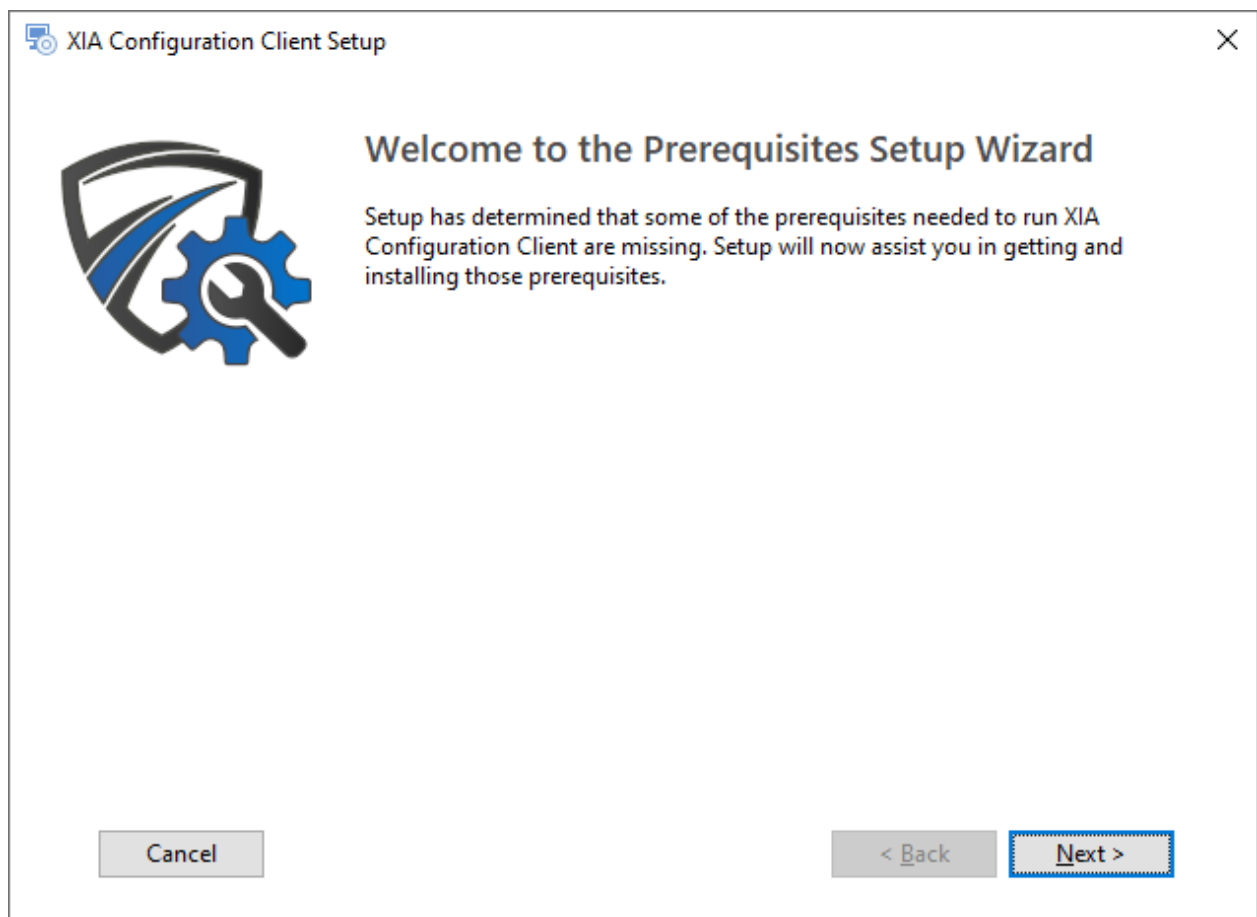


Installation

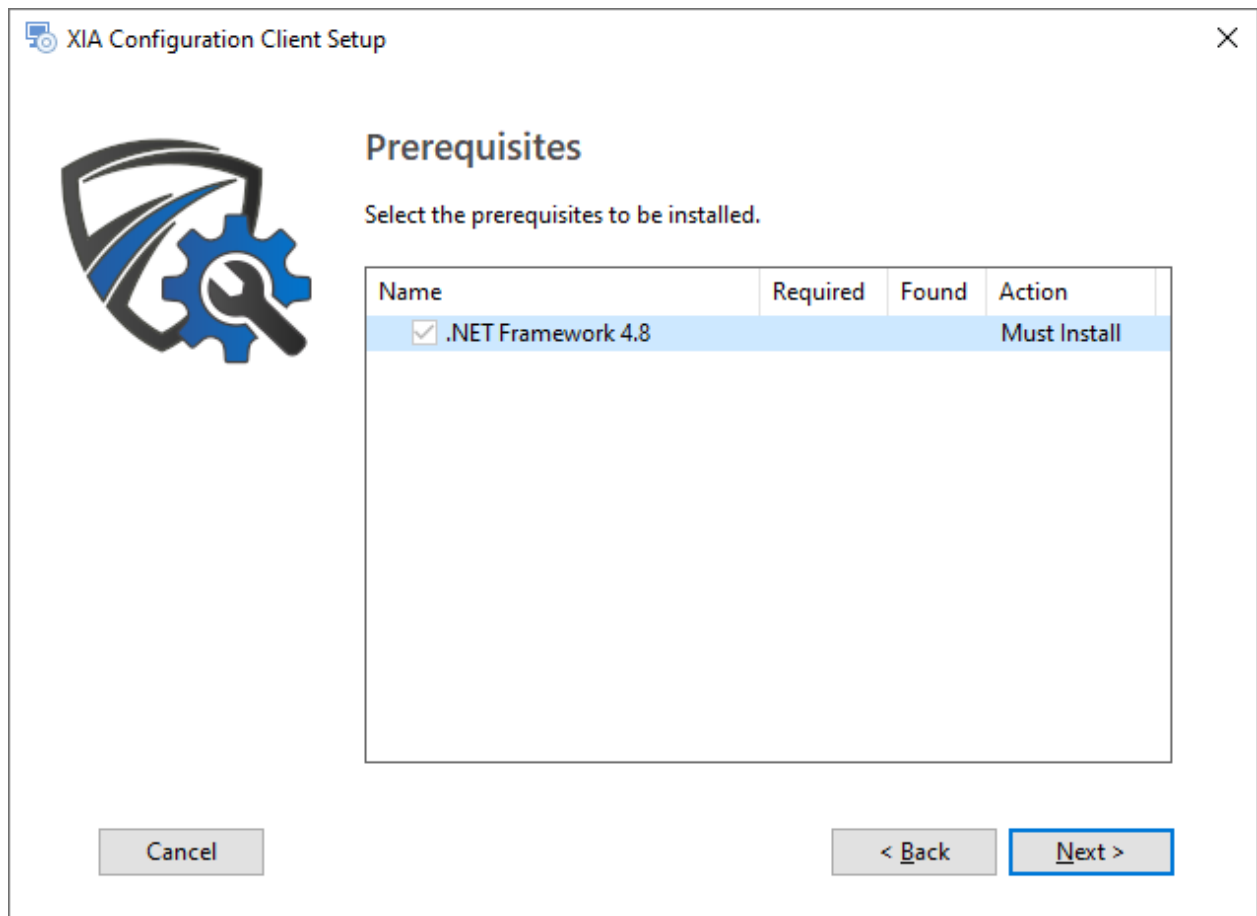
The [XIA Configuration Client](#) runs as a [Windows service](#) and is used to automatically detect and document networked devices, computers and servers.

The client is **installed automatically** when [XIA Configuration Server](#) is **installed**, however it can also be installed on additional machines in other networks or remote sites that are not accessible from the [XIA Configuration Server](#) computer using the following process

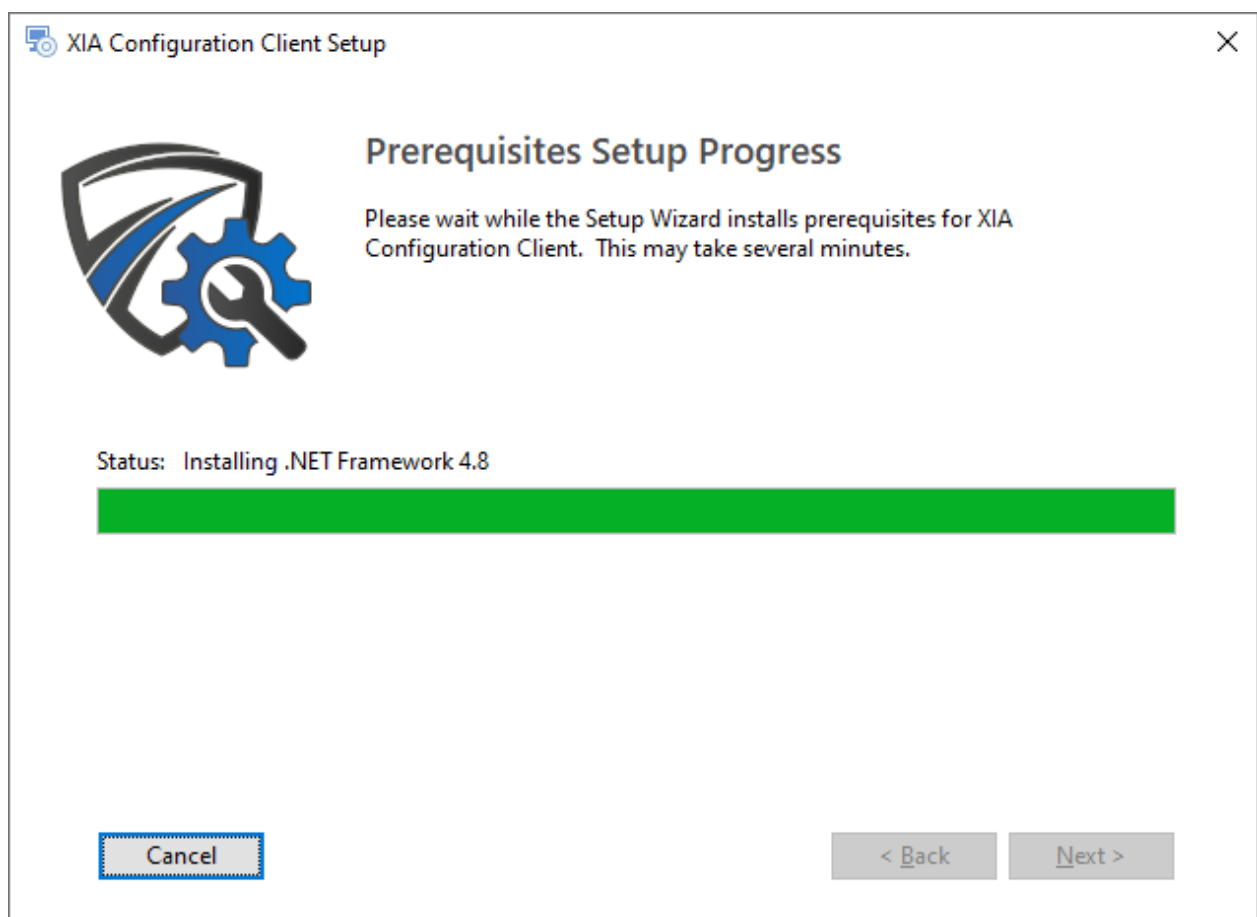
- Review the [roles and features](#) that will be automatically installed.
- Check that the system you are installing on meets the [client requirements](#).
- Within the [XIA Configuration Server](#) web interface select Tools > Download Installers.
- Click the *Download* button under the *XIA Configuration Client* heading and save the file.
- Start the installer, if the [.NET Framework 4.8](#) is not install the *Prerequisites Setup Wizard* will be displayed.



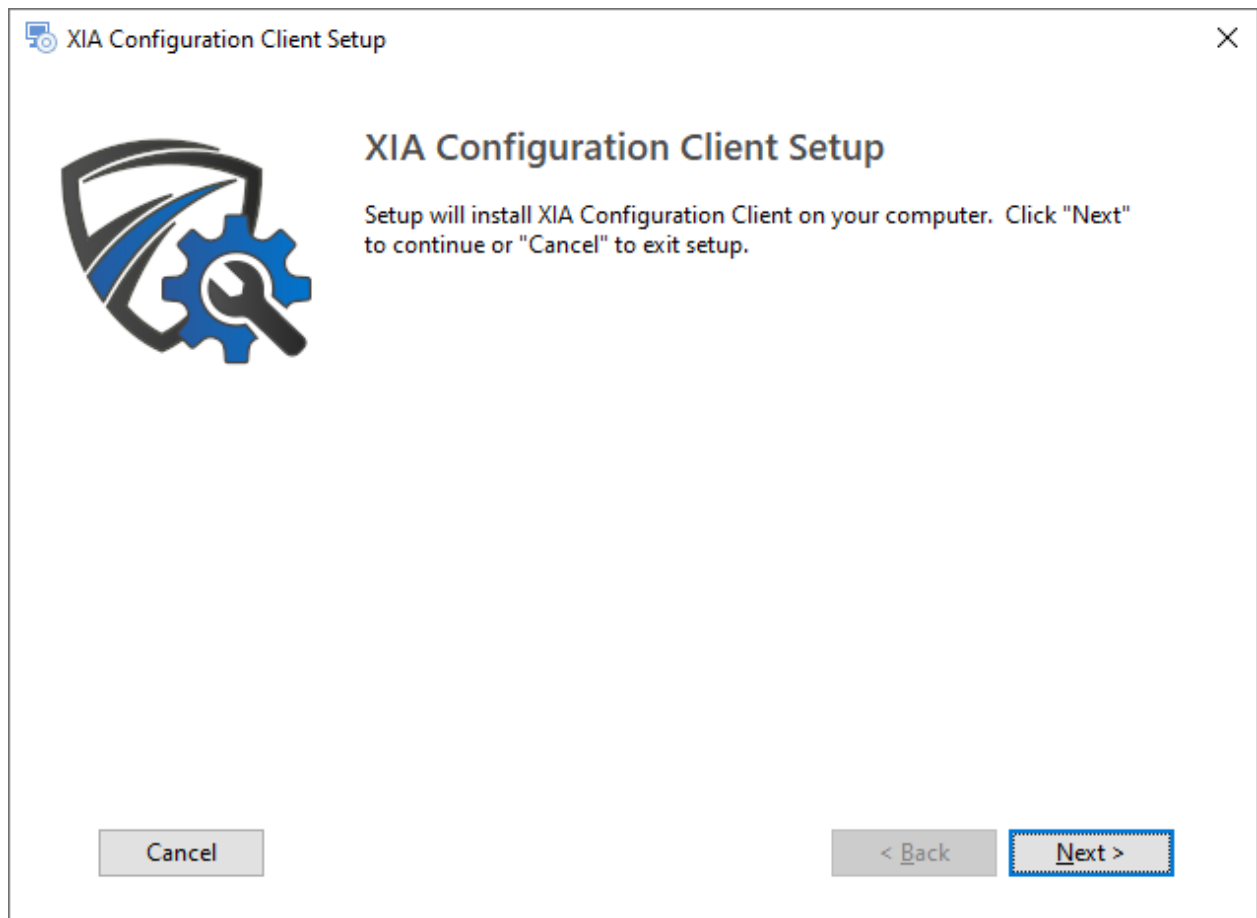
- You will be prompted to install the [.NET Framework 4.8](#).



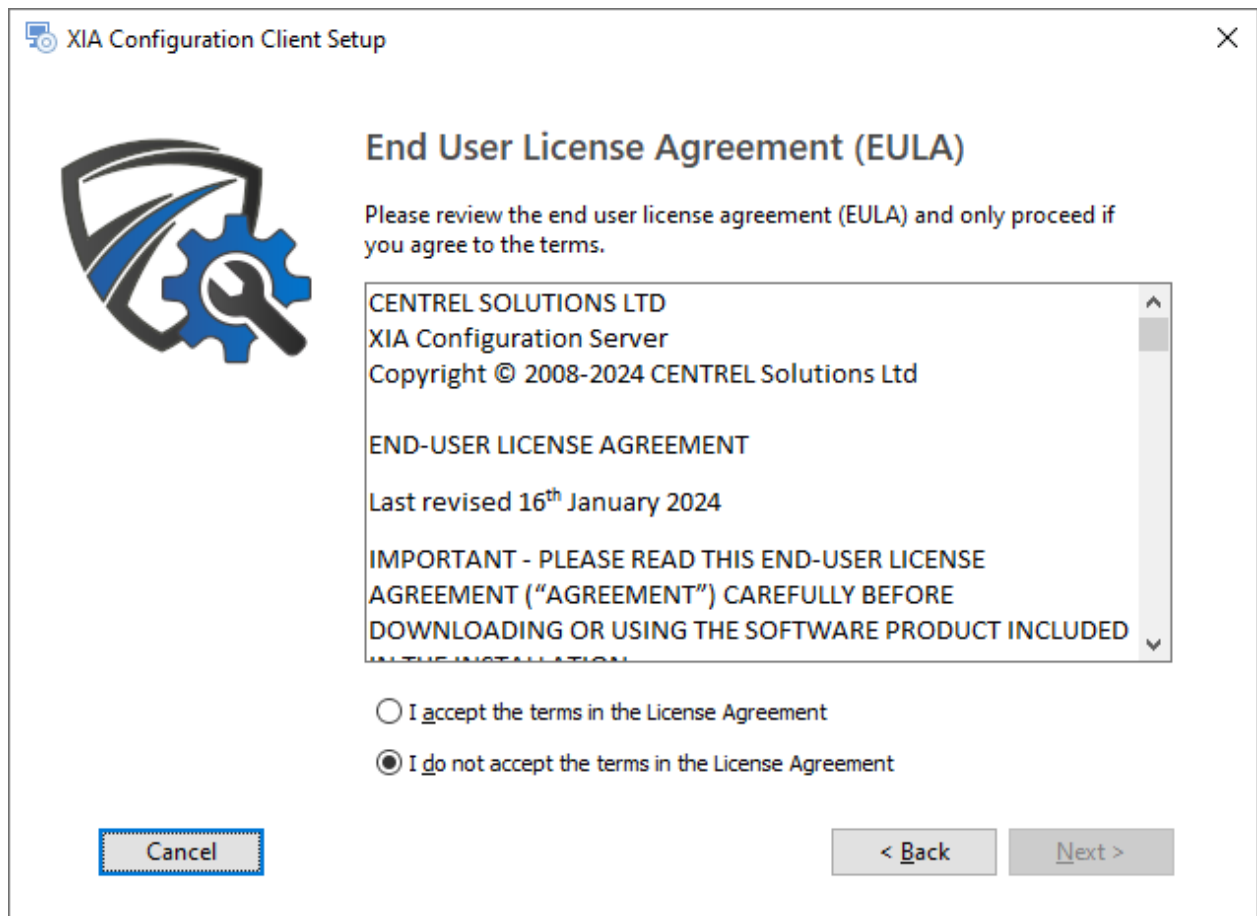
- The [.NET Framework 4.8](#) will be installed immediately and a [log file](#) created for the installation.



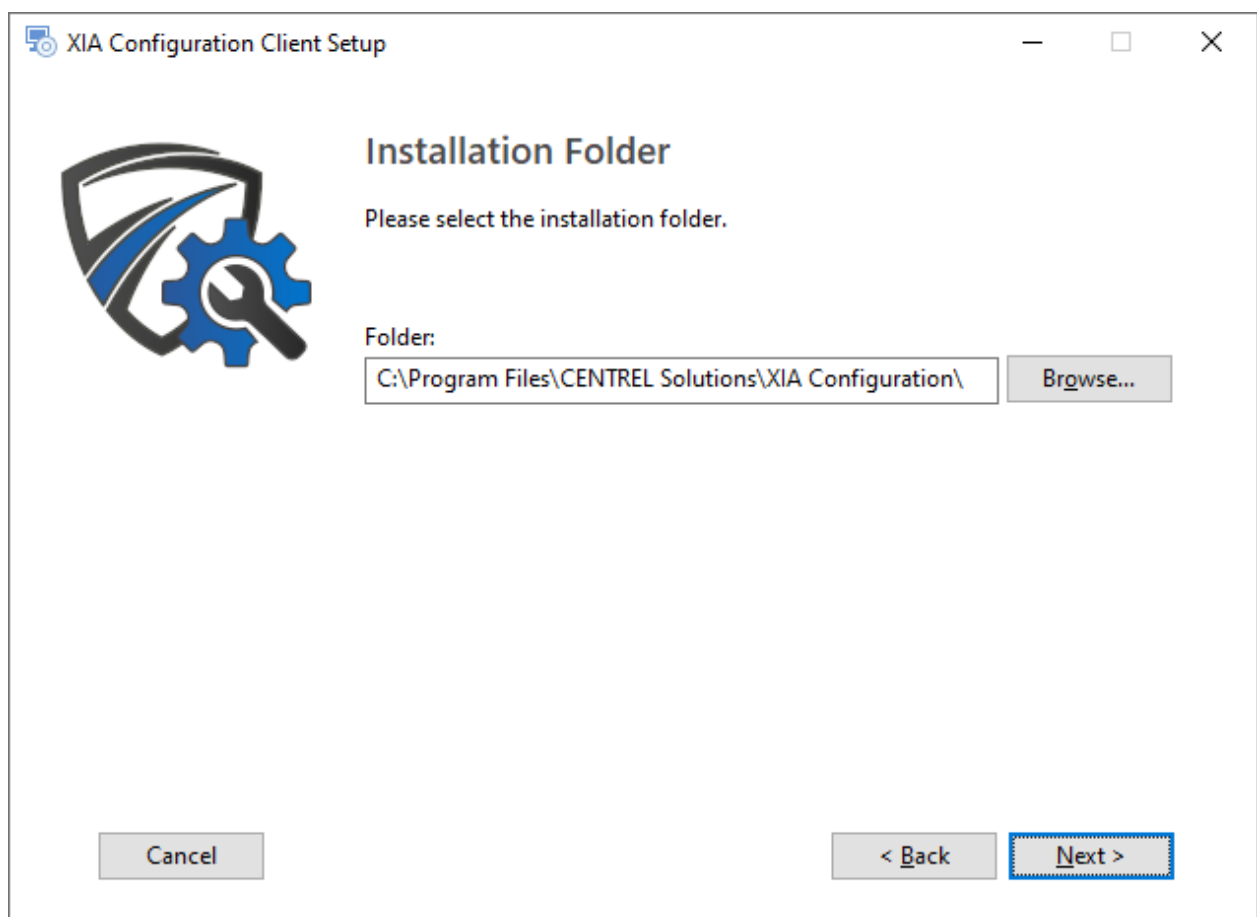
- You may be required to reboot to continue the installation. The installation will resume automatically after logging in following the reboot.
- The main installation screen will be displayed.



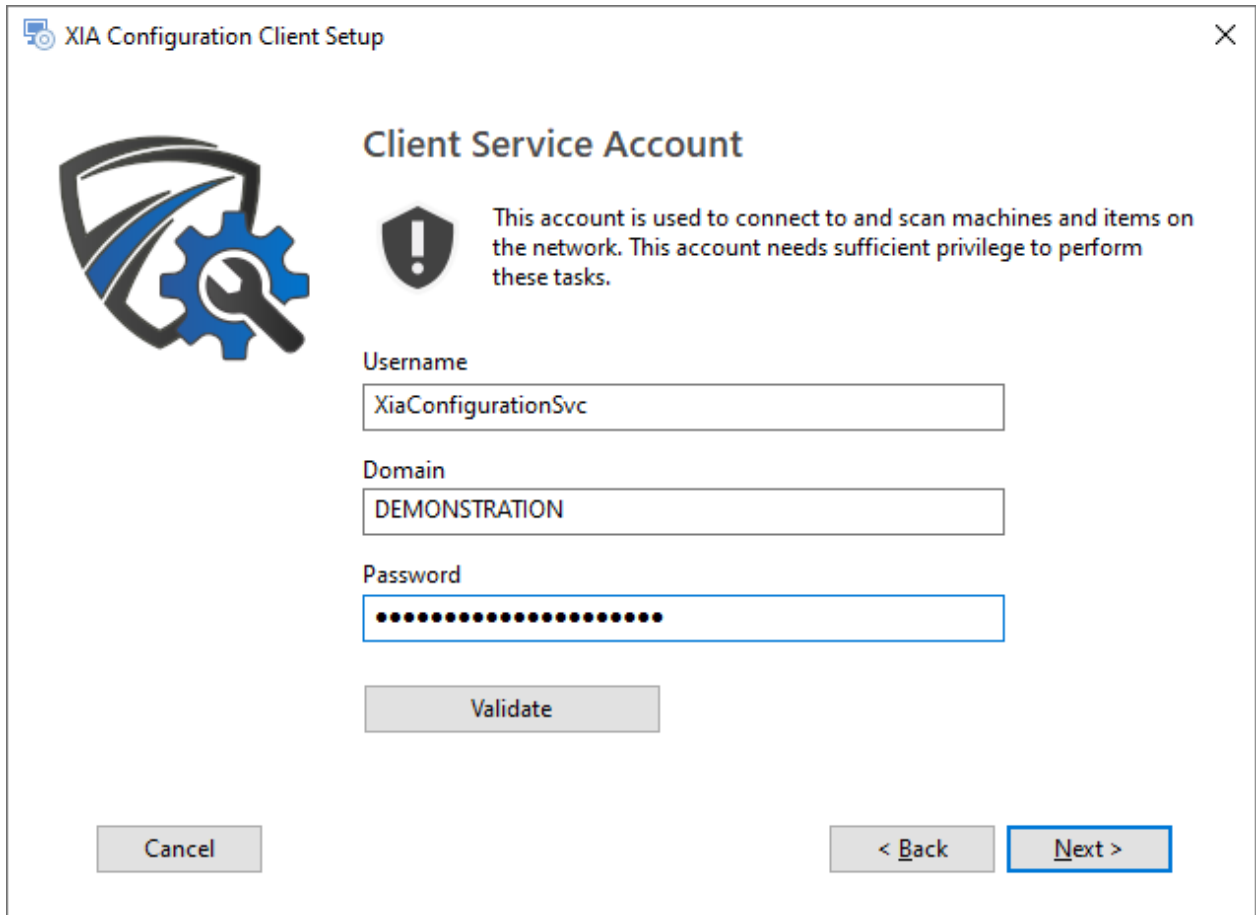
- Review the [end user license agreement \(EULA\)](#) and only accept if you agree to the terms. If you do not accept the terms of the agreement please cancel the installation.



- Select the directory into which the [XIA Configuration Client](#) should be installed and click *Next*.

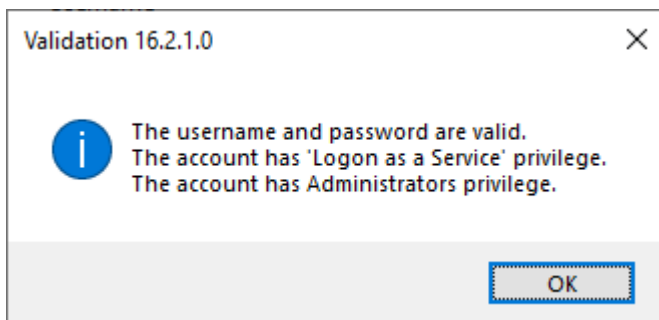


- Enter the credentials to use for the [service account](#), this is the account that will by default be performing the scans of devices and click *Validate*.



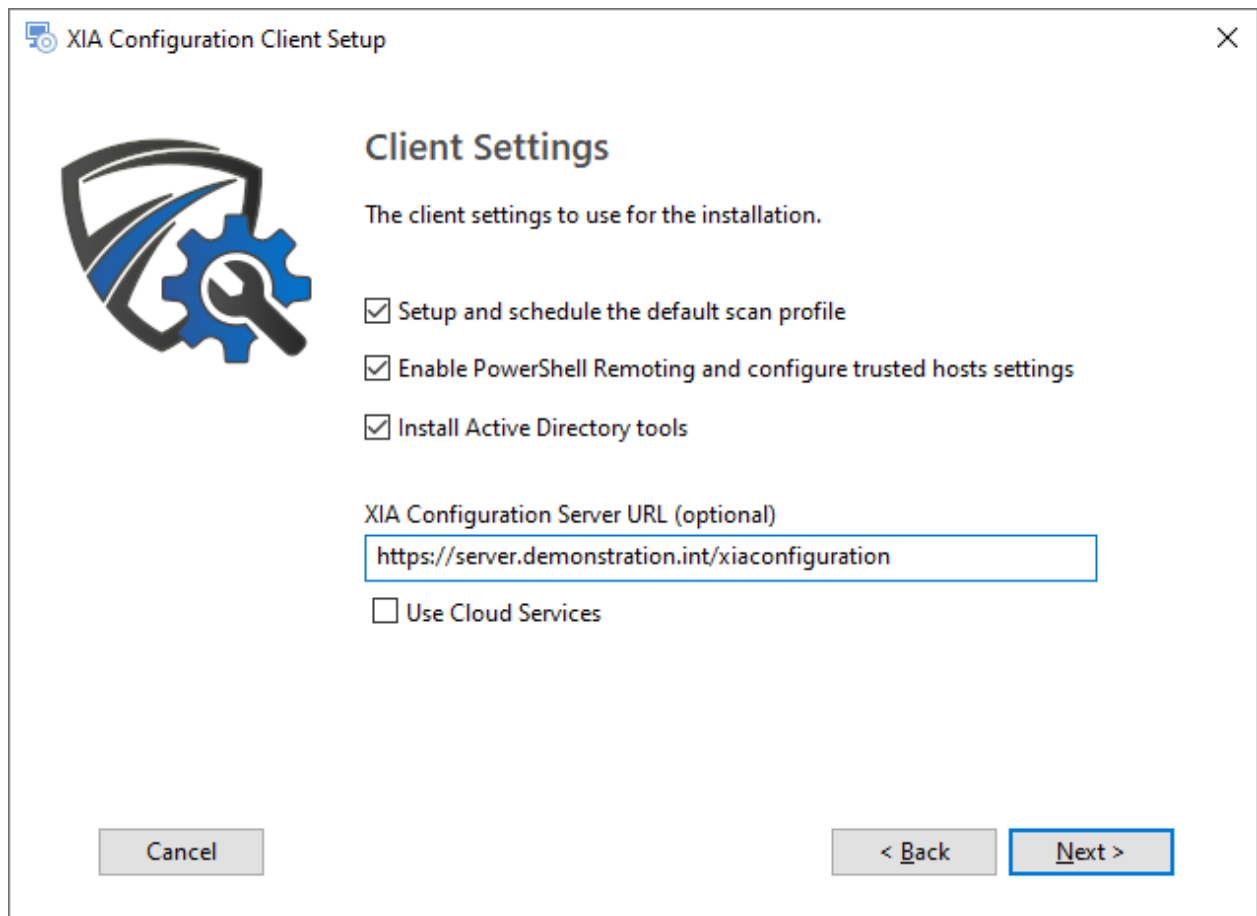
The dialog box is titled "XIA Configuration Client Setup" and "Client Service Account". It features a shield and gear icon on the left. A warning icon and text state: "This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks." Below this are three input fields: "Username" with the value "XiaConfigurationSvc", "Domain" with the value "DEMONSTRATION", and "Password" which is masked with dots. A "Validate" button is positioned below the password field. At the bottom, there are "Cancel", "< Back", and "Next >" buttons.

- **NOTE:** When using a computer on a WORKGROUP enter the **computer name** in the *Domain* field.
- Confirm that the account has the appropriate permissions and click *OK*, then click *Next*.

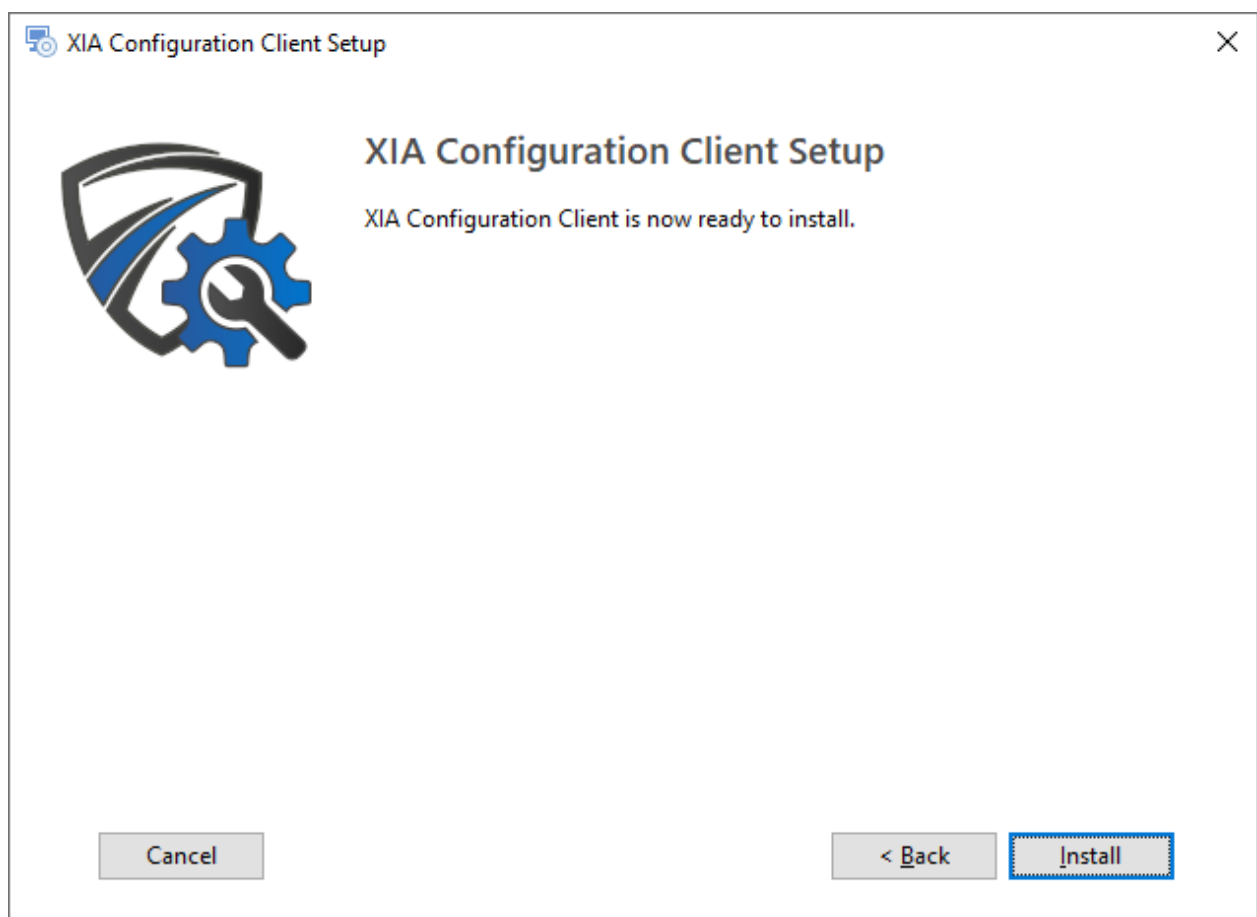


The dialog box is titled "Validation 16.2.1.0". It contains an information icon and the following text: "The username and password are valid. The account has 'Logon as a Service' privilege. The account has Administrators privilege." An "OK" button is located at the bottom right.

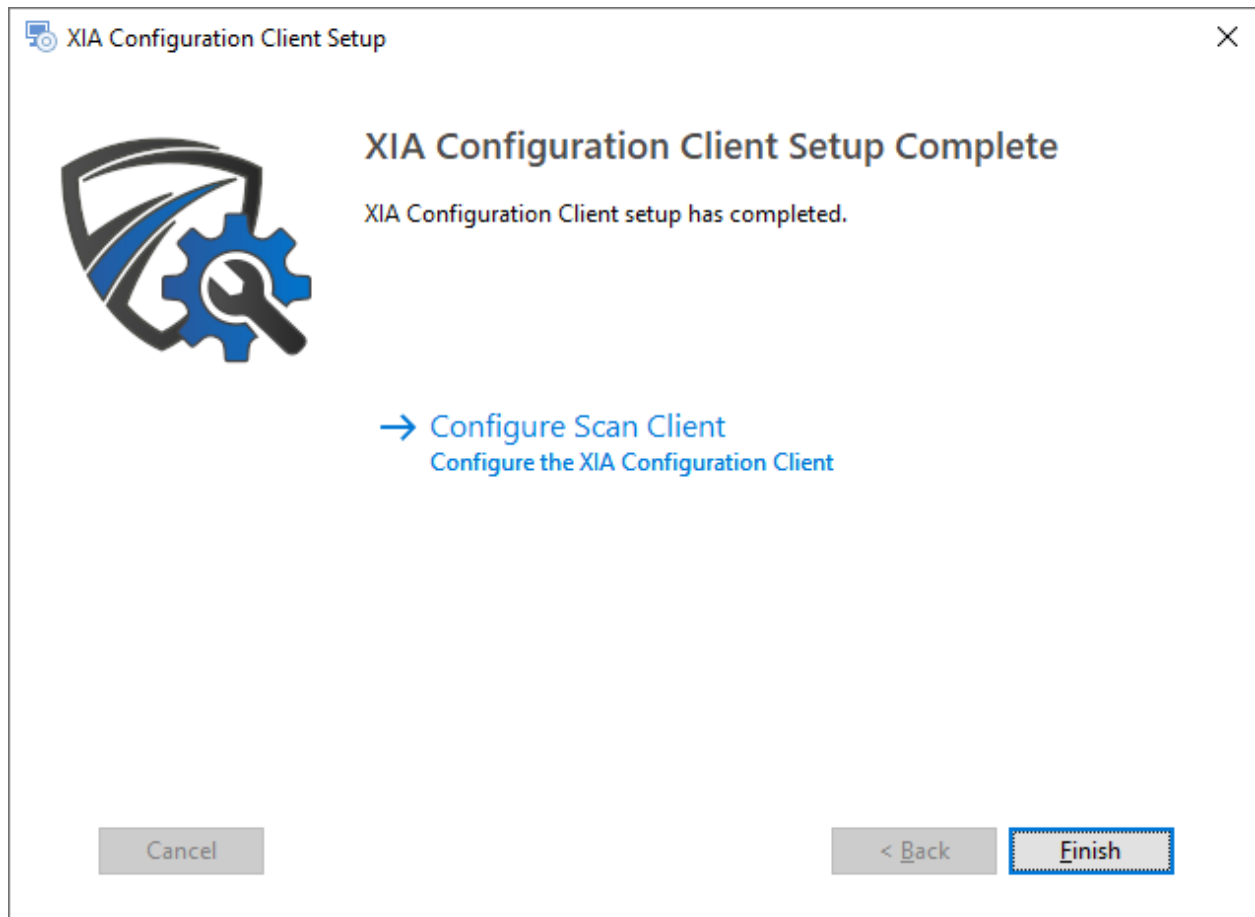
- Determine the appropriate [client advanced settings](#) and click *Next*.



- Click *Install* to begin the installation.



- When the installation is complete you will be prompted to configure the [client](#), click *Finish* to complete the installation.



Automatic Updates

The automatic update feature provides the ability to automatically update the XIA Configuration Client on **remote** machines.

NOTE: Automatic updates cannot be used to update the client on the XIA Configuration Server machine, this is updated as part of the XIA Configuration Server update process.

Server

Deployment settings including approved updates and clients must be configured on the server. More information can be found in the [Automatic Update Settings](#) section.

Client Configuration

Client settings including server URL and update interval must be configured on the client. More information can be found in the [Server Settings](#) and [Automatic Updates](#) sections.

Installer Cache

The installer is downloaded from the server and executed from the following location by default
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration
Service\Installer\setup.exe

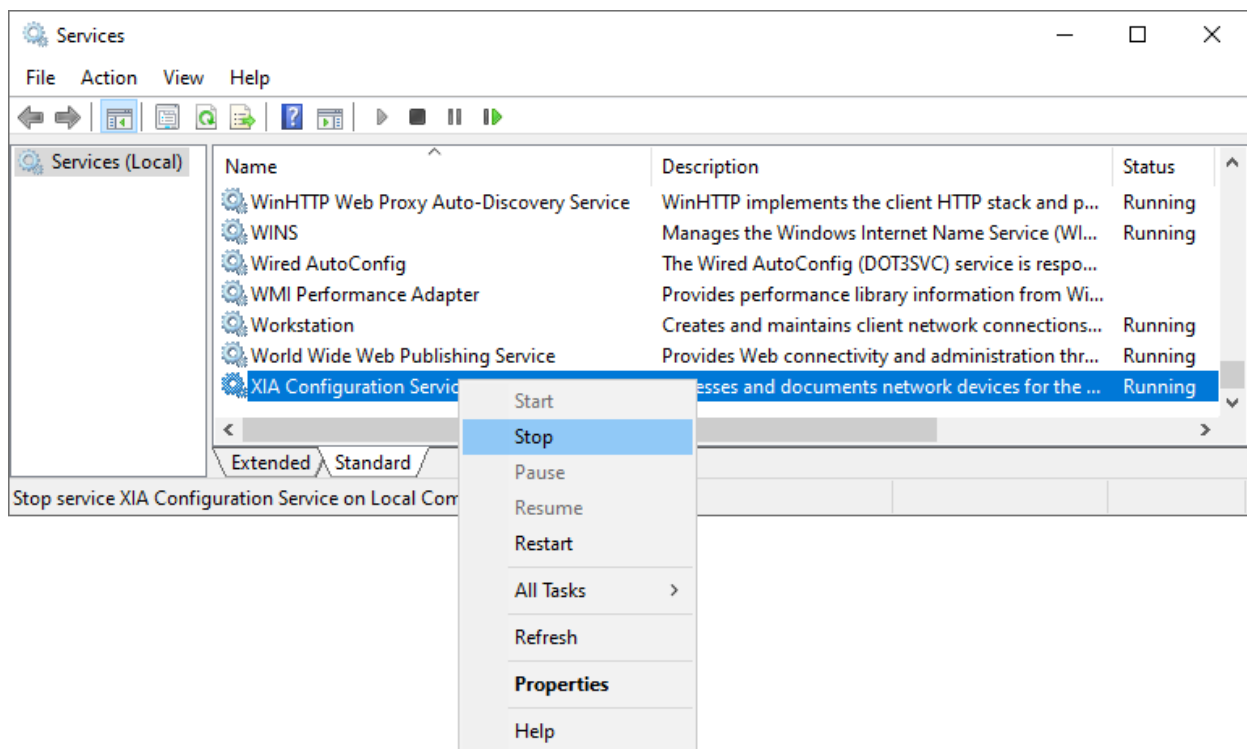
Log Files

The installation log files are created by default
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration
Service\Installer\installer.log

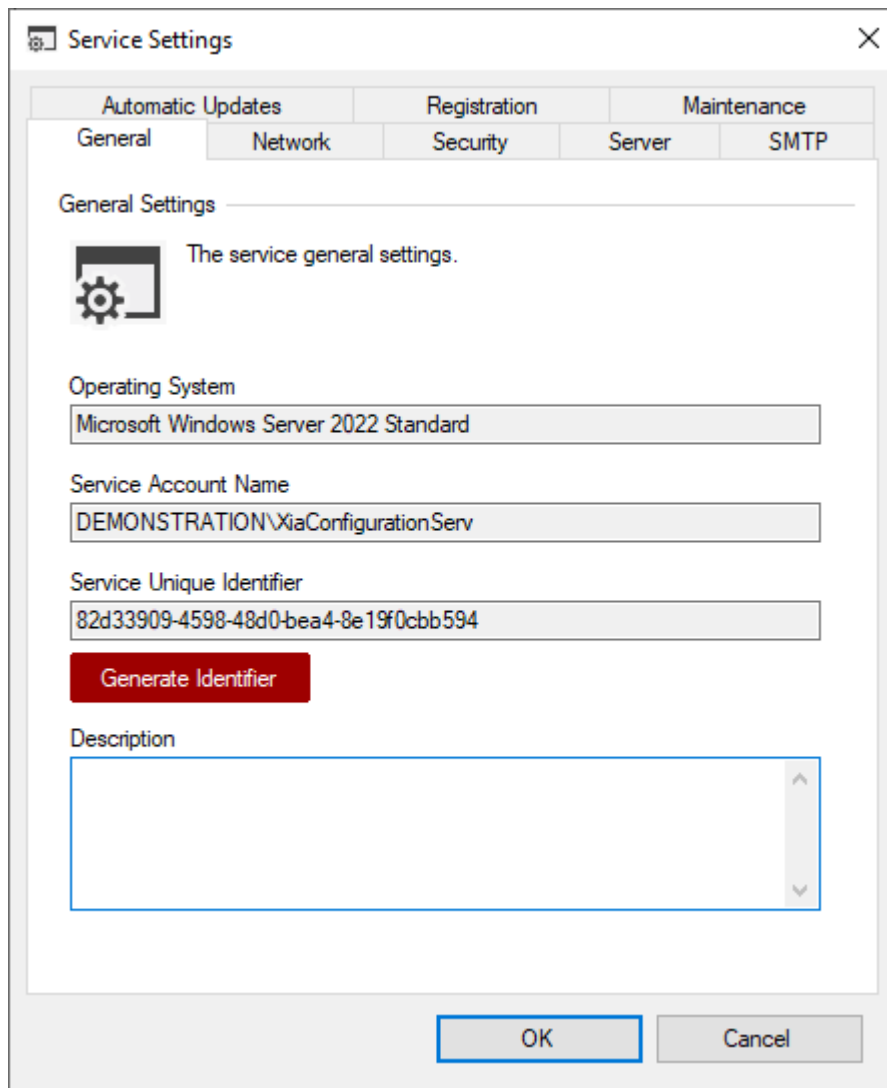
Client Migration

The following steps describe how to migrate the settings from an existing stand-alone installation of the [XIA Configuration Client](#) to a new server. To migrate the settings for the [XIA Configuration Client](#) that is installed as part of the [XIA Configuration Server](#), see the [client migration](#) section.

- Ensure you have a **full system backup** of the existing and new server.
- On the new server, [install](#) the **same version** of [XIA Configuration Client](#) as is [installed](#) on the existing server.
- On the new server, stop the XIA Configuration Service.



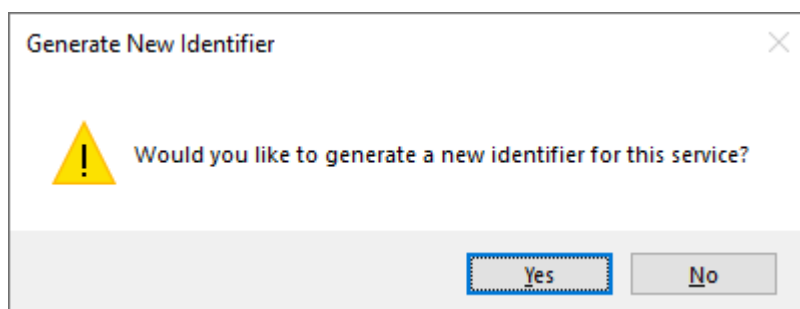
- Copy the **encryption** and **configuration** directories from the existing server to the new server, overwriting any existing files.
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Configuration
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Encryption
- On the new server, start the XIA Configuration Service.
- On the new server, open the [administration tools](#), go to the [service settings, general tab](#) and click the **generate identifier** button.



The Service Settings dialog box is shown with the 'General' tab selected. It contains the following fields and controls:

- General Settings**: A section header with a gear icon and the text 'The service general settings.'
- Operating System**: A text field containing 'Microsoft Windows Server 2022 Standard'.
- Service Account Name**: A text field containing 'DEMONSTRATION\XiaConfigurationServ'.
- Service Unique Identifier**: A text field containing '82d33909-4598-48d0-bea4-8e19f0cbb594'.
- Generate Identifier**: A red button located below the Service Unique Identifier field.
- Description**: A large, empty text area with a blue border and a vertical scrollbar.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

- Click yes when prompted.



The Generate New Identifier dialog box is shown. It contains the following elements:

- Title**: 'Generate New Identifier'.
- Icon**: A yellow warning triangle with a black exclamation mark.
- Text**: 'Would you like to generate a new identifier for this service?'.
- Buttons**: 'Yes' and 'No' buttons at the bottom right.

- Save the settings and close the [administration tools](#).
- Once complete, [uninstall](#) the [XIA Configuration Client](#) from the existing server.

Client Requirements

This section describes the requirements for the [installation](#) of the [XIA Configuration Client](#).

Operating Systems (Server)

The following operating systems are supported for the installation of a production version of the [XIA Configuration Client](#).

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Desktop Operating Systems

The following operating systems are supported for the installation of a production version of the [XIA Configuration Client](#).

- Windows 11 Pro (64-bit)
- Windows 10 Pro Anniversary Edition (64-bit)

Please note that these are the operating systems on which the [XIA Configuration Client](#) can be installed, not the operating systems that can be [scanned](#).

.NET Framework

- [.NET Framework 4.8](#) * (*installed automatically*) **

Windows Management Framework

- [Window Management Framework 5.1](#) (pre-installed on Windows 10, Windows Server 2016 and above).

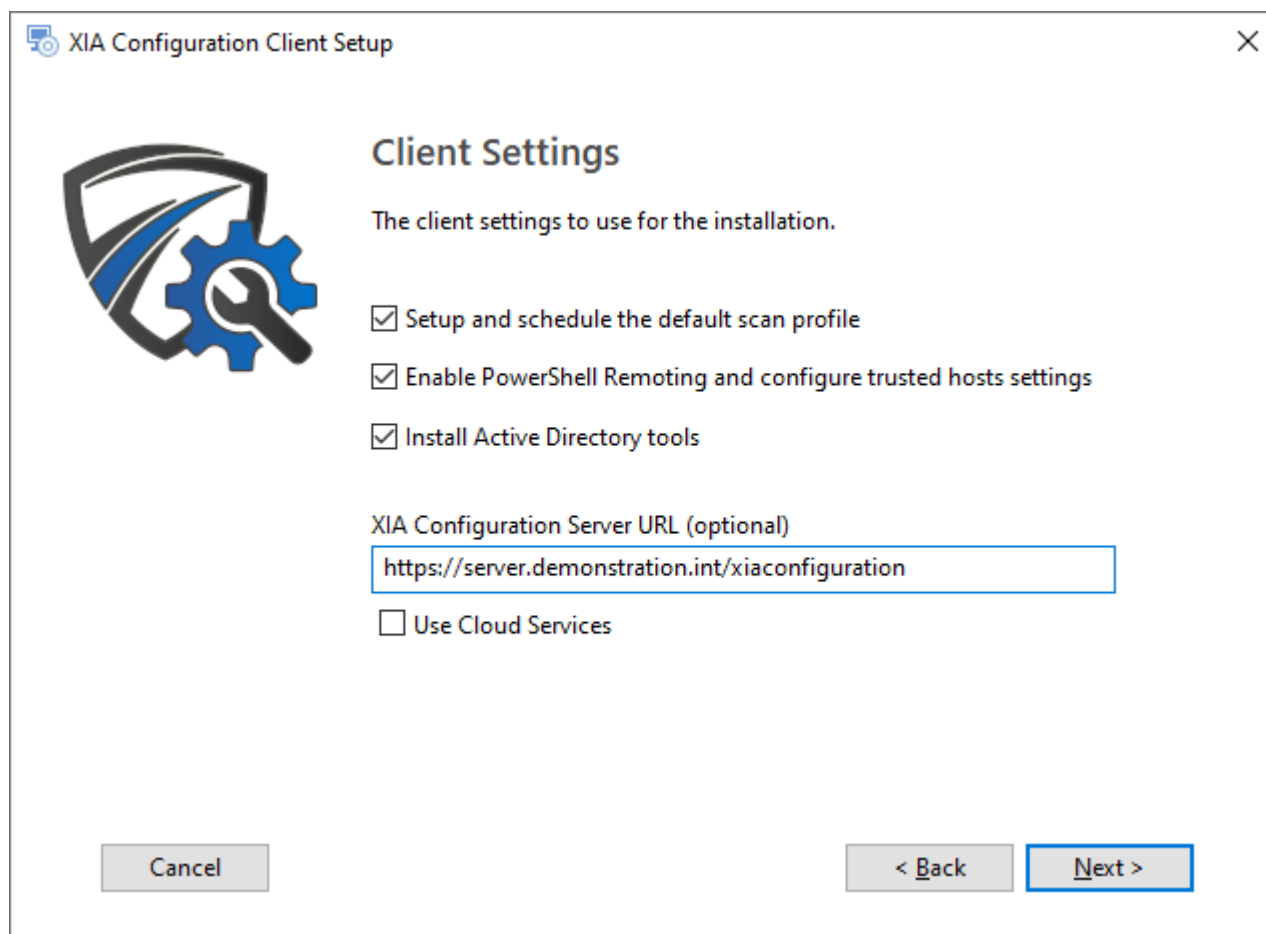
* Please see the [Microsoft .NET Framework 4.8 installation requirements](#) for further information

** When using [automatic updates](#) we recommend that the [.NET Framework 4.8](#) is installed manually

in advance.

Client Advanced Settings

When installing the [XIA Configuration Client](#) the following advanced settings are presented.



The screenshot shows the 'XIA Configuration Client Setup' window. On the left is a shield icon with a gear and a wrench. The title is 'Client Settings'. Below the title is the text 'The client settings to use for the installation.' There are three checked checkboxes: 'Setup and schedule the default scan profile', 'Enable PowerShell Remoting and configure trusted hosts settings', and 'Install Active Directory tools'. Below these is a text box for 'XIA Configuration Server URL (optional)' containing the text 'https://server.demonstration.int/xiaconfiguration'. There is an unchecked checkbox for 'Use Cloud Services'. At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'. The 'Next >' button is highlighted with a blue border.

Setup and schedule the default scan profile

Determines whether the [installation](#) should create a [scan profile](#) which is [scheduled](#) to automatically scan common [items](#).

Enable PowerShell Remoting and configure trusted hosts settings

Determines whether the [installation](#) should enable [PowerShell remoting](#) on the local machine, and configure the [trusted hosts](#) setting to allow connections to any host.

Install Active Directory tools

Determines whether the [installation](#) should install the following Active Directory tools that are required by the [Active Directory](#) agent. For Windows 10 and Windows 11 Windows Update must be enabled and an internet connection available.

- Active Directory module for Windows PowerShell (RSAT-AD-PowerShell)
- DFS Management Tools (RSAT-DFS-Mgmt-Con)
- Group Policy Management (GPMC)

XIA Configuration Server URL (optional)

Determines the URL of the [XIA Configuration Server](#) which information should automatically be uploaded to. This setting can be configured at a later time in the [server settings](#).

Use Cloud Services

Determines whether the hosted [Cloud Services](#) is being used. This setting can be configured at a later time in the [server settings](#).

Client Installation Troubleshooting

This section provides troubleshooting information for the [installation](#) of the [XIA Configuration Client](#).

- Please ensure that your system meets the [client installation requirements](#).
- You can request support by going to our [support page](#).
- For additional information about the installation please see the [custom actions log file](#).

[Service 'XIA Configuration Service' \(XIAConfigurationSvc\) failed to start](#)

Service 'XIA Configuration Service' (XIAConfigurationSvc) failed to start

Symptoms

When [installing](#) either the [XIA Configuration Client](#) or the [XIA Configuration Server](#) (as this contains the [XIA Configuration Client](#)), the following dialog is seen

*Service 'XIA Configuration Service' (XIAConfigurationSvc) failed to start.
Verify that you have sufficient privileges to start system services.*

Issue

There are several possible causes of this issue

- The password for the [service account](#) has expired.
- The account is disabled.
- The account is locked out.
- The [service account](#) stored in the registry is different from that stored in the service management console.
- The [service account](#) has not been assigned the [Log on as a service](#) right.
- The [service account](#) has been assigned the [Deny log on as a service](#) right.

Resolution

- Open *Windows Event Viewer* and check for any log on related errors. [Change the service account password](#) if it has expired.
- Ensure the account is not disabled.
- Unlock the account.
- If you are upgrading and have changed the service account manually since the installation, ensure that you have followed the instructions for [changing the service account](#).
- Ensure that the [service account](#) has been assigned the [Log on as a service right](#). This is automatically granted by the [installation](#), however can be overridden by the Group Policy configuration within your organization.
- Ensure that the [service account](#) has not been assigned the [Deny log on as a service](#) right.

Configuring Client Certificates

To configure the [XIA Configuration Client](#) to use client certificates in conjunction with Microsoft Internet Information Server (IIS) as a method of two factor authentication, complete the following steps:

- Ensure that the IIS server is configured with a valid SSL certificate
- Ensure that the **Connect to server** setting on the [server settings](#) or [server upload](#) uses the appropriate HTTPS address of the server.
- Ensure that the IIS server SSL settings are configured appropriately to either accept or require client certificates



SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

☒ **Require SSL**

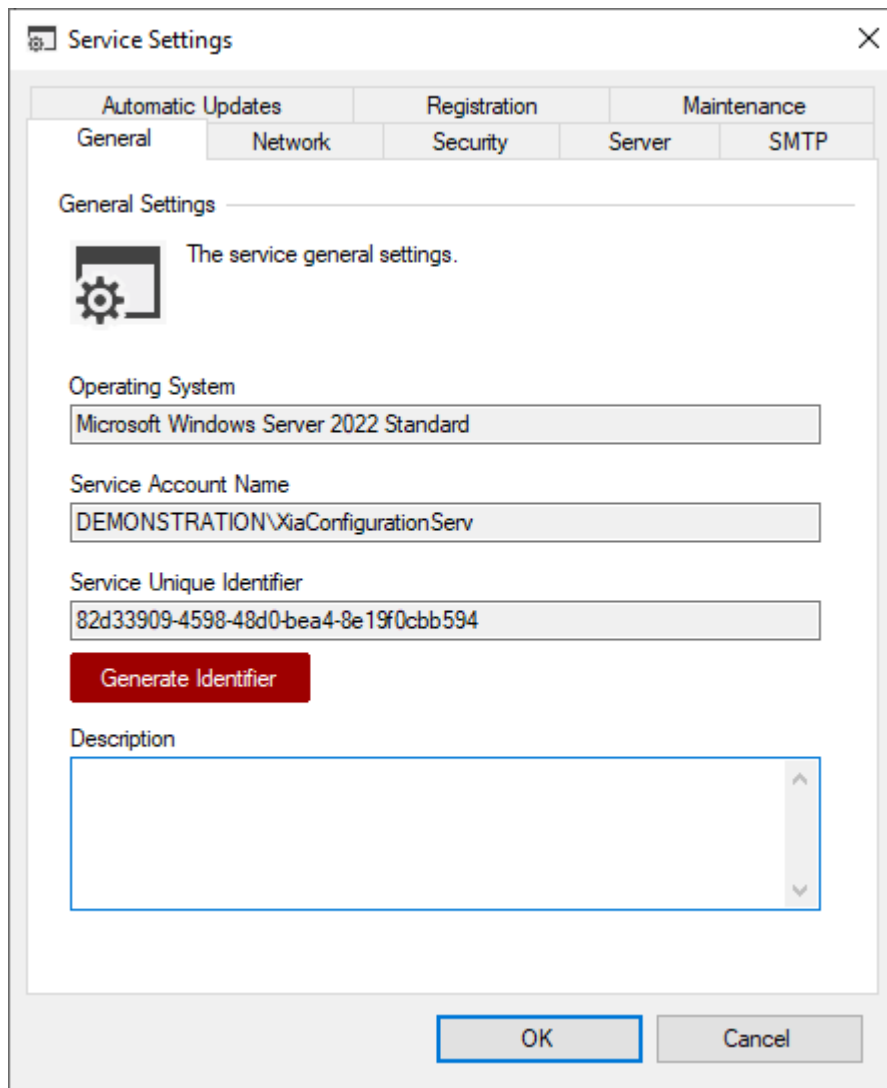
Client certificates:

☐ Ignore

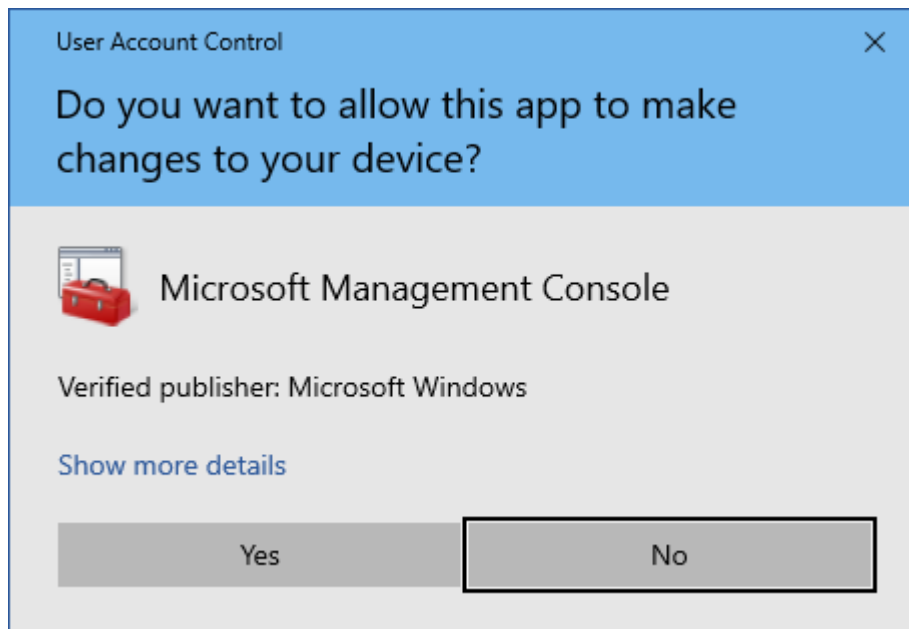
☐ Accept

☒ **Require**

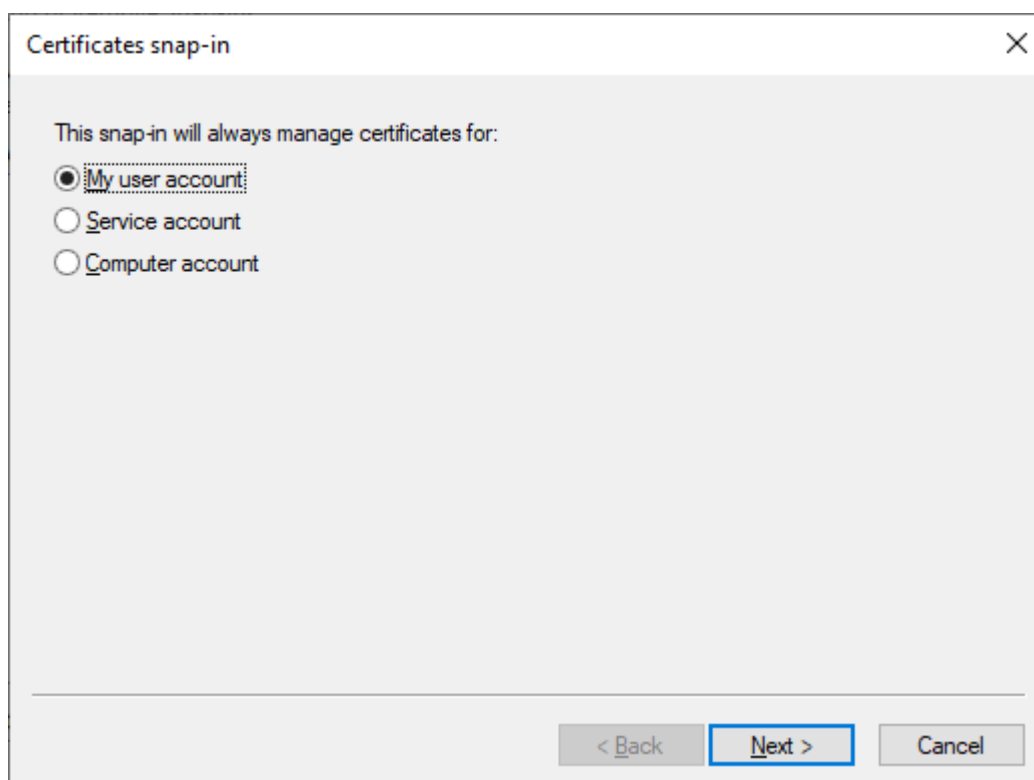
- Determine the name of the [service account](#) by viewing the [general tab](#) of the [service settings](#).



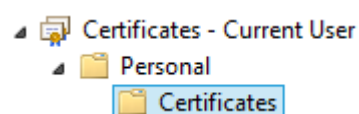
- Logon as the [service account](#) and run mmc.exe or
- or -
- Execute the command substituting the service account name
`runas /user:"domain\user" "cmd /c mmc"`
- Accept the UAC prompt if required



- Add the **Certificates** snap-in and ensure that **My user account** is selected (using the **Service account** option is not supported)



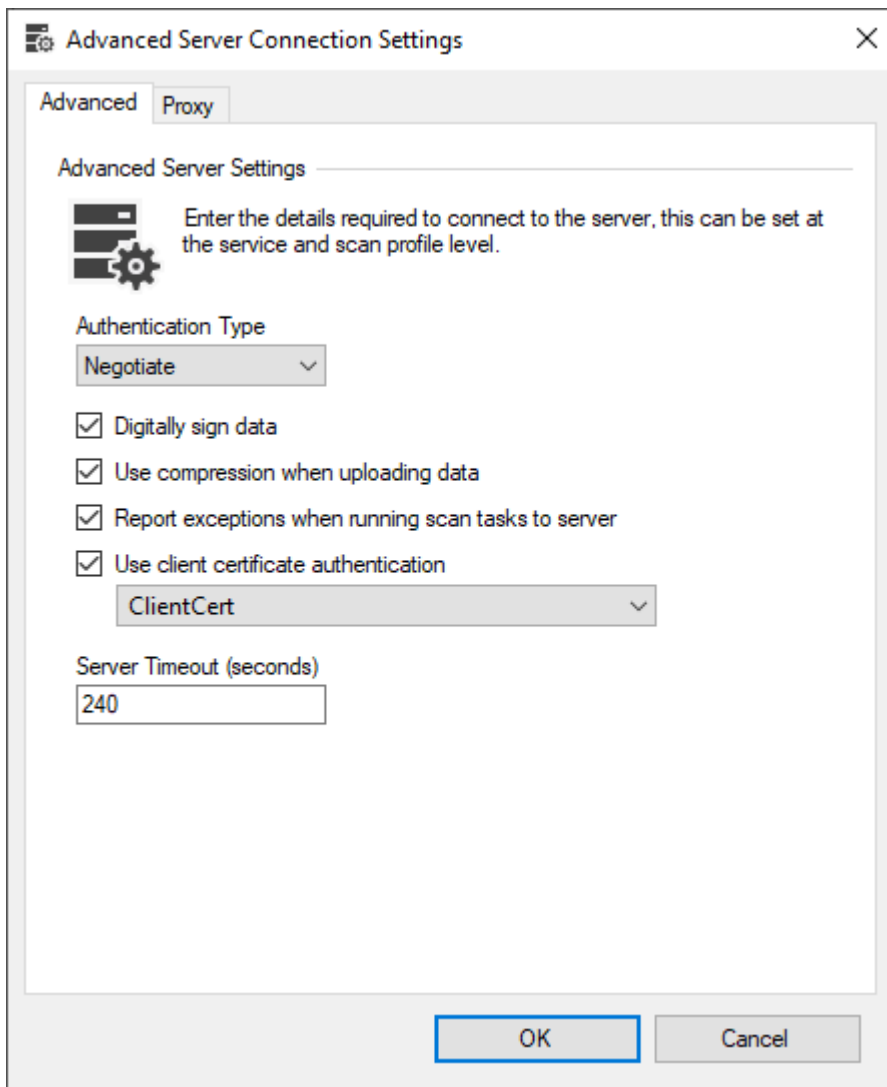
- Import the client certificate into the **Personal** folder for the service user account.



- When imported ensure that the client certificate is within the expiration date and that **Client Authentication** is one of the intended purposes

Issued To	Issued By	Expiration Date	Intended Purposes
 ClientCert	MyPersonalCA	01/01/2018	Client Authentication

- On the [advanced settings tab](#) of either the [server settings](#) or [server upload](#) as appropriate, select the appropriate client certificate



The image shows a Windows-style dialog box titled "Advanced Server Connection Settings". It has two tabs: "Advanced" (selected) and "Proxy". Under the "Advanced" tab, there is a section titled "Advanced Server Settings" with a sub-header "Enter the details required to connect to the server, this can be set at the service and scan profile level." Below this, there is a "Authentication Type" dropdown menu set to "Negotiate". There are four checked checkboxes: "Digitally sign data", "Use compression when uploading data", "Report exceptions when running scan tasks to server", and "Use client certificate authentication". Below these checkboxes is another dropdown menu set to "ClientCert". At the bottom of the settings section is a "Server Timeout (seconds)" text box containing the value "240". At the very bottom of the dialog are "OK" and "Cancel" buttons.

Advanced Server Connection Settings

Advanced Proxy

Advanced Server Settings

Enter the details required to connect to the server, this can be set at the service and scan profile level.

Authentication Type

Negotiate

☒ Digitally sign data

☒ Use compression when uploading data

☒ Report exceptions when running scan tasks to server

☒ Use client certificate authentication

ClientCert

Server Timeout (seconds)

240

OK Cancel

Client Installation Log Files

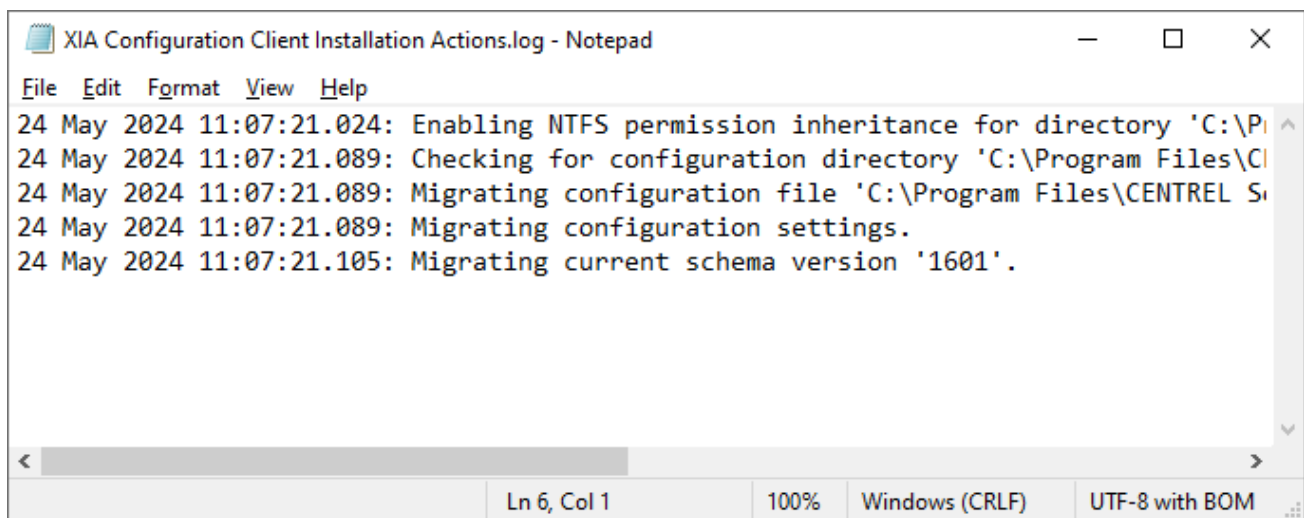
Client Installation Logging

To enable [client installation](#) logging run the setup command with [MSI command line](#) logging parameters - for example
setup.exe /l*v "C:\setup.log"

Custom Action Log Files

Please note additional information related to the installation may be logged to the custom actions log file which is stored in the following location
%temp%\XIA Configuration Client Installation Actions.log

This contains information related to client pre-configuration.



```
XIA Configuration Client Installation Actions.log - Notepad
File Edit Format View Help
24 May 2024 11:07:21.024: Enabling NTFS permission inheritance for directory 'C:\P
24 May 2024 11:07:21.089: Checking for configuration directory 'C:\Program Files\Cl
24 May 2024 11:07:21.089: Migrating configuration file 'C:\Program Files\CENTREL S
24 May 2024 11:07:21.089: Migrating configuration settings.
24 May 2024 11:07:21.105: Migrating current schema version '1601'.
Ln 6, Col 1 100% Windows (CRLF) UTF-8 with BOM
```

.NET Framework Installation Log File

If the [.NET Framework 4.8](#) is installed a log file will be created in the following location
%temp%\Microsoft .NET Framework 4.8 Setup_XXXXXXXX_XXXXXXXXX.html

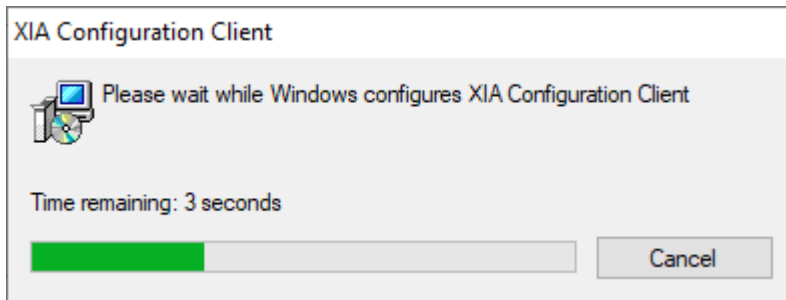
Installed Roles and Features

During the [installation](#) of the [XIA Configuration Client](#) the following features and other shared components will be automatically installed.

- [.NET Framework 4.8](#)
- The Group Policy Management Console when selected on the [client and server advanced options](#).
- The Active Directory tools when selected on the [client and server advanced options](#).

Unattended Installation

It is possible to deploy the [XIA Configuration Client](#) without any user intervention using the following command line parameters.



```
setup /qb /norestart /l logfile.txt SERVICE_USERNAME="Username" SERVICE_DOMAIN="Domain" SERVICE_PASSWORD="Password"
```

SERVICE_USERNAME (required)

The name of the [service account](#).

SERVICE_DOMAIN (required)

The domain name of the [service account](#).

SERVICE_PASSWORD (required)

The password of the [service account](#).

SERVICE_PRECONFIGURE (optional)

Determines whether you want to preconfigure the client service with a default scan profile. By default this is enabled, setting this value to a value other than "True" disables this option.

SERVER_URL (optional)

When the server is being preconfigured determines the URL of the XIA Configuration Server to use. When entering the URL the address must use backslashes for example "http:\\corp-srv01\xiaconfiguration" to be supported by the Windows installer platform.

SERVICE_CONFIGURE_POWERSHELL (optional)

Determines whether the [installation](#) should enable [PowerShell remoting](#) on the local machine, and configure the [trusted hosts](#) setting to allow connections to any host. By default this is enabled, setting this value to a value other than "True" disables this option.

SERVICE_INSTALL_GPM (optional)

Determines whether the Group Policy Management Console should be installed on supported operating systems. When this value is not specified the Group Policy Management Console will be installed on supported operating systems. By default this is enabled, setting this value to a value other than "True" disables this option.

Logfile Path

Logfile.txt is the path to the log file to be created by the [installer](#).
Please note additional logging information may be found in the [custom actions log file](#).

Manual Unattended Upgrades

It is recommended that to automatically update the [XIA Configuration Client](#) you should use the built in [automatic updates](#) functionality.

To perform upgrades manually it is possible to install using the following syntax.

```
setup.exe /qb /norestart /l logfile.txt
```

Logfile Path

Logfile.txt is the path to the log file to create by the installer.

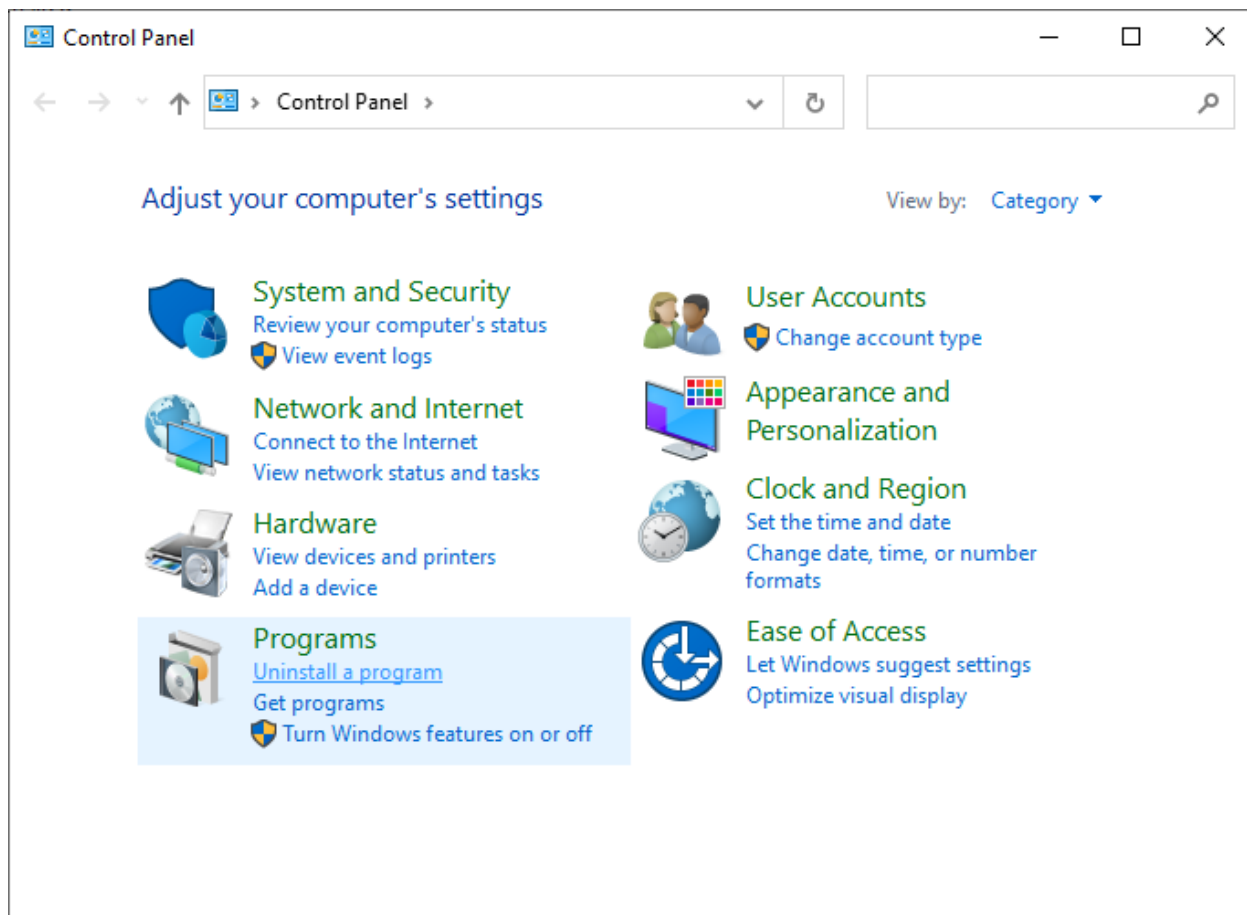
Please note additional logging information may be found in the [custom actions log file](#).

Uninstallation

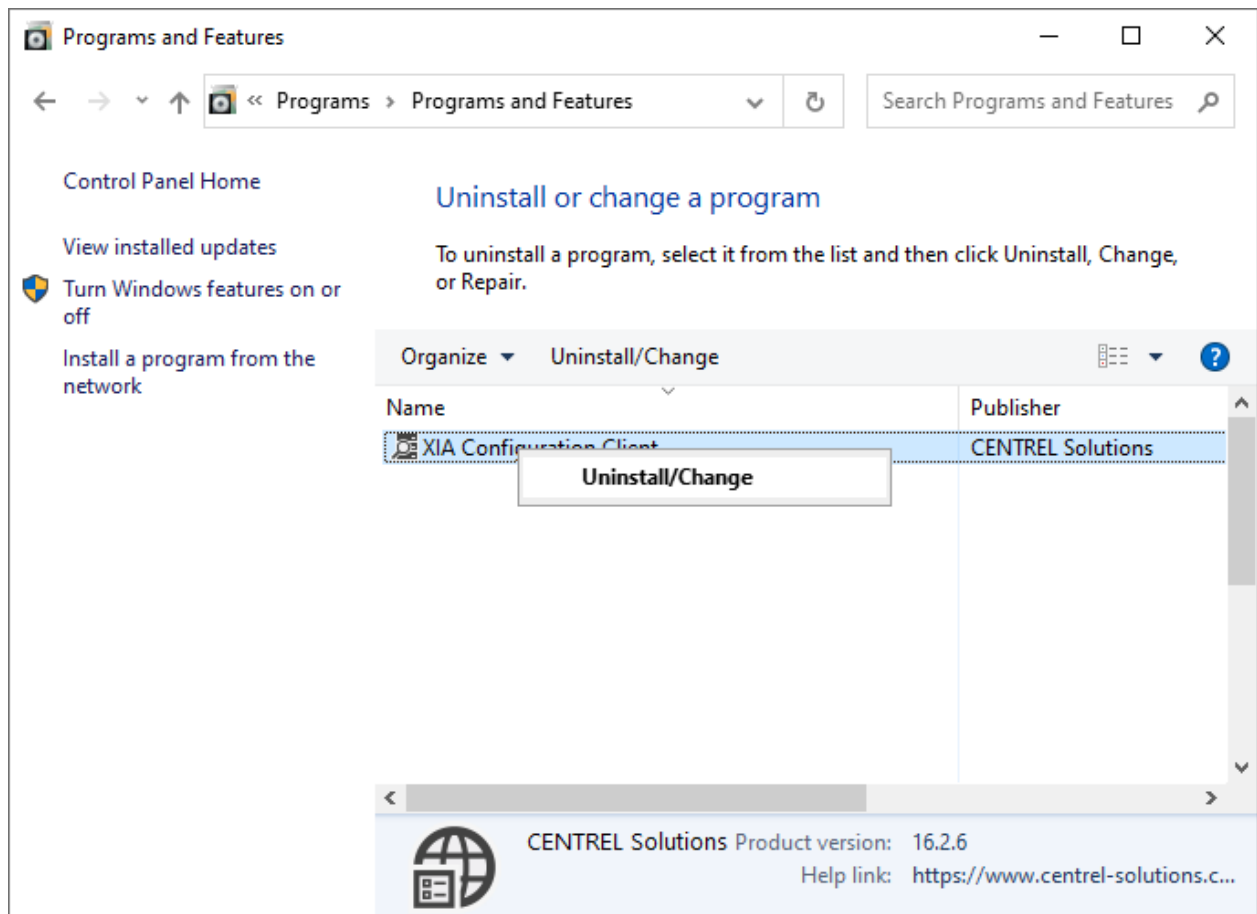
When installed as part of the [XIA Configuration Server](#) please follow the server [uninstallation](#) section.

To uninstall a stand-alone installation of the [XIA Configuration Client](#).

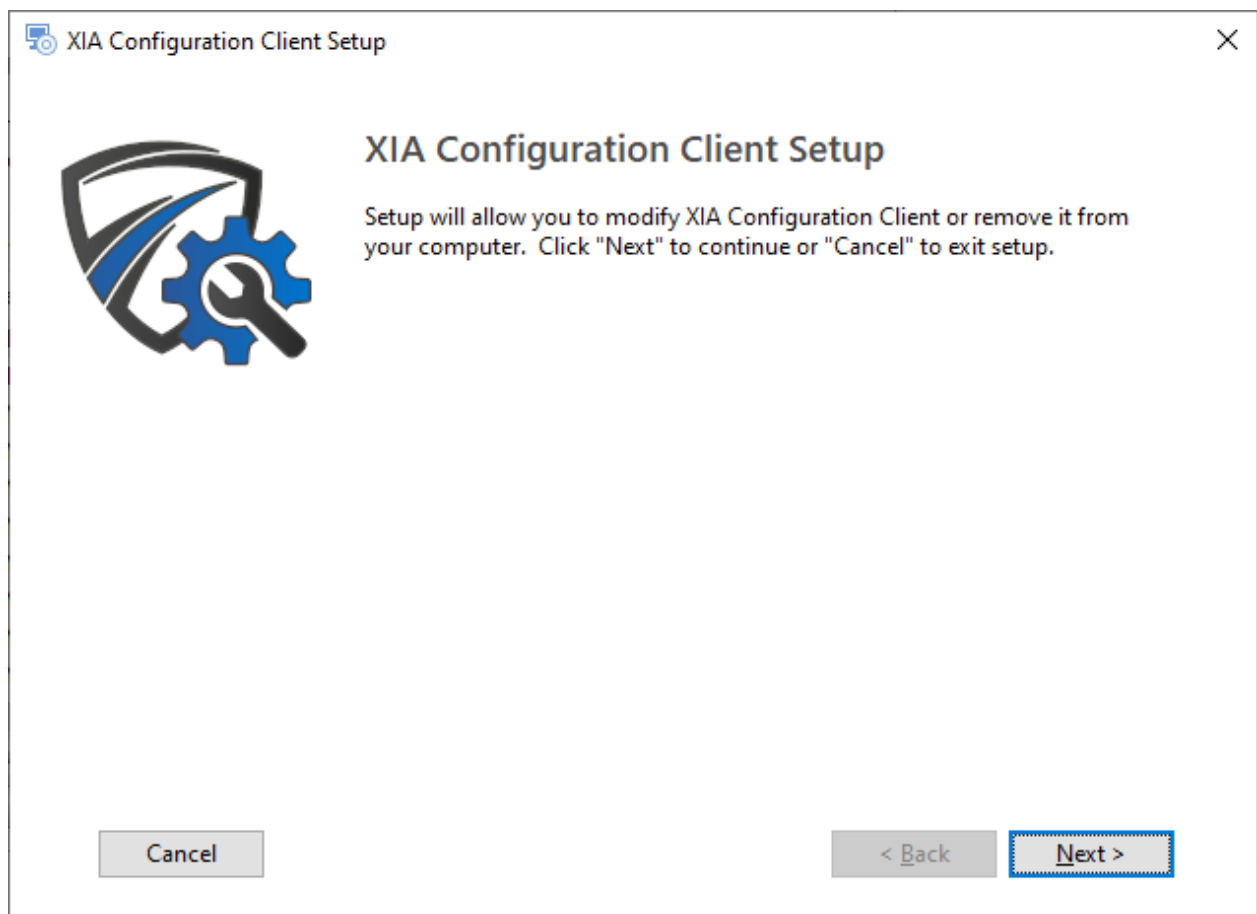
- Go to Control Panel, *Programs*, *Uninstall a program*.



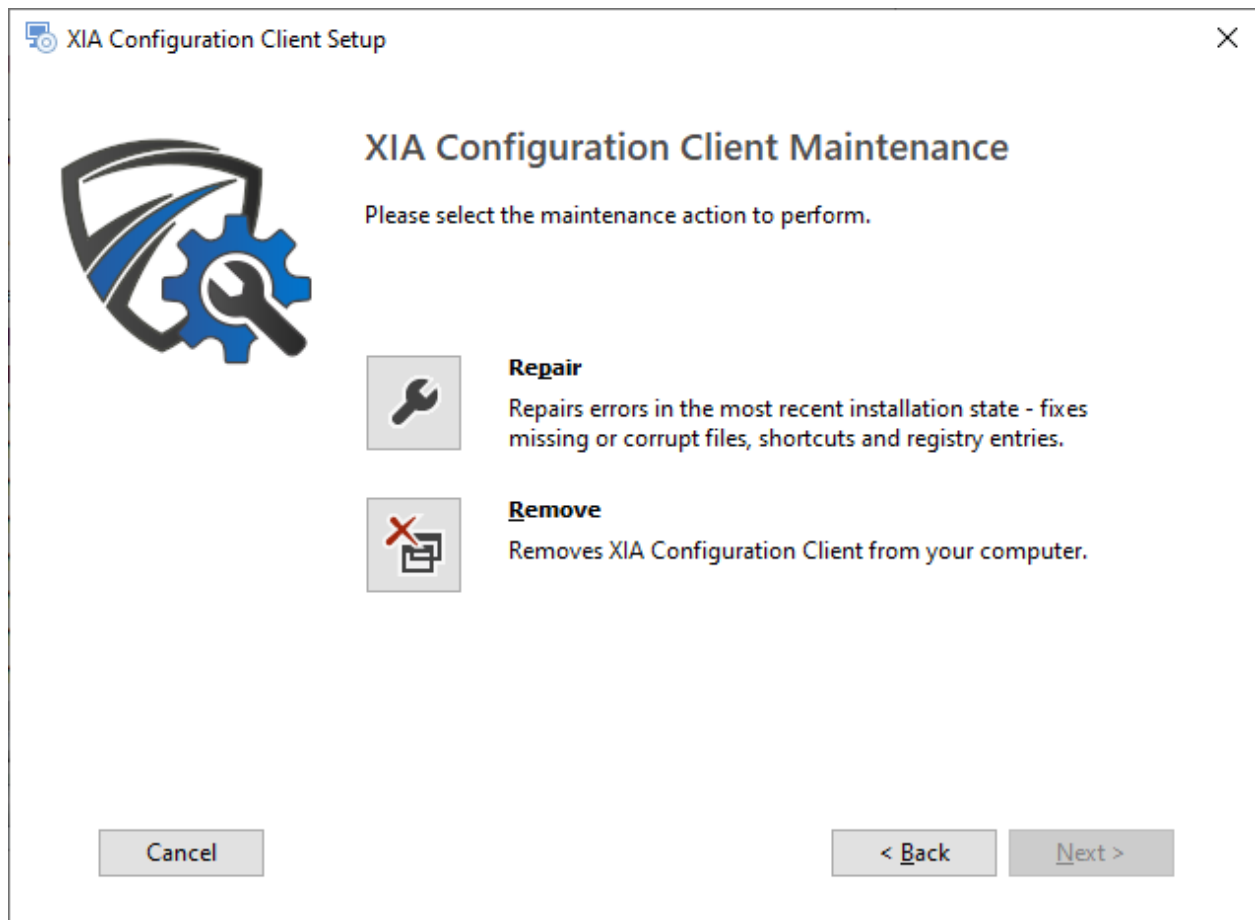
- Right click *XIA Configuration Client* and select *Uninstall/Change*.



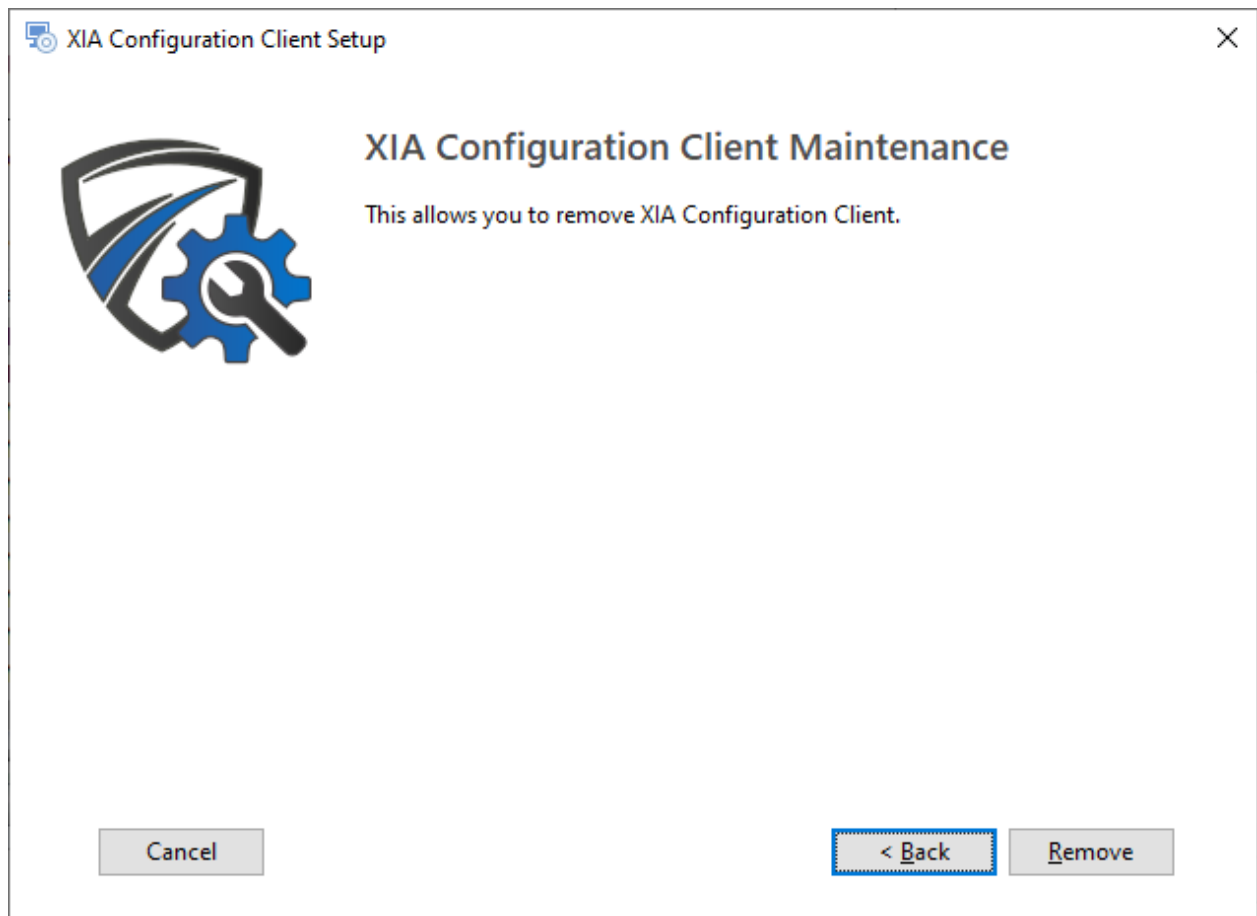
- At the welcome screen click *Next*.



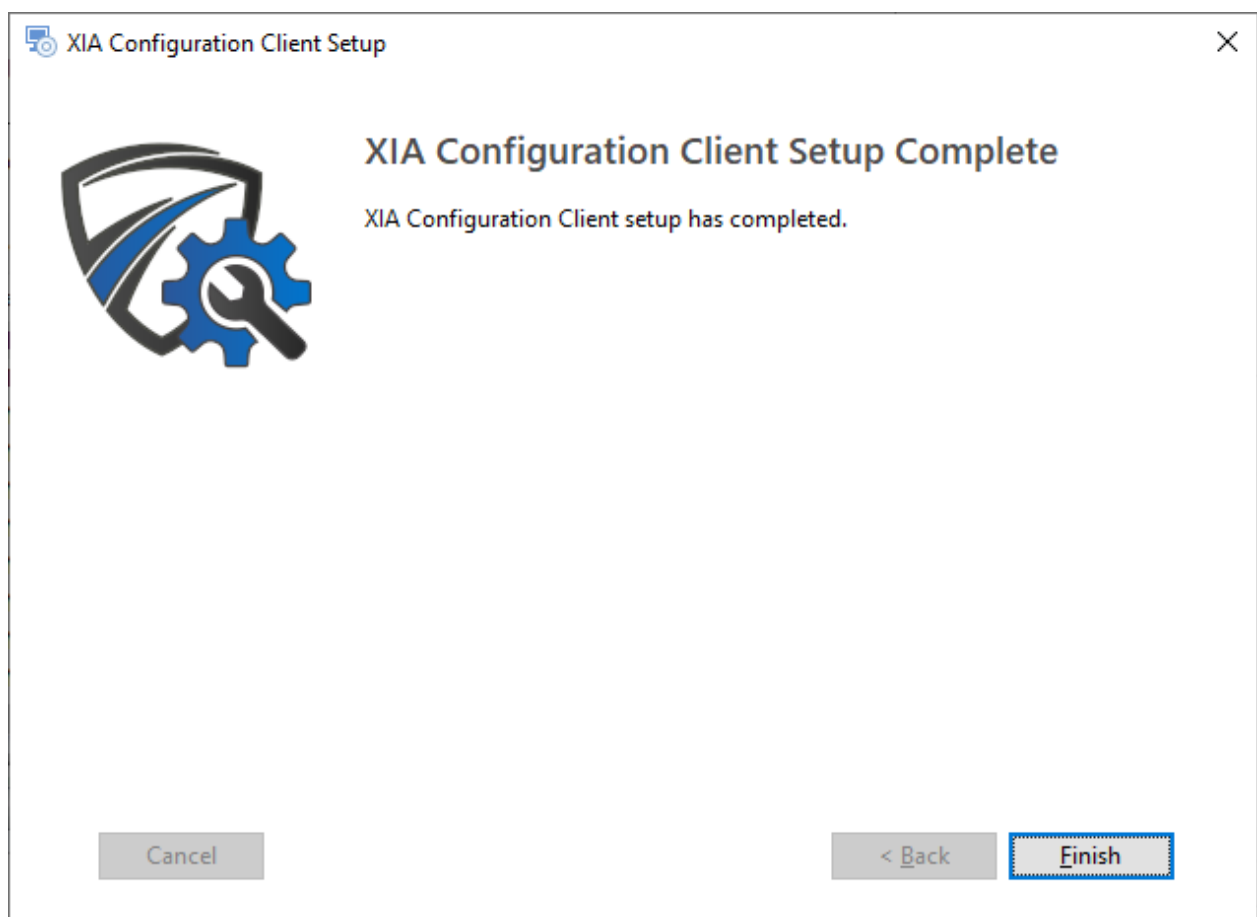
- Click the *Remove* button.



- Click the *Remove* button again to commence the uninstall.



- When complete click the *Finish* button.



Certain shared [roles and features](#) are automatically installed by the product, you may need to review these and remove them manually if they are no longer required.

Unattended Uninstallation

The [XIA Configuration Client](#) product can be [uninstalled](#) without user intervention using the following command line.

```
msiexec /qn /uninstall {C3CB2E94-52A0-402F-BABB-5B22AECB43B8}
```

Certain shared [roles and features](#) are automatically installed by the product, you may need to review these and remove them manually if they are no longer required.

Service Account

The service account is used to communicate with network items such as [Windows servers and computers](#), but also systems running on the [Windows server](#) platform such as [Active Directory](#) and [VMware vCenter](#).

WARNING:

Should you wish to document [Windows machines](#) (without using the [XIA Local Service](#)) the [XIA Configuration Client](#) service account requires administrator privilege on the remote machines that it scans. This is because it requires remote WMI permissions and access to the administrative shares of the remote machines.

In addition, please note that passwords stored in the Windows services database can be decrypted by administrators of the machine, therefore any server that has the [XIA Configuration Client](#) installed should be secure with only appropriate users having local administrator access.

The service account:

- Should be dedicated for this purpose.
- Should have the required privilege to only the machines that you wish to scan.
- Have a suitably secure password.
- Will be configured as the account under which the service being installed is configured to run as.
- Will be granted the [Logon as a service](#) right by the installation.
- Can be a local account or Active Directory domain account.
- Can be a [managed service account](#) (MSA).

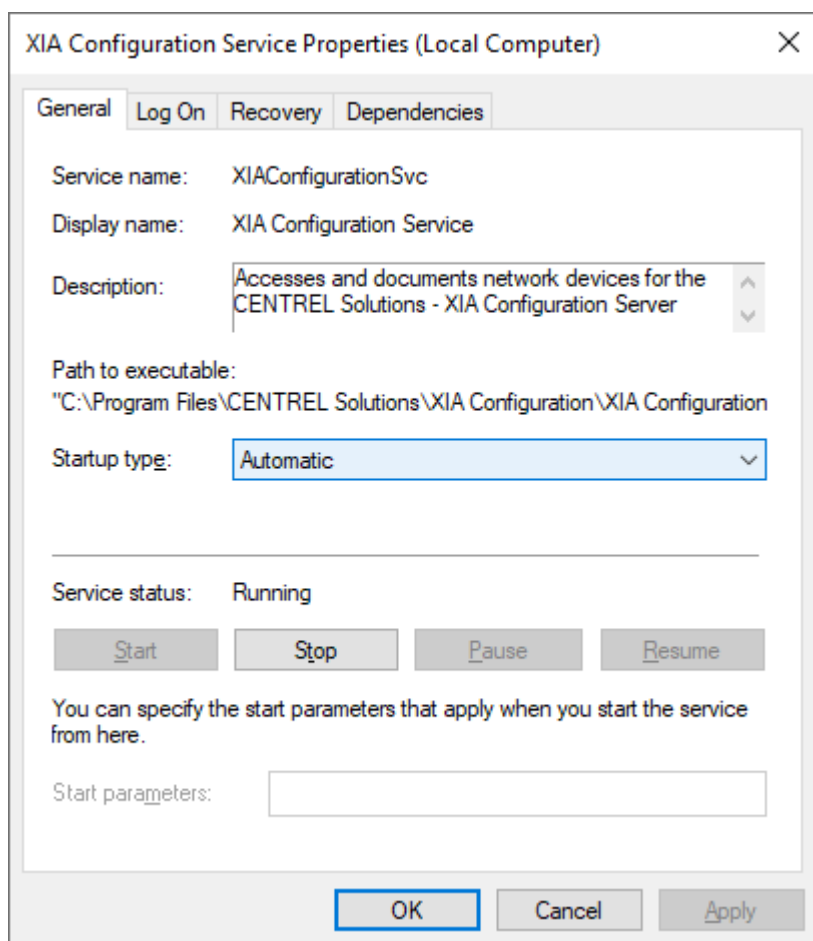
Changing the Service Account

The [XIA Configuration Client](#) uses a Windows service to perform scanning of items and is configured with a [service account](#) that is set during installation.

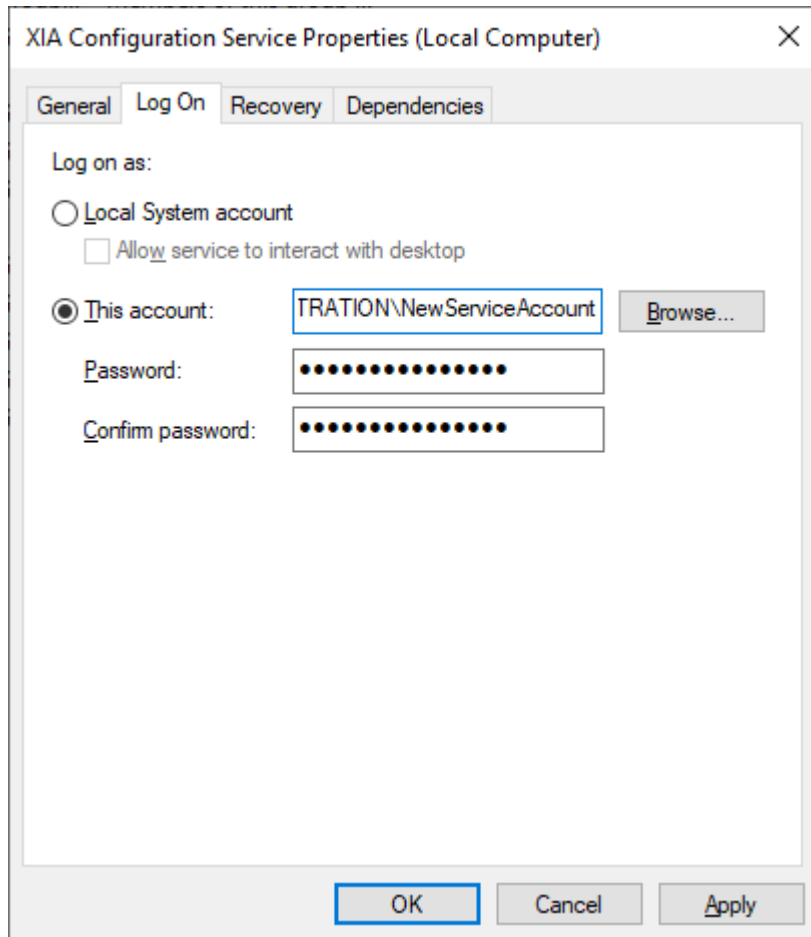
WARNING: It is recommended that you uninstall and reinstall the [XIA Configuration Client](#) instead of manually changing the service account.

To manually change the service account after installation, complete the following steps.

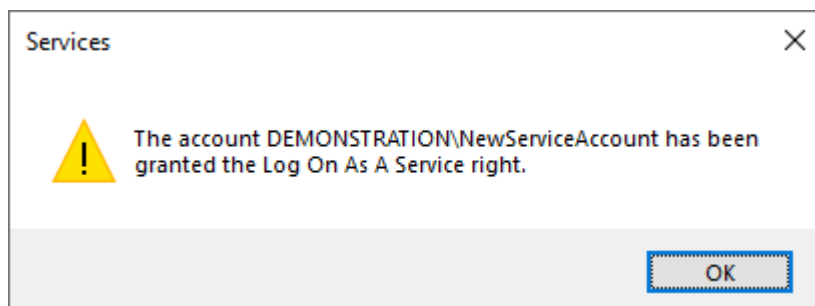
- Ensure that you have a full backup before proceeding.
- Ensure that the new account meets the requirements in the [service account](#) section.
- Open the services management console (Start > Run > Services.msc) and open the **XIA Configuration Service**.



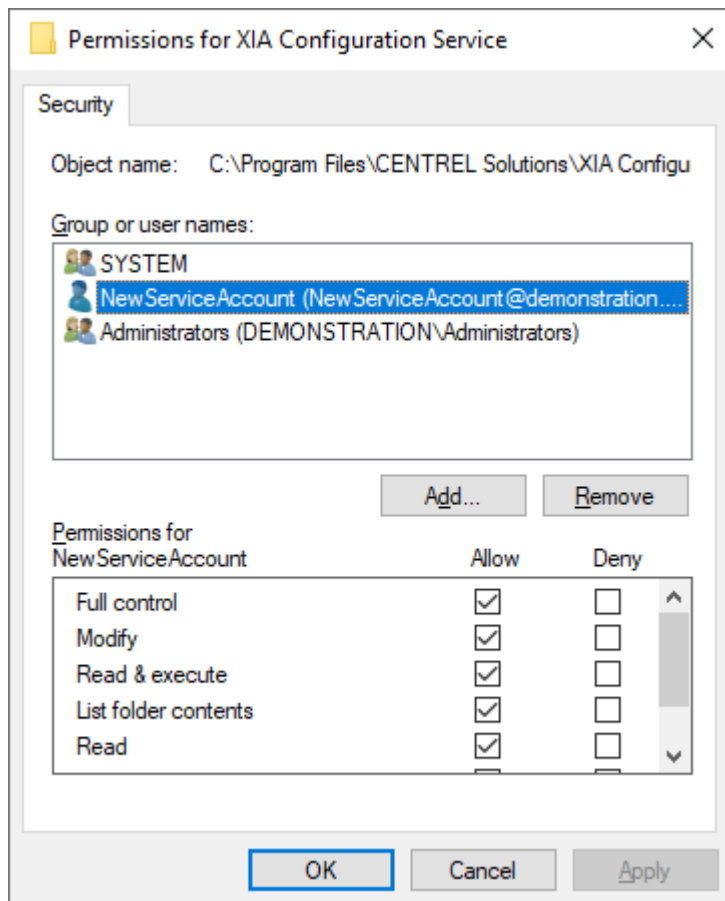
- On the logon tab enter the new account name and password - this **must** be in NetBIOS format "DOMAIN\username", then click OK.



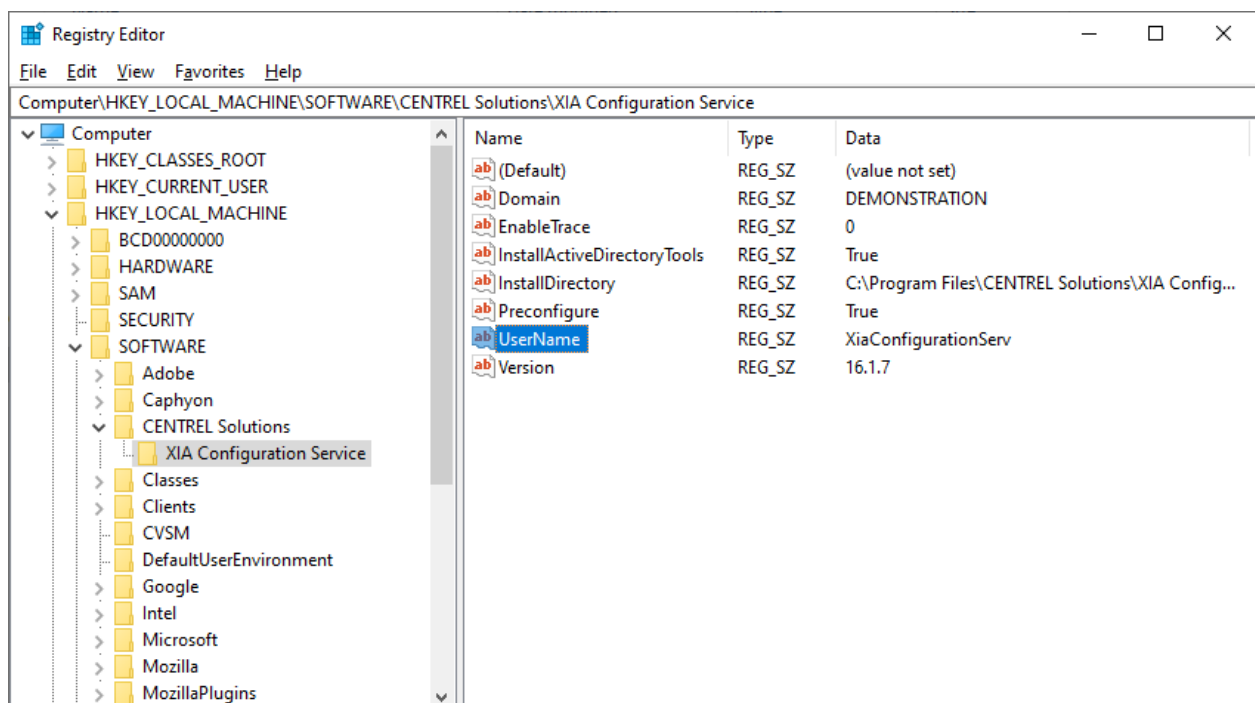
- The service account may be granted additional rights



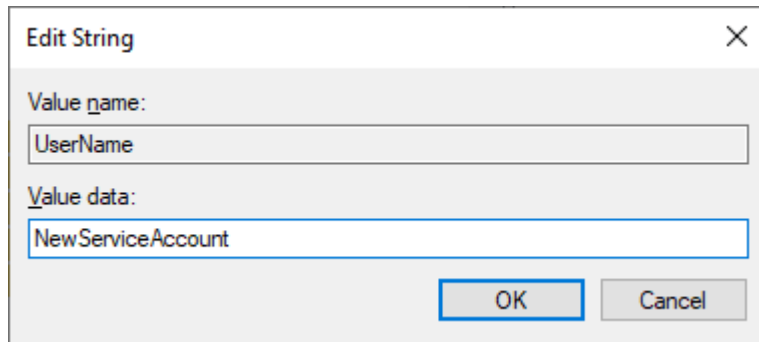
- Open the installation folder - by default "C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service".
- Modify the NTFS permissions of the folder and ensure that the new service account, Administrators, and SYSTEM have full control.



- Open the registry editor to the following location
HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Service

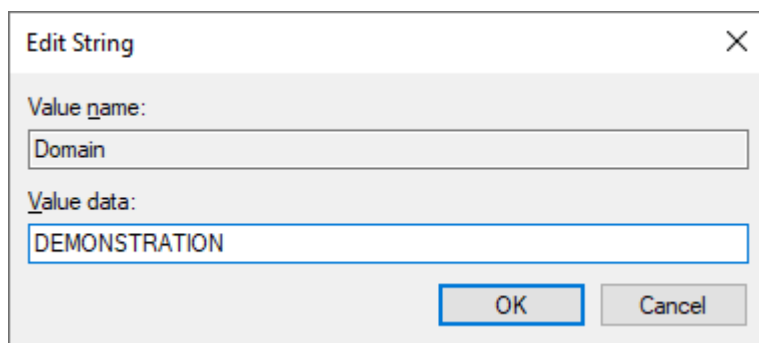


- Modify the **Username** value and enter the new service account name.



Dialog box titled "Edit String" with a close button (X) in the top right corner. It contains two text input fields: "Value name:" with the text "UserName" and "Value data:" with the text "NewServiceAccount". At the bottom right are "OK" and "Cancel" buttons. The "OK" button is highlighted with a blue border.

- Modify the **Domain** value and enter the domain name of the new service account - this **must** be in NetBIOS format.



Dialog box titled "Edit String" with a close button (X) in the top right corner. It contains two text input fields: "Value name:" with the text "Domain" and "Value data:" with the text "DEMONSTRATION". At the bottom right are "OK" and "Cancel" buttons. The "OK" button is highlighted with a blue border.

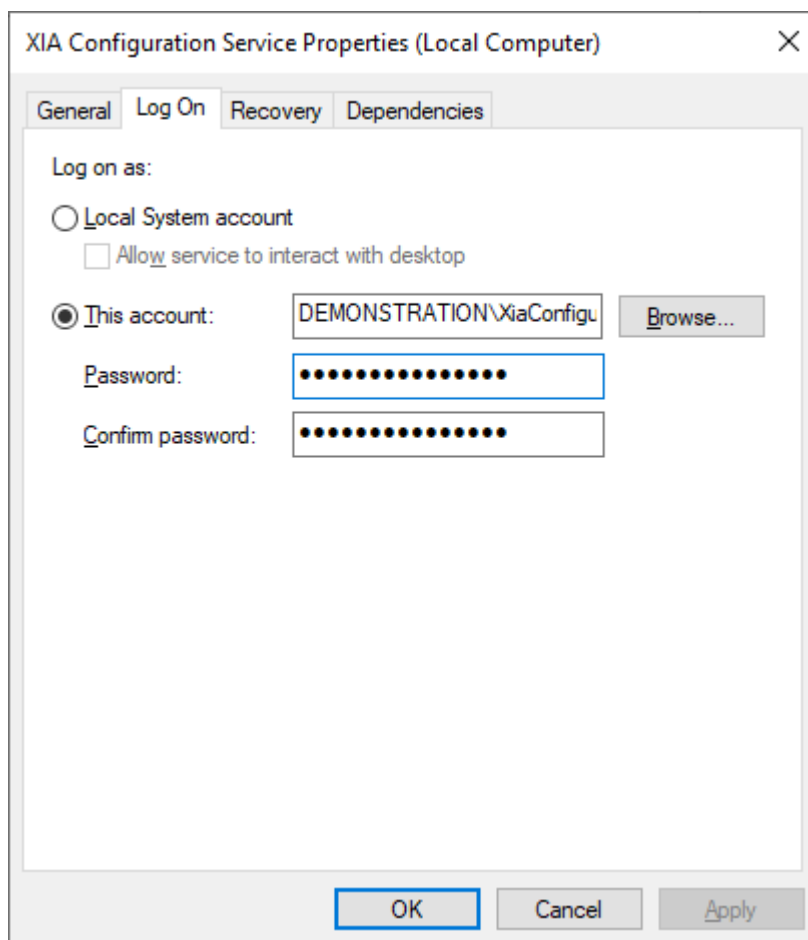
- Restart the XIA Configuration service.

Changing the Service Account Password

The [XIA Configuration Client](#) uses a Windows service to perform scanning of items and is configured with a [service account](#) that is set during installation.

To change the service account password after [installation](#), complete the following steps.

- Change the password for the account in *Active Directory Users and Computers* or in *Local Users and Groups* as normal.
- Open the services management console (Start > Run > Services.msc) and open the *XIA Configuration Service*.
- Select the *Log On* tab.



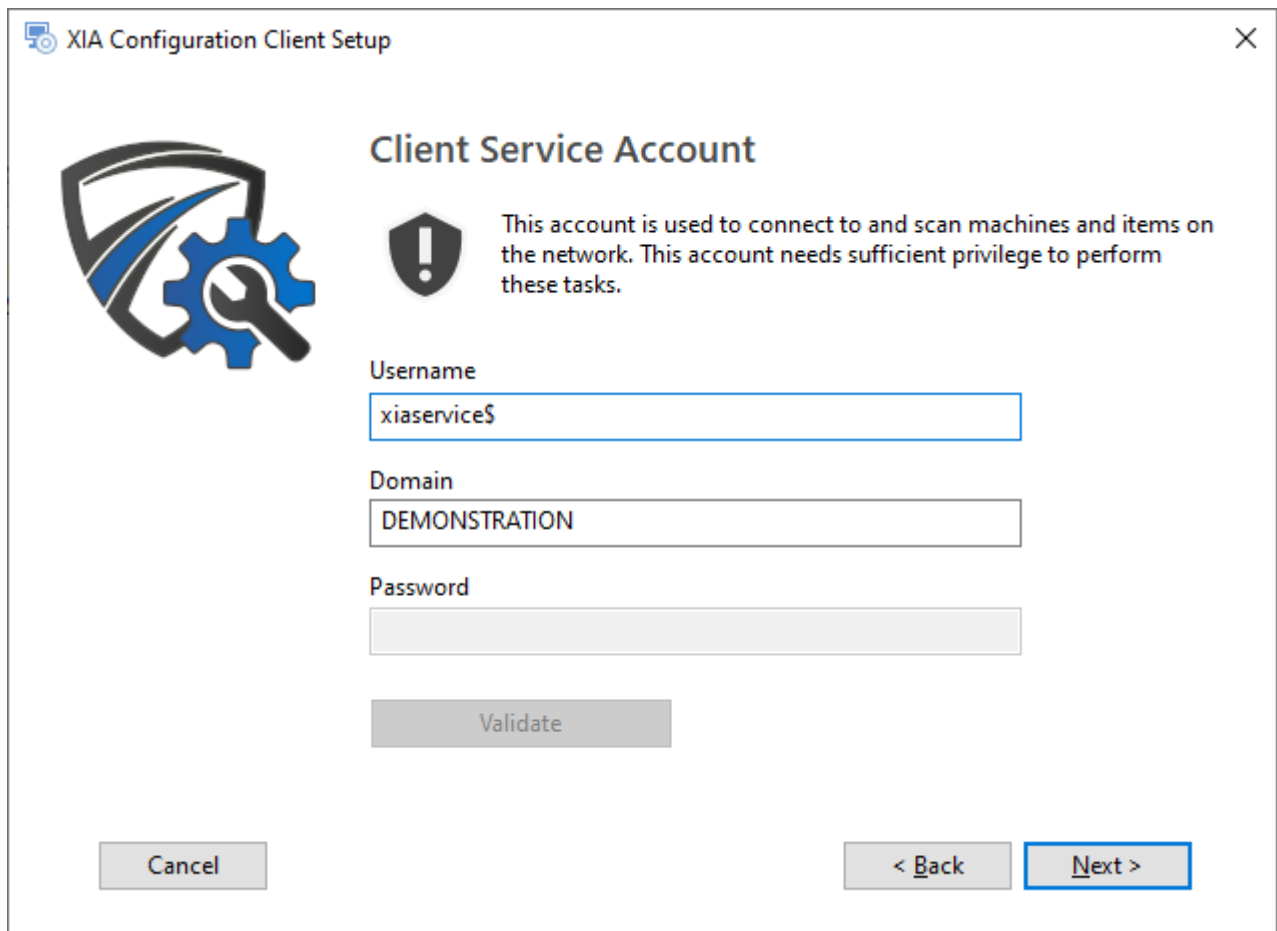
- Enter the new password in the *Password* and *Confirm password* fields then click OK.
- Restart the service.

Managed Service Accounts

The [XIA Configuration Client](#) can use a standalone managed service account (sMSA) or [group managed service account \(gMSA\)](#) for the [Windows service account](#).

When performing an [installation](#) simply enter the managed service account name in the format *username\$*.

The [installation](#) will automatically disable the password field and validate button.



The screenshot shows the 'XIA Configuration Client Setup' window. The title bar includes the application icon and the text 'XIA Configuration Client Setup'. The main content area is titled 'Client Service Account'. On the left, there is a large icon of a shield with a gear and a wrench. To the right of this icon, there is a warning icon (a shield with an exclamation mark) and a text box that reads: 'This account is used to connect to and scan machines and items on the network. This account needs sufficient privilege to perform these tasks.' Below this, there are three input fields: 'Username' with the text 'xiaservice\$', 'Domain' with the text 'DEMONSTRATION', and 'Password' which is currently empty. Below the 'Password' field is a 'Validate' button. At the bottom of the window, there are three buttons: 'Cancel', '< Back', and 'Next >'. The 'Next >' button is highlighted with a blue border.

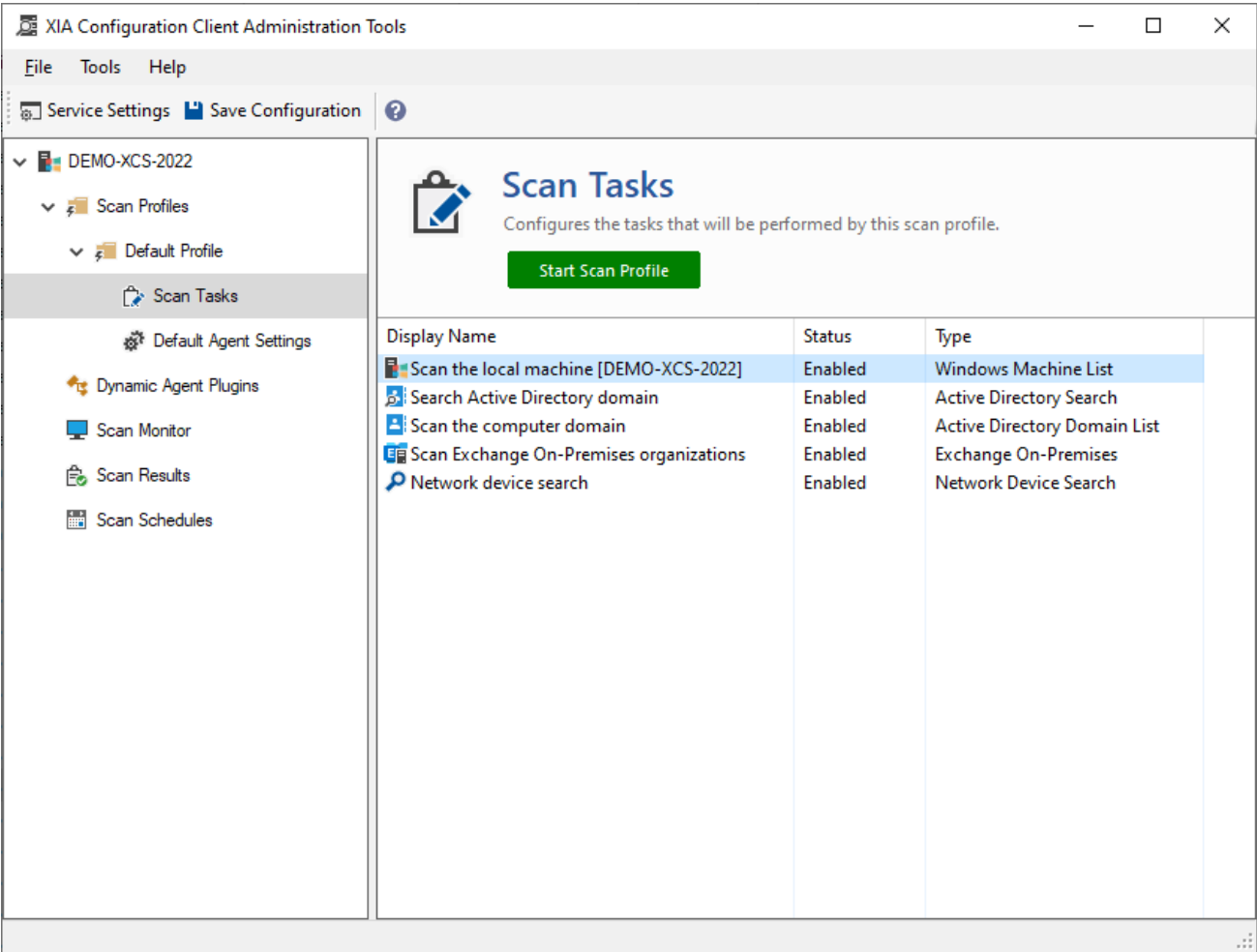
The managed service account must still be given the permissions appropriate for the [service account](#).

NOTE: Microsoft Exchange Server does not support managed service accounts and therefore cannot be used for the [Exchange On-Premises Scan Task](#).

Administration Tools

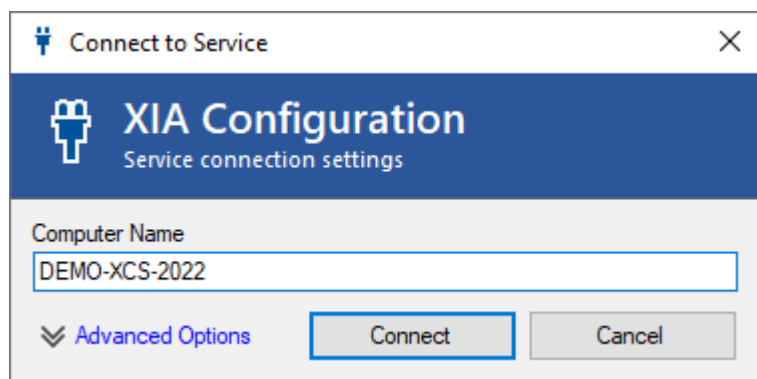
The XIA Configuration Service can be managed by the XIA Configuration Client administration tools.

The administrative tools are installed as part of the installation of [XIA Configuration Server](#) and the [XIA Configuration Client](#).



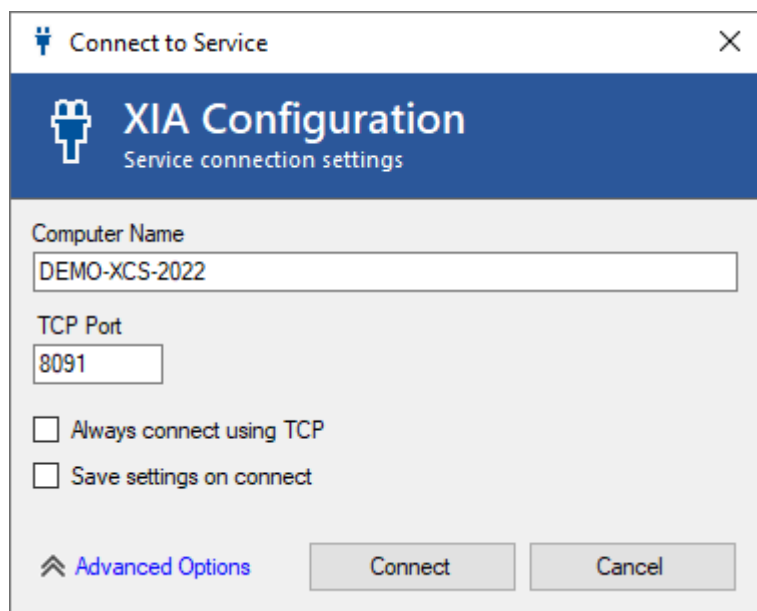
Connecting to a Service

Once started the [administration tools](#) will prompt you to connect to the [XIA Configuration Client](#) service by default on the local machine.



The dialog box titled "Connect to Service" for "XIA Configuration" shows the "Service connection settings". The "Computer Name" field contains "DEMO-XCS-2022". At the bottom, there is a link for "Advanced Options" (indicated by a downward arrow icon), and "Connect" and "Cancel" buttons.

For more options click the *Advanced Options* link



The dialog box shows the "Advanced Options" section expanded. In addition to the "Computer Name" field, there is a "TCP Port" field containing "8091". Below these fields are two checkboxes: "Always connect using TCP" and "Save settings on connect", both of which are currently unchecked. The "Advanced Options" link now shows an upward arrow icon. The "Connect" and "Cancel" buttons remain at the bottom.

Computer Name

The name of the machine to connect to.

NOTE: If a remote machine is specified the service on that machine must be configured to [allow remote connections](#).

TCP Port

The TCP port to use for remote connections or local connections when *always connect using TCP* is checked.

Always connect using TCP

Determines whether TCP connections should be used for local connections instead of IPC.

Save settings on connect

Determines whether the connection settings should be saved when a connection is made.

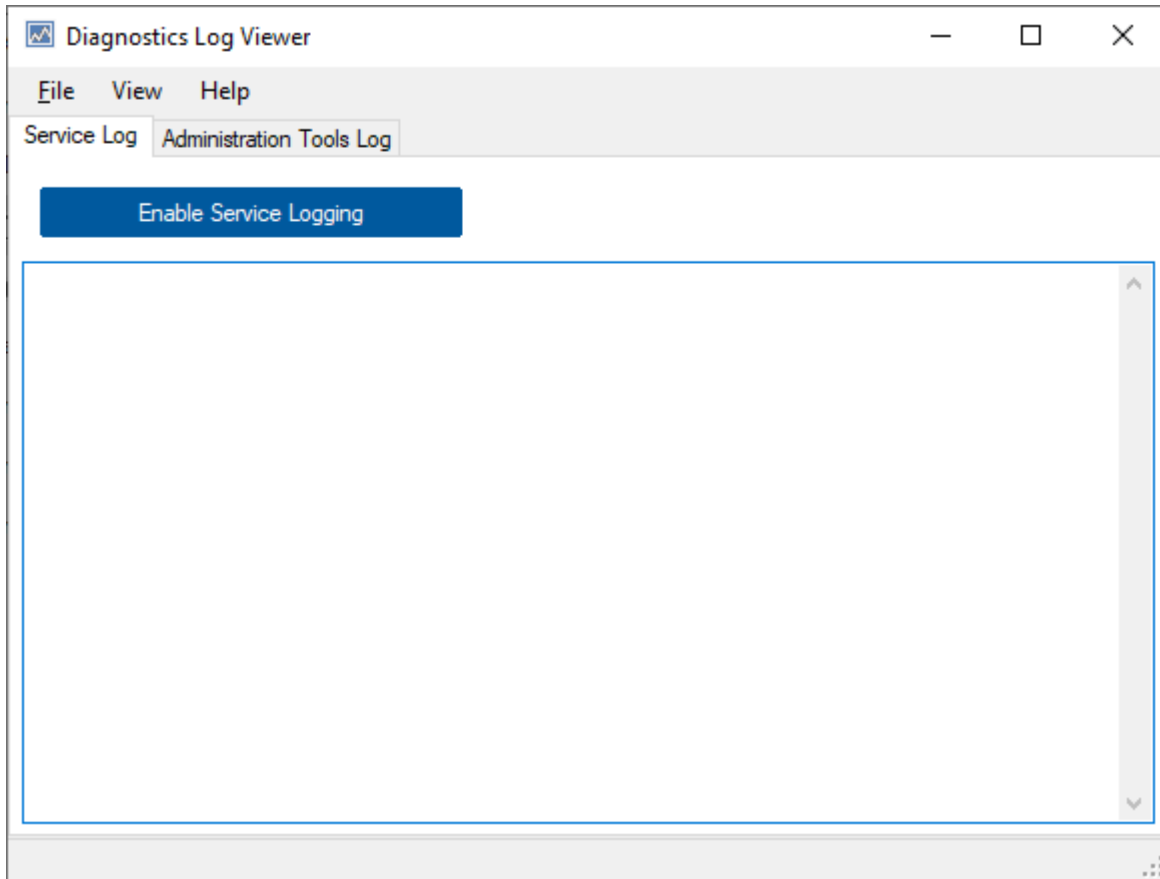
NOTE: The settings will be saved to %LOCALAPPDATA%\CENTREL Solutions\XIA

Configuration\ConnectionSettings.xml.

Diagnostics Log Viewer

The diagnostics log viewer allows the viewing of the [diagnostics trace](#) log through a simple user interface within the [administration tools](#).

The service tab displays the log generated by the [XIA Configuration Client](#) service.

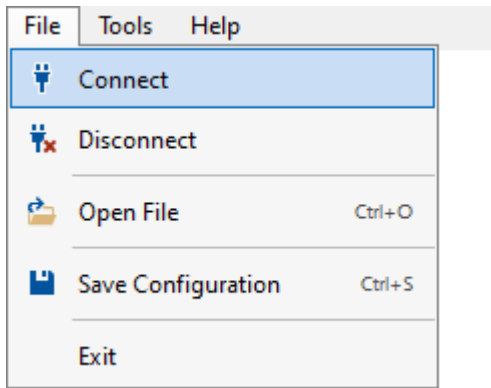


The administration tools log tab displays the diagnostics log generated by the [administration tools](#) user interface.

Menu

The drop down menu displayed in the [administration tools](#).

File Menu



Connect

Displays the [service connection form](#).

Disconnect

Disconnects from the [XIA Configuration Client](#) service.

Open File

Allows the [viewing of a data file](#).

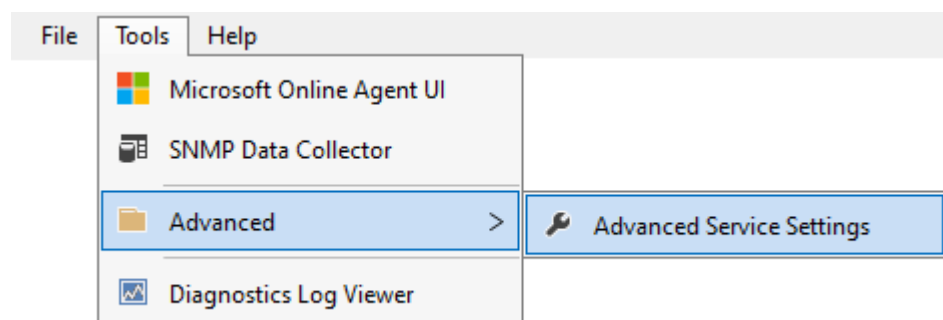
Save Configuration

Saves the configuration to the [XIA Configuration Client](#) service.

Exit

Closes the [Administration Tools](#).

Tools Menu



Azure Tenant Agent UI

Displays the [Azure Tenant Agent UI](#) tool.

IIS Support Installer

Displays the [IIS support installer](#) tool.

Microsoft 365 Agent UI

Displays the [Microsoft 365 Agent UI](#) tool.

SNMP Data Collector

Displays the [SNMP data collector](#) tool.

Advanced Service Settings

Displays the [advanced service settings](#) dialog.

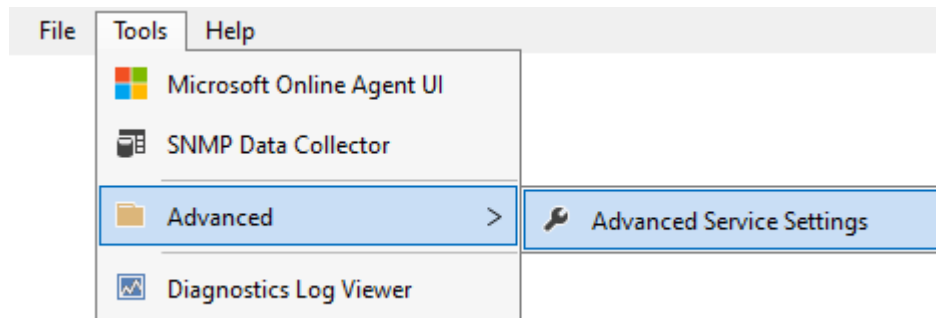
Diagnostics Log Viewer

Displays the [diagnostics log viewer](#).

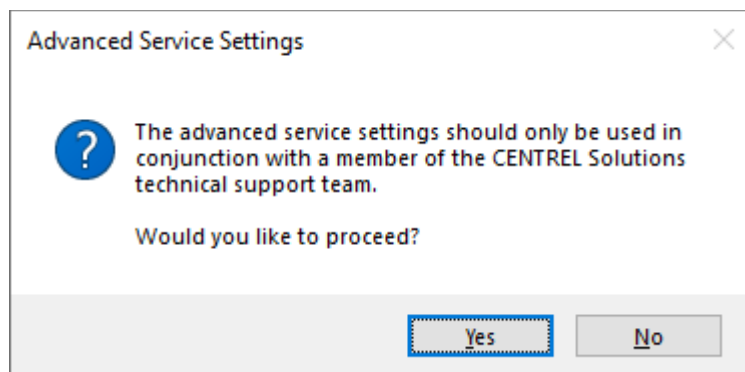
Advanced Service Settings Editor

Typically changes to the settings of the [XIA Configuration Client](#) should be made through the [service settings](#), however additional settings can be accessed through the advanced service settings editor.

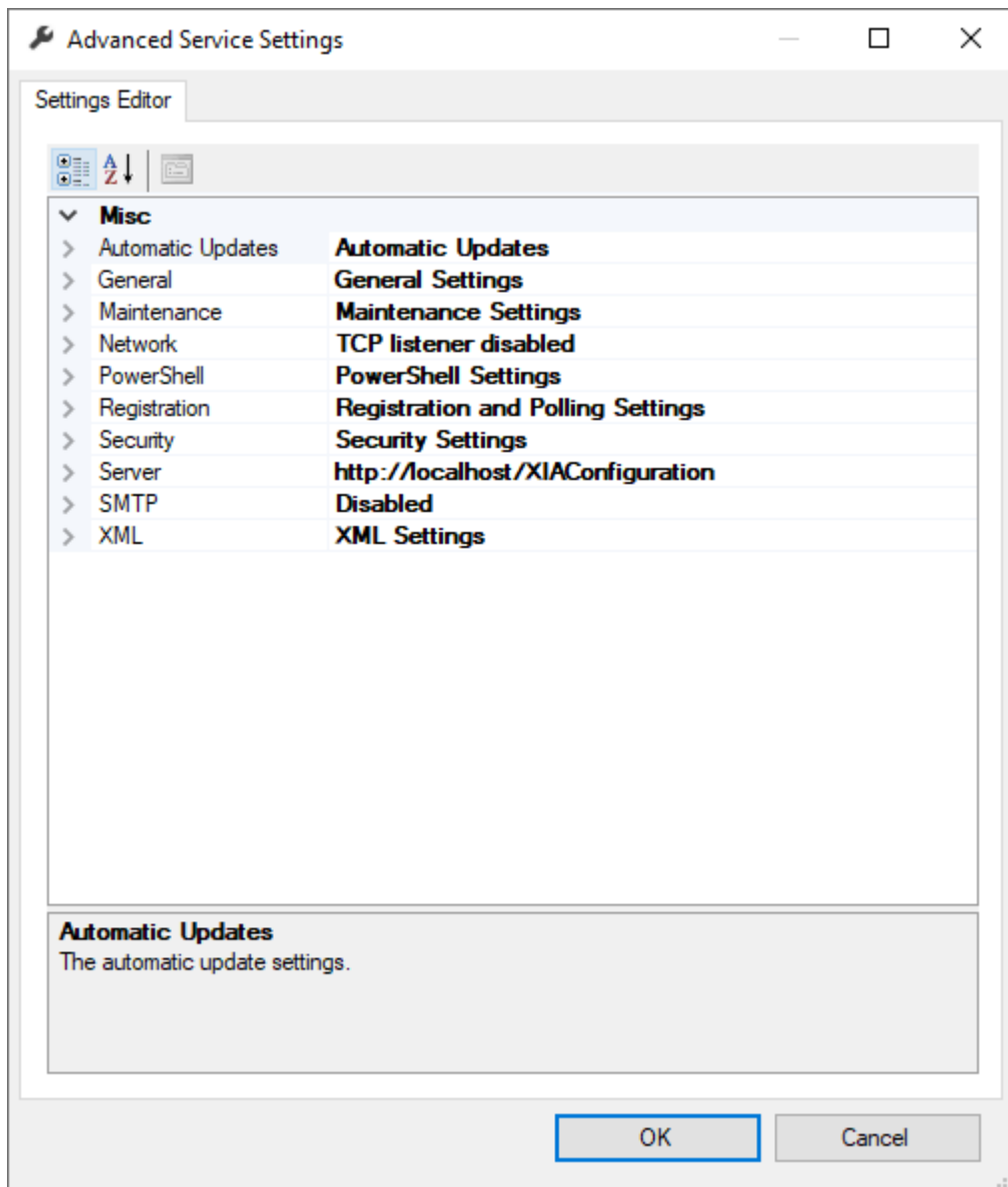
This can be accessed through the tools, advanced menu.



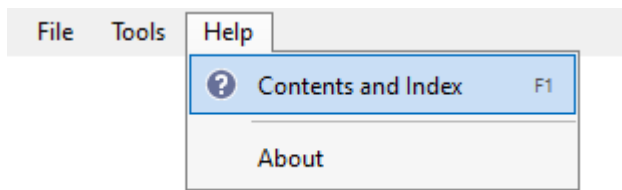
The settings should only be modified in conjunction with a member of the [CENTREL Solutions](#) technical support team.



The settings must be saved following any changes made to the service advanced settings editor.



Help Menu



Contents and Index

Displays the help.

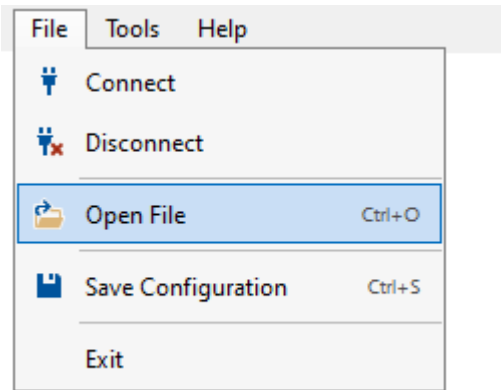
About

Displays the about dialog.

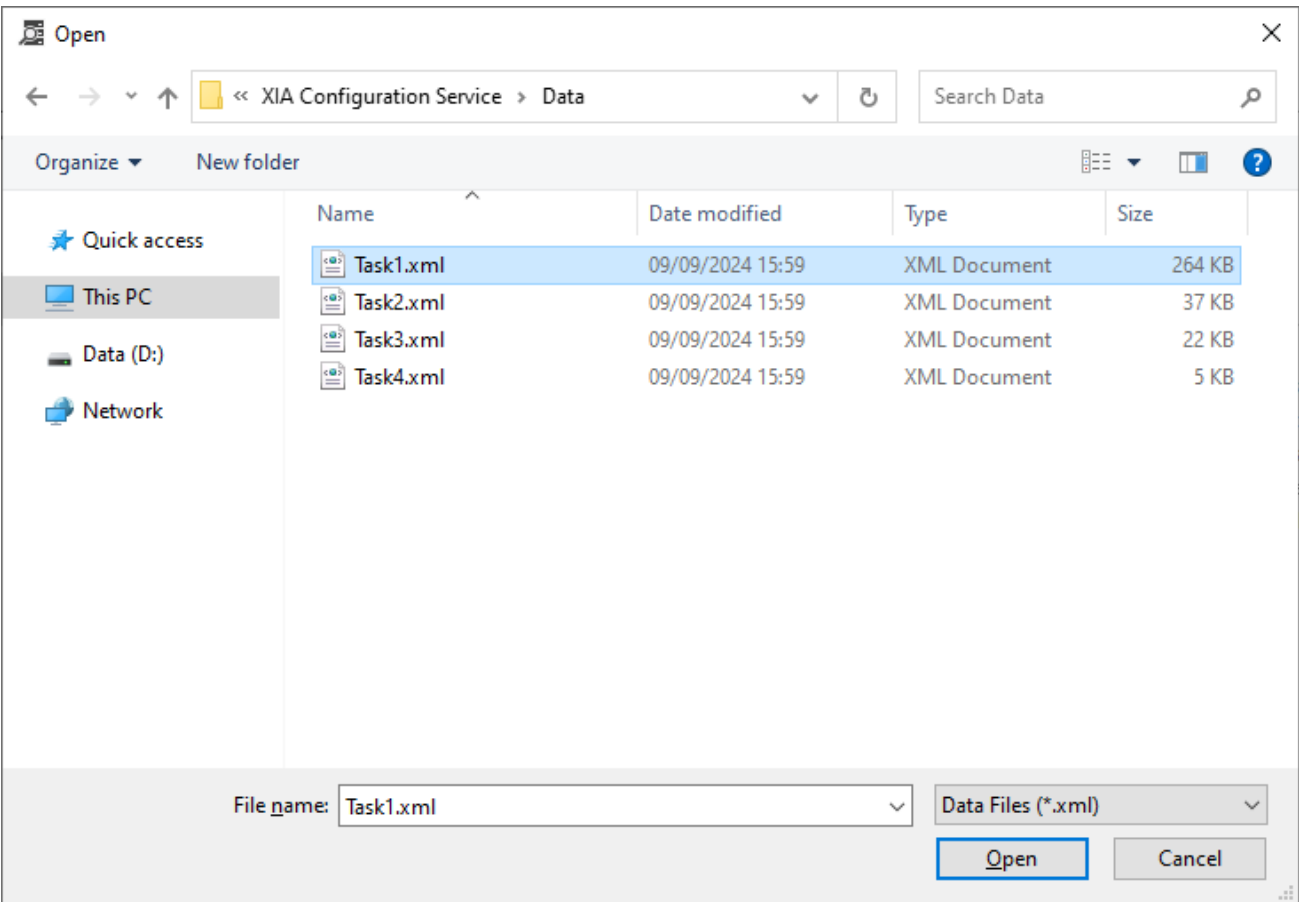
Opening Data Files

To assist with troubleshooting, the [XIA Configuration Client](#) allows you to view data without having to upload the data to the [XIA Configuration Server](#).

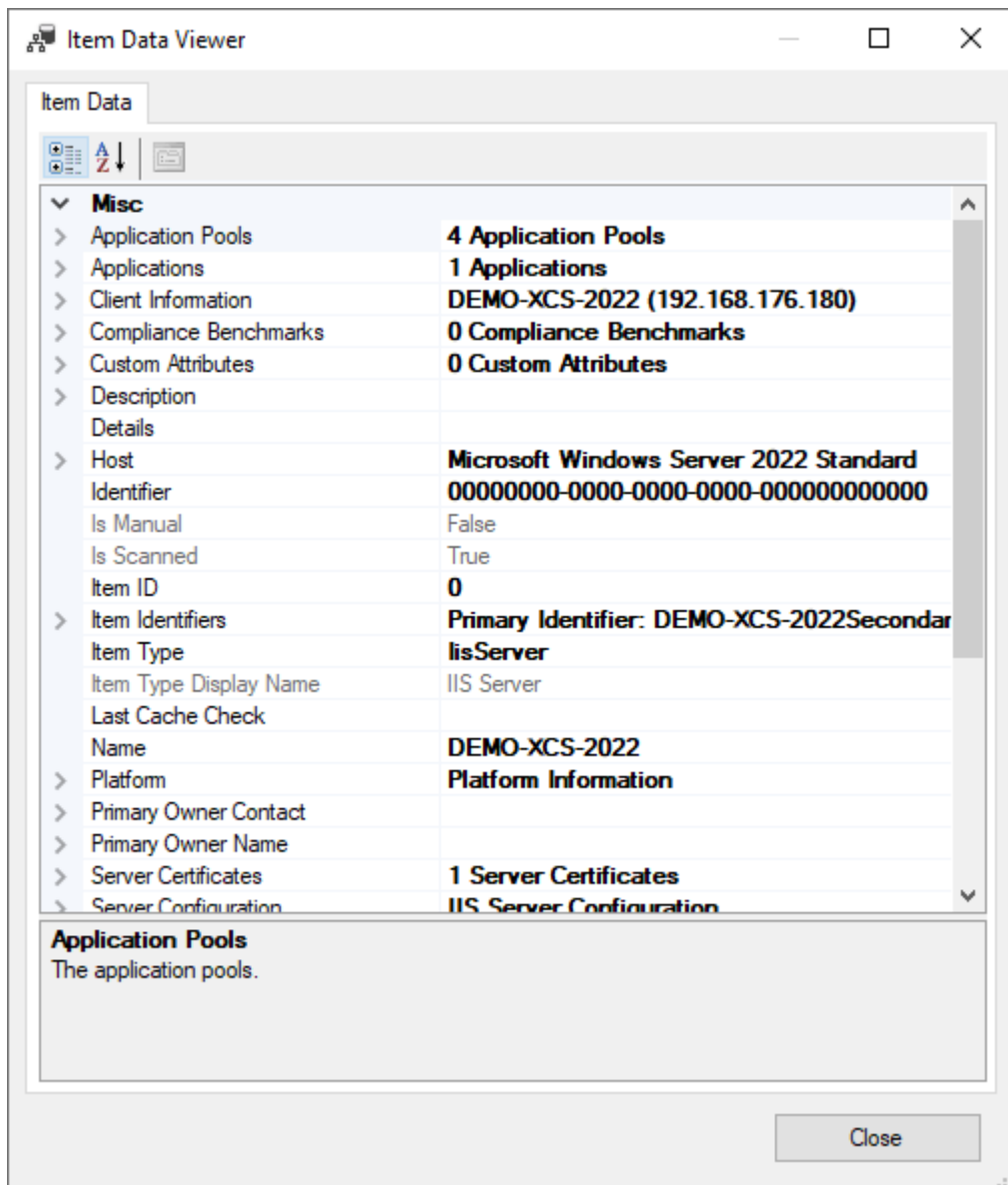
Click File, Open File in the [menu](#).



Browse to the data file you wish to view. By default, these can be found in the following directory
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Data

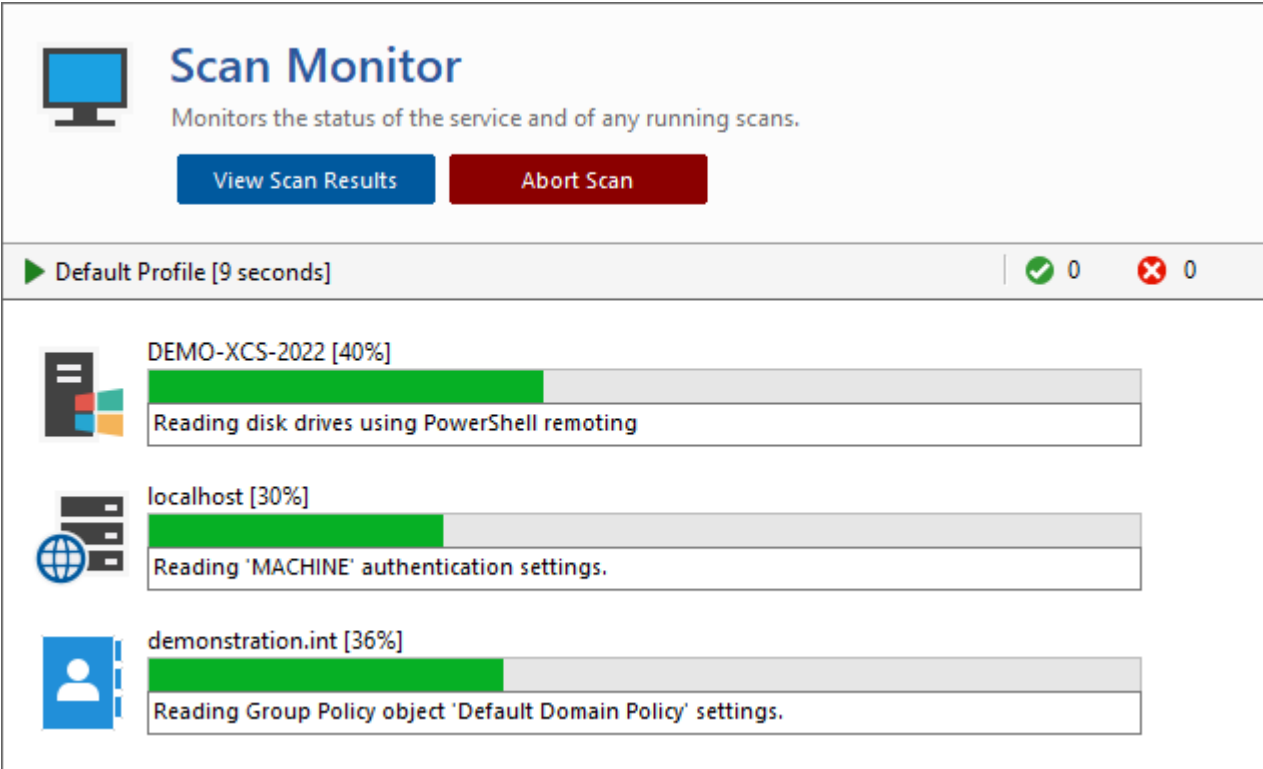


The data can then be viewed in the property grid of the data browser form.



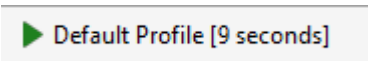
Scan Monitor

To view the scan monitor, select the scan monitor node within the [administration tools](#). Within this section, you can view information about any scan that is currently in progress.



The information displayed includes

- Active scan name and the amount of time that task has been running.



- The number of tasks that have completed successfully (including tasks that completed with warnings), and the number of tasks that have failed



- The current scan tasks that are in progress. The number of concurrent scan tasks can be set within each [scan profile's general](#) tab
- If a scan is currently in progress an option to abort the scan will be shown.
- Using the **view scan results** link it is possible to see the [scan results](#) live when a scan is running, or the results of the mostly recently run scan if there is no scan currently active.

Service Information

The service information interface provides [XIA Configuration Client](#) service related commands.

Service Settings

Displays the [service settings](#).

Diagnostics Log Viewer

Displays the [diagnostics log viewer](#).

Register Now

Registers with the [XIA Configuration Server](#) configured in the [service settings](#).

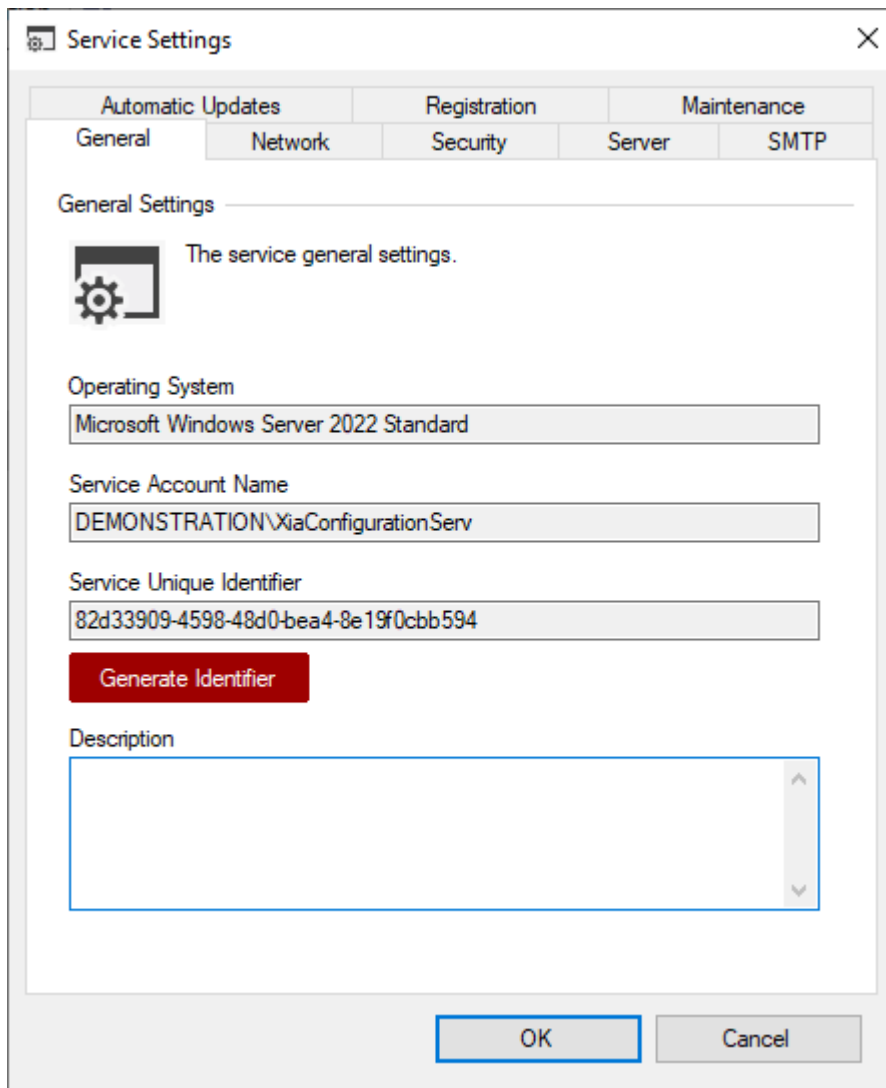
Check For Updates

Checks for software [updates](#) from the [XIA Configuration Server](#) configured in the [service settings](#).

Service Settings

To view and modify the service configuration of the [XIA Configuration Client](#) including security information click the service settings toolbar button.

General



The screenshot shows the 'Service Settings' dialog box with the 'General' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'Automatic Updates', 'Registration', 'Maintenance', 'General', 'Network', 'Security', 'Server', and 'SMTP'. The 'General' tab is active, showing 'General Settings' with a gear icon and the text 'The service general settings.' Below this are four text input fields: 'Operating System' (containing 'Microsoft Windows Server 2022 Standard'), 'Service Account Name' (containing 'DEMONSTRATION\XiaConfigurationServ'), 'Service Unique Identifier' (containing '82d33909-4598-48d0-bea4-8e19f0cbb594'), and 'Description' (empty). A red 'Generate Identifier' button is located below the 'Service Unique Identifier' field. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Operating System

The operating system of the machine running the [XIA Configuration Client](#) service.

Service Account Name

The [service account](#) name of the account running the [XIA Configuration Client](#) service.

Service Unique Identifier

The unique identifier used by the [XIA Configuration Client](#) when it [registers](#) and communicates with the [XIA Configuration Server](#) in [GUID](#) format.

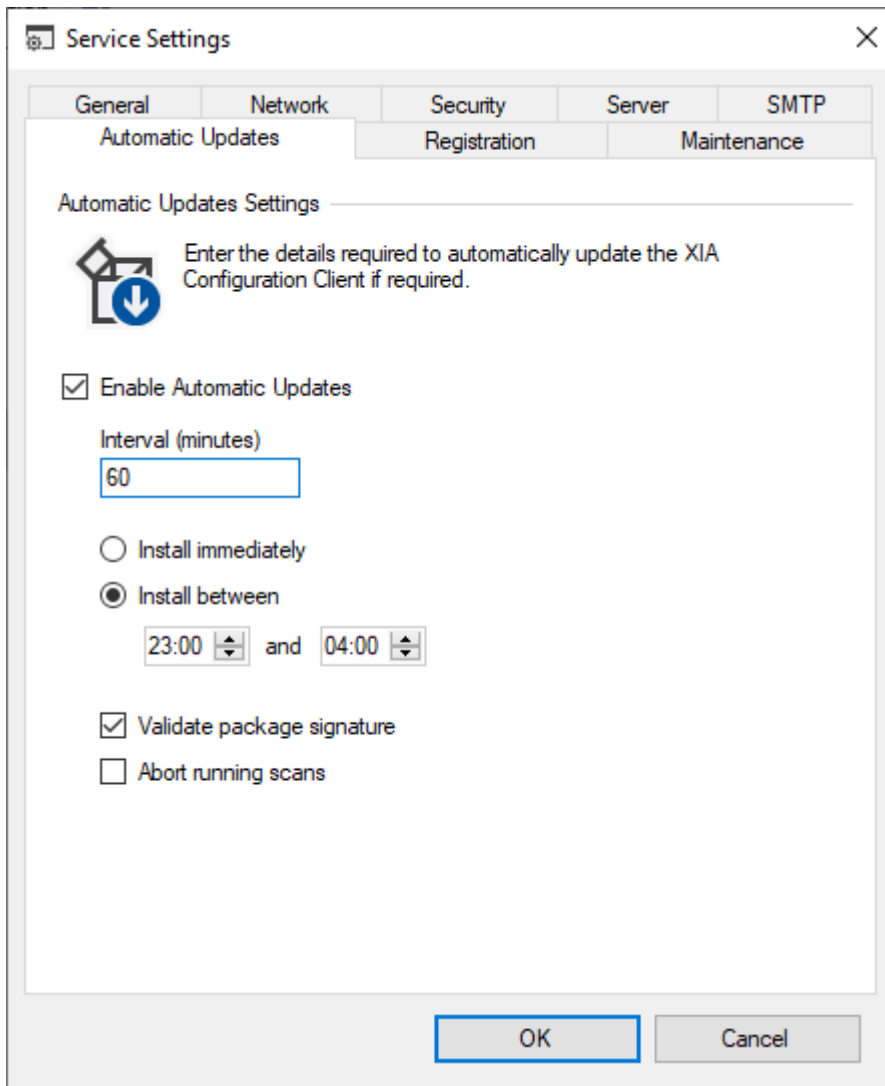
Clicking *Generate Identifier* will generate a new unique identifier for this machine.

Description

Allows the configuration of a description of the service. This information is available in the [client installations](#) section when the [client](#) has [registered](#) with the [server](#).

Automatic Updates

The updates tab allows the system to be configured to receive automatic updates from the XIA Configuration Server specified on the [server](#) tab, the user configured on must also be permitted to *Download Client Installer* on the [security settings](#) section.



The screenshot shows the 'Service Settings' dialog box with the 'Automatic Updates' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'General', 'Network', 'Security', 'Server', and 'SMTP'. Under the 'Automatic Updates' tab, there are sub-tabs for 'Automatic Updates', 'Registration', and 'Maintenance'. The 'Automatic Updates' sub-tab is active, showing a section titled 'Automatic Updates Settings' with a folder and download icon. The text reads: 'Enter the details required to automatically update the XIA Configuration Client if required.' Below this, there is a checkbox for 'Enable Automatic Updates' which is checked. Underneath is a text box for 'Interval (minutes)' containing the value '60'. There are two radio buttons: 'Install immediately' (unselected) and 'Install between' (selected). Below the 'Install between' radio button are two time pickers showing '23:00' and '04:00' separated by 'and'. At the bottom of the settings section are two checkboxes: 'Validate package signature' (checked) and 'Abort running scans' (unchecked). At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Enable Automatic Updates

Determines whether automatic updates should be enabled on this machine.

Interval (minutes)

The interval in minutes at which the service should check for updates.

Install Immediately

Determines whether available updates should be downloaded and installed immediately.

Install Between

Determines whether available updates should only be downloaded and installed between the specified times.

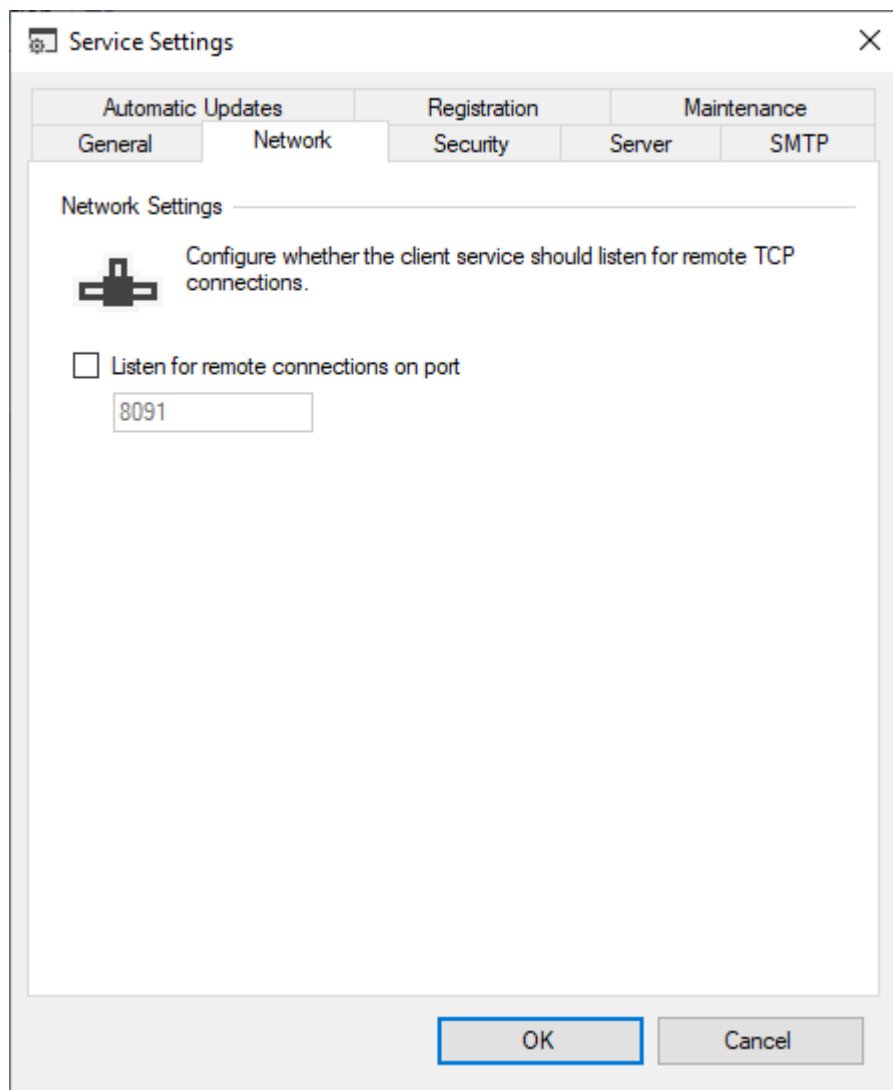
Validate Package Signature

Determines whether the system should validate the installer package's digital signature before performing the installation.

Abort Running Scans

Determines whether the system should abort running scans and perform the update. When disabled if a scan is in progress the automatic update will be aborted to allow the scan to complete and will be installed at the next interval.

Network Settings



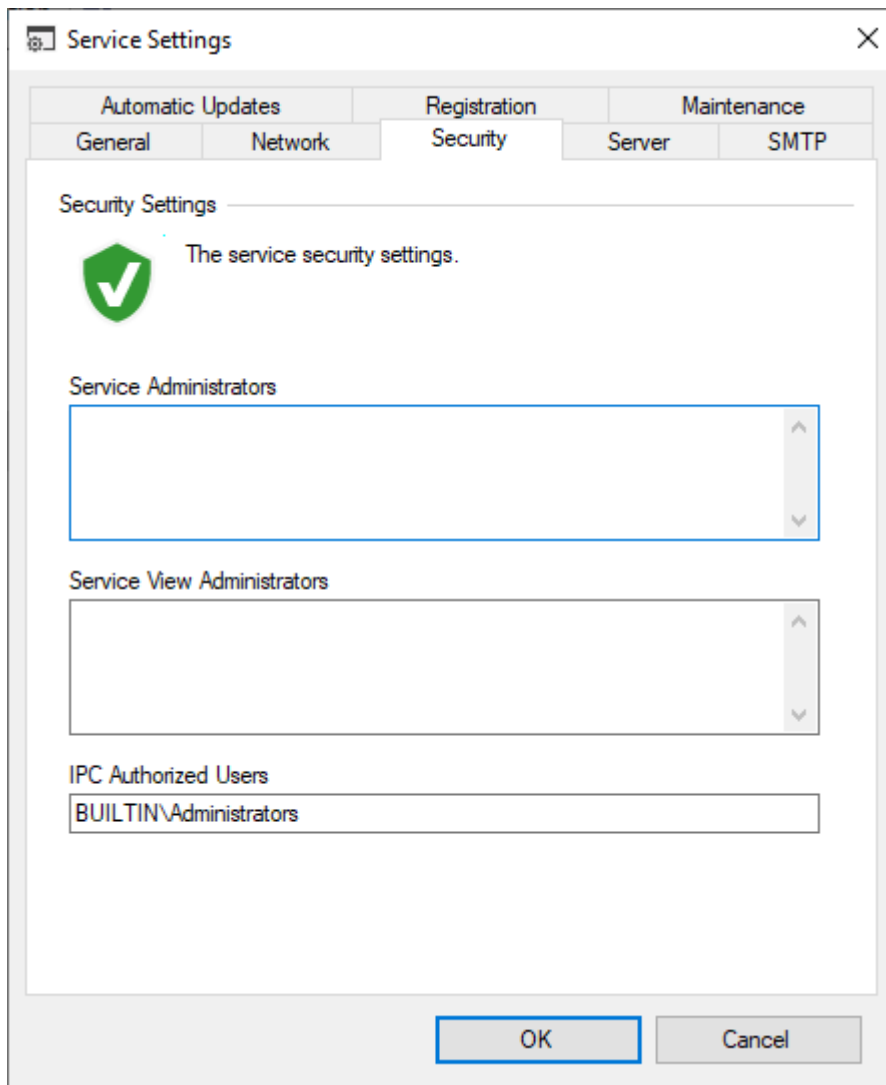
Listen for remote connections on port *

Determines whether the [XIA Configuration Client](#) service should allow the [administration tools](#) to [connect](#) from remote machines on the specified port.

** It is recommended to only enable remote connections if necessary as this increases the attack surface of the service.*

Security

Within the security tab you can view and modify the user accounts that have access to this [XIA Configuration Client](#) service.



IPC Authorized Users

The user or group that is permitted to connect to the service on a local IPC channel, by default this is the local administrators group. Warning misconfiguration of this setting may prevent users from logging onto [administration tools](#) with the error [Failed to connect to an IPC Port: Access is denied](#). The service must be restarted for changes to the setting to take effect.

Service Administrators

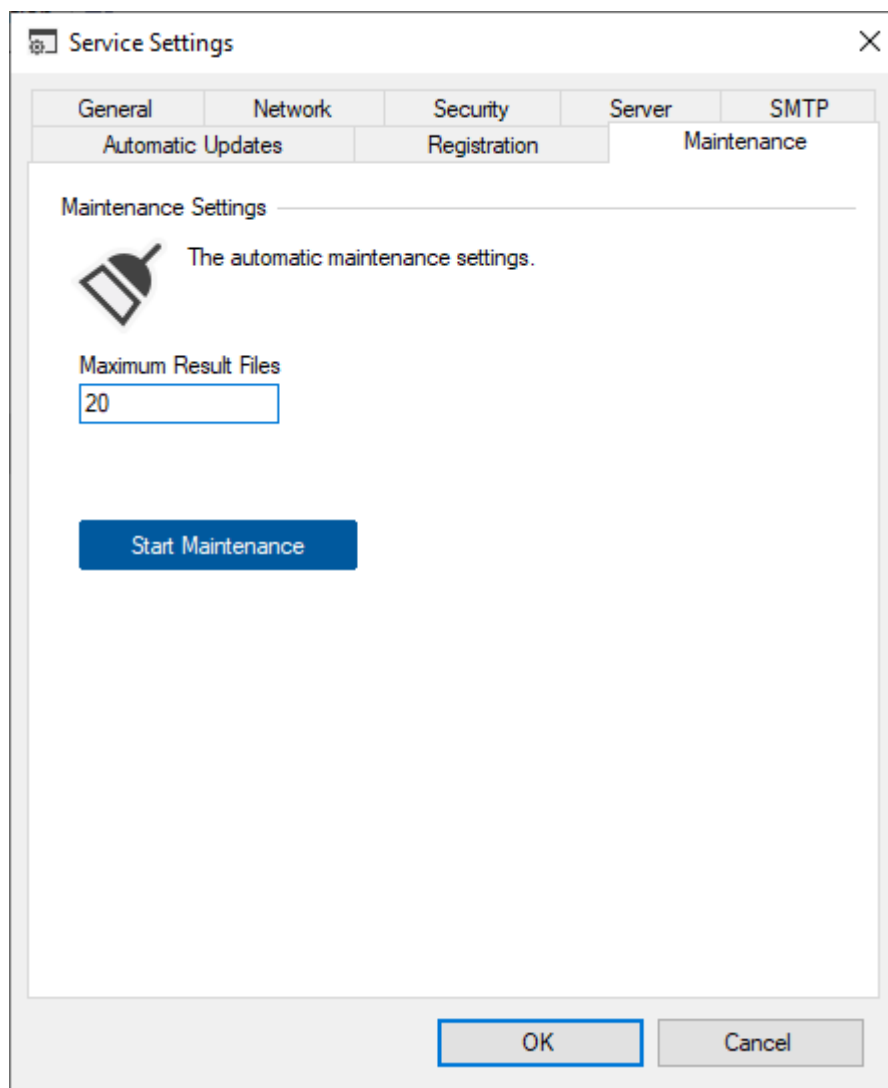
Service administrators have full access to view and configure the service. Members of the local administrators group are automatically made service administrators.

Service View Administrators

Service view administrators have access to view settings and start existing [scan profiles](#). Members of the local administrators group are automatically made service view administrators.

Maintenance

The maintenance system performs common tasks on the XIA Configuration Service at hourly intervals.



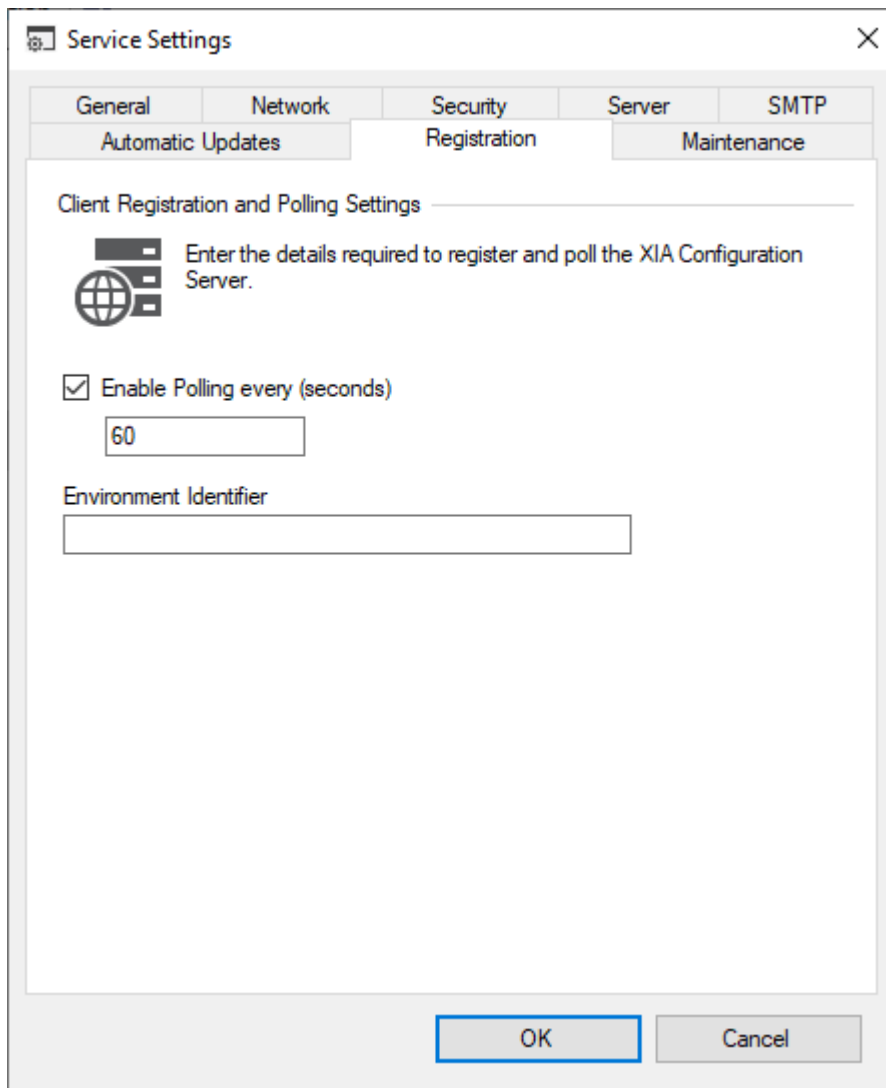
Maximum Results Files

This sets the maximum number of [scan results](#) files that should be maintained in the Logs\ScanResults directory. A value of zero indicates that all scan results files should be preserved.

Start Maintenance

Clicking *Start Maintenance* will cause the maintenance tasks to run immediately rather than waiting for the scheduled interval.

Registration



The screenshot shows the 'Service Settings' dialog box with the 'Registration' tab selected. The dialog has a title bar with a close button. Below the title bar are five tabs: 'General', 'Network', 'Security', 'Server', and 'SMTP'. Under the 'Registration' tab, there are three sub-tabs: 'Automatic Updates', 'Registration', and 'Maintenance'. The 'Registration' sub-tab is active, showing 'Client Registration and Polling Settings'. It includes a globe icon and text: 'Enter the details required to register and poll the XIA Configuration Server.' There is a checked checkbox for 'Enable Polling every (seconds)' with a text box containing '60'. Below this is an 'Environment Identifier' text box. At the bottom are 'OK' and 'Cancel' buttons.

Service Settings

General Network Security Server SMTP

Automatic Updates Registration Maintenance

Client Registration and Polling Settings

Enter the details required to register and poll the XIA Configuration Server.

☒ Enable Polling every (seconds)

60

Environment Identifier

OK Cancel

The registration tab allows the system to be configured to register with and poll the [XIA Configuration Server](#) configured on the [server tab](#). When the client registers with the server is becomes visible within the [client installations configuration settings](#) section.

Enable Polling

Determines whether the [client](#) should regularly poll the [server](#).

Polling Interval

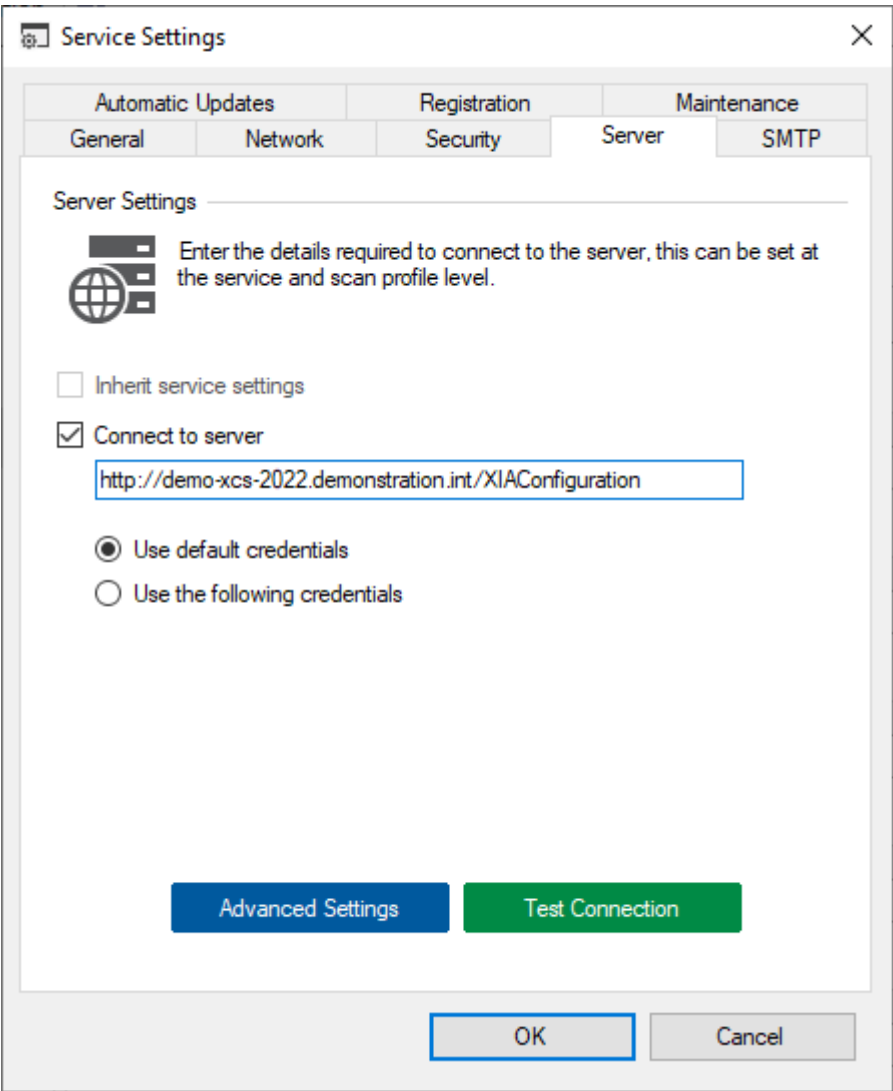
The number of seconds between polling the [server](#).

Environment Identifier

The environment [identifier](#) used to identify this machine.

Server

The server settings tab allows the configuration of a [XIA Configuration Server](#) connection. These settings are used for [automatic updates](#) and also as the settings to use for each [scan profile](#), unless overridden.



Inherit Service Settings

Determines whether the settings should inherit from the [service level server settings](#). This setting is only enabled when viewing the [server upload](#) settings for a [scan profile](#).

Connection to Server

Determines whether a connection should be made to the specified [XIA Configuration Server](#) the address should be a valid URL and accessible to the [XIA Configuration Client](#).

Credentials

The credentials to use to connect to the [XIA Configuration Server](#).

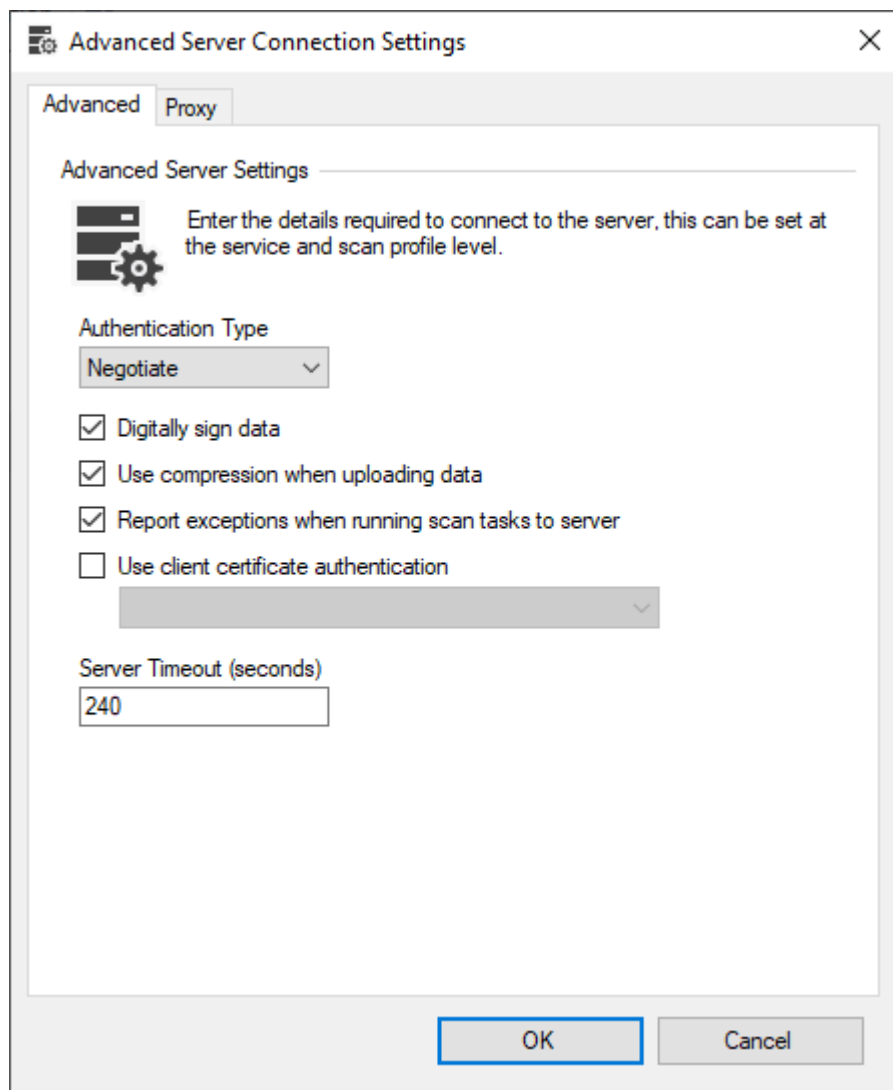
Test Connection

Tests the connection using the currently specified settings.

Advanced Settings

Displays the [advanced settings](#) dialog.

Advanced Tab



The image shows a Windows-style dialog box titled "Advanced Server Connection Settings". It has two tabs: "Advanced" (selected) and "Proxy". The "Advanced" tab contains the following settings:

- Advanced Server Settings**: A section header with a gear icon and a text box for entering details required to connect to the server.
- Authentication Type**: A dropdown menu currently set to "Negotiate".
- Digitally sign data**: A checked checkbox.
- Use compression when uploading data**: A checked checkbox.
- Report exceptions when running scan tasks to server**: A checked checkbox.
- Use client certificate authentication**: An unchecked checkbox, with a disabled dropdown menu below it.
- Server Timeout (seconds)**: A text input field containing the value "240".

At the bottom of the dialog are "OK" and "Cancel" buttons.

Authentication Type

Determines the authentication type to use either *Negotiate* or *Basic*. This setting only applies when specific credentials are used.

Digitally sign data

Determines whether the data being uploaded to the [XIA Configuration Server](#) should be digitally signed to ensure integrity of data between the client and server. If this setting is modified the server must also have the corresponding setting configured in the [import engine settings](#).

Use compression when uploading data

Determines whether the XML data uploaded to the [XIA Configuration Server](#) should be compressed.

Report exceptions when running scan tasks to server

Determines whether exceptions that occur when running [scan tasks](#) should be reported to the [XIA Configuration Server](#).

Use client certificate authentication

Determines whether a client certificate should be used when connecting to the [XIA Configuration](#)

[Server](#). For more information see the [configuring client certificates](#) section.

Selected Certificate

The name of the certificate to use for client certificate authentication - certificates will only be displayed if:

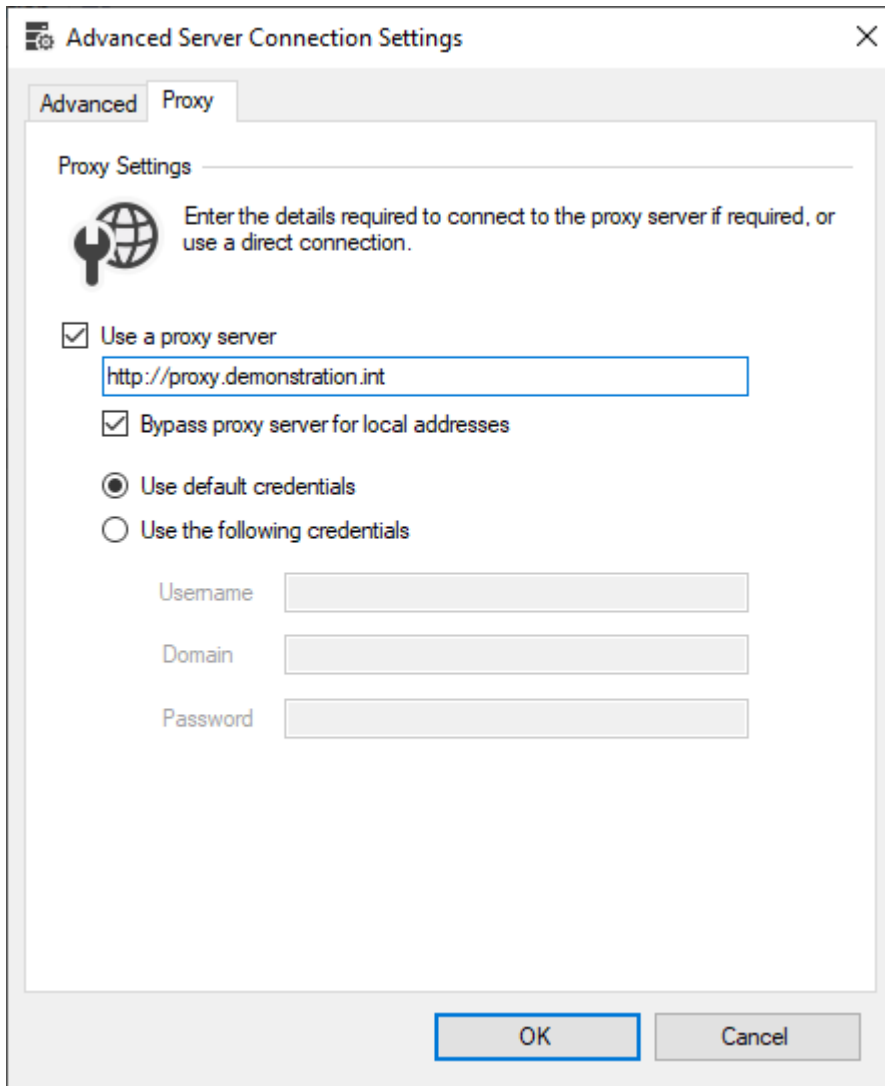
- They support client authentication
- Have the private key available
- Are installed into the **Personal** certificate store of the [service account](#) user

For more information see the [configuring client certificates](#) section.

Server Timeout (seconds)

The server connection timeout in seconds, this has a default value of 240 seconds.

Proxy Tab



The image shows a screenshot of the 'Advanced Server Connection Settings' dialog box, specifically the 'Proxy' tab. The dialog has a title bar with a gear icon and a close button. Below the title bar are two tabs: 'Advanced' and 'Proxy', with 'Proxy' being the active tab. The main content area is titled 'Proxy Settings' and contains a globe icon with a keyhole. Below this is a text instruction: 'Enter the details required to connect to the proxy server if required, or use a direct connection.' There are three main sections of settings: 1. 'Use a proxy server' is checked, with a text box below it containing 'http://proxy.demonstration.int'. 2. 'Bypass proxy server for local addresses' is checked. 3. 'Use default credentials' is selected with a radio button, while 'Use the following credentials' is unselected. Below these are three text boxes labeled 'Username', 'Domain', and 'Password', all of which are currently empty. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Advanced Server Connection Settings

Advanced Proxy

Proxy Settings

Enter the details required to connect to the proxy server if required, or use a direct connection.

☒ Use a proxy server
http://proxy.demonstration.int

☒ Bypass proxy server for local addresses

☒ Use default credentials
☐ Use the following credentials

Username
Domain
Password

OK Cancel

User a proxy server

Determines whether the proxy server specified should be used.

Bypass proxy server for local addresses

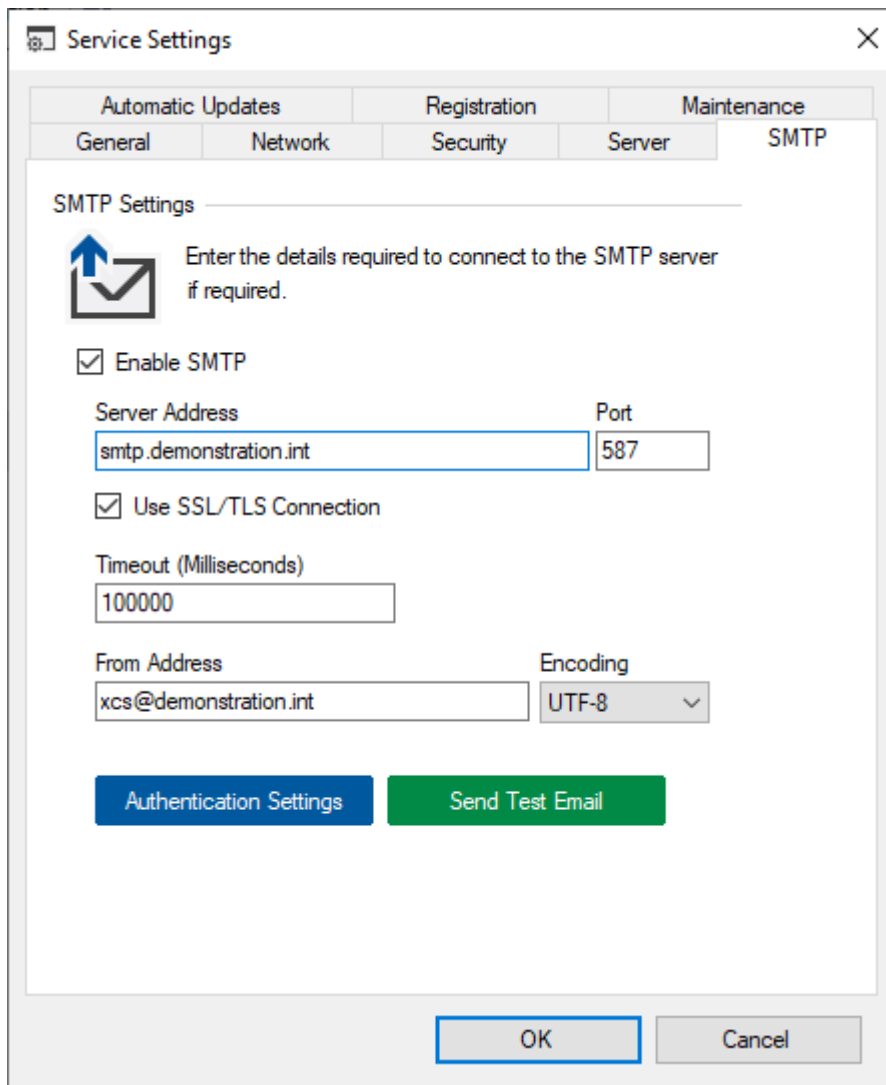
Determines whether the proxy server should be bypassed for local addresses.

Credentials

The credentials to use when using the proxy server.

SMTP

SMTP settings can be configured at the service level to allow the sending of mail notifications to specified users.



The image shows a 'Service Settings' dialog box with the 'SMTP' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'Automatic Updates', 'Registration', 'Maintenance', 'General', 'Network', 'Security', 'Server', and 'SMTP'. The 'SMTP' tab is active, showing 'SMTP Settings'. A blue arrow icon points to a text box with the instruction 'Enter the details required to connect to the SMTP server if required.' Below this is a checkbox for 'Enable SMTP' which is checked. There are two text boxes: 'Server Address' containing 'smtp.demonstration.int' and 'Port' containing '587'. Below these is a checkbox for 'Use SSL/TLS Connection' which is checked. There is a text box for 'Timeout (Milliseconds)' containing '100000'. Below that are two more text boxes: 'From Address' containing 'xcs@demonstration.int' and 'Encoding' with a dropdown menu showing 'UTF-8'. At the bottom of the SMTP settings section are two buttons: 'Authentication Settings' (blue) and 'Send Test Email' (green). At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Service Settings

Automatic Updates Registration Maintenance

General Network Security Server **SMTP**

SMTP Settings

Enter the details required to connect to the SMTP server if required.

☒ Enable SMTP

Server Address: smtp.demonstration.int Port: 587

☒ Use SSL/TLS Connection

Timeout (Milliseconds): 100000

From Address: xcs@demonstration.int Encoding: UTF-8

Authentication Settings Send Test Email

OK Cancel

Enable SMTP

Determines whether SMTP should be enabled.

Server Address

The name or IP address of the SMTP server.

Port

The TCP port that should be used for communication.

Use SSL/TLS Connection

Determines whether an SSL or TLS connection should be used.

Timeout (Milliseconds)

The timeout for the SMTP connection in milliseconds.

From Address

A valid email address that is accepted by the SMTP server

Encoding

The encoding to use for the message body. The available settings are [UTF-8](#) (default), [Unicode \(UTF-16\)](#), or [ASCII](#) encoding.

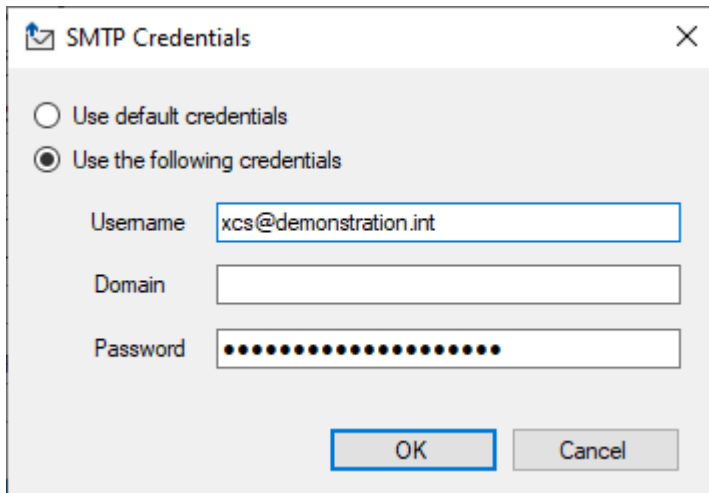
Authentication Settings

Displays the [authentication settings](#) for the SMTP connection.

Send Test Email

Displays the [send test email dialog](#).

Authentication Settings

A screenshot of the 'SMTP Credentials' dialog box. The dialog has a title bar with an envelope icon and a close button. It contains two radio buttons: 'Use default credentials' (unselected) and 'Use the following credentials' (selected). Below the radio buttons are three text input fields: 'Username' containing 'xcs@demonstration.int', 'Domain' which is empty, and 'Password' which is filled with 15 dots. At the bottom are 'OK' and 'Cancel' buttons.

SMTP Credentials

☐ Use default credentials

☒ Use the following credentials

Username

Domain

Password

OK Cancel

Use Default Credentials

Determines whether the connection to the SMTP server should use the [service credentials](#), or [scan profile credentials](#) if specified.

Use Specific Credentials

Determines whether to use the specified credentials.

Username

The username to use for the connection.

Domain

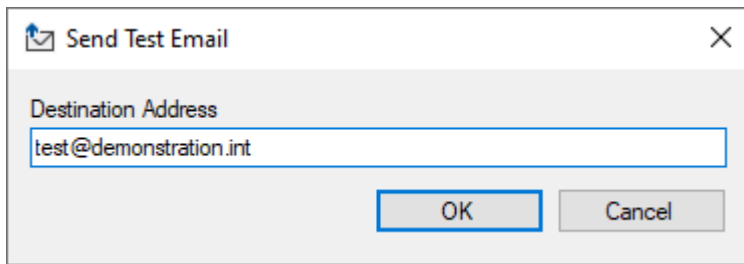
The domain name to use for the connection. If specifying an email address for the username, the domain field can be left blank.

Password

The password to use for the connection.

Send Test Email

The dialog allows a test email to be sent using the configured [SMTP settings](#).

A screenshot of a 'Send Test Email' dialog box. The dialog has a title bar with an envelope icon and a close button (X). Below the title bar, the text 'Destination Address' is displayed above a text input field. The input field contains the email address 'test@demonstration.int'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

Destination Address

The email address to which the test email is to be sent.

Scan Results Files



Scan Results Files

Provides access to the scan results files.

Show More ResultsDelete All Results

Start Time	Profile Name	Initiator
 12/09/2024 13:41:53	Default Profile	DEMONSTRATION\Administrator
 12/09/2024 13:40:41	Default Profile	DEMONSTRATION\Administrator
 06/09/2024 14:59:42	Default Profile	DEMONSTRATION\Administrator

Within this section, you can view information about previously run scans. Double clicking an item in the list displays the [scan results](#) for a single scan.

Start Time

The date and time that the [scan profile](#) was started.

Profile Name

The name of the [scan profile](#) that was executed.

Initiator

The name of the user or scheduled task that executed the [scan profile](#).

Delete All Results

Deletes all of the results XML files from the file system. This action cannot be undone.

Show More Results

By default, only the most recent scan results are displayed in the user interface. Clicking show more results loads more results into the user interface.

Results Maintenance

The scan results are periodically deleted by the system automatically. For more information see the [maintenance](#) section.

Scan Results File

The scan results window displays information about the result of each [scan task](#).

Scan Results File

File Help



Scan Results File

The results of the scan.

Scan Profile: Default Profile

Start Time: 12 September 2024 13:53:40

Finish Time: 12 September 2024 13:54:42

Started By: DEMONSTRATION\Administrator (User Initiated)

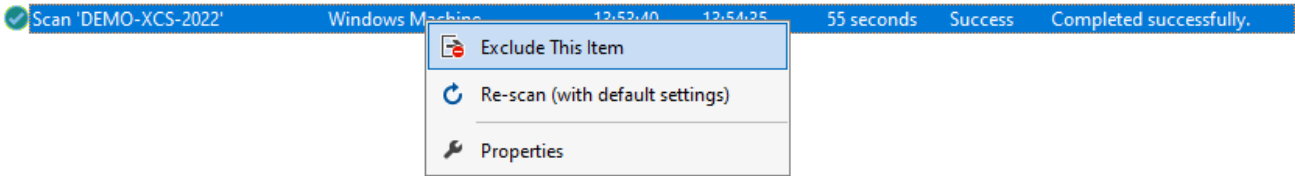
Task Name	Type	Start Time	Finish Time	Scan Time	Status	Details
✓ Search Active Directory domain	Active Directory Search	13:53:40	13:53:40	0 seconds	Success	Completed successfully.
✓ Scan 'DEMO-XCS-2022'	Microsoft DHCP Server	13:54:35	13:54:42	6 seconds	Success	Completed successfully.
✓ Scan 'DEMO-XCS-2022'	Windows Machine	13:53:40	13:54:35	55 seconds	Success	Completed successfully.
✓ Scan 'DEMO-XCS-2022'	Microsoft DNS Server	13:54:35	13:54:42	6 seconds	Success	Completed successfully.
✓ Scan 'demonstration.int'	Active Directory Domain	13:53:40	13:53:55	14 seconds	Success	Completed successfully.
✓ Network device search	Network Device Search	13:53:40	13:54:40	60 seconds	Success	Completed successfully.

- Scan profile name.
NOTE: If the scan profile has been renamed since the scan, the name of the profile at the time of the scan is shown.
- Start date and time
- Finish date and time
- The total scan time (in seconds)
- The user that started the scan and whether the scan was user initiated or started by a [schedule](#).
- A list of tasks that were executed. Double clicking a task displays the [scan result details](#).

Excluding Items

It is possible to exclude an item from being scanned by the current scan profile by right clicking the item and selecting the **Exclude This Item** menu item.

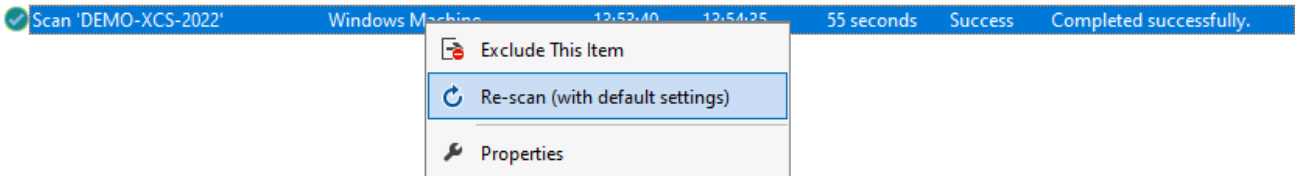
This automatically puts the item in the appropriate [exclusion list](#).



Rescanning Items

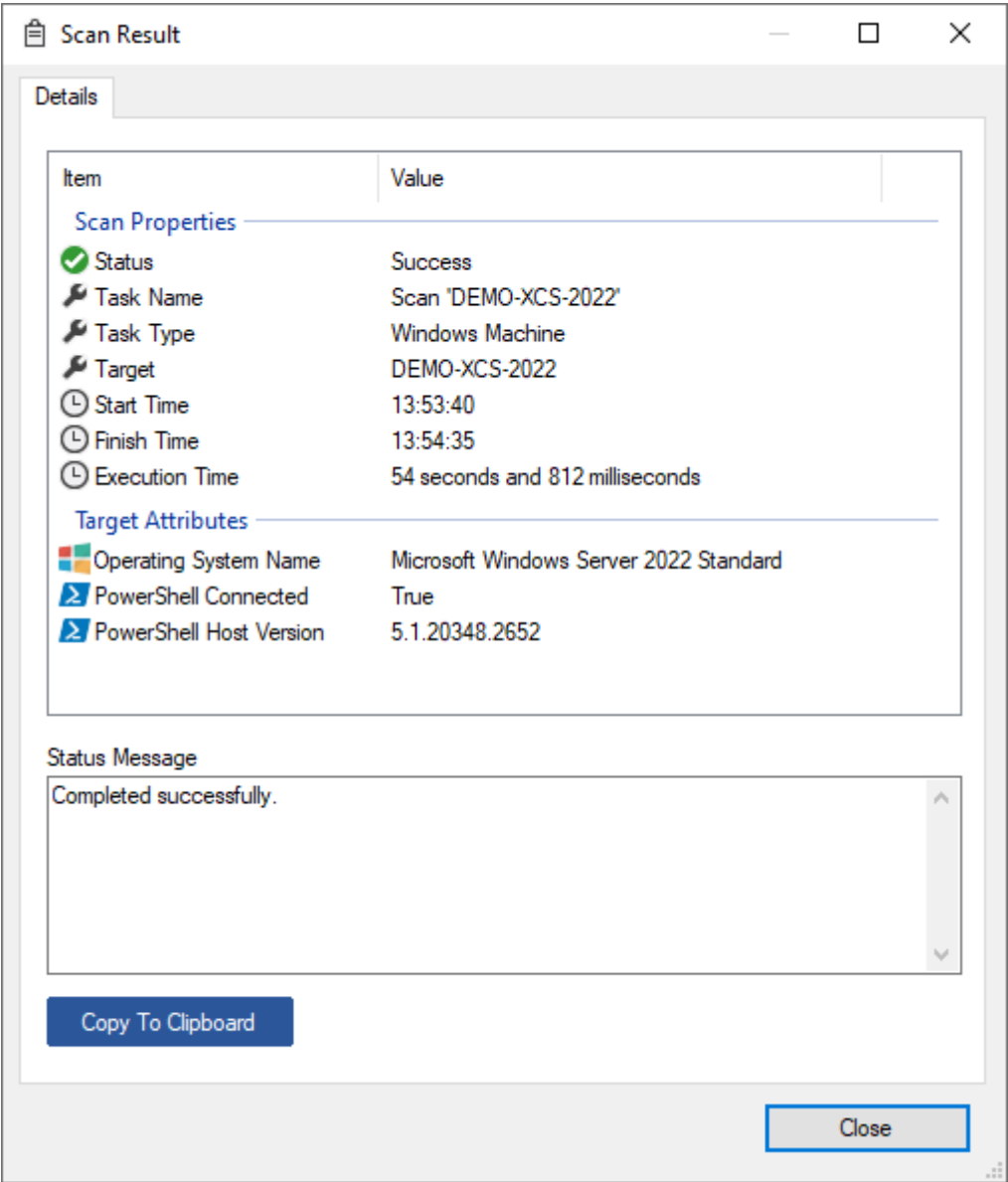
It is possible to rescan an item that has been scanned previously by clicking the **Re-scan (with default settings)** menu item. The current profile settings from the [scan profile](#) that performed the scan will be used, if the scan profile has been deleted the rescan option will be greyed out.

The [default agent settings](#) will be used for the scan.



Scan Result Details

The scan result details dialog provides full information about a specific [scan task](#).



Status

The status of the scan task.

Task Name

The display name of the task that was executed.

Type

The scan task type.

Target

The name of the item that was scanned - for example, in the case of a Windows machine, the computer name.

Start Time

The time at which the scan of this specific item started.

Finish Time

The time at which the scan of this specific item finished.

Execution Time

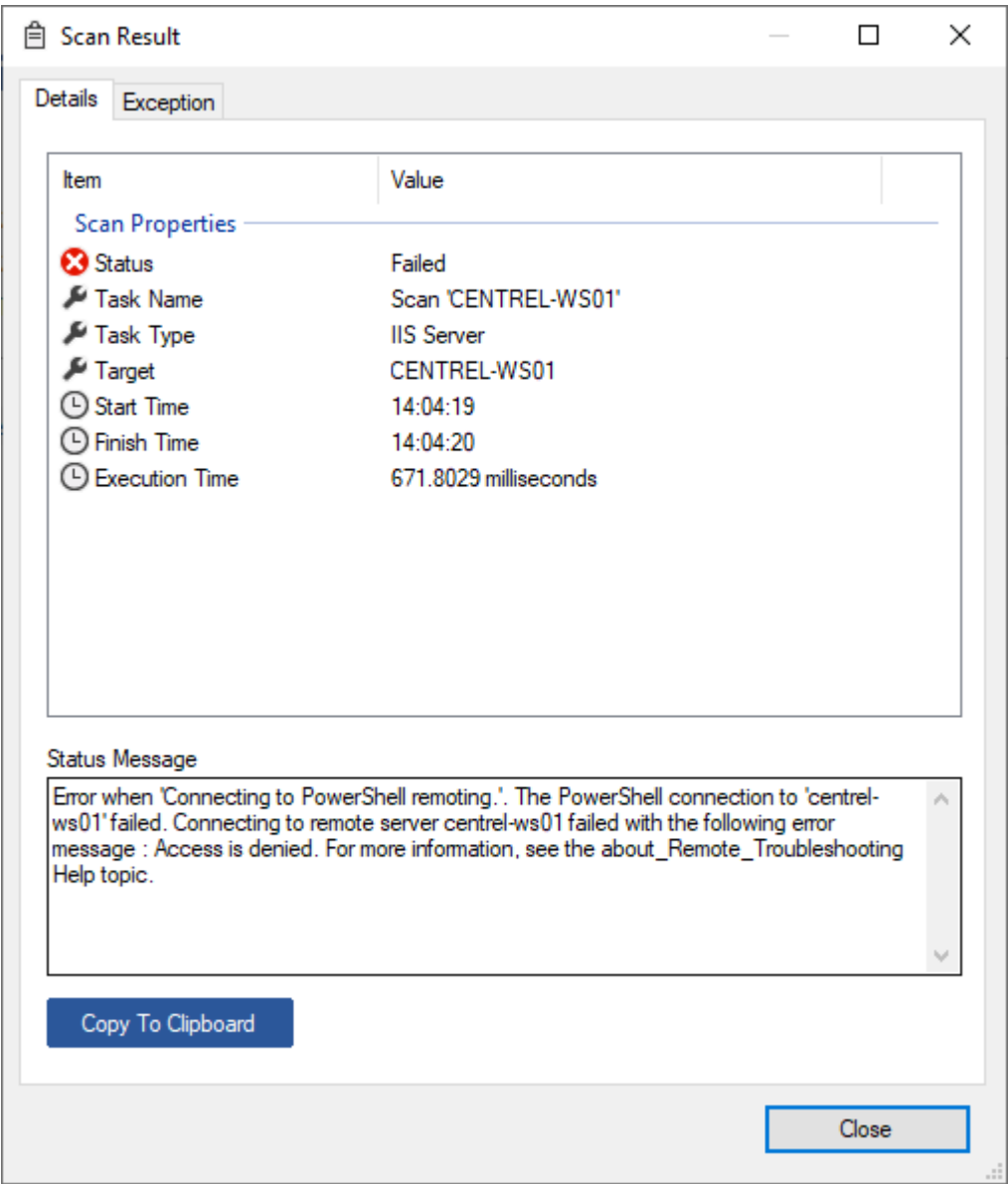
The total time spent executing this specific scan task.

Target Attributes

This section provides additional information about the target system being scanned.

Details

In the case of a scan task failing, the details show the error information which can be used to troubleshoot the issue.



Exception Details

Clicking the view exception link shows the full exception stack trace.

Warnings

Provides details of any warnings that occurred during the scan.

Additional Help

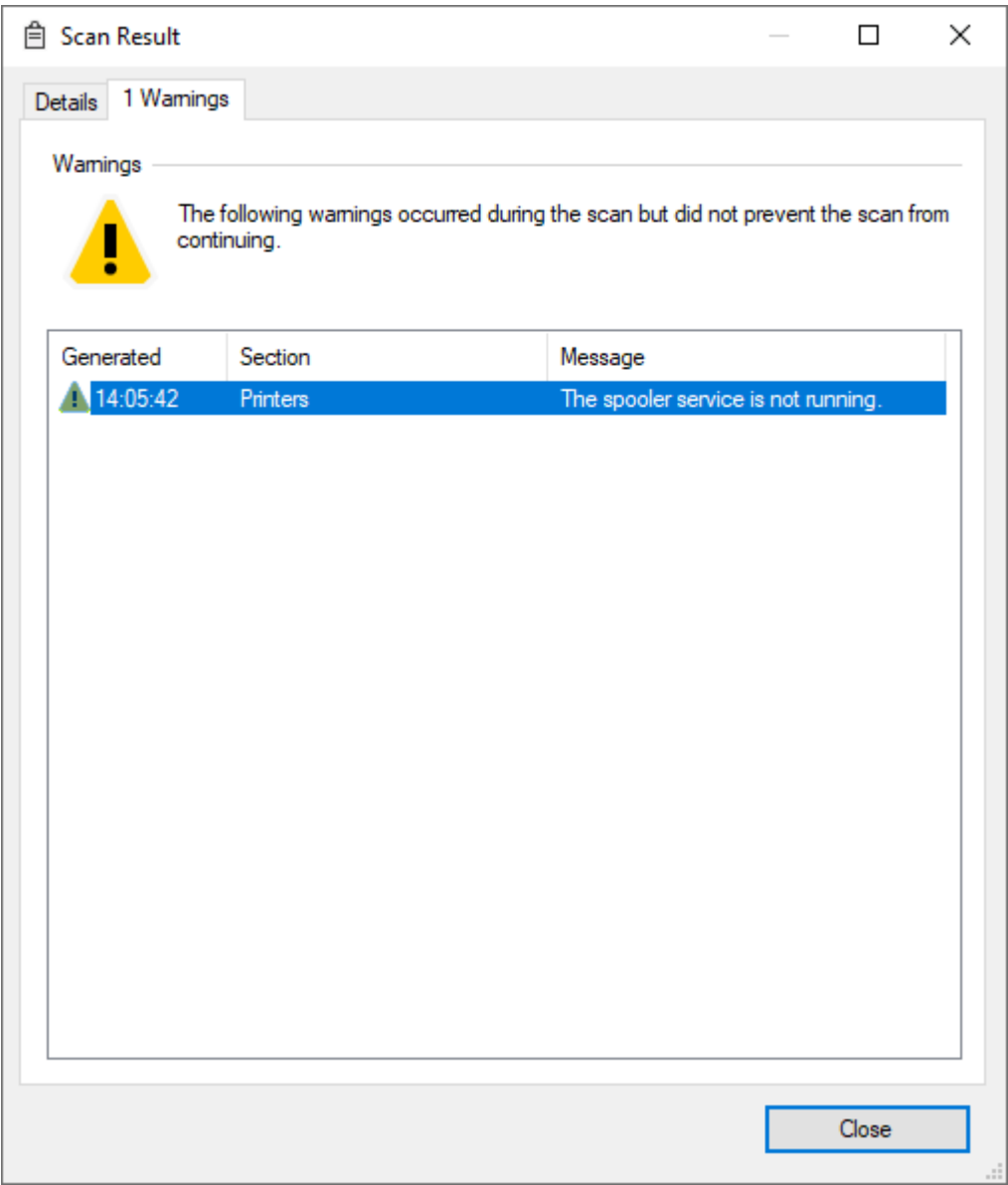
For certain error types, a hyperlink may be displayed that allows the user to view additional help for this specific error.

Copy to Clipboard

Clicking copy to clipboard will copy all of the information displayed into the clipboard.

Scan Result Warnings

This section provides information about any warnings that occurred during the scan.



Generated

The time at which the warning was generated.

Section

The scan section where the warning was encountered.

Message

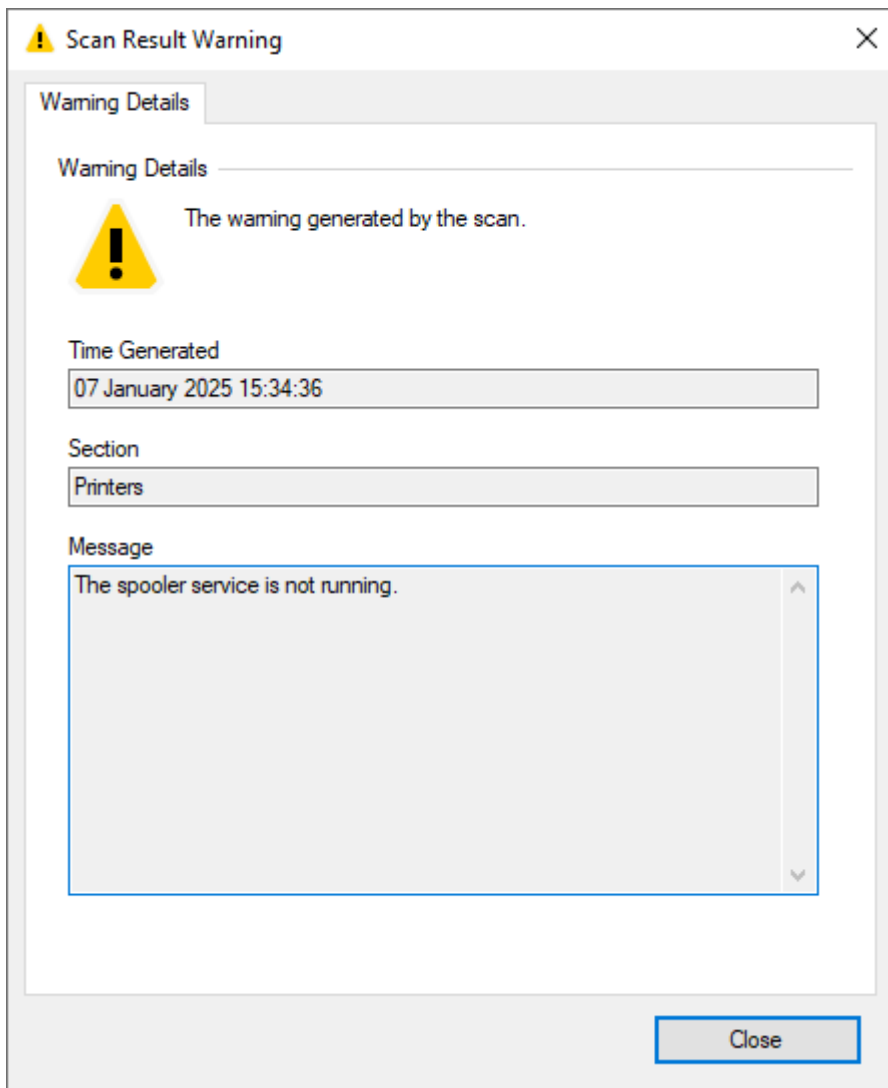
The warning message.

Double clicking a warning displays the [scan result warning dialog](#).

NOTE: For more information on the warning, perform a scan with [diagnostics trace](#) enabled.

Scan Result Warning Dialog

This scan result warning dialog provides full information about a warning that occurred during the scan.



Generated

The time at which the warning was generated.

Section

The scan section where the warning was encountered.

Message

The warning message.

Double clicking a warning displays the [scan result warning dialog](#).

NOTE: For more information on the warning, perform a scan with [diagnostics trace](#) enabled.

Compliance Benchmarks

Compliance benchmarks provide the ability to determine how various [item types](#) adhere to predefined configuration and security standards.

Information in the compliance benchmarks is collected by the [client](#) and can be viewed in the [compliance benchmarks](#) user interface on the [server](#).

For more information see the following sections.

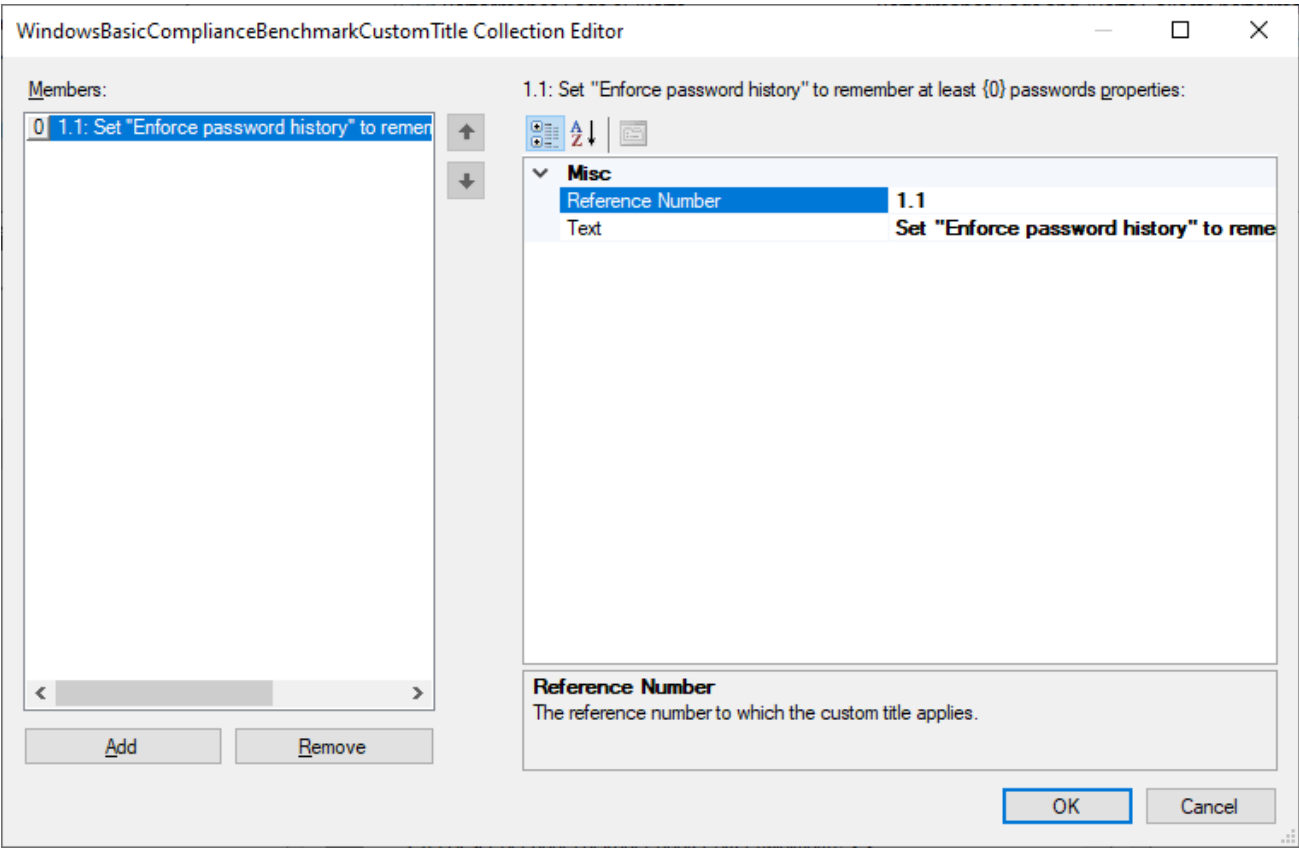
[Windows Machine Basic Compliance Benchmark](#)

[SQL Instance Basic Compliance Benchmark](#)

[Creating Compliance Benchmarks](#)

Custom Titles

Each [compliance benchmark](#) automatically sets the text to be displayed for each section and compliance result, however custom text can be set if required.



Reference Number

The reference number of the section or benchmark result for which custom title text should be applied.

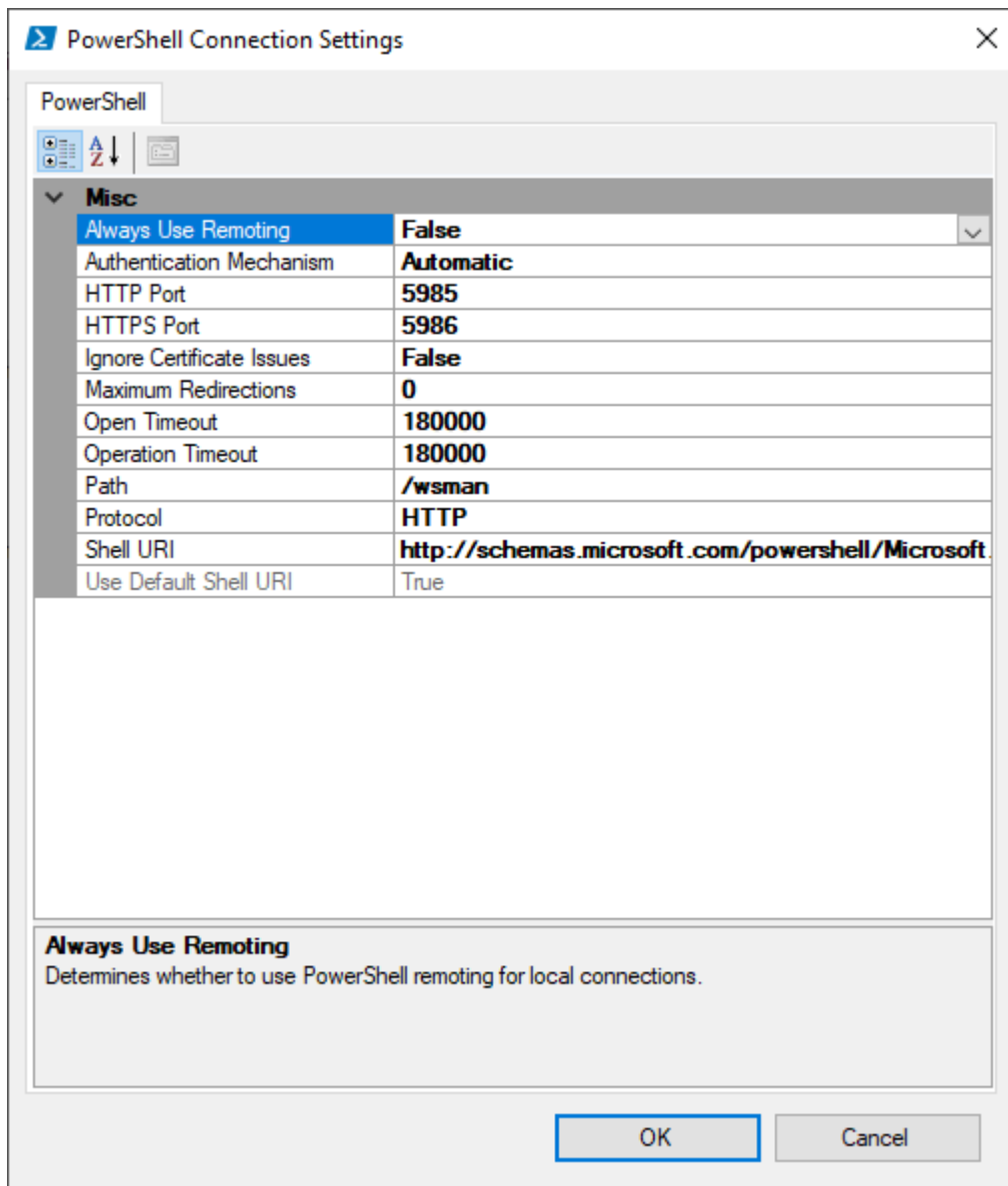
Text

The text to display for the title. Setting the text to blank will cause the default text for this result to be displayed.

Certain titles contain parameters which are automatically substituted in the text using the .NET [String.Format](#) method - for example

Set "Enforce password history" to remember at least {0} passwords

PowerShell Connection Settings

The image shows a Windows-style dialog box titled "PowerShell Connection Settings". It has a tab labeled "PowerShell" and a toolbar with icons for help, settings, and a folder. A tree view on the left shows "Misc" expanded. The main area contains a table of settings. Below the table is a section titled "Always Use Remoting" with a descriptive text. At the bottom are "OK" and "Cancel" buttons.

Misc	
Always Use Remoting	False
Authentication Mechanism	Automatic
HTTP Port	5985
HTTPS Port	5986
Ignore Certificate Issues	False
Maximum Redirections	0
Open Timeout	180000
Operation Timeout	180000
Path	/wsman
Protocol	HTTP
Shell URI	http://schemas.microsoft.com/powershell/Microsoft
Use Default Shell URI	True

Always Use Remoting
Determines whether to use PowerShell remoting for local connections.

OK Cancel

Always Use Remoting

Determines whether PowerShell remoting should be used, even when a connection is being made to the local machine.

Authentication Mechanism

The authentication mechanism to use - Automatic, Basic, Negotiate, or Kerberos. When set to automatic the system will typically use Kerberos authentication, and will use Negotiate only when the machine is on a workgroup, or [custom credentials](#) are in use. Basic authentication is only supported for the [Exchange Organization](#) agent.

HTTP Port

The port to use when making a HTTP connection.

HTTPS Port

The port to use when making a HTTPS connection.

Ignore Certificate Issues

Determines whether to ignore certificate issues when making HTTPS connections.

Maximum Redirections

The maximum number of URI redirections allowed.

Open Timeout *

The maximum amount of time (in milliseconds) that Windows PowerShell will wait for an open operation to complete. By default this is 180 seconds.

Operation Timeout *

The amount of time (in milliseconds) that Windows PowerShell will wait for an operation to complete including a command or script to execute. By default this is 180 seconds.

Path

The path to use for the connection - by default this is /wsman for all connections except the [Exchange Organization](#) agent.

Protocol

The connection protocol to use - HTTP, HTTPS or Automatic. When set to Automatic the system will attempt to connect using HTTPS and will attempt a HTTP connection if the connection is unsuccessful.

Shell URI

The uniform resource identifier for the shell to load, this is configured by the endpoint. This shell may set security, run scripts and load snap-ins automatically. By default this is set to `http://schemas.microsoft.com/powershell/Microsoft.PowerShell`.

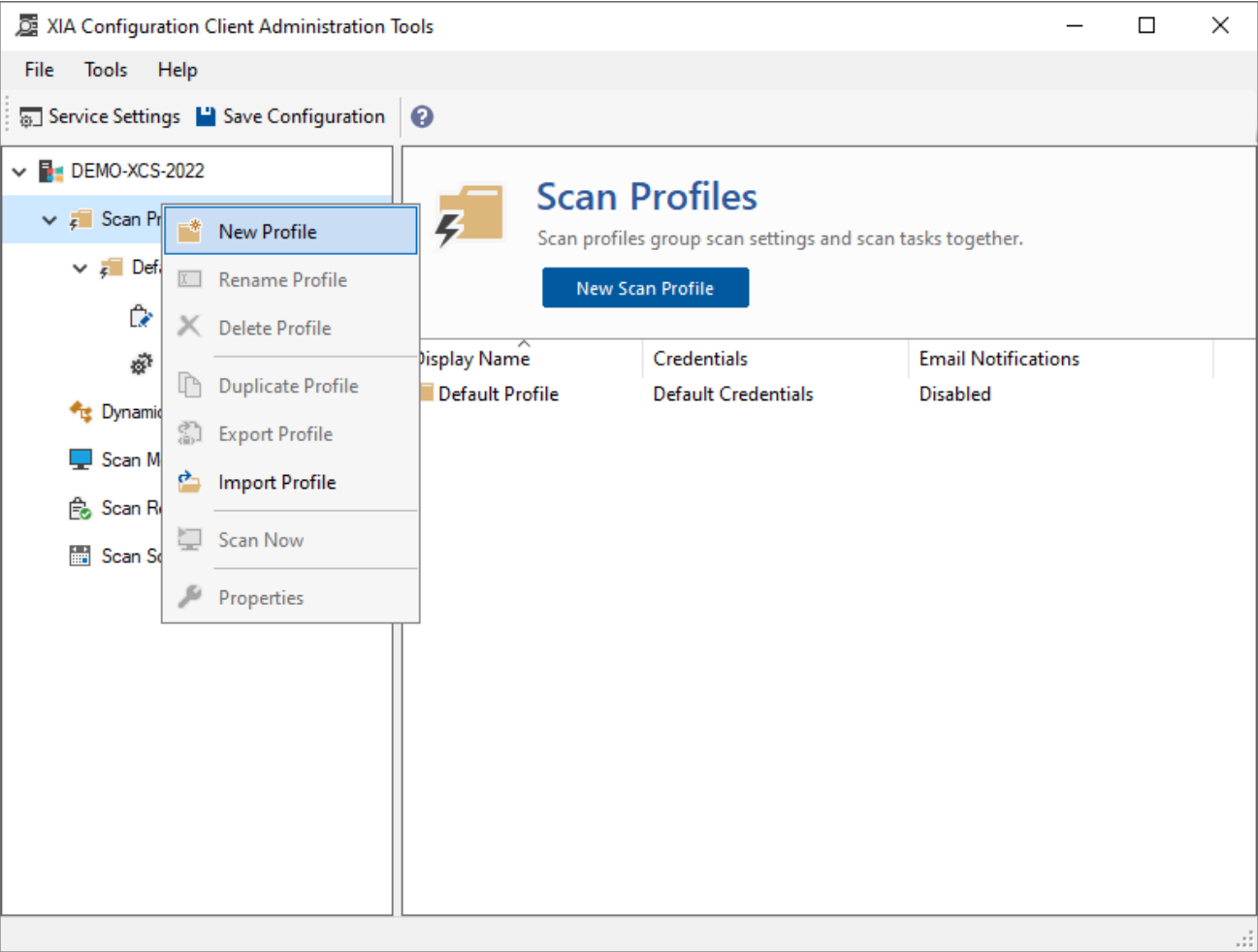
* These settings only apply when a remote connection is made. For these settings to take effect when the connection is made on the local machine the "Always Use Remoting" setting must be applied.

Scan Profiles

Scan profiles allow scan tasks and settings to be grouped together - each scan profile can be started, scheduled and monitored as a single unit. It is possible for example to create a scan profile that is scheduled to scan Windows servers and import infrastructure separately from Windows workstations which may require scanning on a less frequent basis.

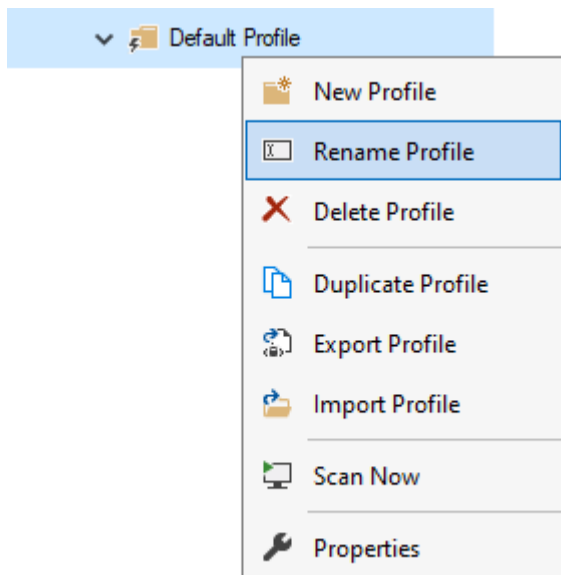
Creating a Scan Profile

To create a scan profile right click the **Scan Profiles** node and select **New Profile**. Enter a suitable name for the newly created scan profile such as "Scan Local Computer", each scan profile name must be unique.



Renaming a Scan Profile

Right click the scan profile you wish to rename and click **Rename Profile**.



Deleting a Scan Profile

Right click the scan profile you wish to delete and click **Delete Profile**.

Exporting a Scan Profile

Scan profiles can be exported and then imported into another XIA Configuration Client. To export a scan profile right click the scan profile you wish to export and select **Export Profile**.

Enter or browse for the location to save the file. Scan Profiles are exported as XML Files.

Importing a Scan Profile

Should you wish to import a scan profile that you have previously exported, right click the scan profiles node and select **Import Profile**.

Enter or browse for the location of the scan profile file that was previously exported.

Duplicating a Scan Profile

To create a duplicate of an existing scan profile right click the profile and select **Duplicate Profile**. Enter a suitable name for the newly duplicated scan profile.

Starting a Scan

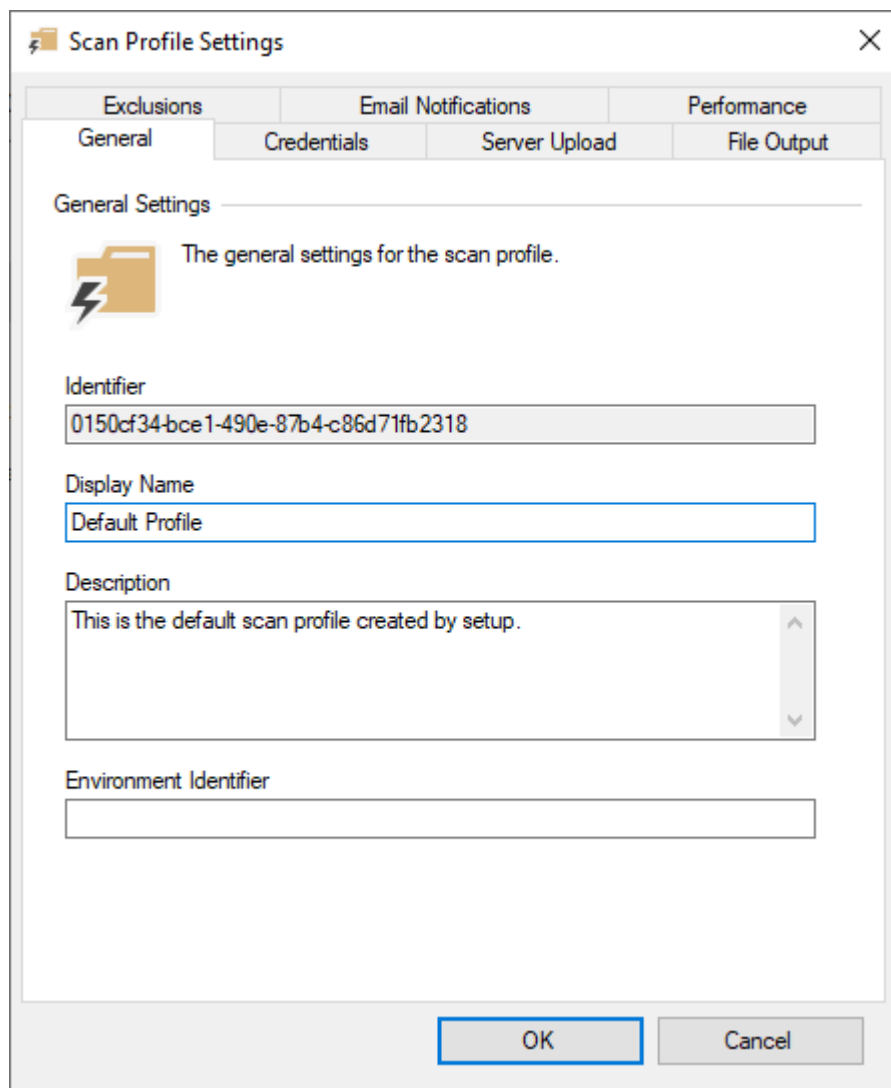
To start a scan right click the scan profile you wish to start and click **Scan Now**. The XIA Configuration Service can run only one scan profile at a time but the scan profile can run many scan tasks simultaneously.

Editing a Scan Profile

To modify the properties of a scan profile, right click the scan profile and select **Properties**.

For more information see the [scan profile settings](#) section.

General



The screenshot shows the 'Scan Profile Settings' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Below the title bar are four tabs: 'Exclusions', 'Email Notifications', 'Performance', and 'General'. The 'General' tab is active, showing a 'General Settings' section with a folder icon and a description: 'The general settings for the scan profile.' Below this are four input fields: 'Identifier' (containing '0150cf34-bce1-490e-87b4-c86d71fb2318'), 'Display Name' (containing 'Default Profile'), 'Description' (containing 'This is the default scan profile created by setup.'), and 'Environment Identifier' (which is empty). At the bottom right are 'OK' and 'Cancel' buttons.

Exclusions	Email Notifications	Performance
General	Credentials	Server Upload
		File Output

General Settings

 The general settings for the scan profile.

Identifier
0150cf34-bce1-490e-87b4-c86d71fb2318

Display Name
Default Profile

Description
This is the default scan profile created by setup.

Environment Identifier

OK Cancel

Identifier

The unique identifier for the scan profile in [GUID](#) format.

Display Name

The display name for the scan profile - for example *"Default Scan Profile"*.

Profile Description

The user defined description of the scan profile.

Environment Identifier

An environment identifier is used to distinguish between multiple identical items. By default, this field is blank.

For more information see the [item identifiers](#) section.

Credentials

The screenshot shows the 'Scan Profile Settings' dialog box with the 'Credentials' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'Exclusions', 'Email Notifications', 'Performance', and 'General'. The 'Credentials' tab is active. Inside the 'Credentials' tab, there is a section titled 'Credentials' with a subtitle 'The credentials to use for the scan profile.' and a green checkmark icon. Below this, there are two radio buttons: 'Use default credentials' (unselected) and 'Use the following credentials' (selected). Under 'Use the following credentials', there are three text input fields: 'Username' with the value 'sysadmin', 'Domain' with the value 'demonstration.int', and 'Password' with a masked password represented by dots. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. A blue information box at the bottom of the 'Credentials' section contains the text: 'The specified credentials will be used to scan remote systems and upload to the XIA Configuration Server when hosted on a remote machine.'

By default, the XIA Configuration service will scan remote machines by using the credentials of the [service account](#) however it is possible to use custom credentials.

This method uses **Network Only** credentials (in a similar manner to the **runas /netonly** command). The following should be noted about using custom credentials:

- These credentials can be used to scan untrusted Active Directory domains and computers on workgroups.
- To scan a machine on a workgroup, enter the workgroup name or "WORKGROUP" as the domain.
- The password is **not** validated by the client and is only used when making remote connections.
- The credentials are used when making a connection to the XIA Configuration Server when the server is not installed on the same machine and custom credentials are not specified on the [server upload](#) tab.

For more information please see [credentials and security contexts overview](#).

Default Agent Settings

Each [scan profile](#) can be configured with the default settings that are to be used by each of the [scan tasks](#) assigned to the profile, unless the [scan task](#) explicitly overrides those settings.



Default Agent Settings

Provides the configuration of the settings each scan agent will use by default.

Restore Defaults

Name	Description
 Active Directory Domain	The agent settings for Active Directory Domain items.
 Azure Tenant	The agent settings for Azure Tenant items.
 Backup Exec Server	The agent settings for Backup Exec Server items.
 Citrix XenApp Farm	The agent settings for Citrix XenApp Farm items.
 Citrix XenDesktop Site	The agent settings for Citrix XenDesktop Site items.
 Entra Directory	The agent settings for Entra Directory items.
 Exchange Organization	The agent settings for Exchange Organization items.
 Generic Network Device	The agent settings for Generic Network Device items.
 Hyper-V Server	The agent settings for Hyper-V Server items.
 IIS Server	The agent settings for IIS Server items.
 Microsoft Cluster	The agent settings for Microsoft Cluster items.
 Microsoft DHCP Server	The agent settings for Microsoft DHCP Server items.
 Microsoft DNS Server	The agent settings for Microsoft DNS Server items.
 Microsoft NLB Cluster	The agent settings for Microsoft NLB Cluster items.
 Network Storage Device	The agent settings for Network Storage Device items.
 Network Switch	The agent settings for Network Switch items.
 SQL Instance	The agent settings for SQL Instance items.
 Terminal (RDP) Server	The agent settings for Terminal (RDP) Server items.
 Unix System	The agent settings for Unix System items.
 VMware System	The agent settings for VMware System items.
 Windows Machine	The agent settings for Windows Machine items.
 WINS Service	The agent settings for WINS Service items.

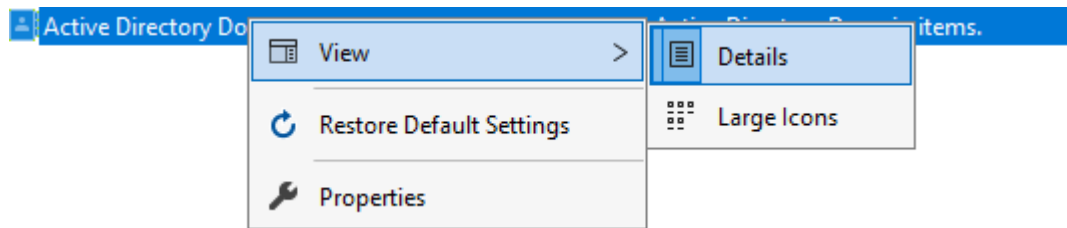
Restore Defaults

Restores all agent default settings to their default values.

Right clicking the default agent settings displays the [context menu](#).

Context Menu

Right clicking the [default agent settings](#) user interface displays the context menu.



View > Details

Displays the listview in details view.

View > Large Icons

Displays the listview in large icons view.

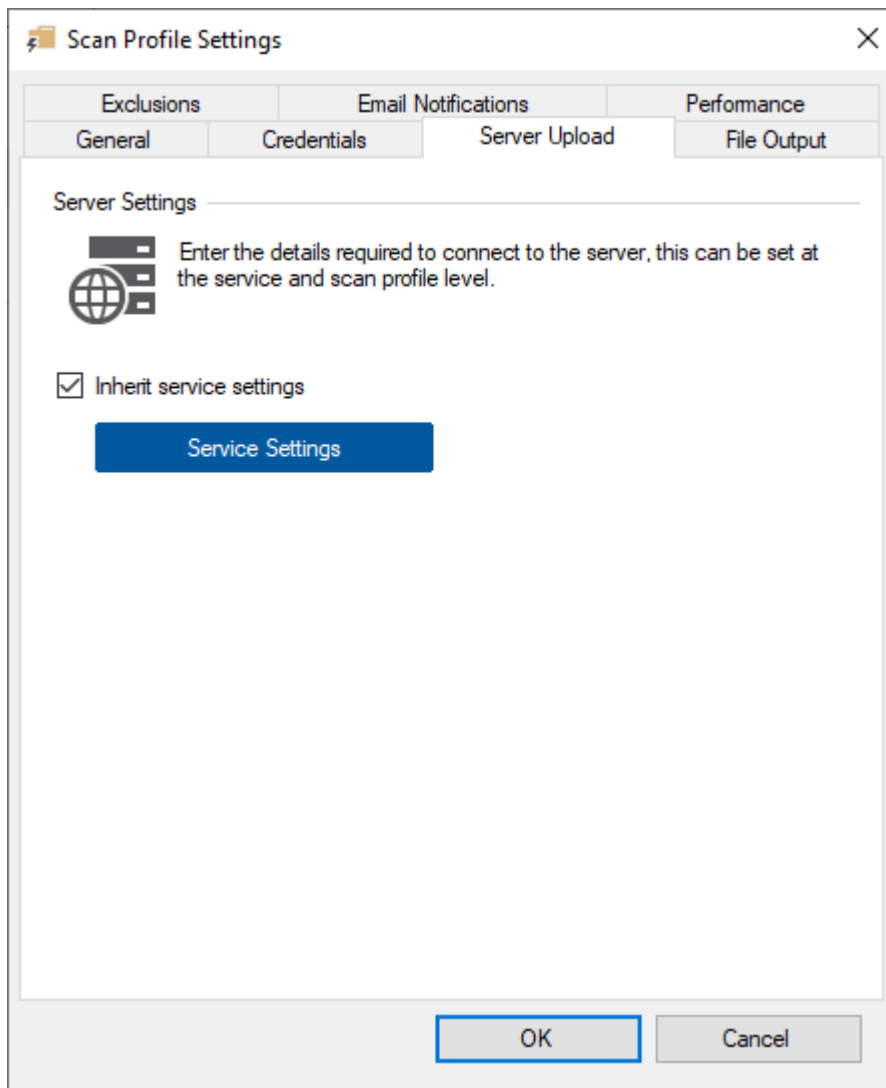
Restore Default Settings

Restores the currently agent default settings to their default values.

Properties

Displays the currently selected agent default settings.

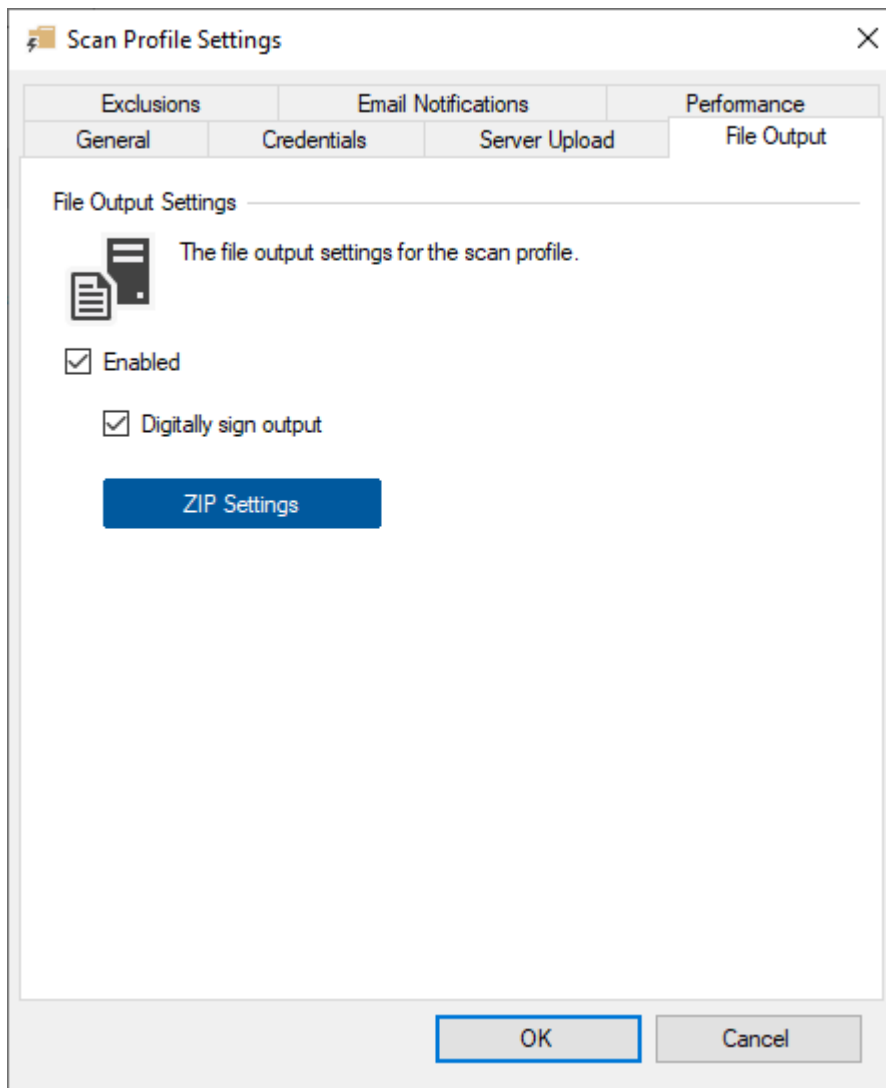
Server Upload



The server upload tab allows data generated by the [XIA Configuration Client](#) to be automatically uploaded to the [XIA Configuration Server](#).

By default these settings are inherited from the [server settings](#) on the [service settings](#) dialog, however can be configured independently for each [scan profile](#).

File Output



Enabled

Determines whether the data generated by the scan profile should be written to the filesystem.

The default directory used is

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Data

Digitally sign output

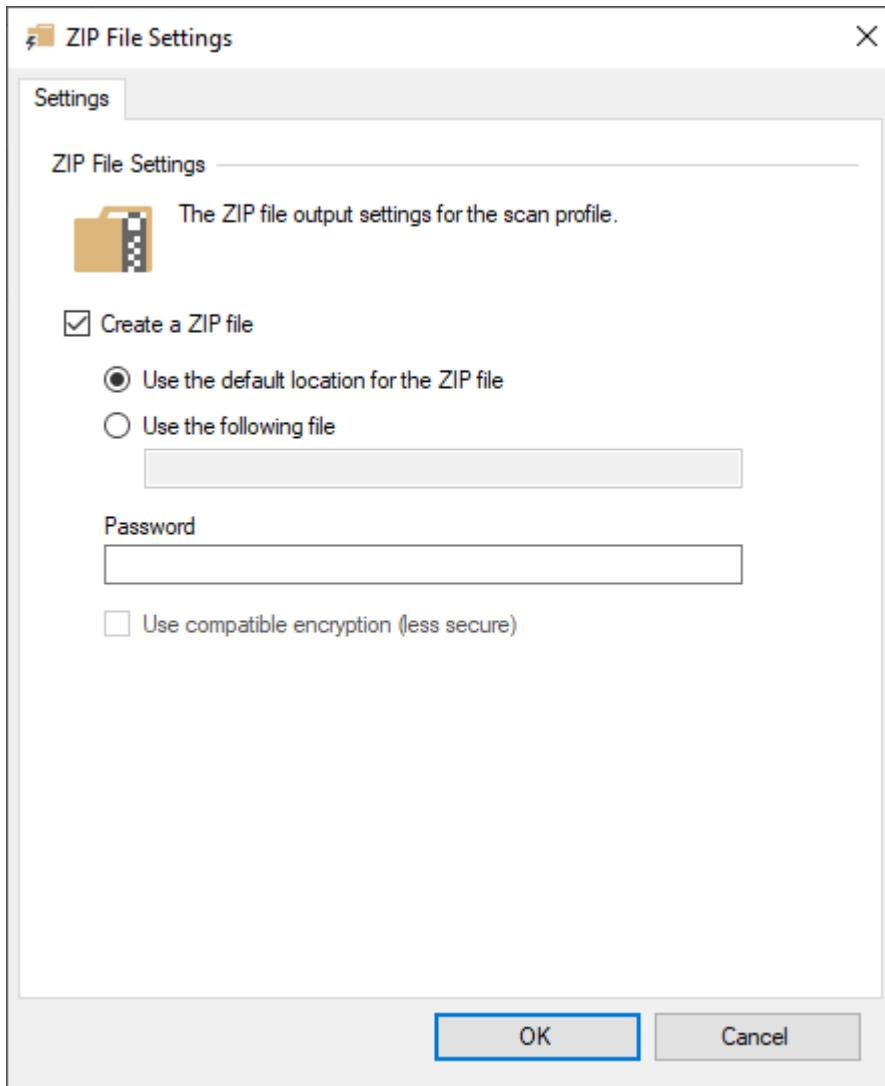
Determines whether the data being written to the filesystem should be digitally signed to ensure integrity of data between the client and [XIA Configuration Server](#). If this setting is modified the server must also have the corresponding setting configured in the [import engine settings](#).

ZIP Settings

Displays the [ZIP file settings](#) dialog.

NOTE: All the files in the file output directory are deleted each time a [scan profile](#) is executed.

ZIP File Settings



The screenshot shows a dialog box titled "ZIP File Settings" with a close button (X) in the top right corner. Inside the dialog, there is a "Settings" tab. Below the tab, the text "ZIP File Settings" is followed by a horizontal line. A folder icon is shown next to the text "The ZIP file output settings for the scan profile." Below this, there is a checked checkbox labeled "Create a ZIP file". Underneath, there are two radio button options: "Use the default location for the ZIP file" (which is selected) and "Use the following file" (which is unselected). Below the "Use the following file" option is a text input field. Below the text input field is a label "Password" followed by another text input field. At the bottom of the dialog, there is an unchecked checkbox labeled "Use compatible encryption (less secure)". At the very bottom of the dialog, there are two buttons: "OK" and "Cancel".

Create a ZIP file

Determines whether the data files created by the [file output](#) should be written to a compressed ZIP file.

Use the default location for the ZIP file

Determines whether the ZIP file should be created in the default location within the [XIA Configuration Client installation](#) directory - for example

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Data\Data.zip

Use the following file

Determines the name or absolute path of the ZIP file to create - this may include environment variables.

The [XIA Configuration Client service account](#) must have permission to write to the location specified.

Password

The optional password to use to encrypt the ZIP file.

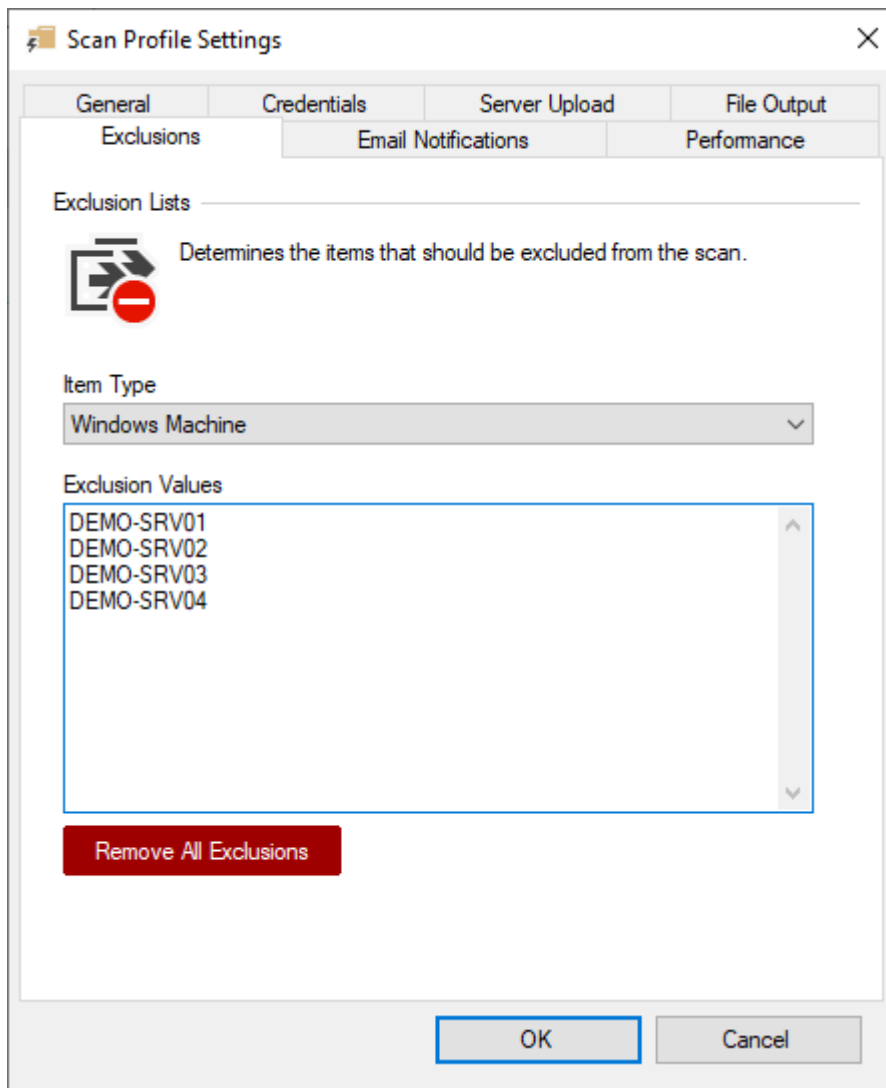
Use compatible encryption

Determines whether to use the less secure compatible encryption instead of the default AES encryption. This option only applies when a password is set.

Exclusions

Scan exclusions allow for the bypassing of items based on type and item name. The screenshot below demonstrates the exclusion of the following IIS Servers.

- DEMO-SRV01
- DEMO-SRV02
- DEMO-SRV03
- DEMO-SRV04



Wildcards

Wildcards can be used at the start or end of an item name - for example DEMO-SRV* will exclude any item whose name starts with DEMO-SRV. Entering a value of * will exclude all items of that type.

Remove all exclusions

Clicking **remove all exclusions** will remove all exclusions configured for all item types in this scan profile

Detection Support

Exclusions are applied regardless of how the item was assigned including

- Manually entered in a scan list
- Detected automatically from a search task (for example [Active Directory Search](#) or [Network Device Search](#))
- Detected during the scan of another item (for example [Windows Machine Scan Task](#))

Logging Output

When an item is bypassed this is written to the diagnostics trace log. The message format is as follows.

Bypassing adding a new '*Item Type*' scan task for target '*Target Name*' as this target is configured as an exclusion in the scan profile.

Active Directory Search

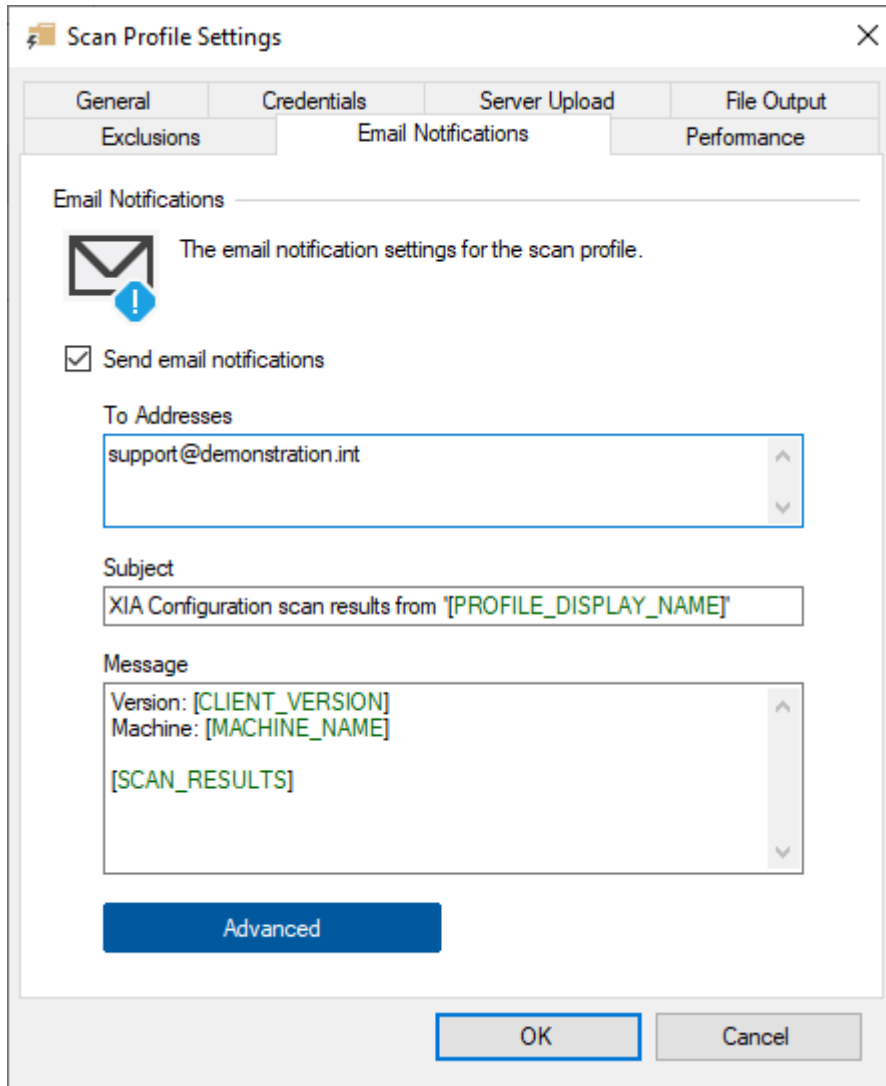
Please note that when using the [Active Directory Search](#) if using the [Use Fully Qualified Domain Names](#) setting you must use this naming format for the exclusions for example

demo-srv01.demonstration.int or
demo-srv01.*

Email Notifications

Notifications allow users to be notified of the results of a scan by email.

Please see the [SMTP](#) settings for more information on the configuration of the SMTP server hostname and connection credentials.



The screenshot shows the 'Scan Profile Settings' dialog box with the 'Email Notifications' tab selected. The dialog has a title bar with a close button (X) and a tab bar with 'General', 'Credentials', 'Server Upload', 'File Output', 'Exclusions', 'Email Notifications', and 'Performance'. The 'Email Notifications' tab is active, showing a description 'The email notification settings for the scan profile.' with an envelope icon and a blue exclamation mark. Below this is a checkbox 'Send email notifications' which is checked. There are three text input fields: 'To Addresses' containing 'support@demonstration.int', 'Subject' containing 'XIA Configuration scan results from '[PROFILE_DISPLAY_NAME]'' (where PROFILE_DISPLAY_NAME is a variable), and 'Message' containing 'Version: [CLIENT_VERSION]', 'Machine: [MACHINE_NAME]', and '[SCAN_RESULTS]' (where CLIENT_VERSION, MACHINE_NAME, and SCAN_RESULTS are variables). At the bottom of the tab is a blue 'Advanced' button. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

Send email notifications

Determines whether an email should be sent to the specified address(es) following the completion of a scan

To Addresses

A list of email addresses to which the notification should be sent

Subject

The subject of the email. This can include [variables](#).

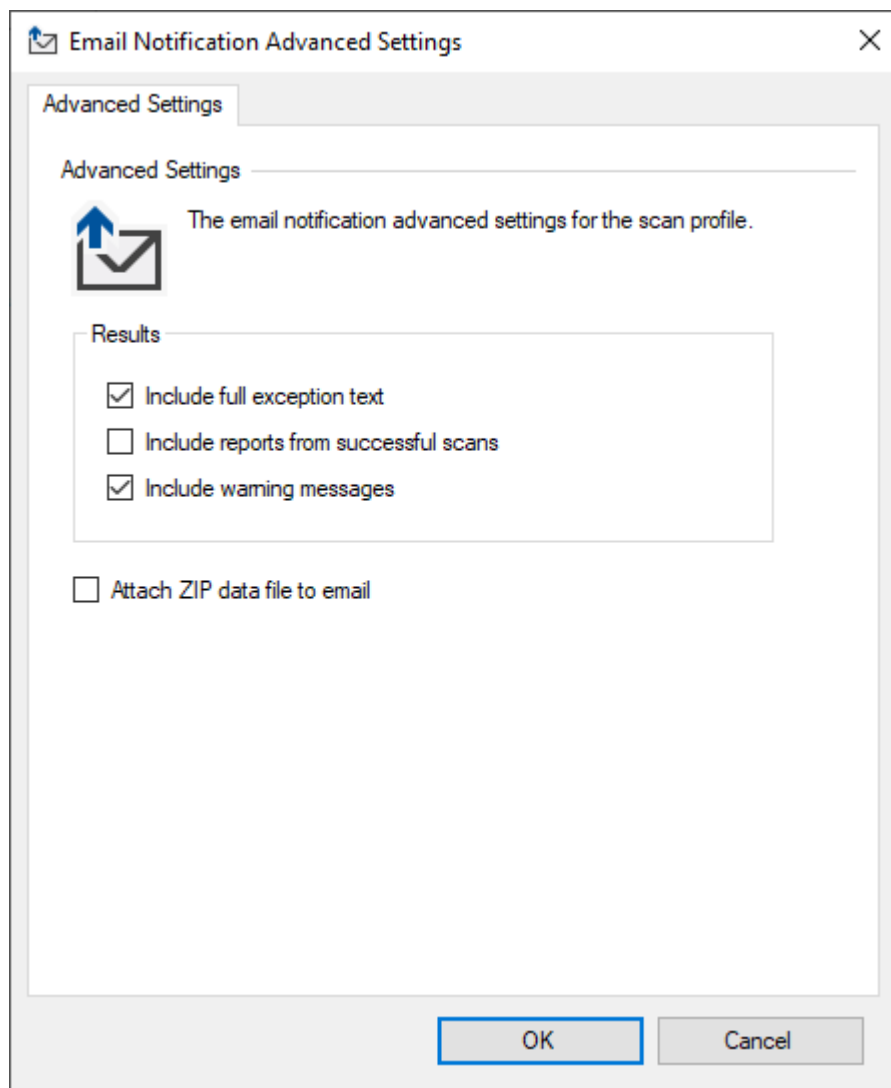
Message

The message body. This can include [variables](#).

Advanced

Displays the [email notification advanced settings](#) dialog.

Email Notification Advanced Settings



Include full exception text

Determines whether the full exception text should be included in the email for failed [scan tasks](#).

Include reports from successful scans

By default, only detailed information about failed scans is included, by selecting this option information about successful [scan tasks](#) is included in the notification

Include warning messages

Determines whether information about [warnings](#) should be included in the email for [scan tasks](#) that completed with [warnings](#).

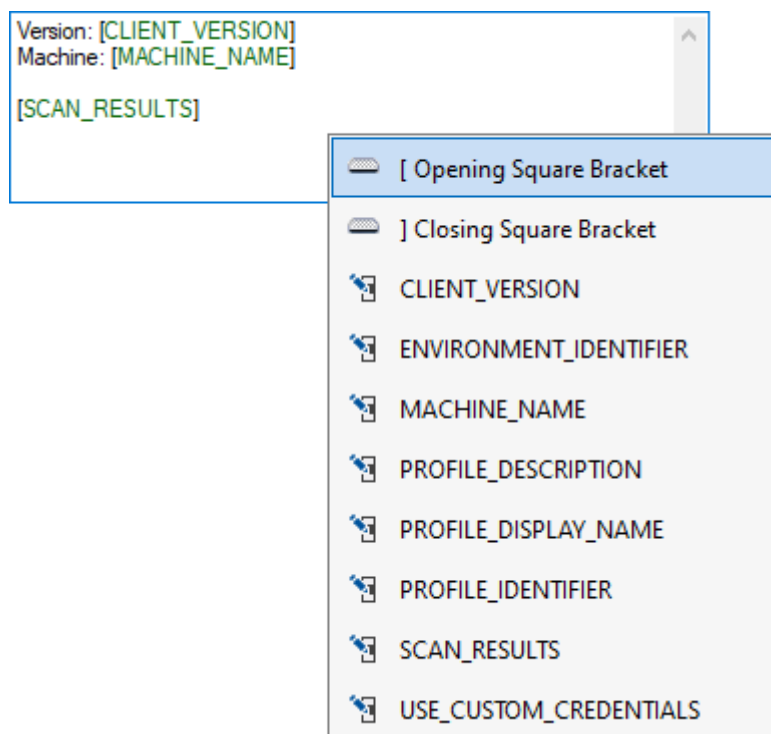
Attach ZIP data file to email

Determines whether the ZIP file created by the agent when running this [scan profile](#) should be attached to the email. For this option to be enabled the [create a ZIP file setting](#) must be enabled for

the [scan profile](#).

Email Notification Variables

Right clicking or pressing the [button whilst in a field in the [email notifications](#) user interface displays a context menu with the available variables.



[CLIENT_VERSION]

The version number of the [XIA Configuration Client](#) software.

[ENVIRONMENT_IDENTIFIER]

The [environment identifier](#) of the [scan profile](#) if configured.

[MACHINE_NAME]

The NetBIOS name of the computer running [XIA Configuration Client](#).

[PROFILE_DESCRIPTION]

The description of the [scan profile](#).

[PROFILE_IDENTIFIER]

The unique identifier of the [scan profile](#) in [GUID](#) format.

[PROFILE_DISPLAY_NAME]

The [display name](#) of the [scan profile](#).

[SCAN_RESULTS]

The [scan results](#) information.

[USE_CUSTOM_CREDENTIALS]

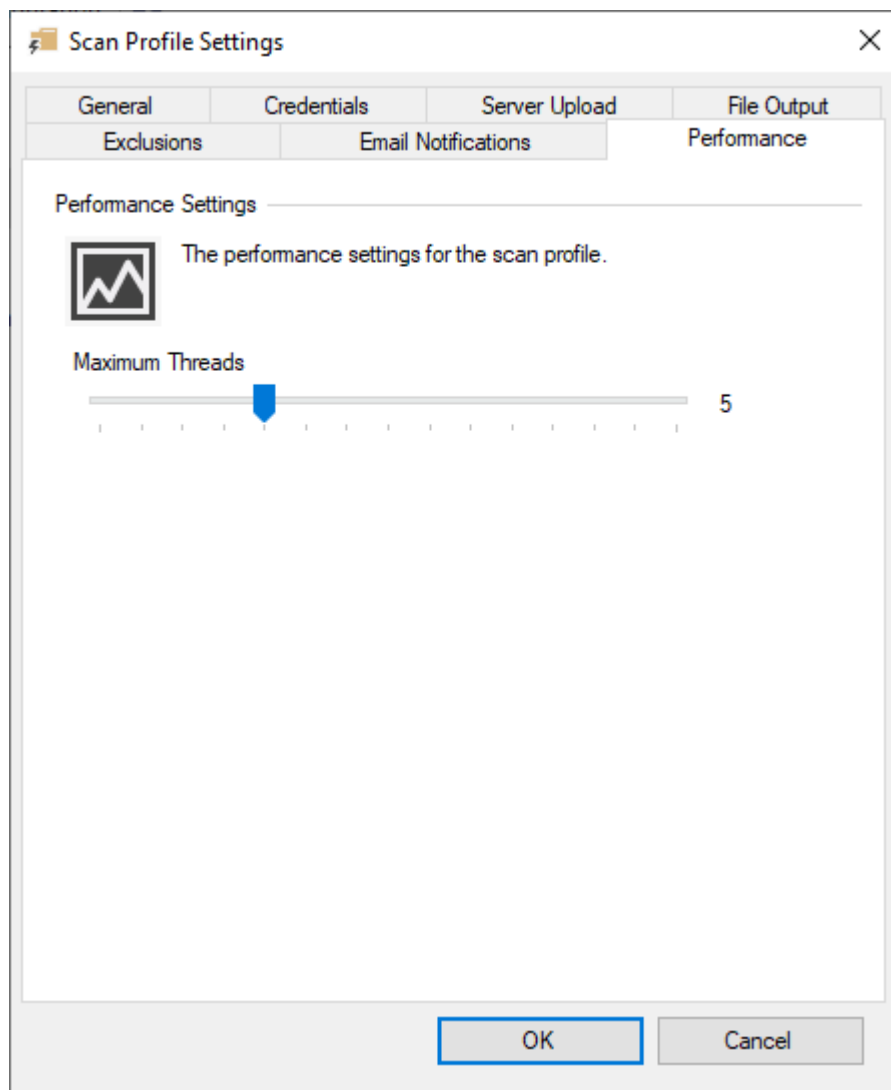
A true or false value that indicates whether the [scan profile](#) used [custom credentials](#).

Special Characters

The square brackets characters [and] are used to identify the variable tokens.

To include these characters in the property use the HTML entity numbers [for the opening bracket and] for the closing bracket.

Performance



Maximum Threads

Determines the number of [tasks](#) this [scan profile](#) will run simultaneously. The more threads configured the more quickly the scan may complete, however more processor and network resources will be used.

Scan Schedules

Scan schedules allow for [scan profiles](#) to be executed automatically at specific dates and times.



Scan Schedules

Provides the ability to configure schedules on which scans are to be executed.

New Scan Schedule

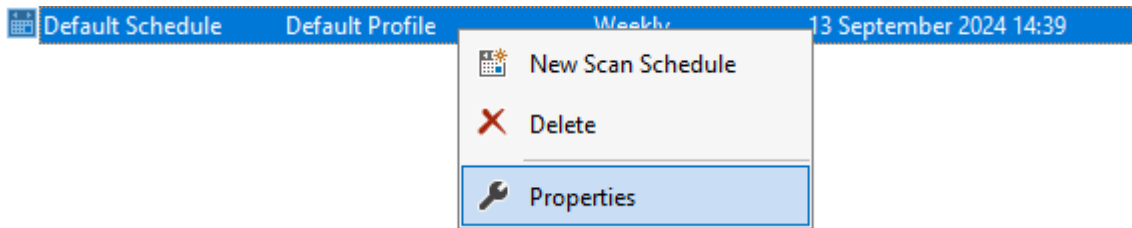
Display Name	Profile Name	Schedule Type	Next Execution Date
 Default Schedule	Default Profile	Weekly	13 September 2024 14:39

Multiple schedules can be created for a single [scan profile](#) if required.

Right clicking the listview displays the [context menu](#).

Context Menu

The context menu is displayed when right clicking in [scan schedule](#) user interface.



New Scan Schedule

Creates a new [scan schedule](#).

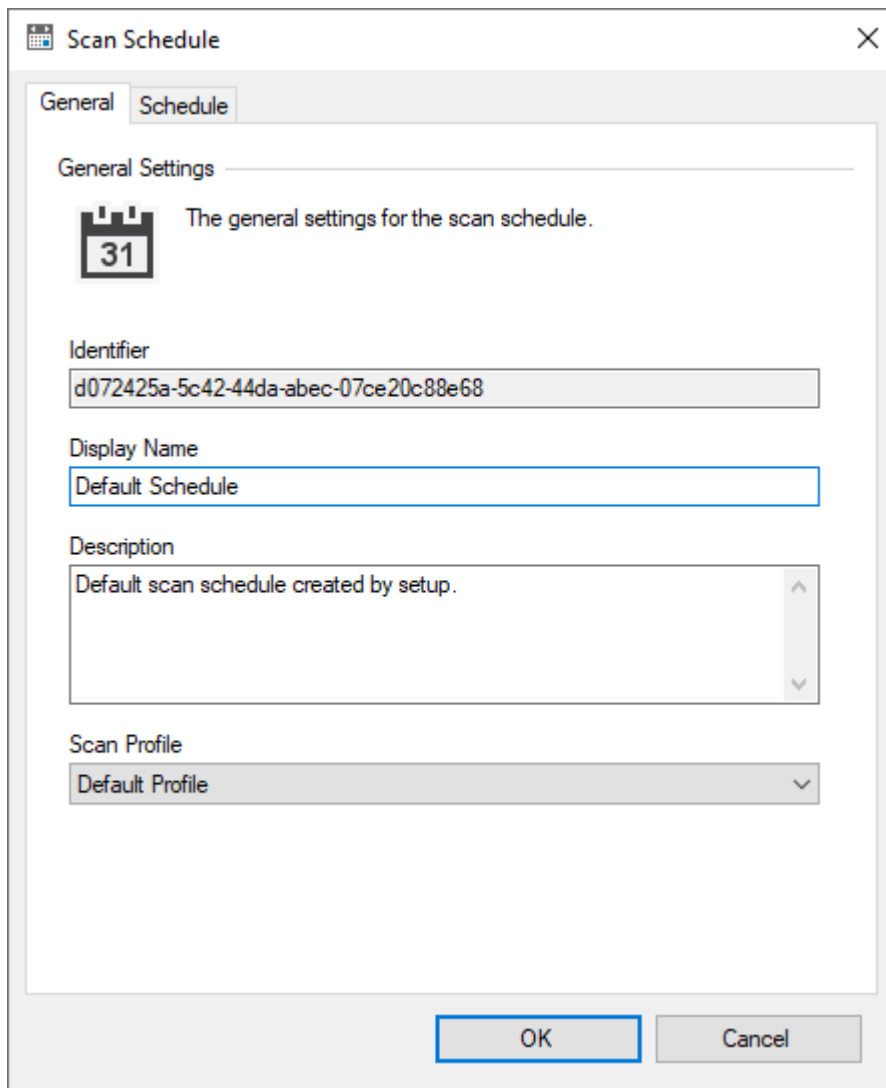
Delete

Deletes the currently selected [scan schedule](#).

Properties

Displays the [properties](#) of the currently selected [scan schedule](#).

Scan Schedule Settings



The screenshot shows a Windows-style dialog box titled "Scan Schedule" with a close button (X) in the top right corner. It has two tabs: "General" and "Schedule", with "Schedule" being the active tab. The "General Settings" section is highlighted with a horizontal line. Below this, there is a calendar icon showing the date "31" and the text "The general settings for the scan schedule." The "Identifier" field contains the GUID "d072425a-5c42-44da-abec-07ce20c88e68". The "Display Name" field contains "Default Schedule". The "Description" field contains "Default scan schedule created by setup." and has a vertical scrollbar. The "Scan Profile" dropdown menu is set to "Default Profile". At the bottom right, there are "OK" and "Cancel" buttons.

General Settings

The general settings for the scan schedule.

Identifier
d072425a-5c42-44da-abec-07ce20c88e68

Display Name
Default Schedule

Description
Default scan schedule created by setup.

Scan Profile
Default Profile

OK Cancel

Identifier

The unique identifier of the scan schedule in [GUID](#) format.

Display Name

The display name of the scan schedule.

Description

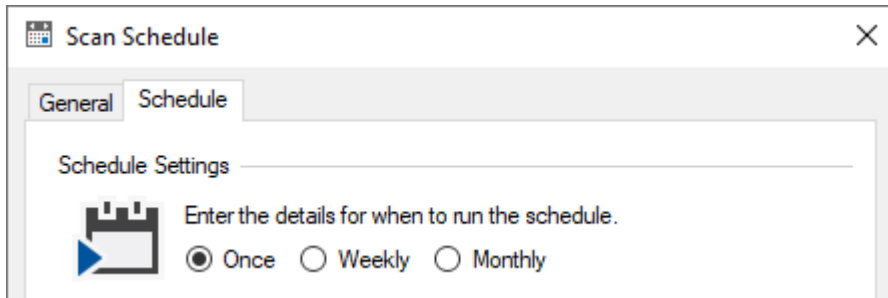
A description of the scan schedule.

Scan Profile

The [scan profile](#) that should be executed by the scan schedule.

Schedule

The schedule tab allows the assignment of the schedule using one of the following schedule types



Once

The [once schedule](#) causes the selected [scan profile](#) to be executed once at the specified date and time.

Weekly

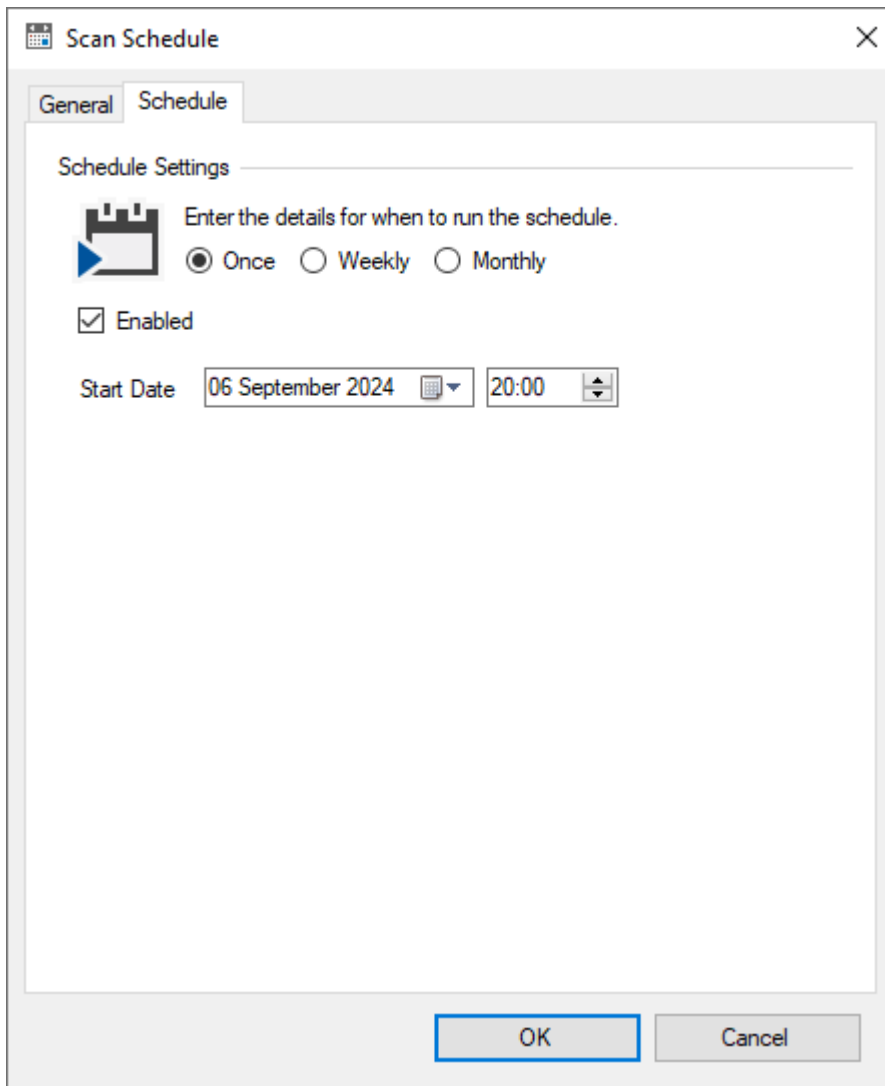
The [weekly schedule](#) causes the selected [scan profile](#) to be executed at the specified time on each of the selected days of the week.

Monthly

The [monthly schedule](#) causes the selected [scan profile](#) to be executed at the specified time on each of the selected days of the selected months.

Once

The [scan profile](#) will be executed once only at the specified date and time.



The image shows a 'Scan Schedule' dialog box with a close button (X) in the top right corner. It has two tabs: 'General' and 'Schedule', with 'Schedule' being the active tab. Under the 'Schedule Settings' section, there is a calendar icon and the text 'Enter the details for when to run the schedule.' Below this, there are three radio buttons: 'Once' (selected), 'Weekly', and 'Monthly'. There is also a checkbox labeled 'Enabled' which is checked. At the bottom, there is a 'Start Date' field showing '06 September 2024' with a calendar icon, and a time field showing '20:00' with a time selection icon. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Enabled

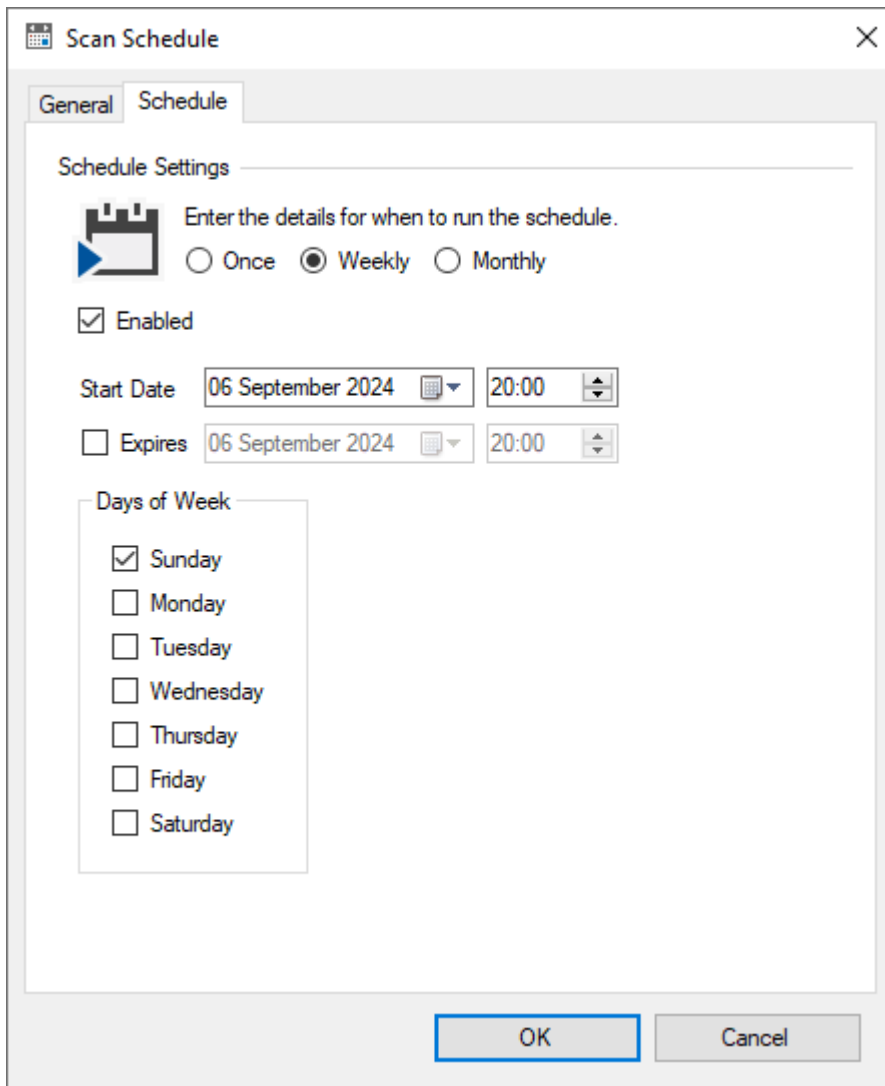
Determines whether the schedule is enabled.

Start Date

The date and time that the schedule will be executed.

Weekly

The [scan profile](#) will be executed at the specified time on each of the selected days of the week.



The image shows a 'Scan Schedule' dialog box with two tabs: 'General' and 'Schedule'. The 'Schedule' tab is active. Under 'Schedule Settings', there is a calendar icon and the text 'Enter the details for when to run the schedule.' Below this are three radio buttons: 'Once', 'Weekly' (which is selected), and 'Monthly'. There is a checked checkbox for 'Enabled'. The 'Start Date' is set to '06 September 2024' and the time is '20:00'. The 'Expires' checkbox is unchecked, with the same date and time. A 'Days of Week' section contains a list of days from Sunday to Saturday, with 'Sunday' checked and the others unchecked. At the bottom are 'OK' and 'Cancel' buttons.

Enabled

Determines whether the schedule is enabled.

Start Date

The date on which the schedule becomes effective, and the time on which the [scan profile](#) will be executed.

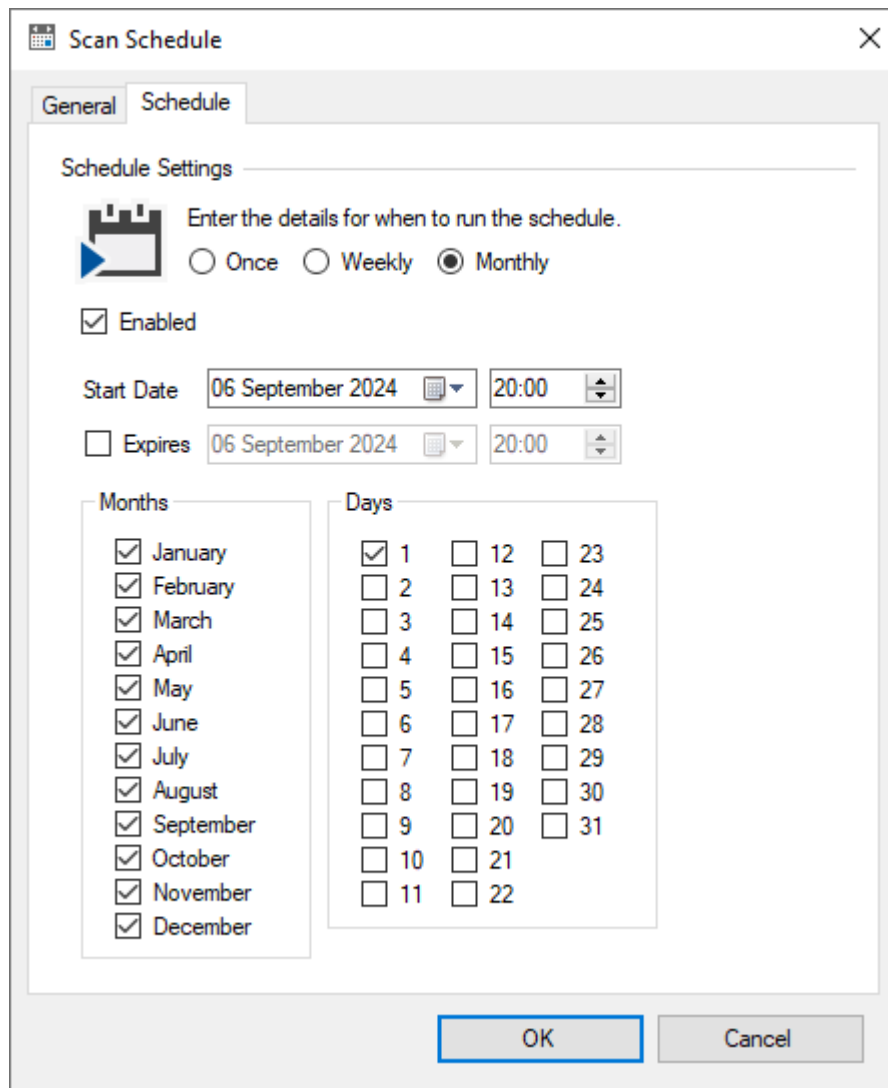
Expires

An optional date and time after which the schedule will no longer be effective.

Days of Week

The days of the week on which the [scan profile](#) will be executed.

Monthly



The image shows a 'Scan Schedule' dialog box with a 'General' tab and a 'Schedule' tab. The 'Schedule' tab is active, showing 'Schedule Settings'. A calendar icon is next to the text 'Enter the details for when to run the schedule.' Below this are three radio buttons: 'Once', 'Weekly', and 'Monthly'. The 'Monthly' radio button is selected. There is a checked checkbox for 'Enabled'. Below this are two date and time fields: 'Start Date' and 'Expires'. Both are set to '06 September 2024' and '20:00'. Below these are two sections: 'Months' and 'Days'. The 'Months' section has a list of months from January to December, all of which are checked. The 'Days' section has a grid of days from 1 to 31, with day 1 checked. At the bottom are 'OK' and 'Cancel' buttons.

Scan Schedule

General **Schedule**

Schedule Settings

Enter the details for when to run the schedule.

☐ Once ☐ Weekly ☒ Monthly

☒ Enabled

Start Date: 06 September 2024 20:00

☐ Expires: 06 September 2024 20:00

Months

- ☒ January
- ☒ February
- ☒ March
- ☒ April
- ☒ May
- ☒ June
- ☒ July
- ☒ August
- ☒ September
- ☒ October
- ☒ November
- ☒ December

Days

☒ 1	☐ 12	☐ 23
☐ 2	☐ 13	☐ 24
☐ 3	☐ 14	☐ 25
☐ 4	☐ 15	☐ 26
☐ 5	☐ 16	☐ 27
☐ 6	☐ 17	☐ 28
☐ 7	☐ 18	☐ 29
☐ 8	☐ 19	☐ 30
☐ 9	☐ 20	☐ 31
☐ 10	☐ 21	
☐ 11	☐ 22	

OK Cancel

Enabled

Determines whether the schedule is enabled.

Start Date

The date on which the schedule becomes effective, and the time on which the [scan profile](#) will be executed.

Expires

An optional date and time after which the schedule will no longer be effective.

Months

The months on which the [scan profile](#) will be executed.

Days

The days of the month on which the [scan profile](#) will be executed.

Scan Tasks

Each [scan profile](#) can be configured with one or more scan tasks that will be executed when the [scan profile](#) is started.



Scan Tasks

Configures the tasks that will be performed by this scan profile.

Start Scan Profile

Display Name	Status	Type
 Scan the local machine [DEMO-XCS-2022]	Enabled	Windows Machine List
 Search Active Directory domain	Enabled	Active Directory Search
 Scan the computer domain	Enabled	Active Directory Domain List
 Scan Exchange On-Premises organizations	Enabled	Exchange On-Premises
 Network device search	Enabled	Network Device Search

Start Scan Profile

Clicking start scan profile starts the execution of the currently selected [scan profile](#).

Right clicking a scan task displays the [context menu](#).

Active Directory Domain

The Active Directory domain [scan tasks](#) are able to document Microsoft on-premises [Active Directory](#) domains running on [Windows Server](#) 2012 and above using [PowerShell](#).

Active Directory List Scan Task

The Active Directory domain list [scan task](#) allows you to enter a list of [Active Directory](#) domain names to scan. The name of a domain controller may also be used to perform the scan against a specific machine.

Targets

The screenshot shows a Windows-style dialog box titled "Active Directory Domain List Scan Task". It has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the tab, there is a section titled "Active Directory Domain Targets" with a blue icon of a person. Below this is a text box labeled "Active Directory Domains or Domain Controllers" containing the text "demonstration.int". At the bottom of the tab are three checkboxes: "Scan the computer domain" (checked), "Scan the user domain" (unchecked), and "Recurse child domains" (unchecked). At the bottom of the dialog box are "OK" and "Cancel" buttons.

Active Directory Domains or Domain Controllers

The fully qualified DNS names of the Active Directory domains or a domain controller in a domain to scan, one per line. When the Scan Method of the [agent settings](#) is set to "Connect directly to Domain Controller" the value should be a domain controller name.

Scan the computer domain

Selecting this option causes the Active Directory domain of which the computer running the XIA Configuration Service is a member of to be scanned.

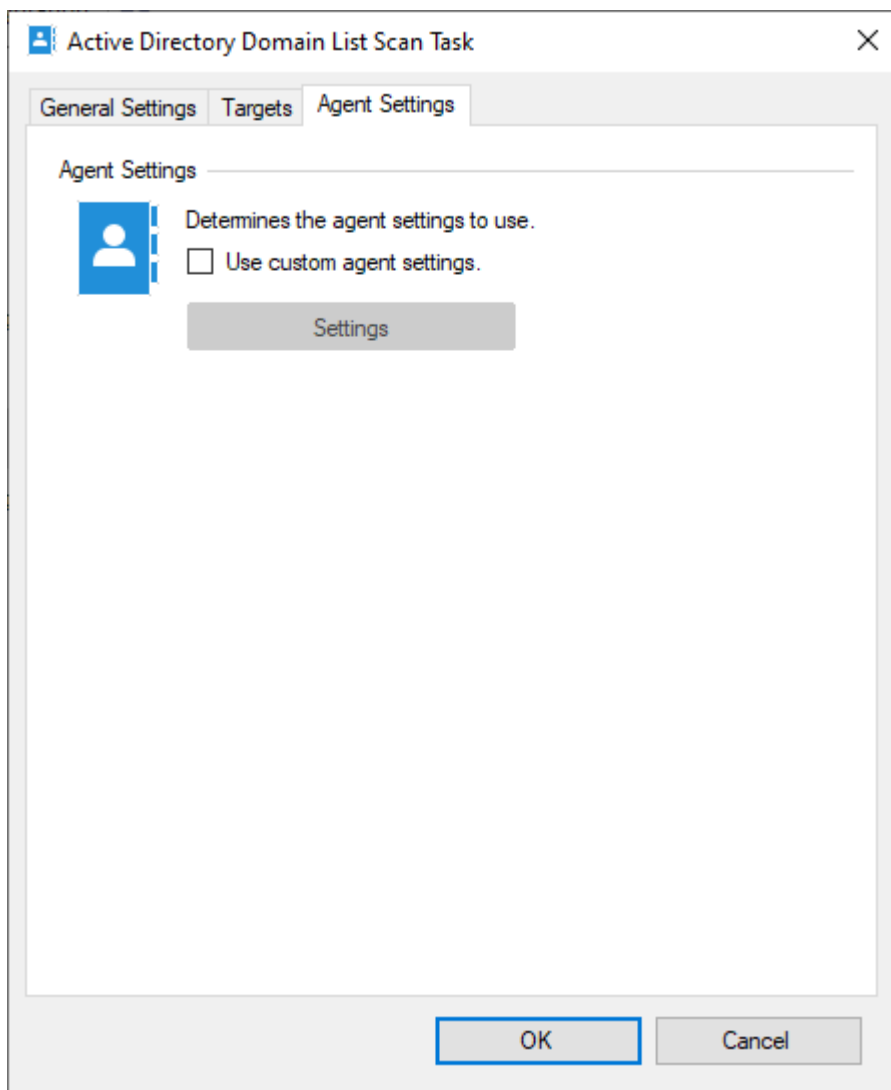
Scan the user domain

Selecting this option causes the Active Directory domain of which the user account running the XIA Configuration Service is a member of to be scanned.

Recurse child domains

Determines whether to scan child domains.

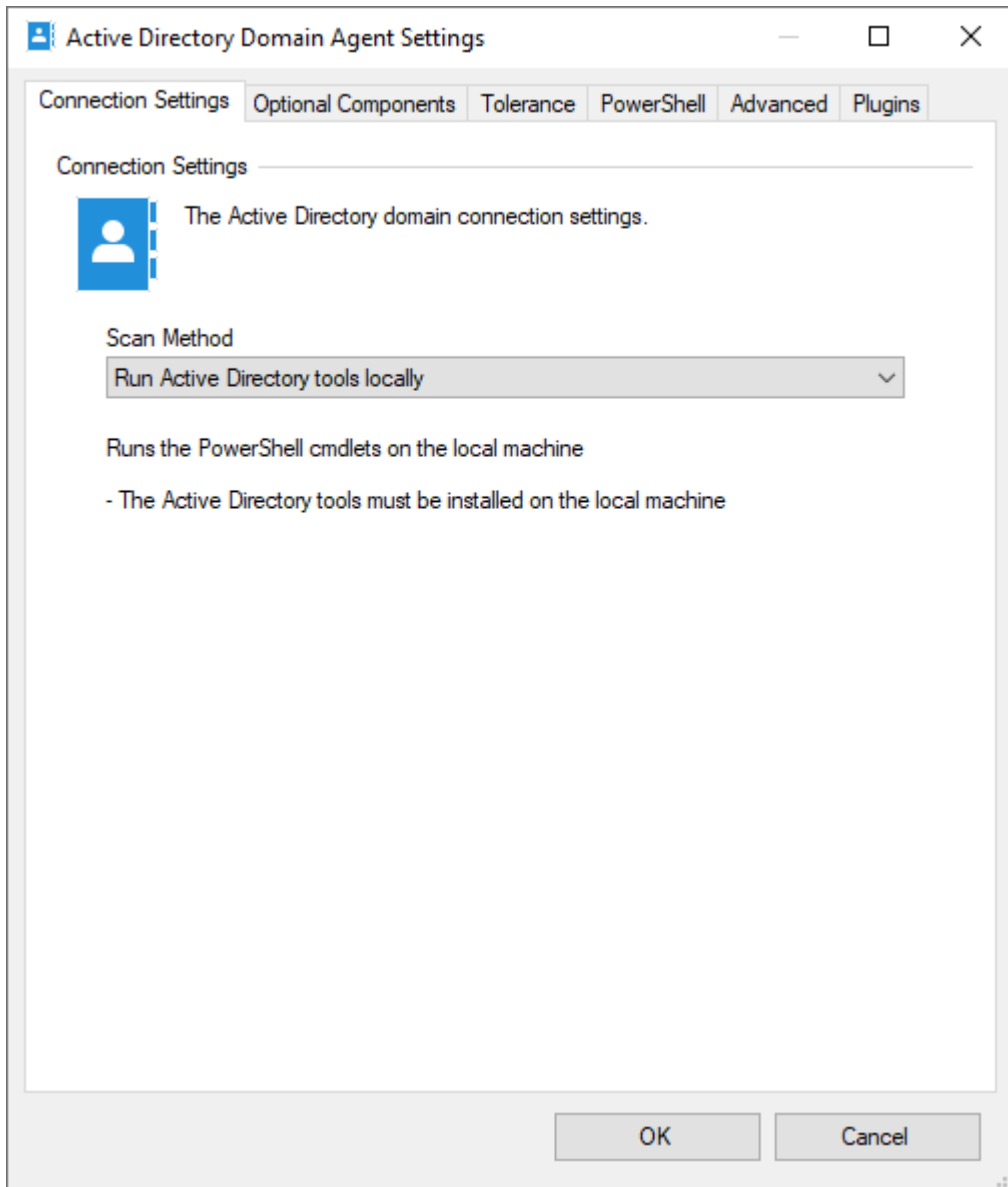
Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Agent Settings



Scan Method: Run Active Directory tools locally (default)

Runs the PowerShell cmdlets on the local machine.

- The Active Directory tools must be installed on the local machine running the [XIA Configuration Client](#).

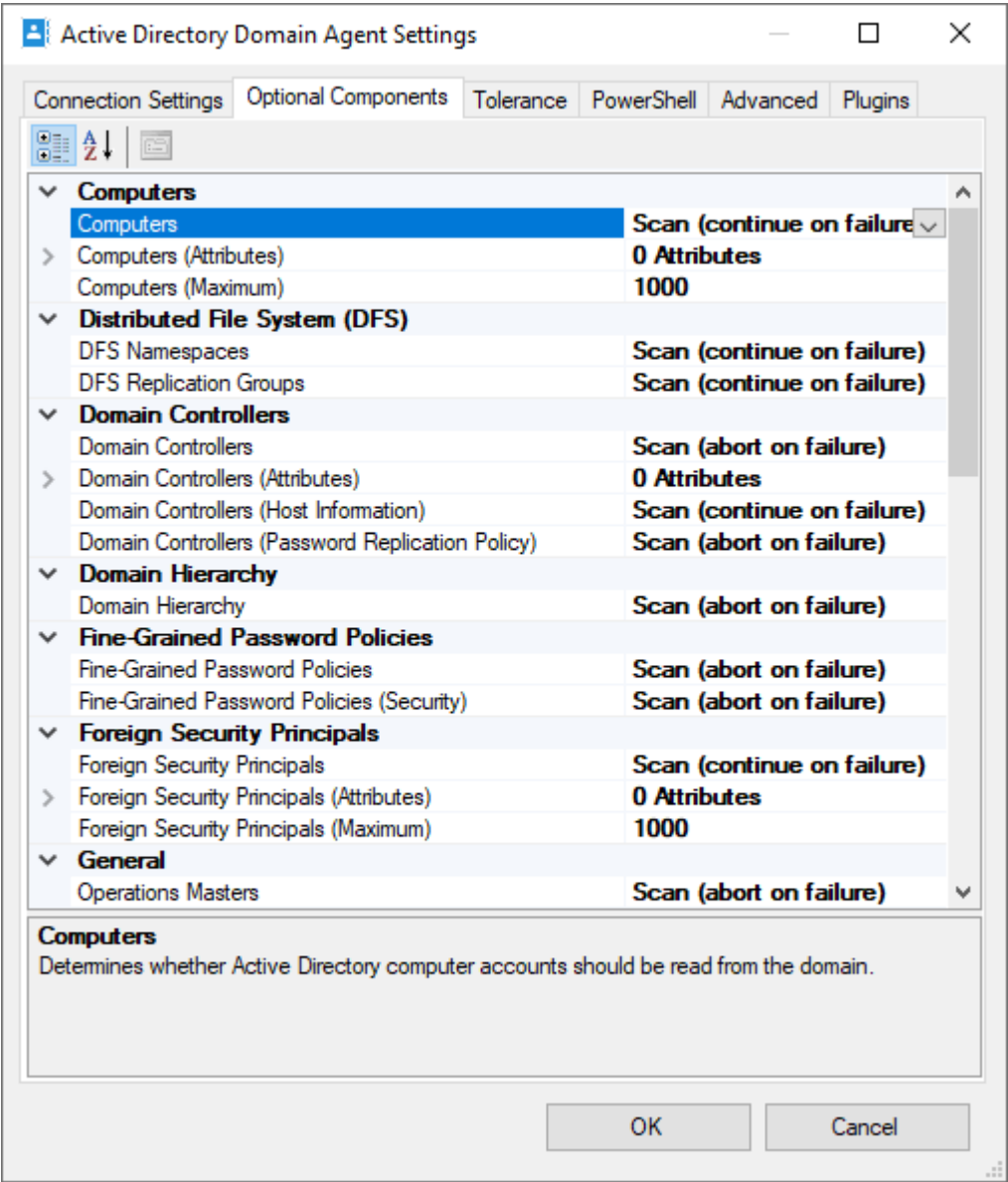
Scan Method: Connect directly to Domain Controller

Connects directly to a domain controller using [PowerShell remoting](#), and executes the PowerShell cmdlets directly on the domain controller.

- The Active Directory tools must be installed on the domain controller.

- The domain controller must be a global catalog.

Optional Components



Computers

Determines whether Active Directory computer accounts should be read from the domain.

Computers (Attributes)

The additional [attributes](#) to read for computer objects.

Computers (Maximum)

The maximum number of computers that the Active Directory domain can contain before the section is bypassed.

DFS Namespaces

Determines whether [DFS namespaces](#) should be read from the domain.

DFS Replication Groups

Determines whether [DFS replication groups](#) should be read from the domain.

Domain Controllers

Determines whether domain controllers are read for the domain.

Domain Controllers (Host Information)

Determines whether the host information is read for domain controllers in the domain.

Domain Controllers (Password Replication Policy)

Determines whether the password replication policy is read for domain controllers in the domain. This only applies to read-only domain controllers.

Domain Controllers (Attributes)

The additional [attributes](#) to read for domain controllers.

Domain Hierarchy

Determines whether the domain hierarchy is read for the domain.

Fine-Grained Password Policies

Determines whether the [fine-grained password policies](#) are read for the domain.

Fine-Grained Password Policies (Security)

Determines whether the security descriptor should be read for [fine-grained password policies](#).

Foreign Security Principals

Determines whether Active Directory foreign security principals should be read from the domain.

Foreign Security Principals (Attributes)

The additional [attributes](#) to read for foreign security principals.

Foreign Security Principals (Maximum)

The maximum number of foreign security principals that the Active Directory domain can contain before the section is bypassed.

Groups

Determines whether Active Directory [groups](#) should be read from the domain.

Groups (Attributes)

The additional [attributes](#) to read for [groups](#).

Groups (Maximum)

The maximum number of [groups](#) of the configured type that the Active Directory domain can contain before the section is bypassed.

Groups Scan Type

The type of [groups](#) to scan.

- Built-in
- Security
- All

Group Policy Hierarchy

Determines whether the Group Policy hierarchy is read for the domain.

Group Policy Objects

Determines whether the Group Policy objects are read for the domain.

Group Policy Objects (Settings)

Determines whether the settings for individual Group Policy objects are read for the domain.

Managed Service Accounts

Determines whether Active Directory [managed service accounts](#) should be read from the domain.

Managed Service Accounts (Attributes)

The additional attributes to read for [managed service accounts](#).

Managed Service Accounts (Maximum)

The maximum number of [managed service accounts](#) that the Active Directory domain can contain before the section is bypassed.

Operations Masters

Determines whether information about the operations masters should be read for the domain.

Recycle Bin

Determines whether information about the [Active Directory recycle bin](#) should be read for the domain.

Replication Inter-Site Transports

Determines whether information about the Active Directory inter-site transports should be read for the domain.

Replication Site Links (Security)

Determines whether the security descriptor should be read for [replication site links](#).

Replication Sites

Determines whether information about the Active Directory [replication sites](#) should be read for the domain.

Replication Sites (Security)

Determines whether the security descriptor should be read for [replication sites](#).

Replication Sites (Servers)

Determines whether the servers should be read for [replication sites](#).

Replication Subnets

Determines whether information about the Active Directory [replication subnets](#) should be read for the domain.

Schema Attributes

Determines whether information about the Active Directory [schema attributes](#) should be read for the domain.

Schema Attributes (Include Schema Base Objects)

Determines whether to include schema base objects when reading [schema attributes](#).

Schema Classes

Determines whether information about the Active Directory [schema classes](#) should be read for the domain.

Schema Classes (Include Schema Base Objects)

Determines whether to include schema base objects when reading [schema classes](#).

Starter Group Policy Objects

Determines whether the [Starter Group Policy objects](#) are read for the domain.

Starter Group Policy Object (Settings)

Determines whether the settings for individual [Starter Group Policy objects](#) are read for the domain.

Trusts

Determines whether the trusts are read for the domain.

Users

Determines whether Active Directory user accounts should be read from the domain.

Users (Attributes)

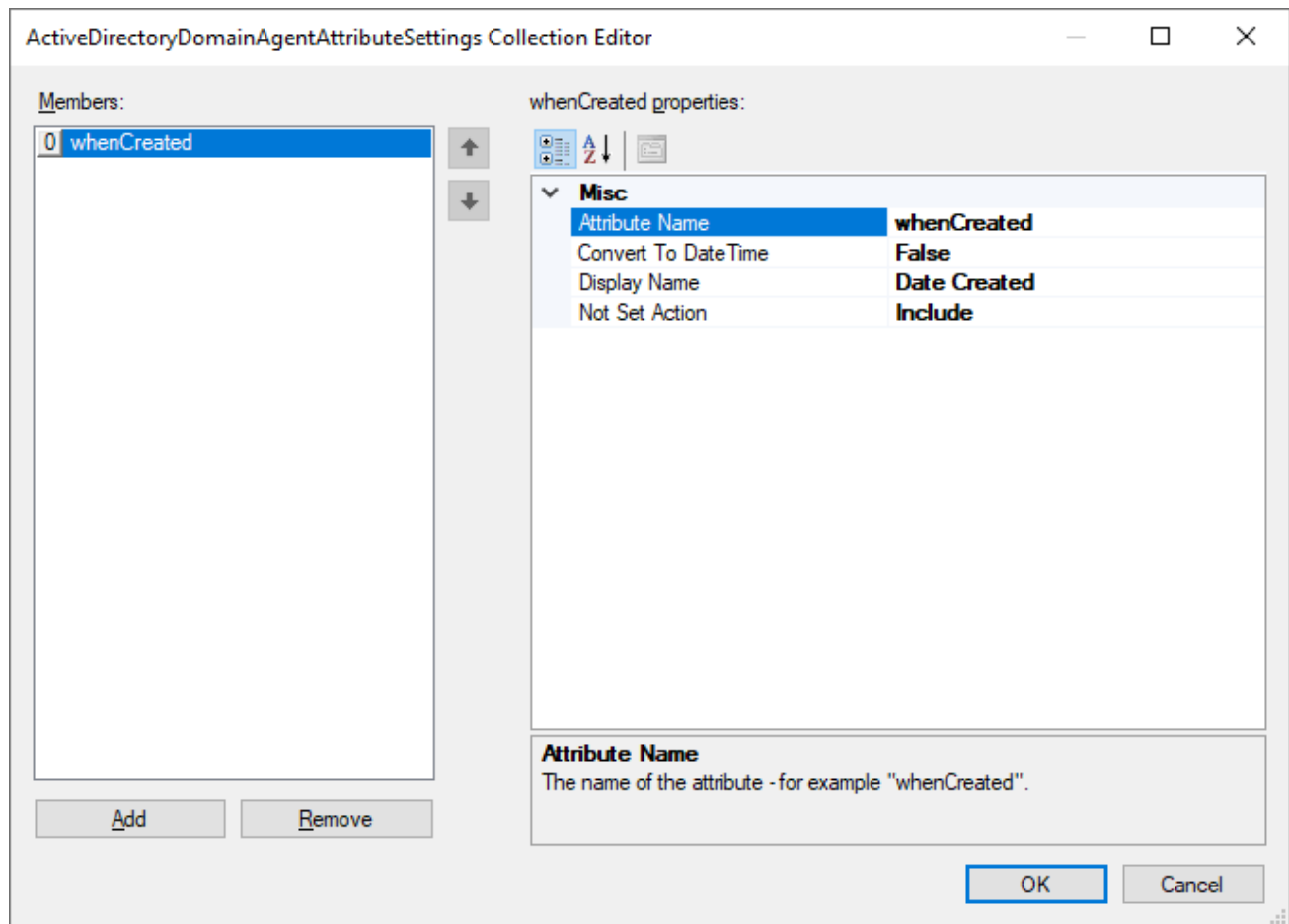
The additional attributes to read for user objects.

Users (Maximum)

The maximum number of users that the Active Directory domain can contain before the section is bypassed.

Active Directory Attributes

It is possible to collect information from additional [Active Directory attributes](#) where the value is a [supported value type](#).



Attribute Name

The [Active Directory attribute](#) name.

Convert To DateTime

Determines whether values should be converted to [System.DateTime](#) values. This applies when the date is stored in the directory as a large integer attribute or string value.

Display Name

The name to display for the attribute in the user interface and output. This can be the same as the attribute name.

Not Found Action

Determines the action to take if the [Active Directory attribute](#) is not set.

- Include - the attribute is always included.

- Exclude - the attribute is excluded.
- Throw Exception - the scan will fail if the attribute is not set.

Active Directory Attribute Value Types

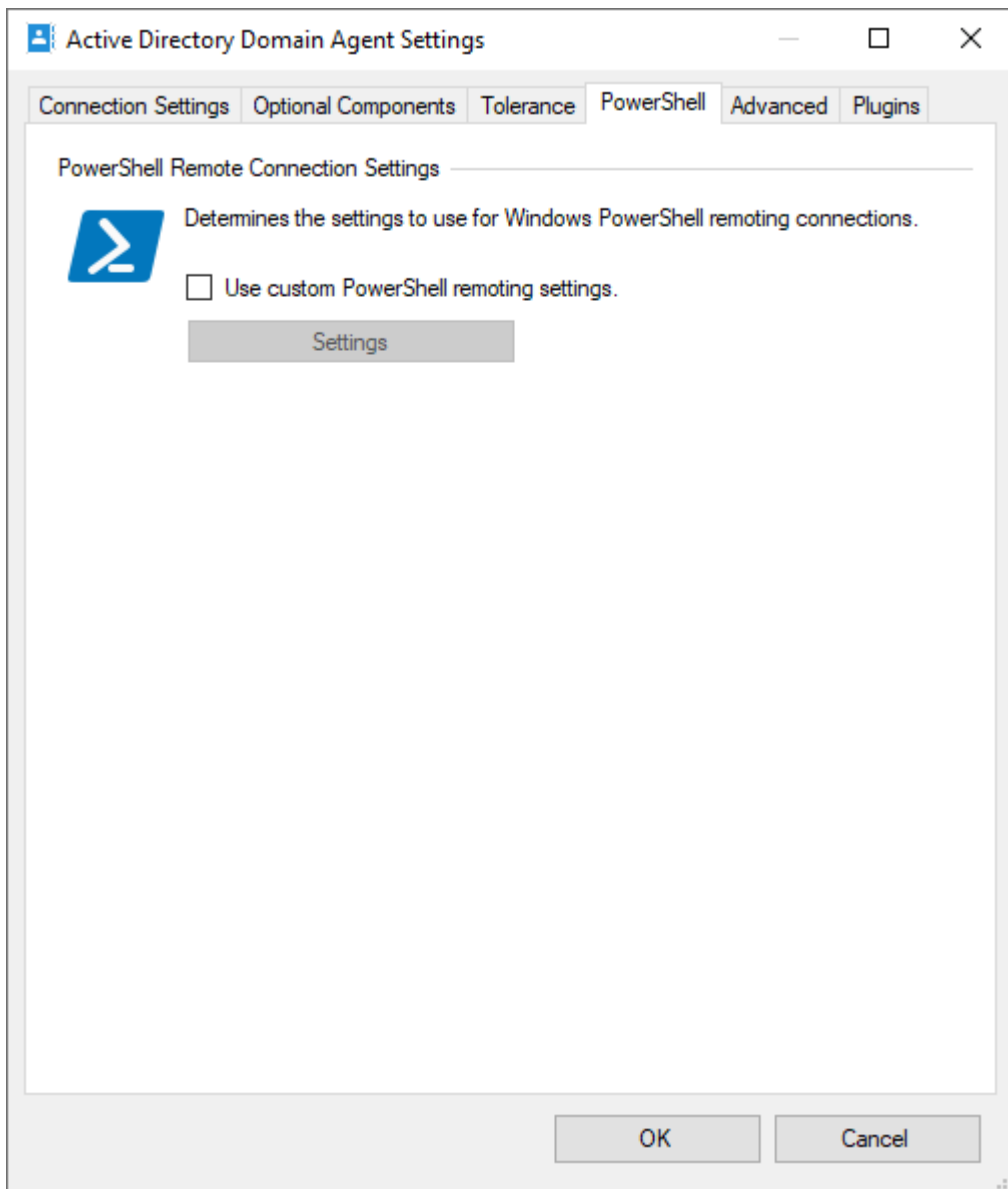
The following [Active Directory attributes](#) value types are supported

- Boolean
- Case Insensitive String
- Distinguished Name
- DN Binary
- IA5-String
- Integer
- Large Integer / Interval
- Numerical String
- Object Identifier
- Unicode String
- UTC Coded Time

The following attribute types are not decoded and are not supported. Information from these attributes can be gathered using [agent plugins](#).

- NT Security Descriptor
- Octet String
- SID

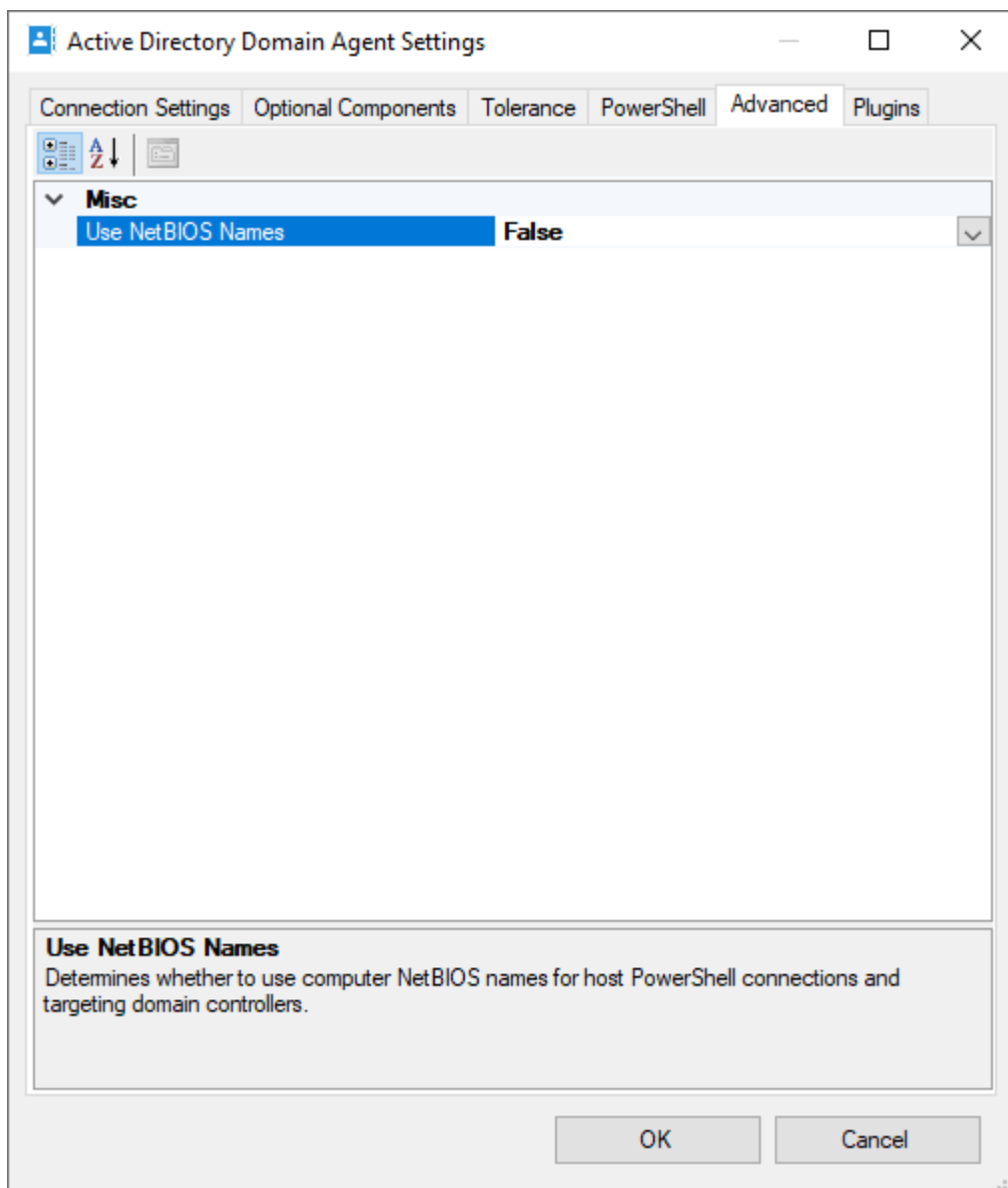
PowerShell



Use custom PowerShell remoting settings

Determines whether to use custom [PowerShell connection settings](#).

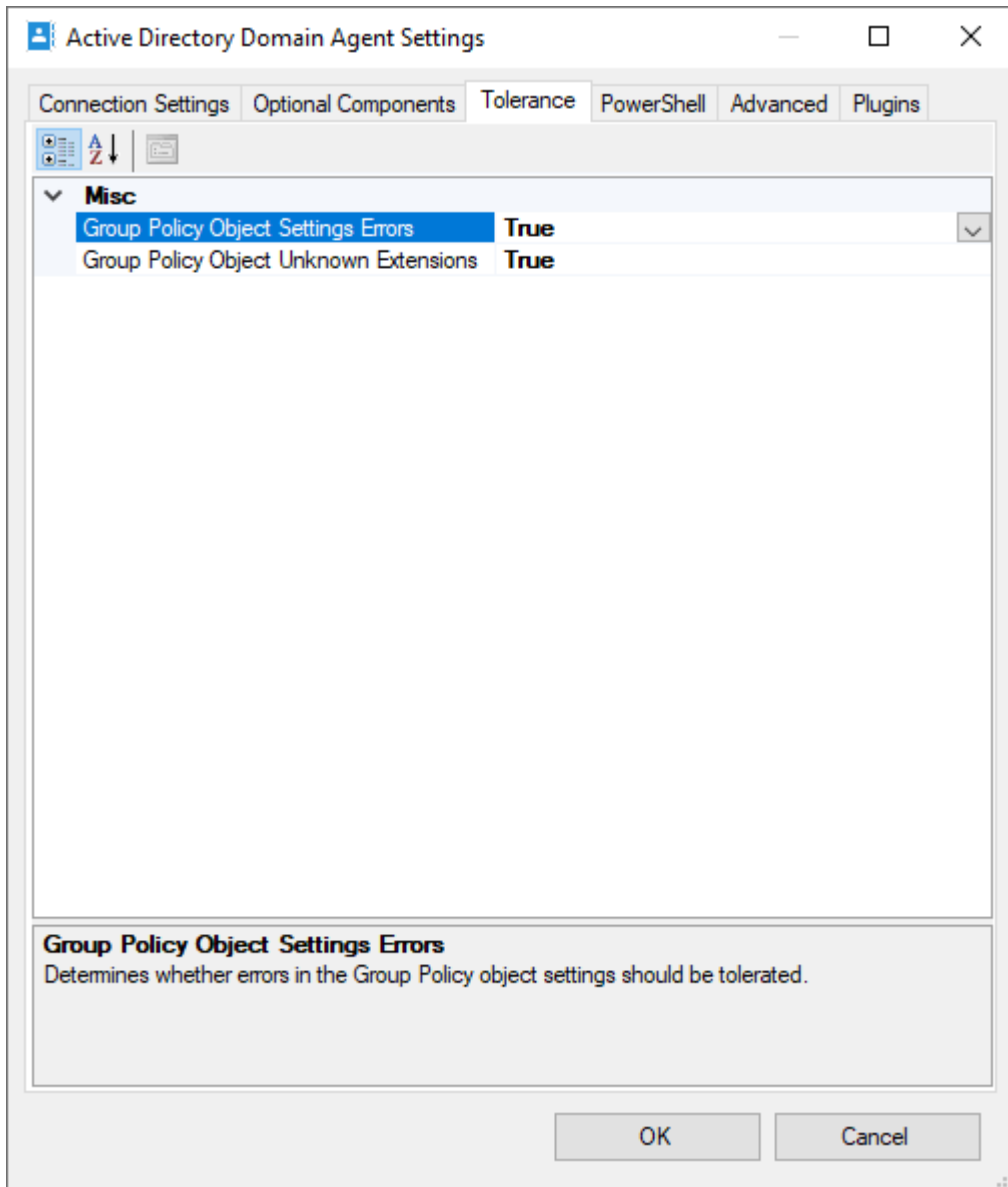
Advanced



Use NetBIOS Names

Determines whether to use computer NetBIOS names for host PowerShell connections and targeting domain controllers.

Tolerance Settings



Group Policy Object Settings Errors

Determines whether errors in the Group Policy object settings should be tolerated.

Group Policy Object Unknown Extensions

Determines whether unknown extensions in the Group Policy object settings should be tolerated. This can lead to incomplete information being collected.

Item Identifiers

For more information please see the [item identifiers](#) section.

Primary Identifier

The domain DNS name.

Secondary Identifier

The security identifier (SID) of the domain.

Tertiary Identifier

Not used

Requirements

Supported Target Systems

The Active Directory domain [scan tasks](#) are supported on the following [Active Directory](#) domain versions

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Access Settings

- Domain user credentials are required to scan the Active Directory domain.
- When reading Group Policy settings, the user should have **Read** permissions to all Group Policy objects.
- To obtain more detailed information about the domain controllers on the network including serial number, manufacturer and model, the user credentials must have administrator rights on the remote domain controllers.

Active Directory PowerShell Module

The agent requires that the [Active Directory PowerShell module](#) is installed.

Distributed File System

To read distributed file system namespaces and replication groups the [DFS Management Tools](#) must be installed. For more information see the [DFS Management Tools](#) section.

Group Policy Objects

To read Group Policy objects the [Group Policy management console](#) must be installed.

Windows Firewall (Run Active Directory tools locally)

When the [scan method](#) is set to [Run Active Directory tools locally](#) the following ports must be open on the domain controller.

- ✓ Active Directory Web Services (TCP-In)

Required for the execution of the [Active Directory PowerShell module](#).

✓ mDNS (UDP-In)

This is only required when using NetBIOS names for the [DFS Management Tools](#).

✓ Active Directory Domain Controller - LDAP (TCP-In)

Required for LDAP connections for the [DFS Management Tools](#) and [Group Policy Management Console](#).

✓ Active Directory Domain Controller - LDAP (UDP-In)

Required for LDAP connections for the [DFS Management Tools](#) and [Group Policy Management Console](#).

Windows Firewall (Connect directly to Domain Controller)

When the [scan method](#) is set to [Connect directly to Domain Controller](#) the following ports must be open on the domain controller.

✓ Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

Windows Firewall (Hosts)

To obtain more detailed information about the domain controllers on the network such as serial number and manufacturer.

✓ Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

Local Service

The Active Directory domain [scan tasks](#) do not support the [local service](#).

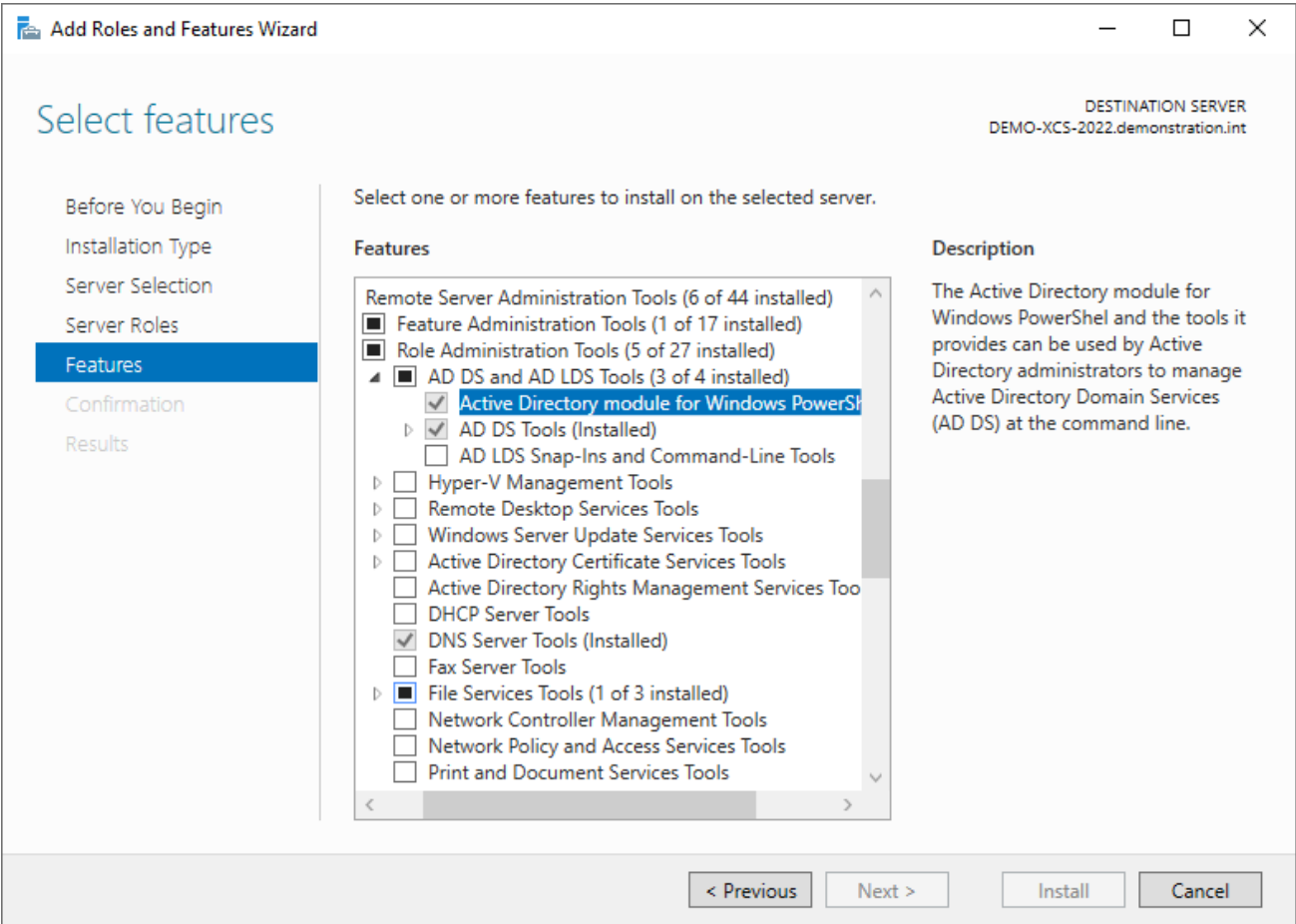
Active Directory PowerShell module

To read an [Active Directory domain](#) the Active Directory PowerShell module must be installed.

Installation (Windows Server)

To install the Active Directory PowerShell module on Windows Server install the following Windows Server feature

Remote Server Administration Tools > AD DS and AD LDS Tools > Active Directory module for Windows PowerShell.



Installation (Windows Server PowerShell)

To install the Active Directory PowerShell module on Windows Server using Windows PowerShell execute the following command.

Install-WindowsFeature "RSAT-AD-PowerShell"

Installation (Windows 10/Windows 11)

To install the Active Directory PowerShell module on Windows 10 or Windows 11 go to

Settings > Apps > Option Features > Add a feature > RSAT: Active Directory Domain Services and Lightweight Directory Services Tools

Add an optional feature

RSAT: Active Directory Domain Services and Lightweight Directory Services Tools



Sort by: Name ▾



RSAT: Active Directory Domain Services and Lightweight Directory Services Tools

37.5 MB

Install (0)

Cancel

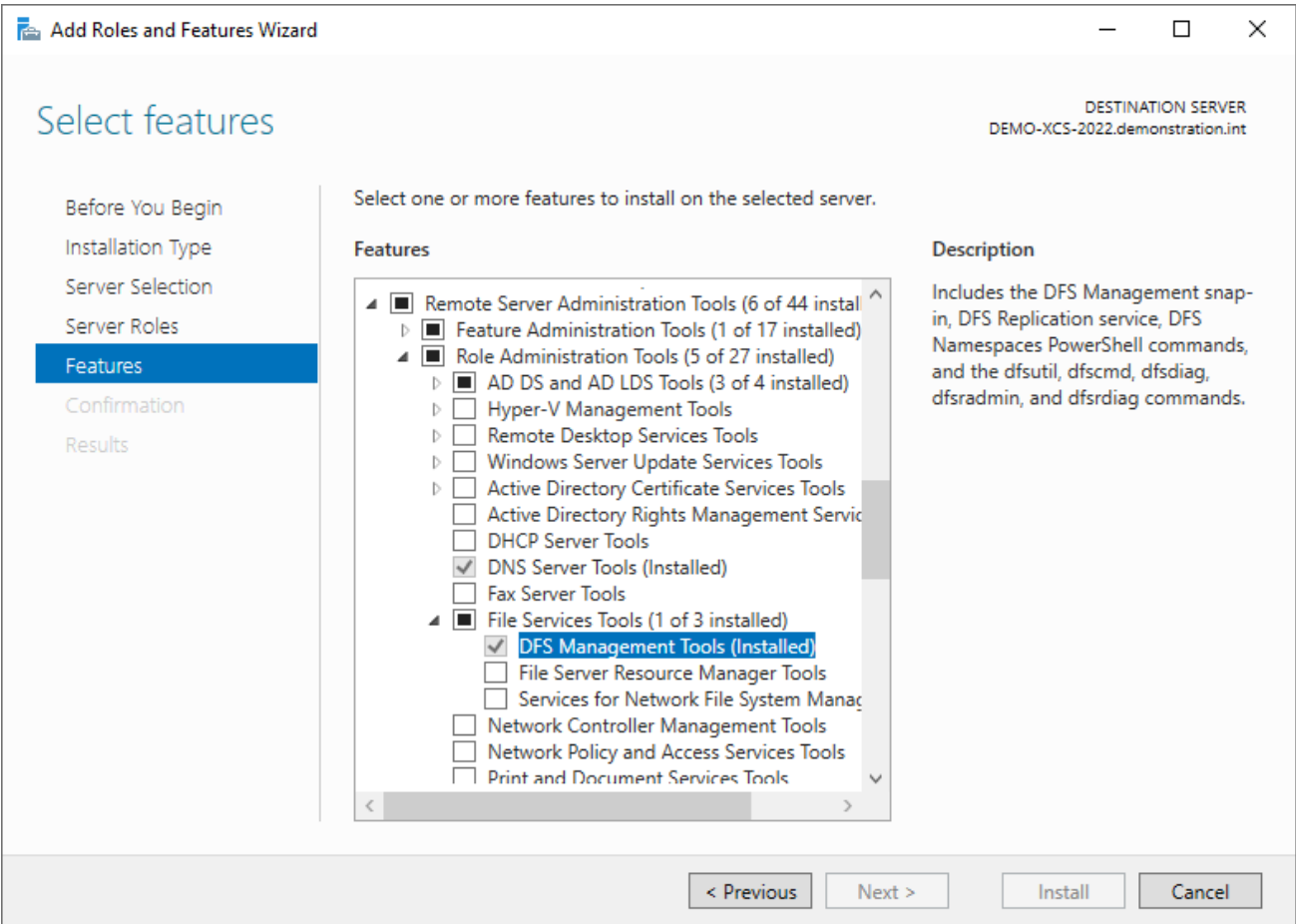
DFS Management Tools

To read the [DFS namespaces](#) or [DFS replication groups](#) in an [Active Directory domain](#) the DFS Management Tools must be installed.

Installation (Windows Server)

To install the DFS Management Tools on Windows Server install the Windows Server feature

Remote Server Administration Tools > File Services Tools > DFS Management Tools



Installation (Windows Server PowerShell)

To install the DFS Management Tools on Windows Server using Windows PowerShell execute the following command.

```
Install-WindowsFeature "RSAT-DFS-Mgmt-Con"
```

Installation (Windows 10/Windows 11)

To install the DFS Management Tools on Windows 10 or Windows 11 goto

Settings > Apps > Option Features > Add a feature > RSAT: File Services Tools

Add an optional feature

RSAT: File Services Tools



Sort by: **Name** ▾



RSAT: File Services Tools

26.7 MB

Install (1)

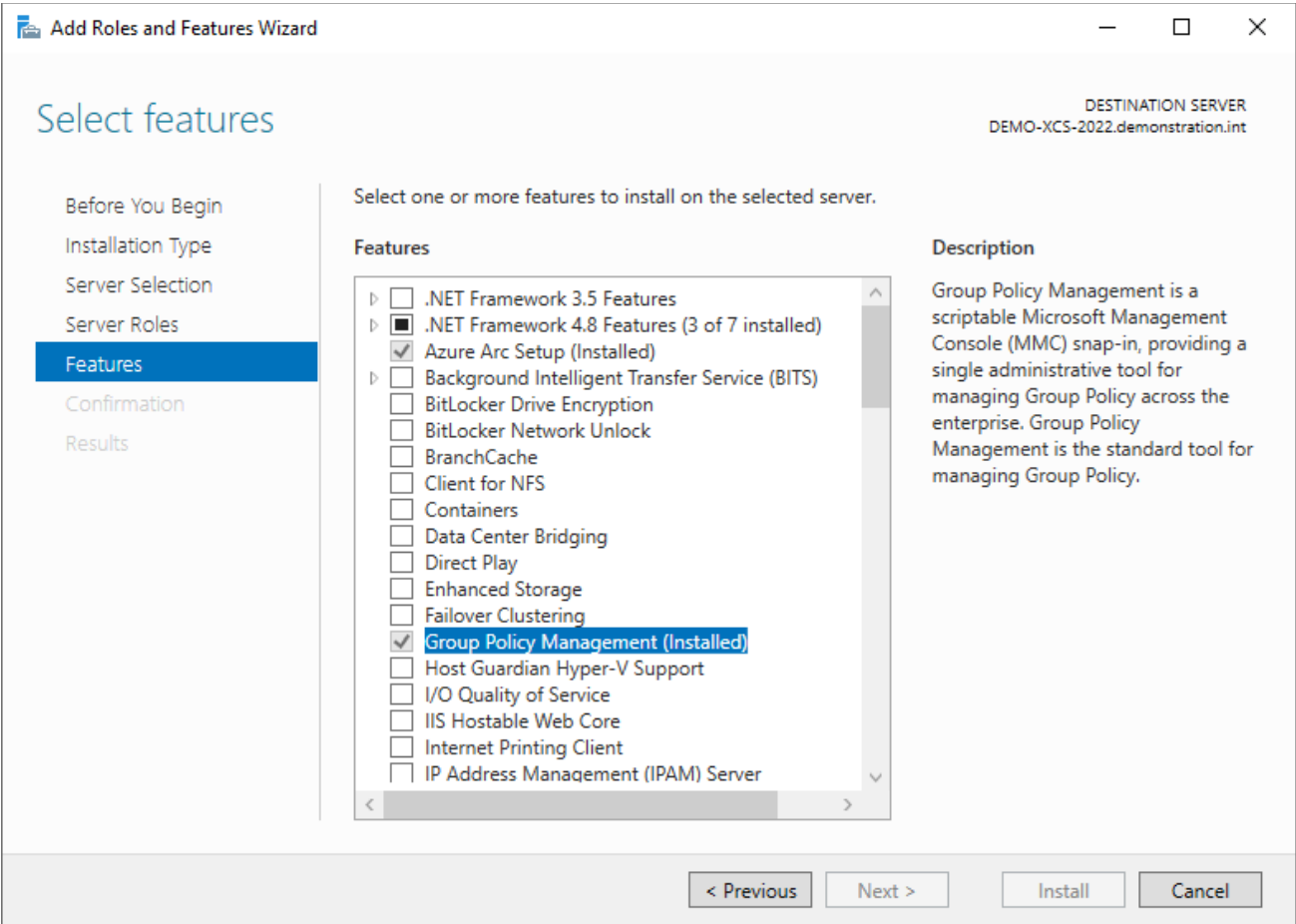
Cancel

Group Policy Management Console

To read the Group Policy information in an [Active Directory domain](#) the Group Policy Management Console must be installed.

Installation (Windows Server)

To install the Group Policy Management Console on Windows Server install the Windows Server feature



Installation (Windows Server PowerShell)

To install the Group Policy Management Console on Windows Server using Windows PowerShell execute the following command.

Install-WindowsFeature "GPMC"

Installation (Windows 10/Windows 11)

To install the Group Policy Management Console on Windows 10 or Windows 11 goto

Settings > Apps > Option Features > Add a feature > RSAT: Group Policy Management Tools

Add an optional feature

RSAT: Group Policy Management Tools



Sort by: Name ▾



RSAT: Group Policy Management Tools

16.1 MB

Install (0)

Cancel

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

The Active Directory PowerShell module is not installed

Symptoms

When you scan an [Active Directory domain](#), you see the following error

The Active Directory PowerShell module is not installed.

Cause

This can occur if the Active Directory PowerShell module is not installed.

Resolution

- Install the [Active Directory PowerShell module](#).

More Information

For more see the [Active Directory PowerShell module](#) section.

The domain functionality '10' is unknown

Symptoms

When you scan an [Active Directory domain](#), you see the following error

The domain functionality '10' is unknown.

Cause

This can occur when a domain is running in Windows Server 2025 domain functional level

Resolution

Update to the latest version of XIA Configuration.

<https://www.centrel-solutions.com/xiaconfiguration/download.aspx>

More Information

Support for Windows Server 2025 was added in XIA Configuration version 16.2.

The Distributed File System (DFS) tools are not installed

Symptoms

When you scan an [Active Directory domain](#), you see the following error

The Distributed File System (DFS) tools are not installed.

Cause

This can occur Distributed File System (DFS) tools are not installed and DFS namespaces or replication groups exist in the domain.

Resolution

Install the Distributed File System (DFS) tools.

More Information

For more see the [DFS Management Tools](#) section.

The Group Policy Management Console (GPMC) is not installed

Symptoms

When you scan an [Active Directory domain](#), you see the following error

The Group Policy Management Console (GPMC) is not installed.

Cause

This can occur if the Group Policy Management console is not installed.

Resolution

- Install the [Group Policy Management Console](#).
- or -
- Set the Group Policy related [optional components](#) to **Do Not Scan**.

More Information

For more see the [Group Policy Management Console](#) section.

The Group Policy object was not found in the SYSVOL

Issue

When viewing an [Active Directory domain](#) you may see the following warning.

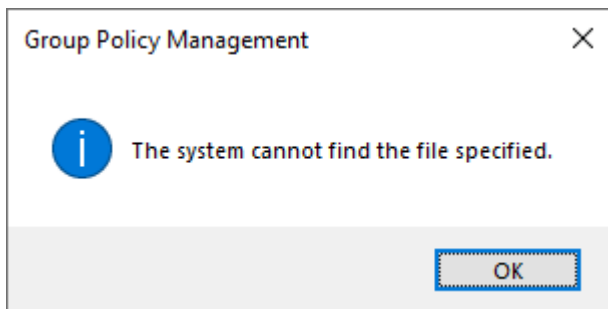
The Group Policy object was not found in the SYSVOL

Cause

This issue is caused when a Group Policy object is configured in Active Directory however is not found in the SYSVOL location.

Resolution

Open the Group Policy Management Console and select the Group Policy object specified in the warning. If there are files missing or SYSVOL corruption the following error message will be displayed.



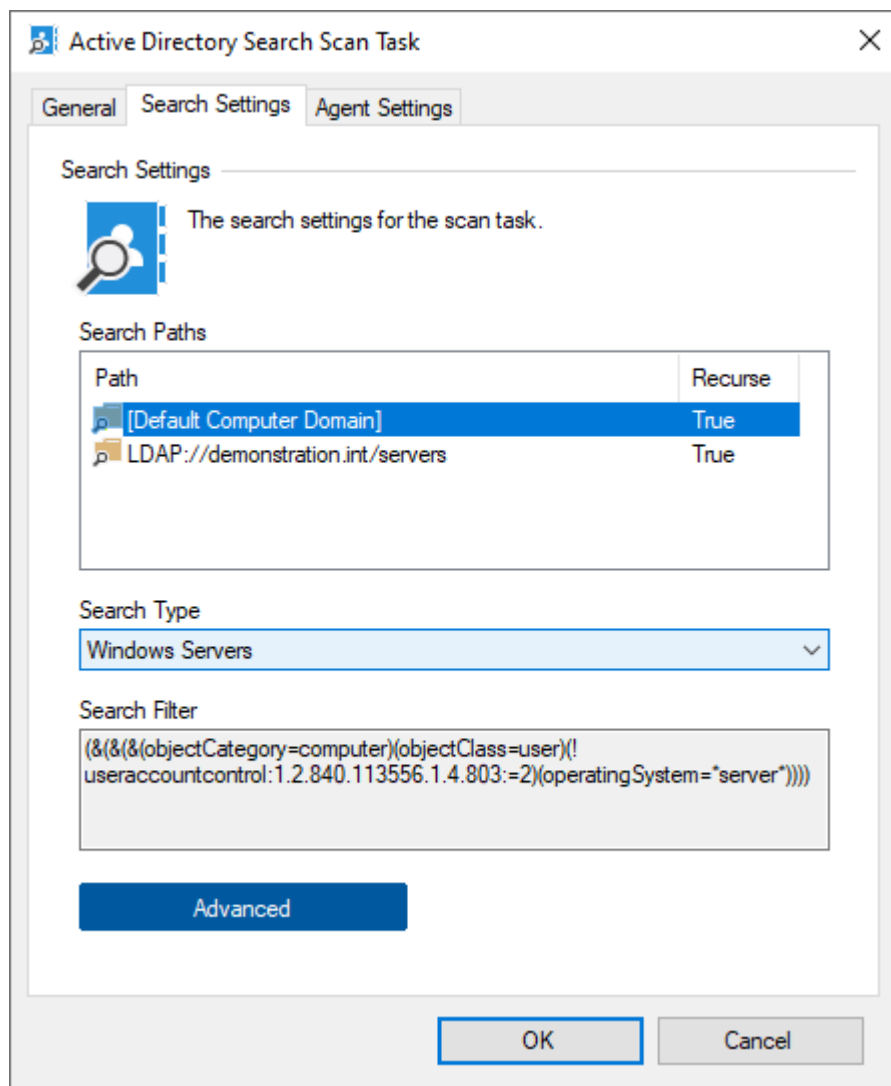
NOTE: ensure that replication is working correctly in the environment as it may be that the files are available on the domain controller you are viewing however not on the specific domain controller that was being used by the [XIA Configuration Client](#) during the scan.

Active Directory Search

The Active Directory search task allows you to search one or more [Active Directory domains](#) for [Windows workstations and servers](#) to document.

Search Settings

The following settings are available for the [Active Directory search](#) scan task.



Search Paths

The Active Directory domains or custom LDAP paths to search.
Right clicking the search paths listview displays the [search paths context menu](#).

Search Type

Determines the LDAP query used to locate systems within Active Directory.

- Custom
- Windows Servers
- Windows Workstations
- Windows Workstations and Servers

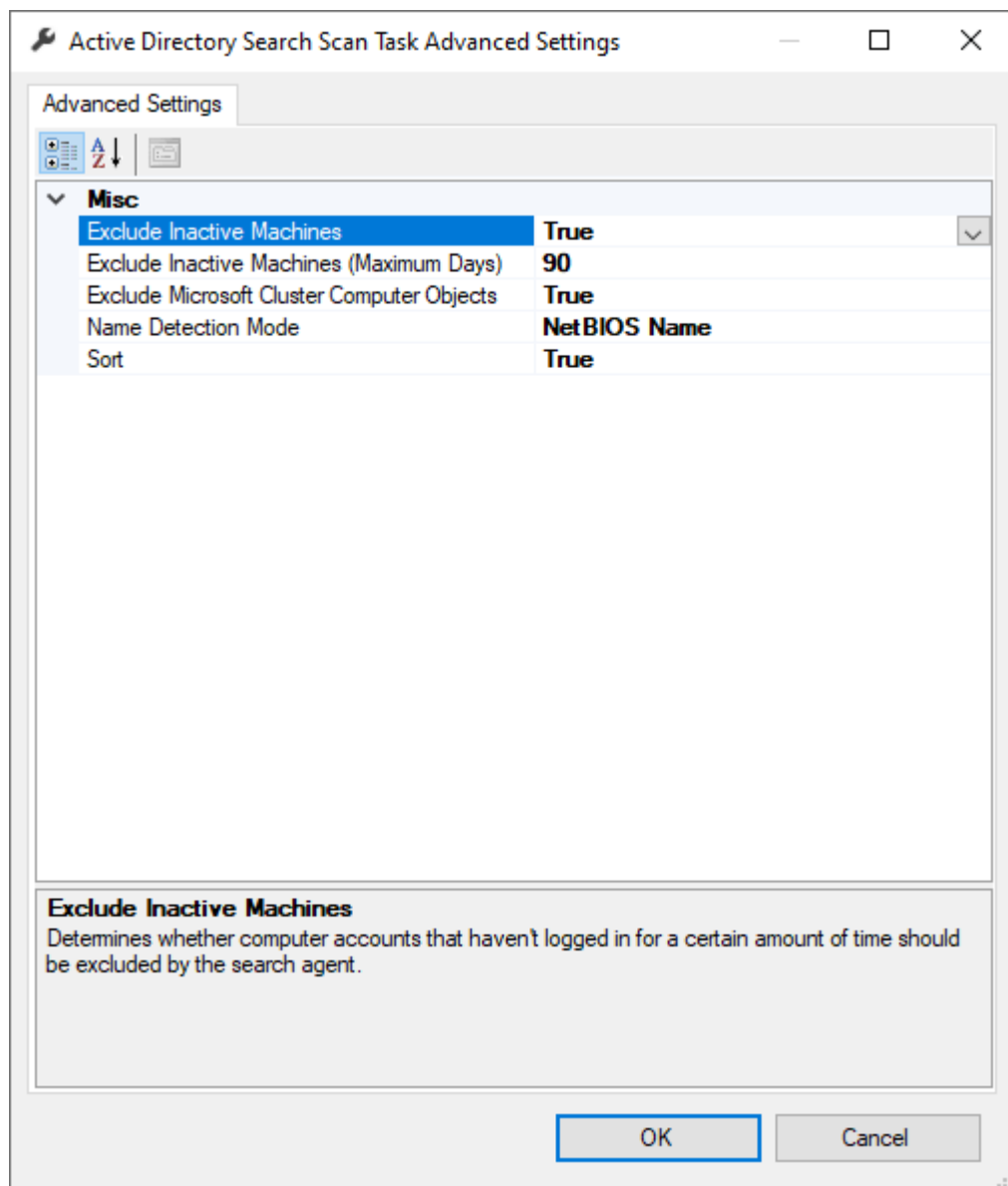
Search Filter

The LDAP filter to use to locate Windows machines. This field is read-only unless the *search type* is set to *custom*.

Advanced

Displays the [advanced search settings](#) dialog.

Advanced Search Settings



Exclude Inactive Machines

Determines whether computer accounts that haven't logged in for a certain amount of time should be excluded by the search agent. This method uses the [lastLogonTimestamp](#) Active Directory attribute.

Exclude Inactive Machines (Maximum Days)

The maximum number of days since the computer last logged onto the domain. This setting only applies if the *exclude inactive machines* setting is set to true. The minimum value is 14 days.

Exclude Microsoft Cluster Computer Objects

Determines whether Microsoft cluster name objects (CNOs) or virtual computer objects (VCOs) should be excluded by the search agent.

Name Detection Mode

The type of name to use when connecting to detected Windows machines.

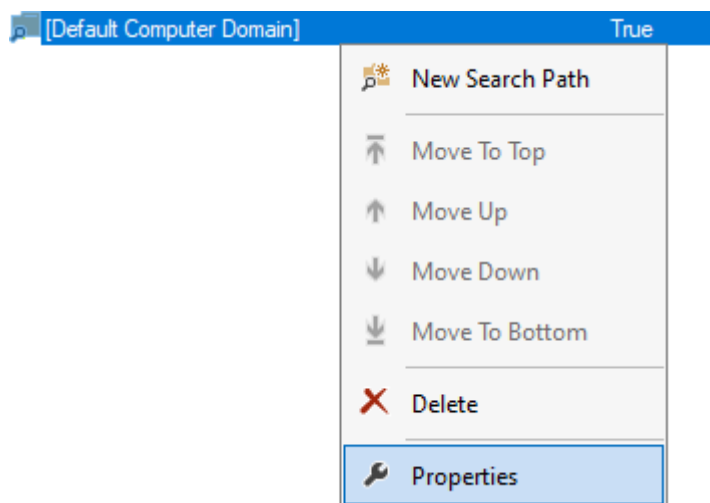
- NetBIOS Name
- Fully Qualified Domain Name

Sort

Determines whether the results should be sorted alphabetically by machine name.

Search Paths Context Menu

The context menu is displayed when a search path is right clicked in the [search settings](#) user interface.



New Search Path

Displays the [search path dialog](#) to create a new search path.

Move To Top

Moves the currently selected search path to the top of the list.

Move Up

Moves the currently selected search path up the list.

Move Down

Moves the currently selected search path down the list.

Move To Bottom

Moves the currently selected search path to the bottom of the list.

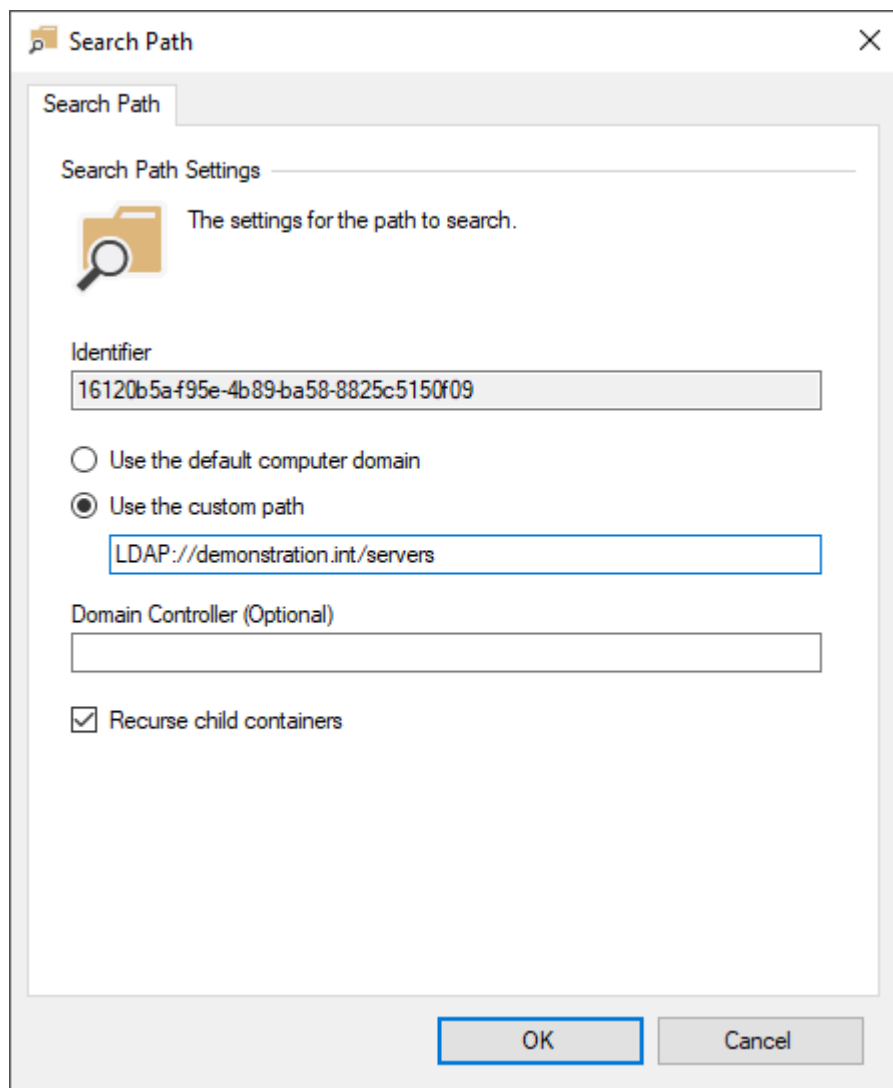
Delete

Deletes the currently selected search path.

Properties

Displays the currently selected search path in the [search path dialog](#).

Search Path



Search Path

Search Path Settings

The settings for the path to search.

Identifier
16120b5a-f95e-4b89-ba58-8825c5150f09

☐ Use the default computer domain

☒ Use the custom path

LDAP://demonstration.int/servers

Domain Controller (Optional)

☒ Recurse child containers

OK Cancel

Identifier

The unique identifier of the search path in [GUID](#) format.

Use the default computer domain

The search path is the root of the domain to which the computer running the [XIA Configuration Client](#) is a member.

Use the custom path

Uses the specified custom search path in canonical format.

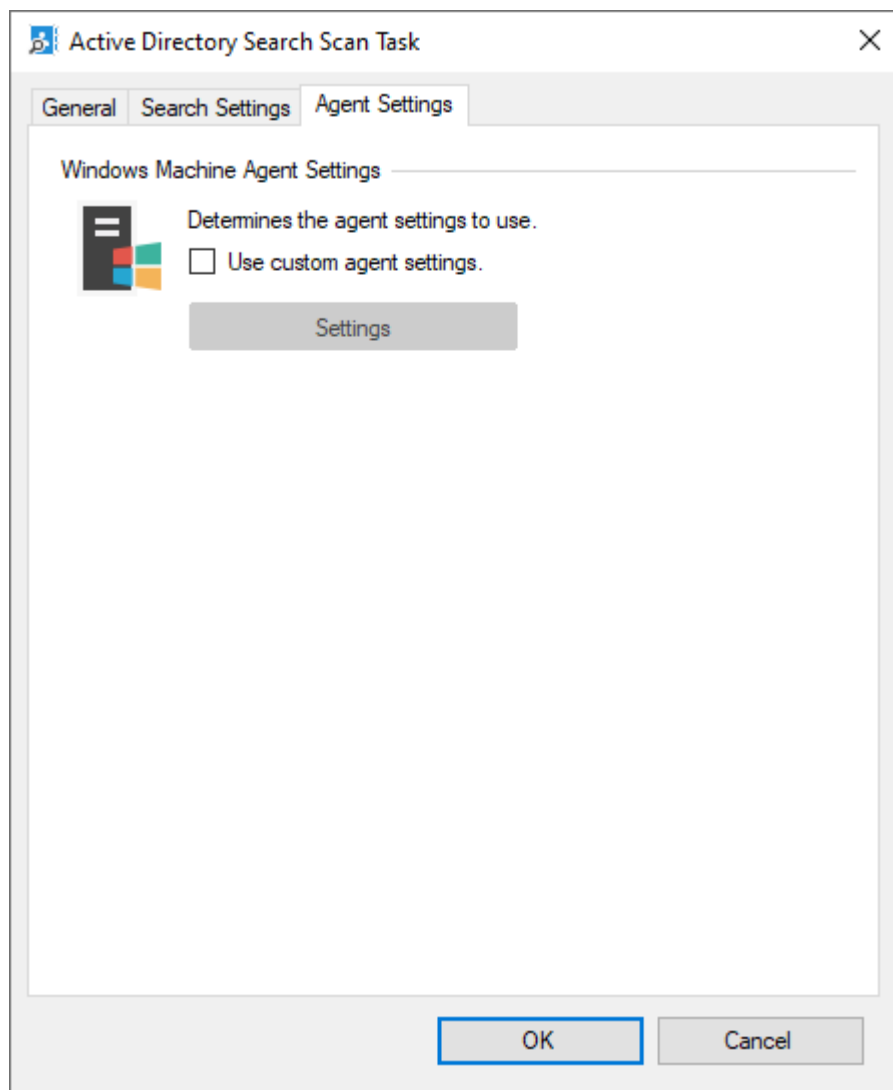
Domain Controller (Optional)

The optional fully qualified domain name of an Active Directory domain controller to use to perform the operation.

Recurse child containers

Determines whether the [Active Directory Search task](#) should recursively search the child containers and organizational units.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) for [Windows machines](#) detected by the [Active Directory search scan task](#), rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

All [Active Directory](#) versions and functional levels are supported.

The exclusion of inactive systems is supported on the Windows 2003 domain functional level or greater.

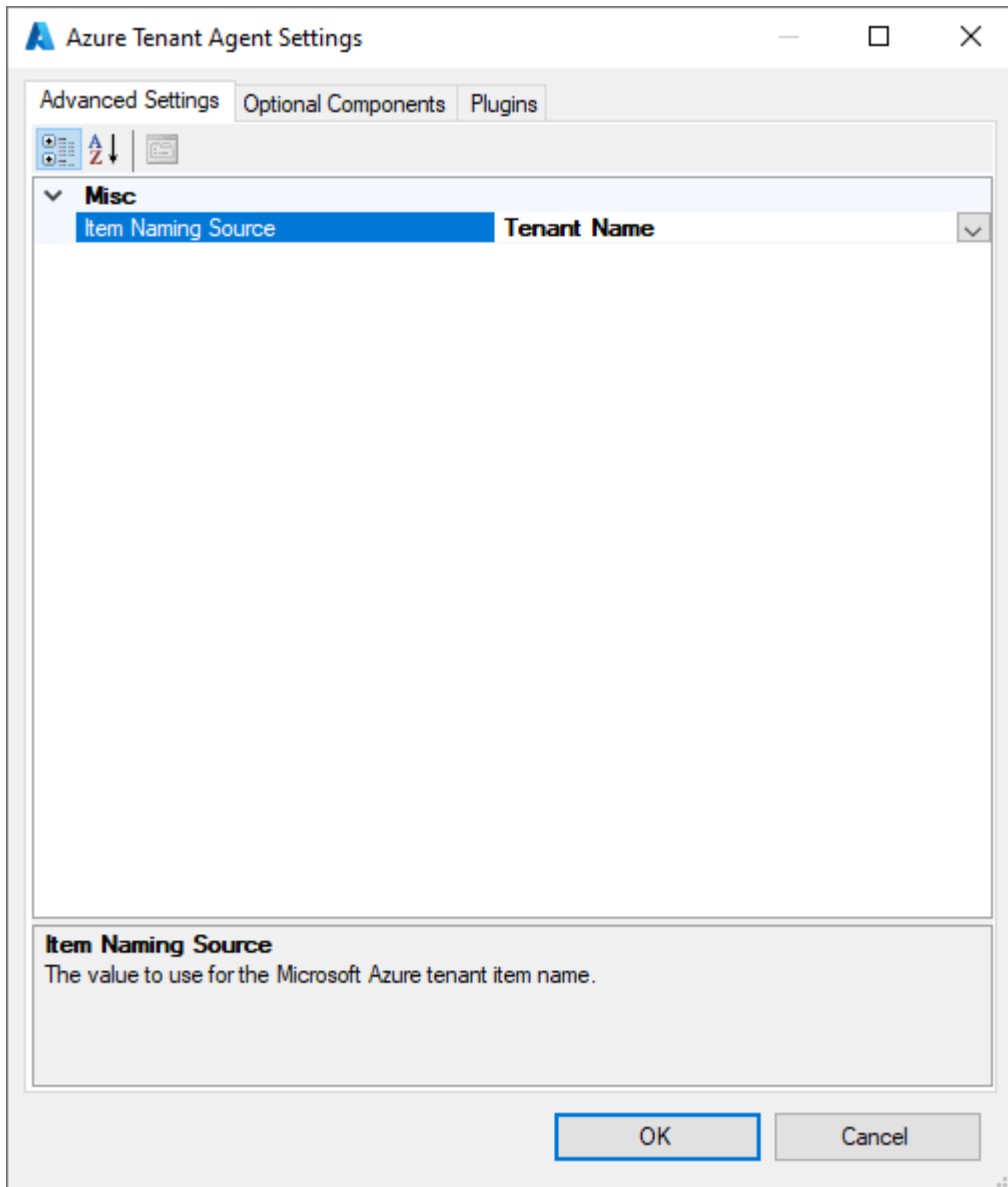
Azure Tenants



The Azure Tenant [scan tasks](#) are able to document [Microsoft Azure tenant items](#).

[Microsoft Azure](#) is a cloud computing platform and infrastructure created by [Microsoft](#) for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

Agent Settings



Item Naming Source

Determines the value to use for the [item name](#) of the [Azure tenant item](#).

- **Tenant Name**

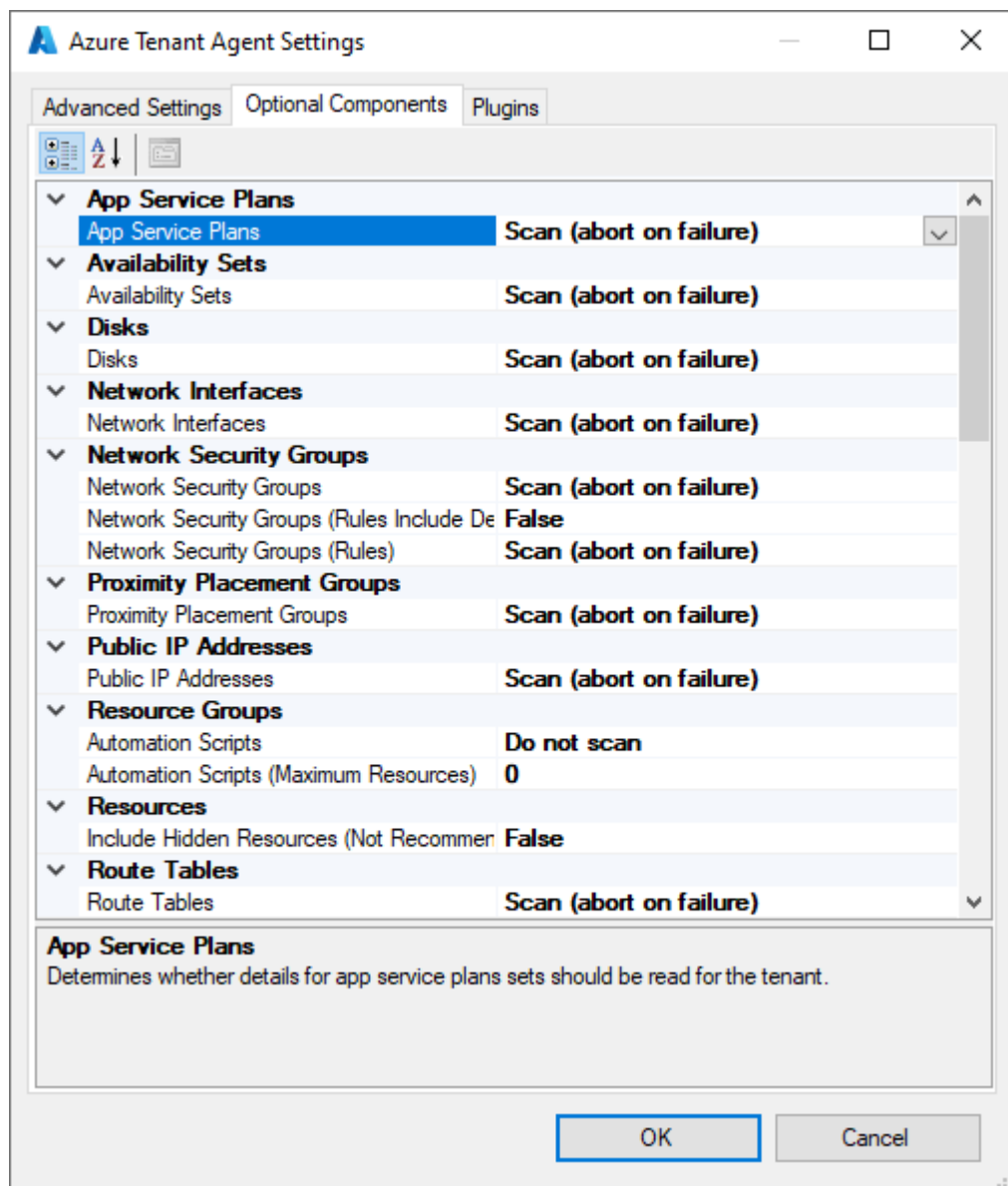
The name of the tenant - for example "CONTOSO" set in the [Azure portal](#).

For more information see [changing the tenant name in Azure](#).

- **Primary Domain**

The primary domain name - for example "contoso.com".

Optional Components



App Service Plans

Determines whether details for app service plans sets should be read for the tenant.

Availability Sets

Determines whether details for availability sets should be read for the tenant.

Disks

Determines whether details for managed disks should be read for the tenant.

Network Interfaces

Determines whether details for network interfaces should be read for the tenant.

Network Security Groups

Determines whether details for network security groups should be read for the tenant.

Network Security Groups (Rules)

Determines whether network security group rules should be read for the tenant.

Network Security Groups (Rules Include Default)

Determines whether to include default rules should be included when reading network security group rules.

Proximity Placement Groups

Determines whether details for proximity placement groups should be read for the tenant.

Public IP Addresses

Determines whether the details for public IP addresses should be read for the tenant.

Resource Groups > Automation Scripts

Determines whether the automation scripts should be read for resource groups.

Resource Groups > Automation Scripts (Maximum Resources)

Determines the maximum number of resources a resource group can contain for the automation script to be read.

Valid values are between 1 and 200.

Resources > Include Hidden Resources (Not Recommended)

Determines whether the resources that are hidden in the Azure portal should be included.

Route Tables

Determines whether the route tables should be read for the tenant.

SQL Databases

Determines whether details for SQL databases should be read for the tenant.

SQL Databases (Audit Policy)

Determines whether audit policy details for SQL databases should be read for the tenant.

SQL Databases (Replicas)

Determines whether details for SQL database replicas should be read for the tenant.

SQL Databases (Sync Groups)

Determines whether details for SQL database sync groups should be read for the tenant.

SQL Elastic Pools

Determines whether details for SQL elastic pools should be read for the tenant.

SQL Servers

Determines whether details for SQL servers should be read for the tenant.

SQL Servers (Audit Policy)

Determines whether audit policy for SQL servers should be read for the tenant.

SQL Servers (Failover Groups)

Determines whether the failover groups for SQL servers should be read for the tenant.

SQL Servers (Network Settings)

Determines whether the network settings for SQL servers should be read for the tenant.

SQL Servers (Private Endpoint Connections)

Determines whether the private endpoint connections for SQL servers should be read for the tenant.

SQL Servers (Transparent Data Encryption)

Determines whether the transparent data encryption settings for SQL servers should be read for the tenant.

Storage Accounts

Determines whether details for storage accounts should be read for the tenant.

Subscriptions

Storage Accounts (Access Keys) ¹

Determines whether the access keys should be read for storage accounts. This is security sensitive information and is disabled by default.

Subscriptions > Alert Rules

Determines whether the alert rules should be read for each subscription.

Subscriptions > Invoices ¹

Determines whether the invoices should be read for each subscription.

Subscriptions > Invoices (Months)

The number of months in the past for which invoices should be read for each subscription. By default this is the last 12 months.

Subscriptions > Policy Assignments

Determines whether the policy assignments should be read for each subscription.

Subscriptions > Locks

Determines whether the resource locks should be read for each subscription.

Subscriptions > Role Assignments

Determines whether the role assignments should be read for each subscription.

Subscriptions > Role Assignments (Include Classic Administrators)

Determines whether the role assignments read for each subscription should include classic administrators.

Tenant Configuration > Management Groups ¹

Determines whether the management groups should be read for the tenant.

Tenant Configuration > Role Definitions

Determines whether the role definitions should be read for the tenant.

Tenant Configuration > Role Definitions (Include Built-In)

Determines whether the built-in role definitions should be read for the tenant.

Virtual Machines

Determines whether details for virtual machines should be read for the tenant.

Virtual Machines (Extensions)

Determines whether virtual machine extensions should be read for the tenant.

Virtual Machines (Extensions Public Settings)

Determines the virtual machine extensions for which the public settings should be read.

- None
The public settings should not be read from any extensions.
- Default
The public settings should be read from the default extensions.
- All
The public settings should be read from all extensions.

Virtual Machines (Network Settings)

Determines whether virtual machine networking information should be read for the tenant.

Virtual Machines (Screenshot) ¹

Determines whether screenshots for virtual machines should be read for the tenant.

Virtual Machines (Storage)

Determines whether storage details for virtual machines should be read for the tenant.

Virtual Networks

Determines whether details for virtual networks should be read for the tenant.

Virtual Networks (Peerings)

Determines whether details for the peerings of the virtual networks should be read for the tenant.

Web Apps

Determines whether details of the web apps should be read for the tenant.

Web Apps (Authentication Settings)

Determines whether details of the authentication settings for the web apps should be read for the tenant.

Web Apps (Application Settings) ¹

Determines whether details of the app settings for the web apps should be read for the tenant. These may contain security sensitive information.

Web Apps (FTP Publishing Settings)

Determines whether details of the FTP publishing settings for the web apps should be read for the tenant.

Web Apps (FTP Publishing Settings Password) ¹

Determines whether the FTP publishing password for the web apps should be read for the tenant.

¹ These settings require [optional additional permissions](#).

Azure Tenant Scan Task

The Azure Tenant Task allows an individual [Azure](#) tenant to be scanned by the [XIA Configuration Client](#).

Connection Settings

The connection settings determines how to connect to the [Azure](#) tenant.

Service Principal (Certificate)

This is the recommended authentication method.

Service Principal (Client Secret)

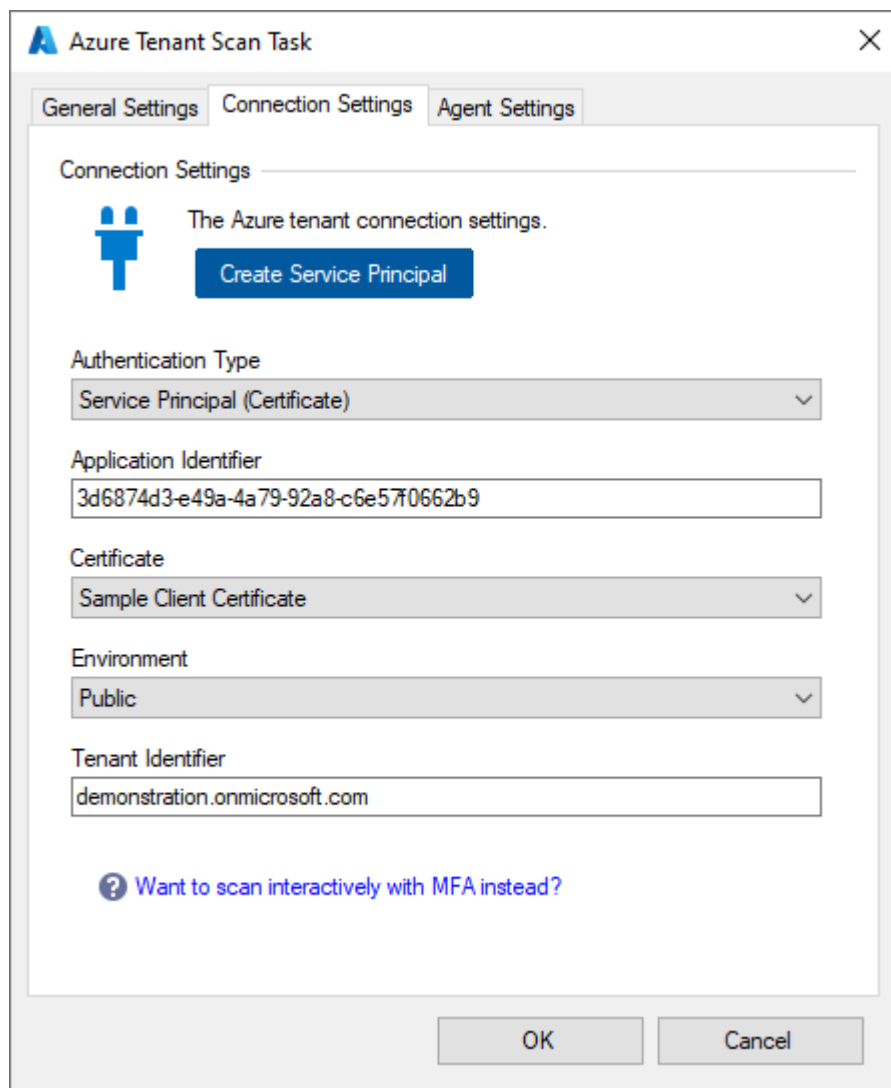
This method uses a client secret (password) for security - which is easier to share however is less secure than the certificate method.

Credentials (Deprecated)

This method uses a username and password and has been deprecated and is not recommended.

To scan interactivity instead using multi-factor authentication use the [Microsoft Online Agent UI](#).

Service Principal (Certificate)



The screenshot shows the 'Azure Tenant Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has three tabs: 'General Settings', 'Connection Settings', and 'Agent Settings'. The 'Connection Settings' tab contains the following fields and options:

- Connection Settings**: A section header with a blue plug icon and the text 'The Azure tenant connection settings.' Below this is a blue button labeled 'Create Service Principal'.
- Authentication Type**: A dropdown menu with 'Service Principal (Certificate)' selected.
- Application Identifier**: A text box containing the GUID '3d6874d3-e49a-4a79-92a8-c6e57f0662b9'.
- Certificate**: A dropdown menu with 'Sample Client Certificate' selected.
- Environment**: A dropdown menu with 'Public' selected.
- Tenant Identifier**: A text box containing 'demonstration.onmicrosoft.com'.
- Footer**: A link with a question mark icon and the text 'Want to scan interactively with MFA instead?'. At the bottom right are 'OK' and 'Cancel' buttons.

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Certificate

The certificate to use for authentication. The certificate must be installed in the user store of the [XIA Configuration Client service account](#) and support client authentication.

Environment

The [environment](#) to connect to.

Tenant Identifier

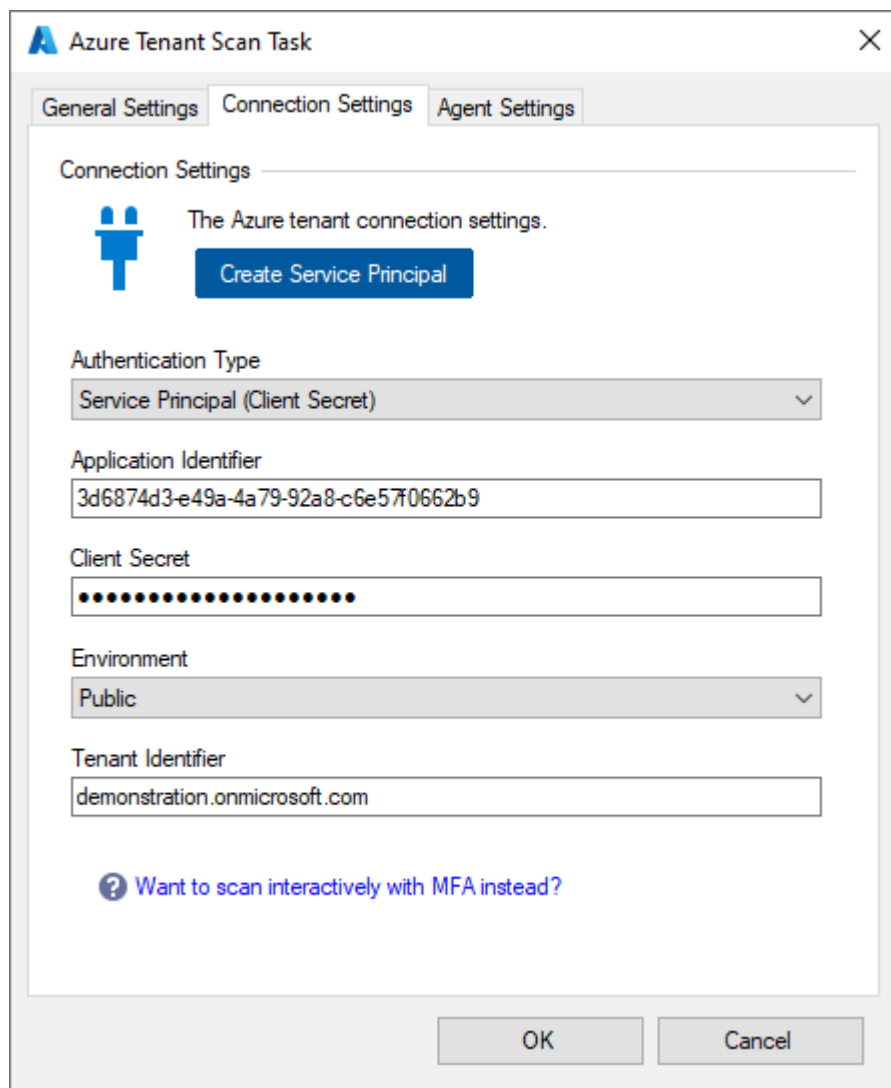
The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Service Principal (Client Secret)



The screenshot shows a dialog box titled "Azure Tenant Scan Task" with a close button (X) in the top right corner. It has three tabs: "General Settings", "Connection Settings", and "Agent Settings". The "Connection Settings" tab is active. Inside this tab, there is a section titled "Connection Settings" with a blue plug icon and the text "The Azure tenant connection settings." Below this is a blue button labeled "Create Service Principal".

Below the button, there are several input fields:

- Authentication Type:** A dropdown menu with "Service Principal (Client Secret)" selected.
- Application Identifier:** A text box containing the GUID "3d6874d3-e49a-4a79-92a8-c6e57f0662b9".
- Client Secret:** A text box filled with 16 black dots, representing a masked password.
- Environment:** A dropdown menu with "Public" selected.
- Tenant Identifier:** A text box containing "demonstration.onmicrosoft.com".

At the bottom of the dialog box, there are two buttons: "OK" and "Cancel". Above the "OK" button, there is a link that says "? Want to scan interactively with MFA instead?".

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Client Secret

The client secret (password) to use for authentication.

Environment

The [environment](#) to connect to.

Tenant Identifier

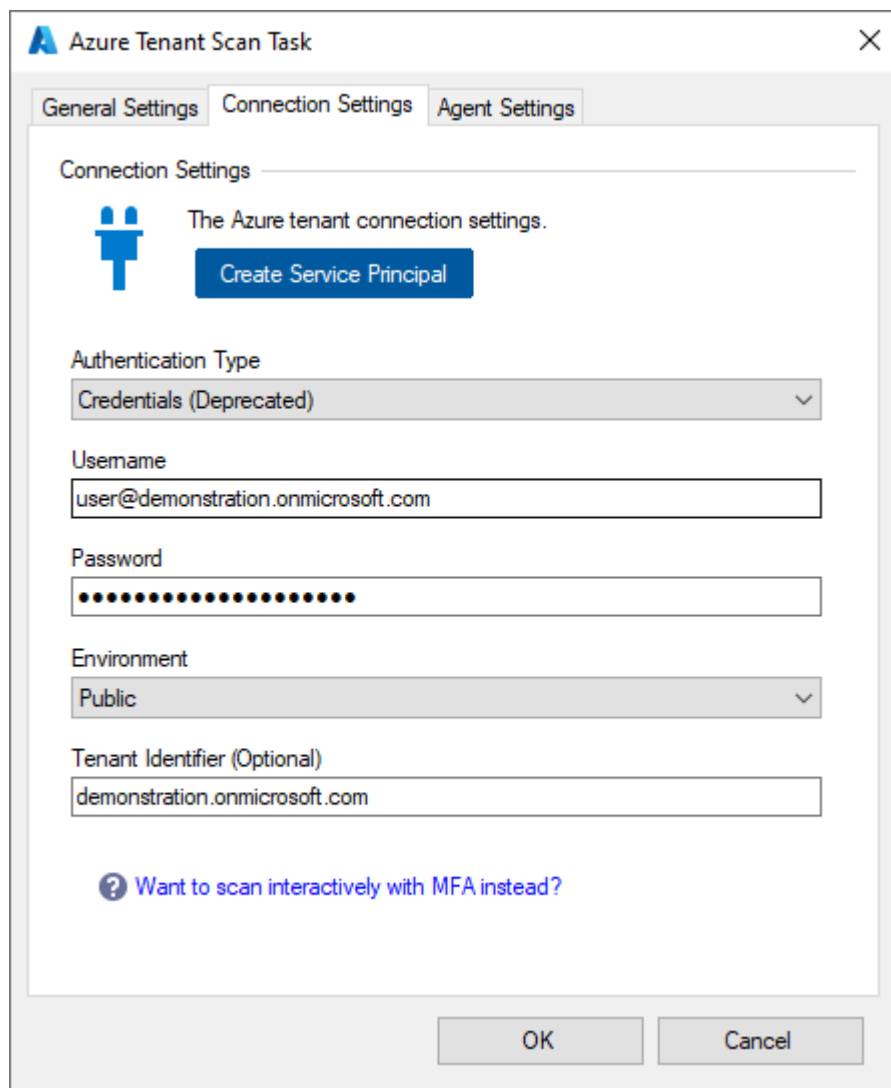
The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Credentials (Deprecated)



The screenshot shows the 'Azure Tenant Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has three tabs: 'General Settings', 'Connection Settings', and 'Agent Settings'. The 'Connection Settings' tab contains the following elements:

- A blue icon of a person with a plus sign.
- The text 'The Azure tenant connection settings.'
- A blue button labeled 'Create Service Principal'.
- A dropdown menu for 'Authentication Type' with 'Credentials (Deprecated)' selected.
- A text input field for 'Username' containing 'user@demonstration.onmicrosoft.com'.
- A text input field for 'Password' filled with dots.
- A dropdown menu for 'Environment' with 'Public' selected.
- A text input field for 'Tenant Identifier (Optional)' containing 'demonstration.onmicrosoft.com'.
- A link with a question mark icon: '? Want to scan interactively with MFA instead?'.
- 'OK' and 'Cancel' buttons at the bottom.

Authentication Type

The authentication type is Credentials (Deprecated). This method is deprecated and not recommended.

It is recommended to use a [service principal with a certificate](#), or login interactively using multi-factor authentication using the [Azure Tenant agent UI](#).

Username

The username of the account to use for login.

Password

The password of the user account.

Environment

The [environment](#) to connect to.

Tenant Identifier

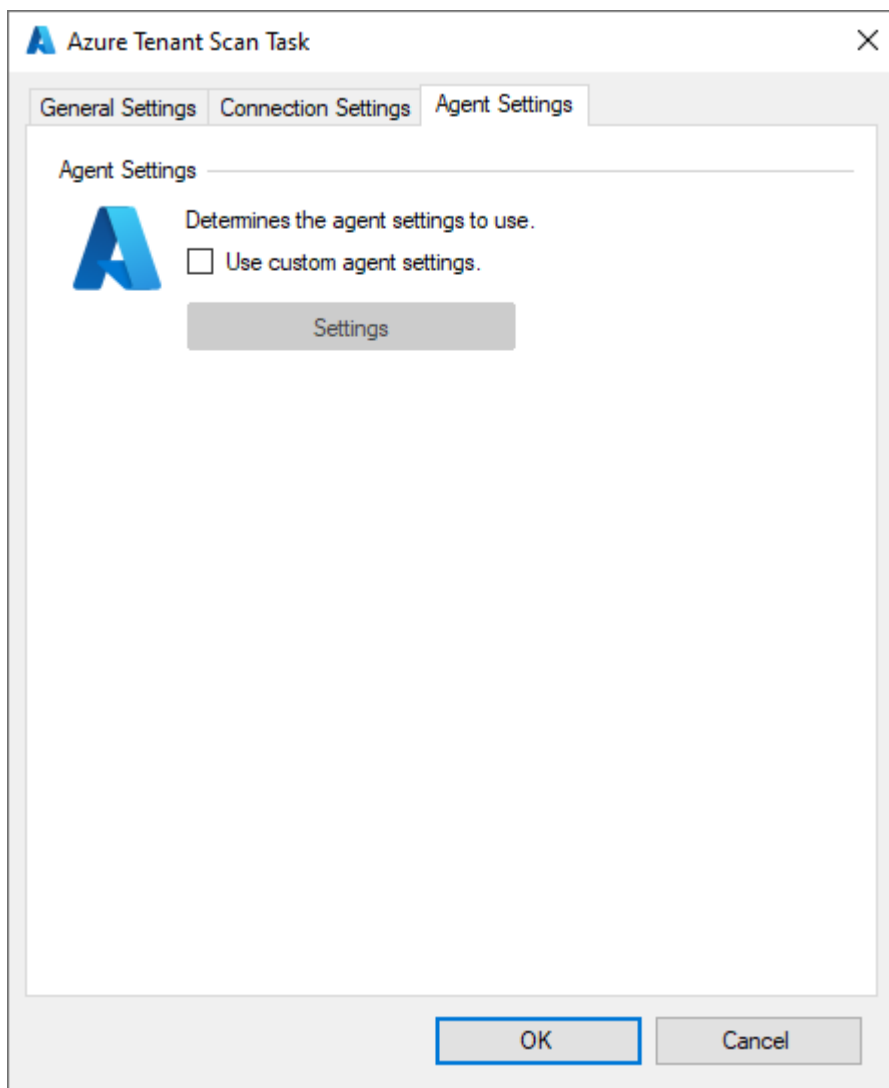
The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will help automate the process of creating and configuring a [service principal with a certificate](#).

For more information see the [requirements](#) section.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

[Azure tenant scan tasks](#) scan tasks support scanning a [Microsoft Azure](#) tenant.

Windows Firewall Requirements

- ✓ The [Azure tenant agent](#) must be able to connect to [Microsoft Azure REST API](#) using HTTPS.

Access Settings

- ✓ The [Azure tenant agent](#) must have [Global Reader](#) rights in the [Entra directory](#).
- ✓ The [Azure tenant agent](#) must have [Reader](#) rights in the [Microsoft Azure](#) tenant.

Optional Access Settings

- ✓ The [Azure tenant agent](#) has several [optional components](#) that may require [optional additional permissions](#).

Local Service

- ⬇️ [Azure tenant scan tasks](#) scan tasks do not support the [XIA Configuration Local Service](#).

Service Principal Setup

Follow these steps to enable the [Azure tenant agent](#) to access the [Microsoft Azure](#) tenant using a service principal.

[Service Principal \(Certificate\)](#)

[Service Principal \(Client Secret\)](#)

Service Principal (Certificate)

Follow these steps to enable the [Azure tenant tasks](#) to access [Microsoft Azure](#) using a service principal with certificate.

For more information see <https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal>

- Ensure that a client certificate and private key that supports client authentication is installed on the machine running the [XIA Configuration Client](#) and that the certificate is accessible to the [service account](#).

Issued To	Issued By	Expiration Date	Intended Purposes
 CSolutionsClient.org	MyRootCA	24/05/2031	Client Authentication, Server Authentication

- Export the public key of the client certificate in CER, PEM, or CRT format.
- Logon to the [Azure Portal](#) as a user account with the sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Server".
- For supported account types select *Accounts in this organizational directory only*
- Do not specify a Redirect URI.
- Click Register.
- Make a note of the following values

Application (client) ID
Directory (tenant) ID

- Go to Certificates & secrets > Certificates.
- Click Upload Certificate.

- Browse for the certificate and provide a description.

* Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

"ClientCert.cer" 

Description

XIA Configuration client certificate

- Copy and record the thumbprint.

Thumbprint	Description	Start date	Expires
BE4BCA8C388AF02EE1C50C3F5F74D6A34FE97DAF	XIA Configuration client certificate	5/24/2021	5/24/2031

- Go to Azure Active Directory > Roles and Administrators > Global reader.

Role	↑↓	Description	Type
  Global reader		Can read everything that a global administrator can, but ...	Built-in

- Click Add assignments and search for and select the service principal and click *Add*.

Search ⓘ

 XIA Configuration Server



XIA Configuration Server

fbf87ee4-cdb8-4e82-b4fd-0db0c8f9d315

- Go to Subscriptions and for each subscription select *Access Control (IAM)*.
- Click Add > Add role assignment and select the *Reader* role and click *Next*.
- Add the service principal to the role.

Selected role
 Reader

Assign access to
☒ User, group, or service principal
☐ Managed identity

Members
[+ Select members](#)

Name	Object ID	Type
XIA Configuration Server	ff08f3c6-916a-4389-a939-b46661d72b0e	App

Service Principal (Client Secret)

Follow these steps to enable the [Azure tenant tasks](#) to access [Microsoft Azure](#) using a service principal with client secret.

For more information see

<https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal>

- Logon to the [Azure Portal](#) as a user account with the sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Server".
- For supported account types select
Accounts in this organizational directory only
- Do not specify a Redirect URI.
- Click Register.
- Make a note of the following values

Application (client) ID

Directory (tenant) ID

- Go to Certificates & secrets > Client secrets.
- Click *New Client Secret*.
- Enter a description and appropriate expiry, and click *Add*.

Add a client secret



Description

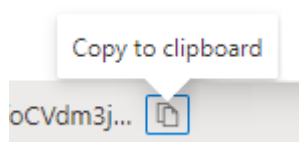
XIA Configuration access

Expires

Recommended: 6 months



- Copy and record the client secret value. This value is only available at this point.



- Go to Azure Active Directory > Roles and Administrators > Global reader.

Role	↑↓	Description	Type
☒  Global reader		Can read everything that a global administrator can, but ...	Built-in

- Click Add assignments and search for and select the service principal and click *Add*.

Search ⓘ

 XIA Configuration Server

 XIA Configuration Server
fbf87ee4-cdb8-4e82-b4fd-0db0c8f9d315

- Go to Subscriptions and for each subscription select *Access Control (IAM)*.
- Click Add > Add role assignment and select the *Reader* role and click *Next*.
- Add the service principal to the role.

Role Members Review + assign

Selected role Reader

Assign access to

☒ User, group, or service principal

☐ Managed identity

Members + Select members

Name	Object ID	Type
XIA Configuration Server	ff08f3c6-916a-4389-a939-b46661d72b0e	App

Managed Service Providers Azure Best Practice

Managed service providers (MSPs) typically have a single [XIA Configuration Server](#) installation and one or more [XIA Configuration Client](#) installations in each customer environment.

This allows a single managed repository of technical information whilst allowing the [XIA Configuration Client](#) to be installed behind each customer's firewall and configured with credentials appropriate for the customer environment.

As a cloud based solution the [Azure tenant](#) scan tasks can either be executed by the [XIA Configuration Client](#) installed in each customer environment, or directly from the [MSP](#) environment.

The following compares the two options.

Customer Environment

- The [Azure tenant scan task](#) must be configured for the [XIA Configuration Client](#) in each customer environment.
- The customer retains control of their connection credentials, and these credentials must be updated in each customer environment when they are changed.
- [Item creation rules](#) are used when data is sent to the [XIA Configuration Server](#).

Managed Service Provider Environment

- An [Azure tenant scan task](#) must be configured within the [XIA Configuration Client](#) for each customer with the appropriate [Azure credentials](#).

 Scan Tasks Configures the tasks that will be performed by this scan profile. Start Scan Profile			
Display Name	Status	Type	
 Customer 1	Enabled	Azure Tenant	
 Customer 2	Enabled	Azure Tenant	
 Customer 3	Enabled	Azure Tenant	

- The managed service provider retains control of all connection credentials.
- [Item creation rules](#) are not used when data is sent to the [XIA Configuration Server](#) so the Managed Service Provider must move the [Azure Tenant](#) item to the appropriate [container](#) or [customer](#) when it is created.

Optional Additional Permissions

Invoices

- ✓ The [Azure tenant agent](#) must have the [Billing Reader](#) role to read the invoices [optional component](#).

Management Groups

- ✓ The [Azure tenant agent](#) must have the following right to read the management groups [optional component](#).

Microsoft.Management/managementGroups/read over scope
/providers/Microsoft.Management

For more information see the [error reading management groups](#) support article.

Storage Accounts (Access Keys)

- ✓ The [Azure tenant agent](#) must have the [Storage Account Key Operator Service](#) role or following right to read the Storage Accounts (Access Keys) [optional component](#).

Microsoft.Storage/storageAccounts/listKeys/action

Virtual Machines (Screenshot)

- ✓ The [Azure tenant agent](#) must have the following right to read the Virtual Machines (Screenshot) [optional component](#).

Microsoft.Compute/virtualMachines/retrieveBootDiagnosticsData/action

Web Apps (Application Settings)

- ✓ The [Azure tenant agent](#) must have the [Website Contributor](#) role or following right to read the Web Apps (Application Settings) [optional component](#).

Microsoft.Web/sites/config/list/action over the config/appsettings scope.

Web Apps (FTP Publishing Settings Password)

✓ The [Azure tenant agent](#) must have the [Website Contributor](#) role or following right to read the Web Apps (FTP Publishing Settings Password) [optional component](#).

Microsoft.Web/sites/config/list/action over the config/publishingCredentials scope.

Troubleshooting

This section highlights the known issues for the [Azure tenant agent](#), and provides details of the solutions.

Changing the tenant name in Azure

Issue

When scanning an [Azure tenant](#) and the *item naming source* in the [agent settings](#) is configured to *tenant name*, the [item](#) created doesn't have the desired [item name](#).

Cause

The item is named using the tenant name in [Azure Active Directory](#).

More Information

This behaviour is by design.

Resolution

The item name can be changed in the [Azure portal](#) if required using the following steps.

- Open the [Azure portal](#).
- Select *Azure Active Directory*.
- Select *Properties*.
- Enter the required name.
- Click save.

Error getting the management groups. Access is denied

Issue

When scanning an [Azure Tenant](#) the agent fails to scan management groups and the following error or warning is seen

Error getting the management groups. Access is denied.

Further diagnostics information maybe be seen:

The client 'name' with object id 'identifier' does not have authorization to perform action 'Microsoft.Management/managementGroups/read' over scope '/providers/Microsoft.Management' or the scope is invalid. If access was recently granted, please refresh your credentials."

Cause

By default even members of the [Global Reader](#) role do not have access to all management groups in the directory.

More Information

This behaviour is by design in [Microsoft Azure](#).

Resolution

For more information about granting permissions to management groups see the following article.
<https://docs.microsoft.com/azure/role-based-access-control/elevate-access-global-admin>

The account does not have access to any subscriptions

Issue

When scanning an [Azure tenant](#) the agent fails to connect and the following error is displayed
"The account does not have access to any subscriptions."

Cause

The configured account has not been granted to any [Azure](#) subscriptions, or no subscriptions exist.

Resolution

- If the [Azure tenant](#) does have subscriptions review the [requirements](#) to ensure that the configured account has the correct permissions assigned.

- or -
- If the [Azure tenant](#) does not have any subscriptions you can use the [Microsoft 365 organization](#) agent, [Microsoft 365 Organization](#) agent, or [Entra directory](#) agent instead.

The connected account does not have 'Global reader' access to the directory

Issue

When scanning an [Azure Tenant](#) the agent fails to connect and the following error is displayed "The connected account does not have 'Global reader' access to the directory."

Cause

The configured account has not been granted the 'Global reader' or equivalent access to the Azure Active Directory tenant.

Resolution

To resolve this issue review the [requirements](#).

The subscription is not enabled

Issue

When scanning an [Azure Tenant](#) the agent fails to scan certain sections and one of the following errors is displayed

- *The Azure subscription in which this resource resides is not active.*
- *The subscription '342f80f7-bd74-472b-a234-92cd48892519' is disabled and therefore marked as read only. You cannot perform any write actions on this subscription until it is re-enabled.*
- *The specified account is disabled.*

Cause

An Azure subscription can get disabled because the credit has expired, it has reached the spending or credit card limit, or because the subscription was cancelled by the Account Administrator.

More Information

Certain read commands used by [Microsoft Azure](#) use the POST verb in the REST API. This is incorrectly interpreted by [Azure](#) as being a write operation and prevented whilst the subscription is disabled.

These include but are not limited to reading

- Virtual Machine Screenshots.
- Web App FTP publishing settings.
- Web App authentication settings.
- Storage accounts.

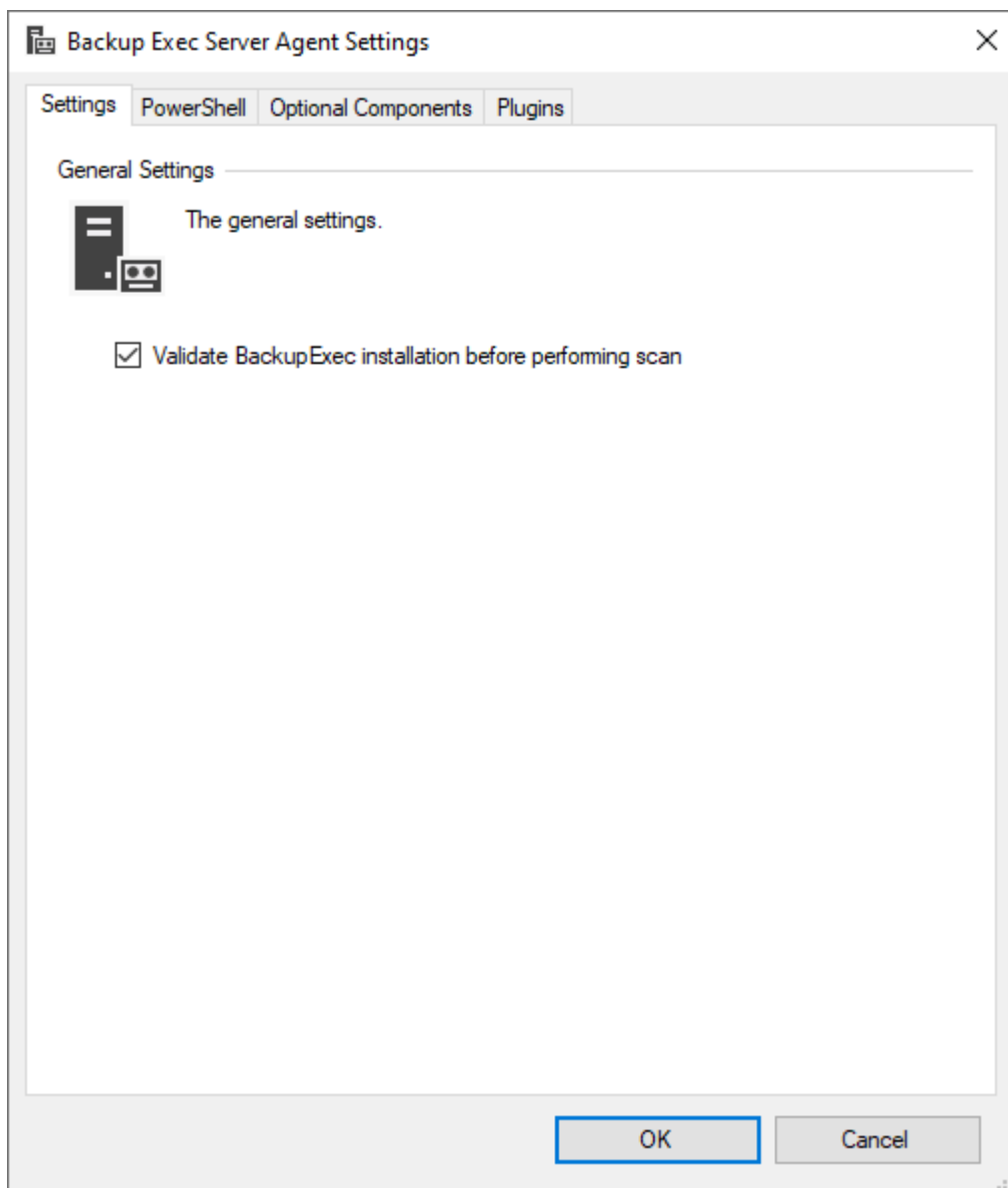
Resolution

Ensure that the Azure subscription is active.

Backup Exec Server

The [Backup Exec](#) server scan tasks are able to document Backup Exec version 14.0 and above using [PowerShell remoting](#) and WMI.

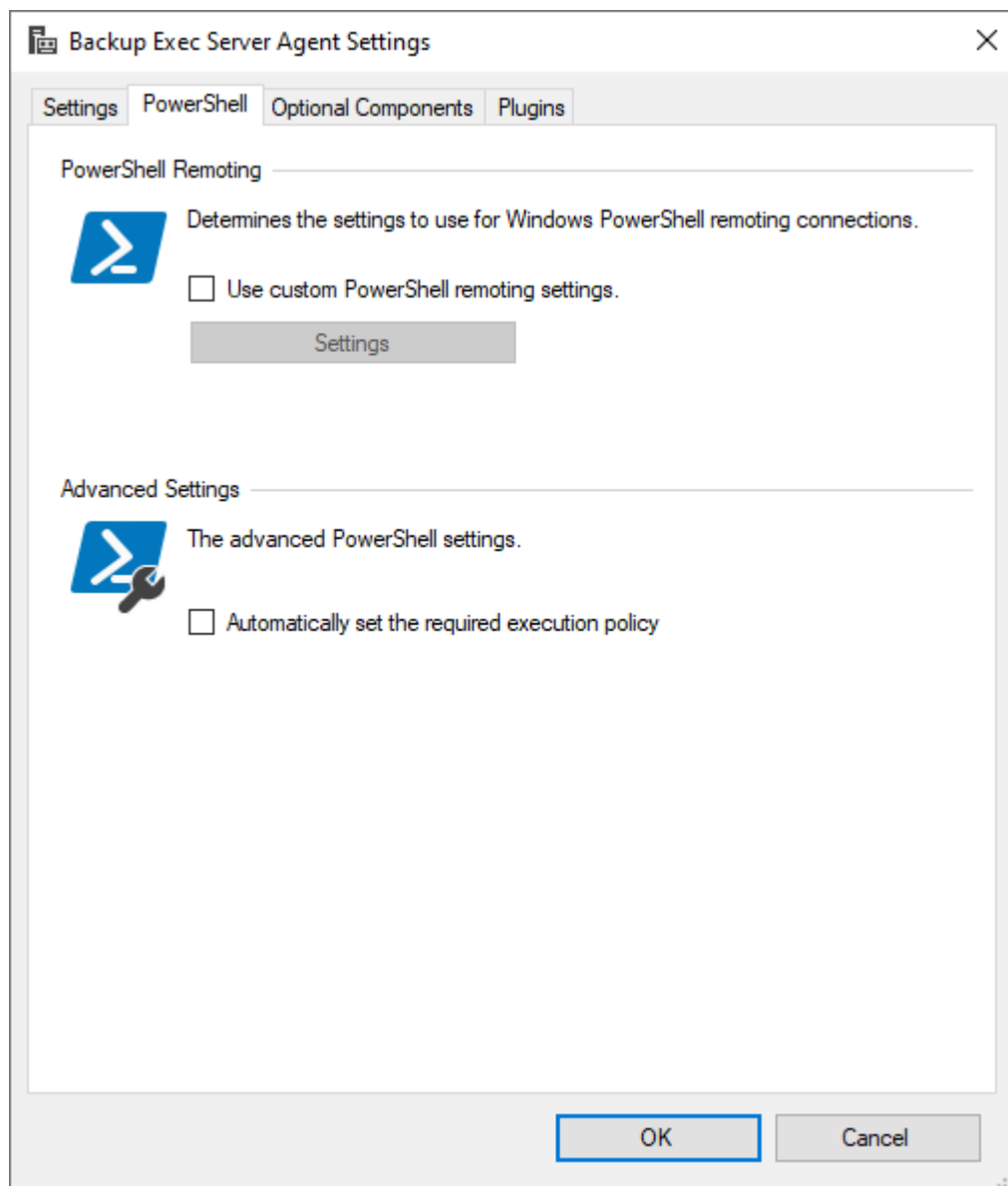
Agent Settings



Perform Validation

Determines whether the agent should validate that the [Backup Exec Server](#) is correctly configured before allowing the scan to be performed by the agent.

PowerShell



PowerShell Remote Connection Settings

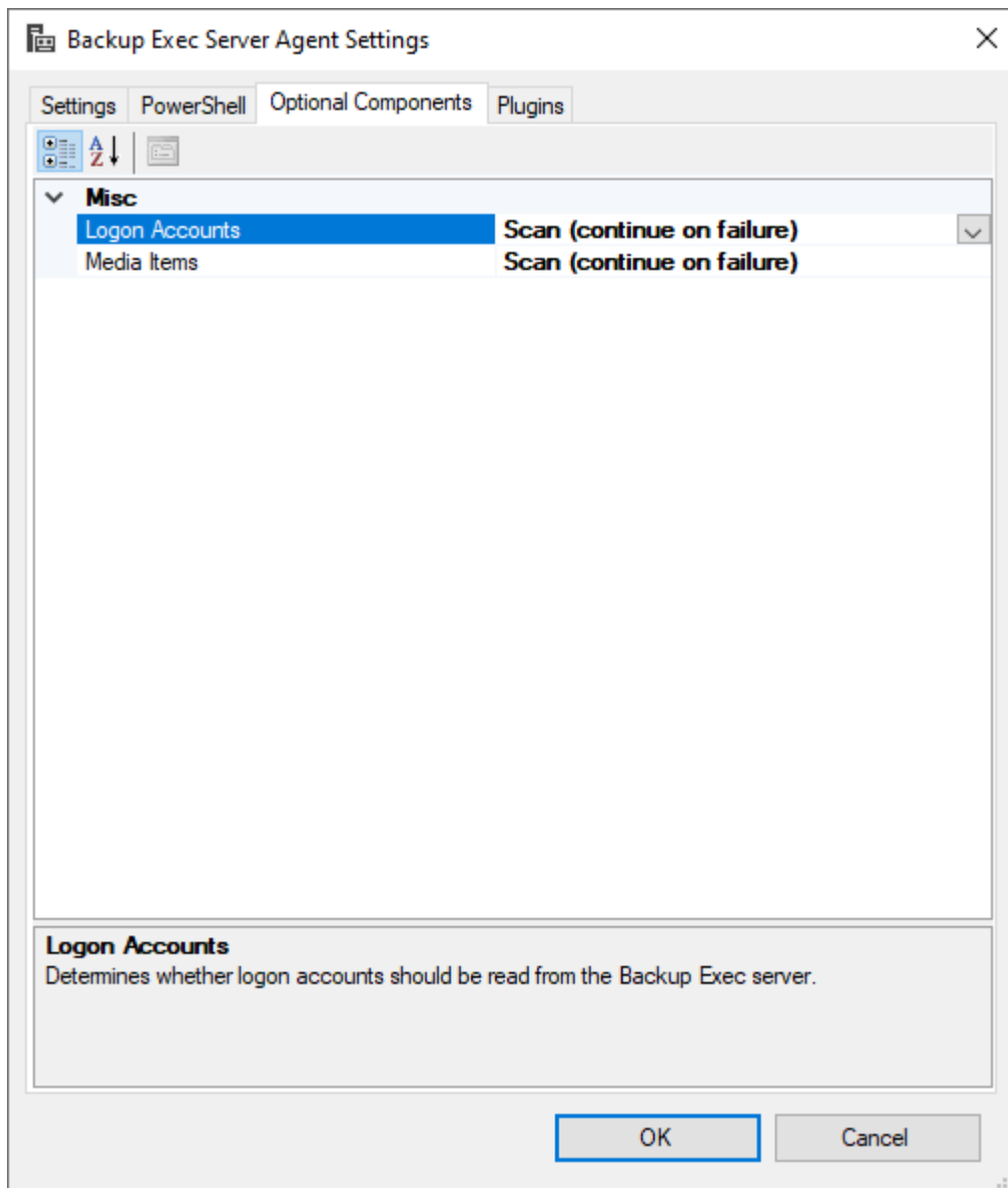
The [PowerShell connection settings](#) to use to connect to the remote machine.

Automatically set the required execution policy

Determines whether to automatically set the execution policy to "RemoteSigned" on the remote machine.

WARNING: This is an active change to the remote machine and is disabled by default.

Optional Components



Logon Accounts

Determines whether logon accounts should be read from the [Backup Exec server](#).

Media Items

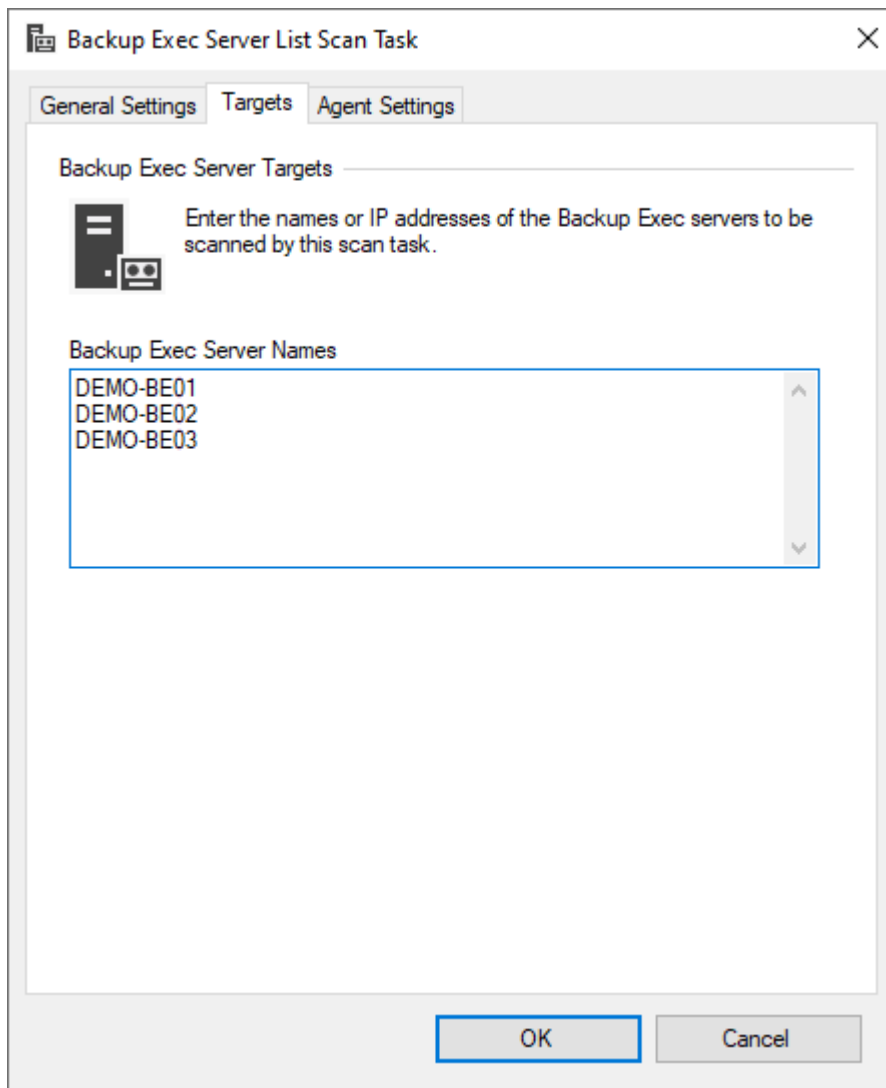
Determines whether individual media items such as tapes should be read from the [Backup Exec server](#).

Backup Exec Server List Scan Task

The [Backup Exec Server](#) list scan task allows you to enter a list of Backup Exec servers that you wish to scan that meet the [requirements](#).

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Backup Exec Servers](#).

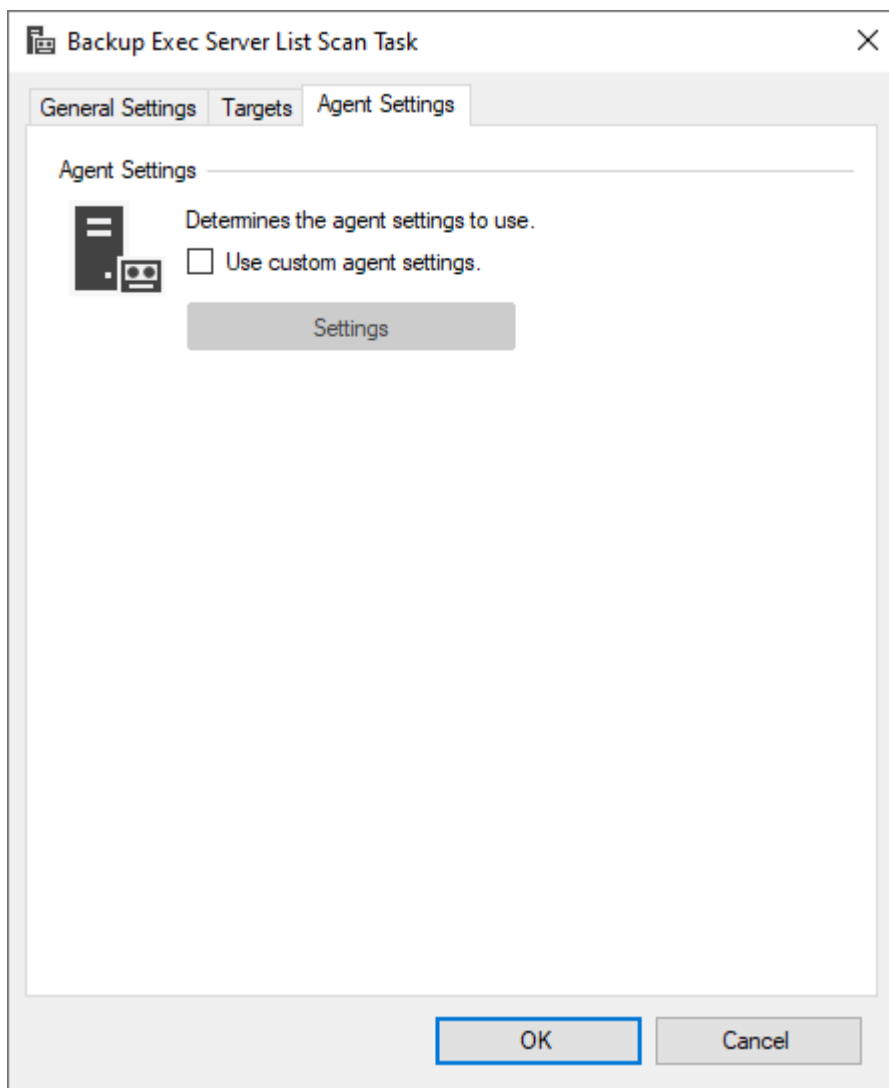
Targets



Backup Exec Server Names

The IP addresses, NetBIOS names, or fully qualified domain names of the Backup Exec servers to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The [Backup Exec Server](#) scan tasks are supported on the following platforms

- Veritas Backup Exec 21.2
- Veritas Backup Exec 21.1
- Veritas Backup Exec 21
- Veritas Backup Exec 20.x
- Veritas Backup Exec 16
- Symantec Backup Exec 15 (14.2)
- Symantec Backup Exec 2014 (14.1)

Access Settings (PowerShell)

The scan tasks use [Windows PowerShell Remoting](#) to obtain information from a computer running [Backup Exec](#).

- [Windows PowerShell Remoting](#) must be [enabled](#) on the machine running [Backup Exec](#).
- The [Windows PowerShell execution policy](#) must be [set to RemoteSigned](#) on the **remote** machine. This can be configured automatically if configured on the [PowerShell](#) setting tab.
- Firewall access must allow access to the PowerShell Remoting (WinRM) port on the remote machine.
- The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) must have Administrator rights to the remote machine.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✓ Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

Local Service

The [Backup Exec Server](#) scan tasks do not support the [XIA Local Service](#).

Automatic Detection

- ✓ [Backup Exec Servers](#) can be [automatically detected](#) and scanned by [Windows Machine Scan](#)

Tasks.

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))

Symptoms

When you scan a [Backup Exec Server](#) you see the following error

"Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))"

Cause

This can occur when the [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) do not have permissions required to the [Backup Exec Server](#) being scanned.

Resolution

Ensure that the service account or [custom credentials](#) are granted sufficient permissions.

BEMCLI.Scripts.psm1 may have been tampered error

Symptoms

When you scan a [Backup Exec Server](#) you see the following error

The Backup Exec server agent encountered an exception when 'Loading the Backup Exec PowerShell module (BEMCLI)'. File C:\Program Files\Symantec\Backup Exec\Modules\BEMCLI\BEMCLI.Scripts.psm1 cannot be loaded.

The contents of file C:\Program Files\Symantec\Backup Exec\Modules\BEMCLI\BEMCLI.Scripts.psm1 may have been tampered because the hash of the file does not match the hash stored in the digital signature. The script will not execute on the system. Please see "get-help about_signing" for more details.

Cause

This is a known issue with the Backup Exec installation.

Resolution

Please see the following [Veritas](#) article for more information
https://www.veritas.com/support/en_US/article.TECH213437

Connecting to remote server failed. Access Denied.

Symptoms

When you scan a [Backup Exec Server](#) you see the following error

"Connecting to remote server failed with the following error message: Access is denied. For more information, see the about_Remote_Troubleshooting Help topic."

Cause

This can occur when the [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) do not have permissions required to the [Backup Exec Server](#) being scanned.

Resolution

- Ensure that the service account or [custom credentials](#) are granted sufficient permissions.
- Ensure the [Windows PowerShell](#) settings are configured correctly - running the [Enable PowerShell Remoting](#) command again may resolve the issue.

Error loading the Backup Exec PowerShell module (BEMCLI)

Symptoms

When you scan a [Backup Exec Server](#) you see the following error

"The Backup Exec server agent encountered an exception when 'Loading the Backup Exec PowerShell module (BEMCLI)'. File C:\Program Files\Symantec\Backup Exec\Modules\PowerShell3\BEMCLI\BEMCLI.Scripts.psm1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at <http://go.microsoft.com/fwlink/?LinkID=135170>."

Cause

This can occur when the PowerShell script execution policy has not been set to **RemoteSigned**.

Resolution

Manually follow the instructions in the section [Set Execution Policy to RemoteSigned](#).

or

Enable the **Automatically Set Execution Policy** setting in the agent's [PowerShell settings](#).

Failed to connect to the Backup Exec server. Verify that the Backup Exec services are running.

Symptoms

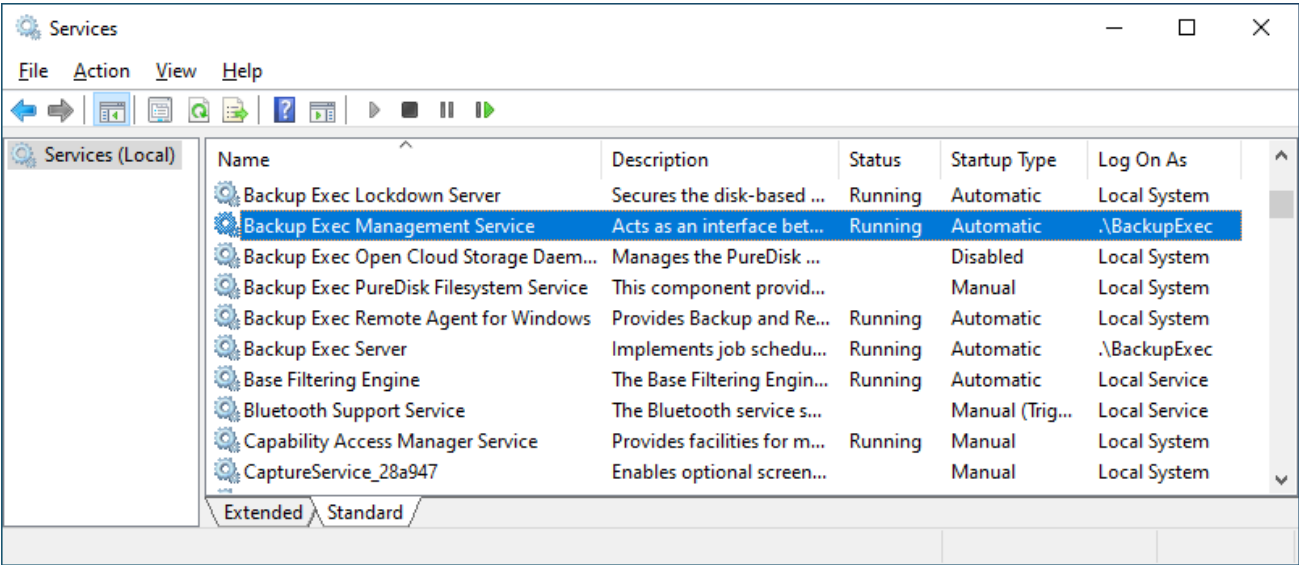
When you scan a [Backup Exec Server](#) you see the following error
"Failed to connect to the Backup Exec server. Verify that the Backup Exec services are running."

Cause

This can occur when the [Backup Exec server](#) services are stopped.

Resolution

Open the Services management console and validate whether the Backup Exec services are running correctly.



Selections show as "Unknown".

Symptoms

When you view a [Backup Exec Server](#) you see "Unknown" in the selections list.

Cause

This is due to a known issue in the underlying Backup Exec PowerShell API that can be seen if you query the same information directly using PowerShell.

Resolution

The problem is caused by a known issue in the Veritas [Backup Exec](#) product. For more information please contact Veritas technical support.

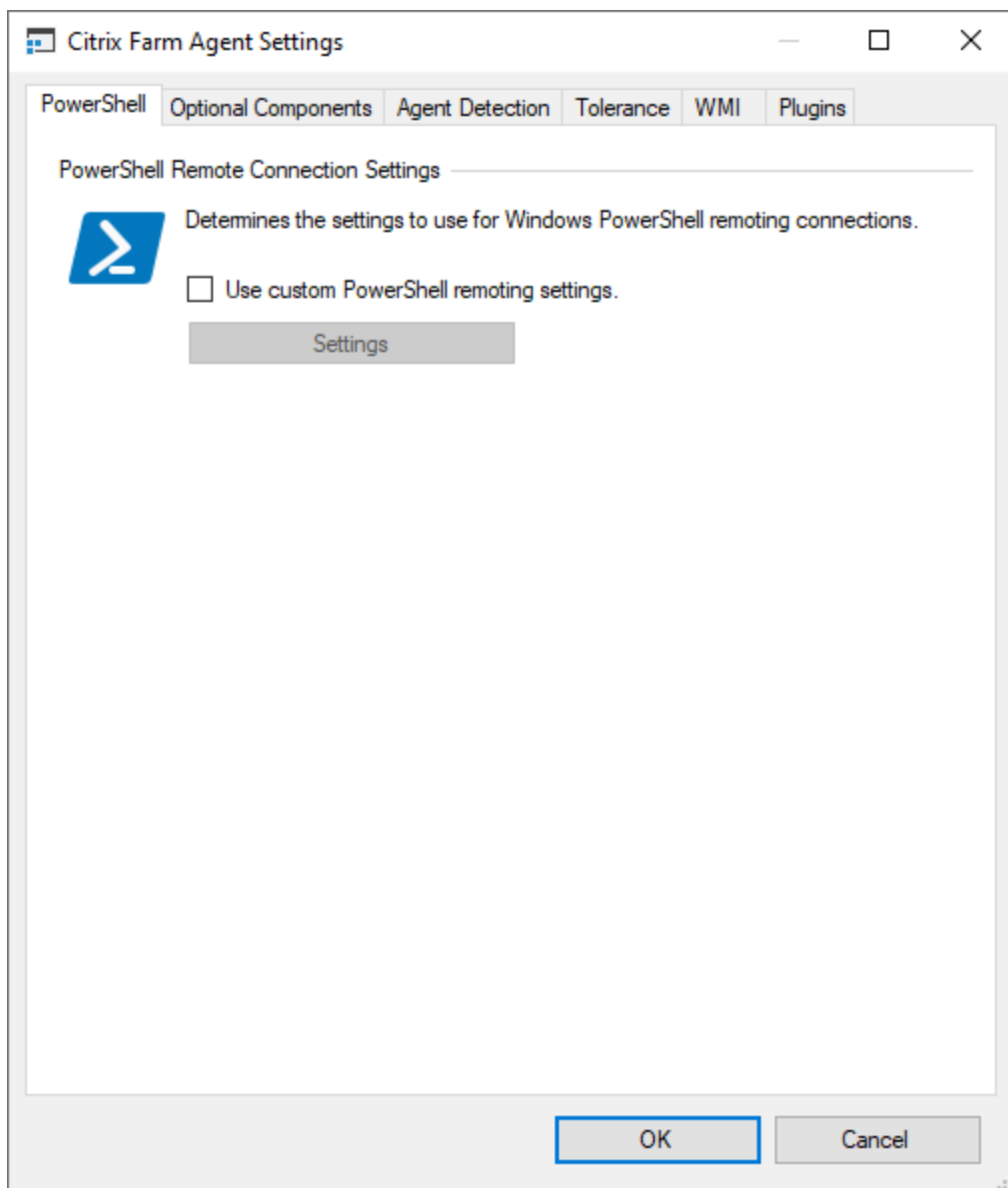
Citrix XenApp Farm (Classic)

Citrix XenApp Farm scan tasks are able to document **Citrix XenApp 6.0 and 6.5 Farms** using [PowerShell remoting](#).

For newer versions of Citrix XenApp and XenDesktop please see the [Citrix XenDesktop Site](#) agent.

The data located by these tasks includes farm configuration, applications, servers, and policies.

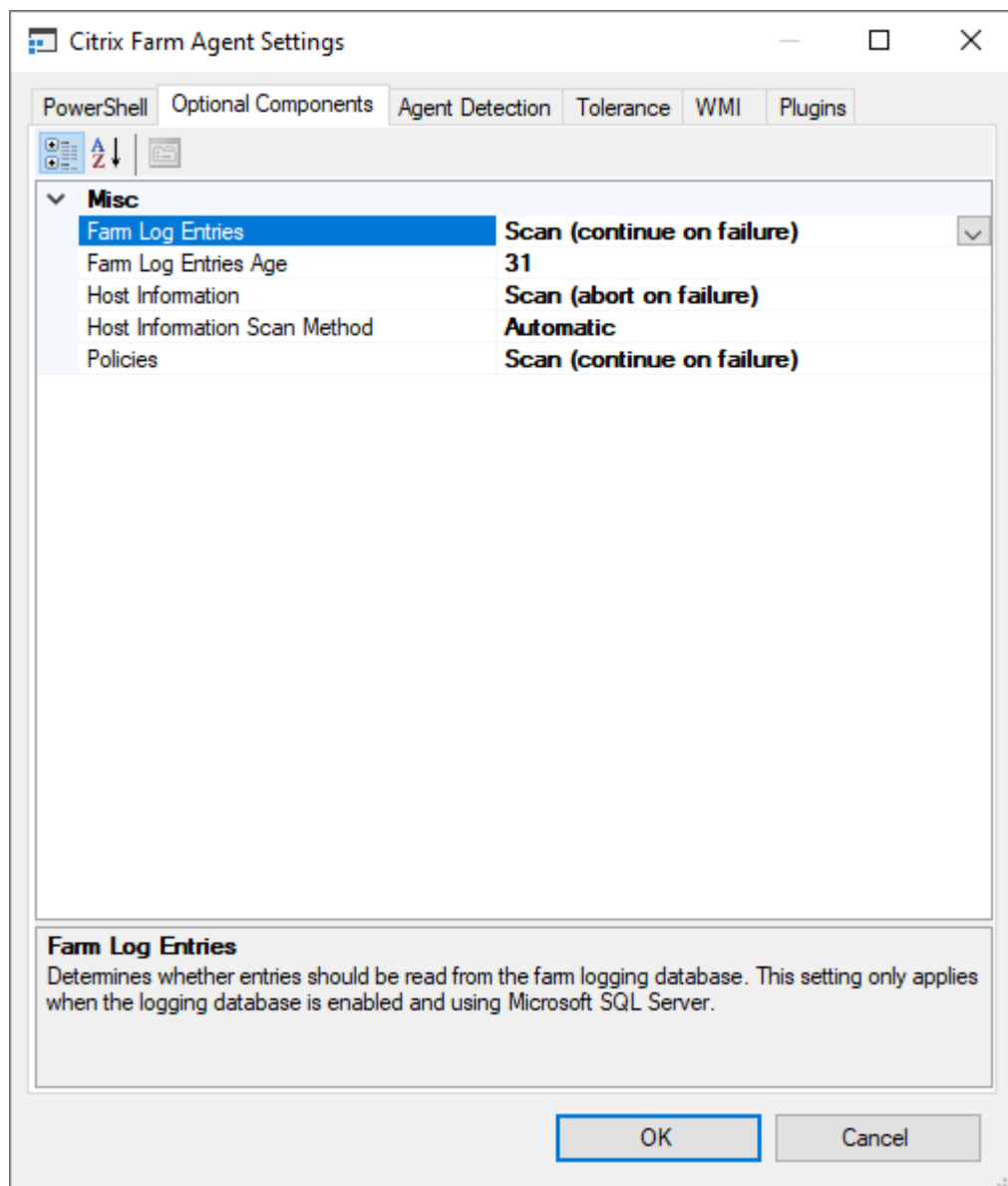
Agent Settings



PowerShell Remote Connection Settings

The [PowerShell connection settings](#) to use to connect to the remote machine.

Optional Components



Farm Log Entries

Determines whether entries should be read from the farm logging database. This setting only applies when the logging database is enabled and using Microsoft SQL Server.

Farm Log Entries Age

The age of the farm log entries to read in days. This setting only applies when the farm log entries are enabled.

Host Information

Determines whether host information such as serial number and operating system should be read from the servers in the farm. This [requires a PowerShell remoting](#) or WMI connection to be made to each host.

Host Information Scan Method

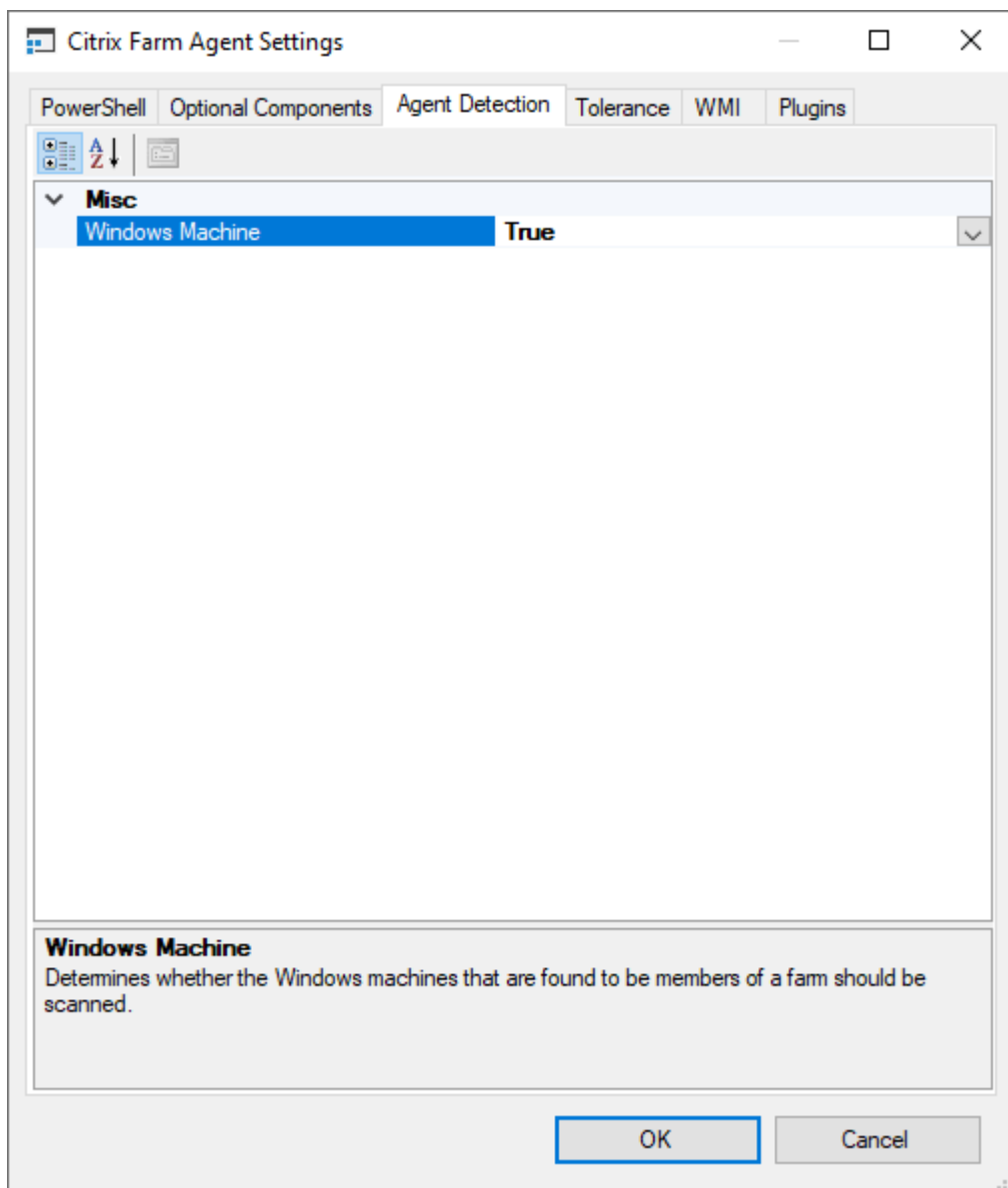
Determines the scan method to use for connecting to each host directly to collect host information - Automatic, PowerShell or WMI. When set to Automatic the system will attempt to connect to each

host using [PowerShell remoting](#), and if it fails will revert to a direct WMI connection.

Policies

Determines whether policies should be read from the farm.

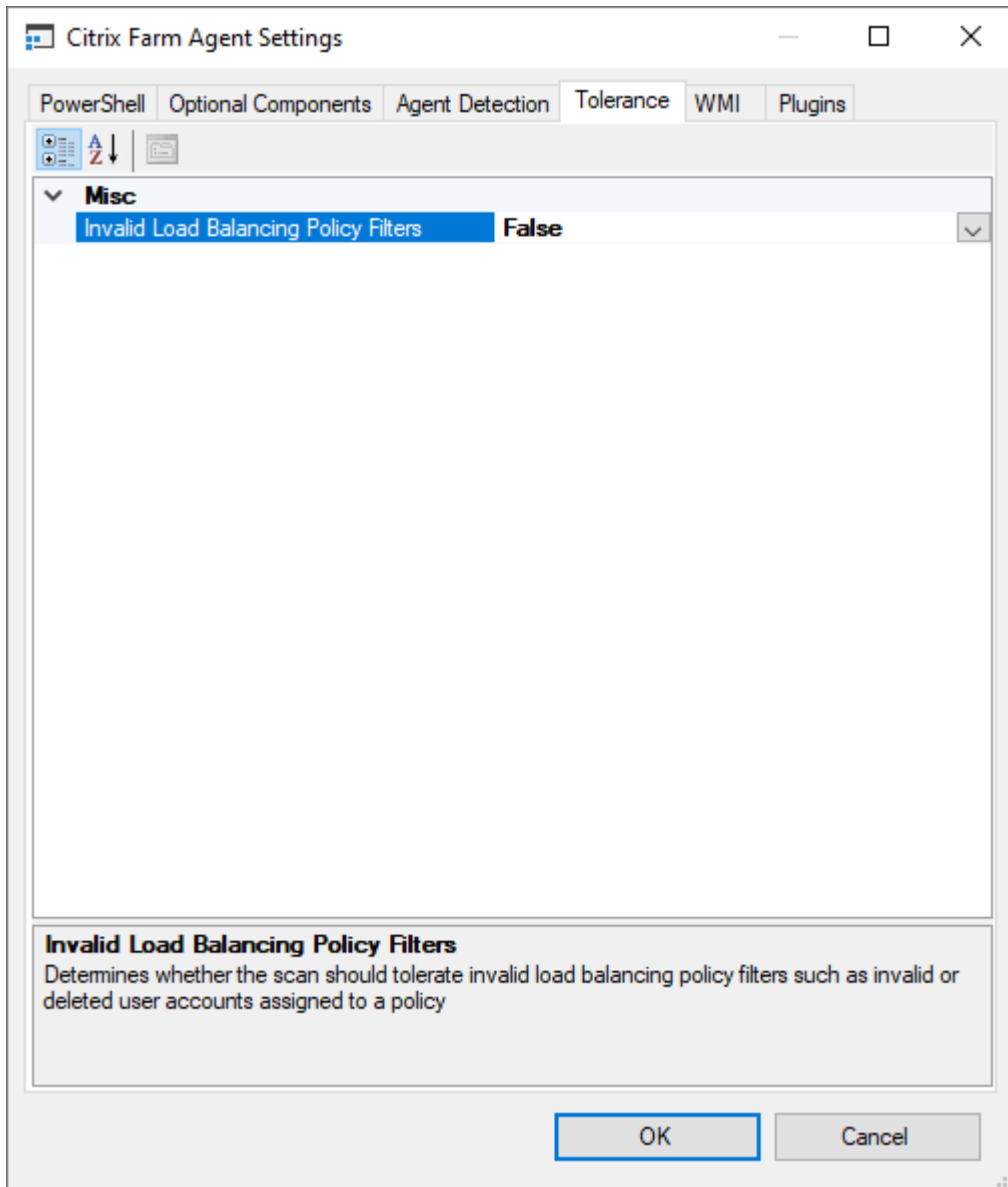
Agent Detection



Windows Machine

Determines whether to automatically launch a [Windows machine](#) scan agent against all servers participating in the [Citrix XenApp Farm](#). By default, this is true.

Tolerance

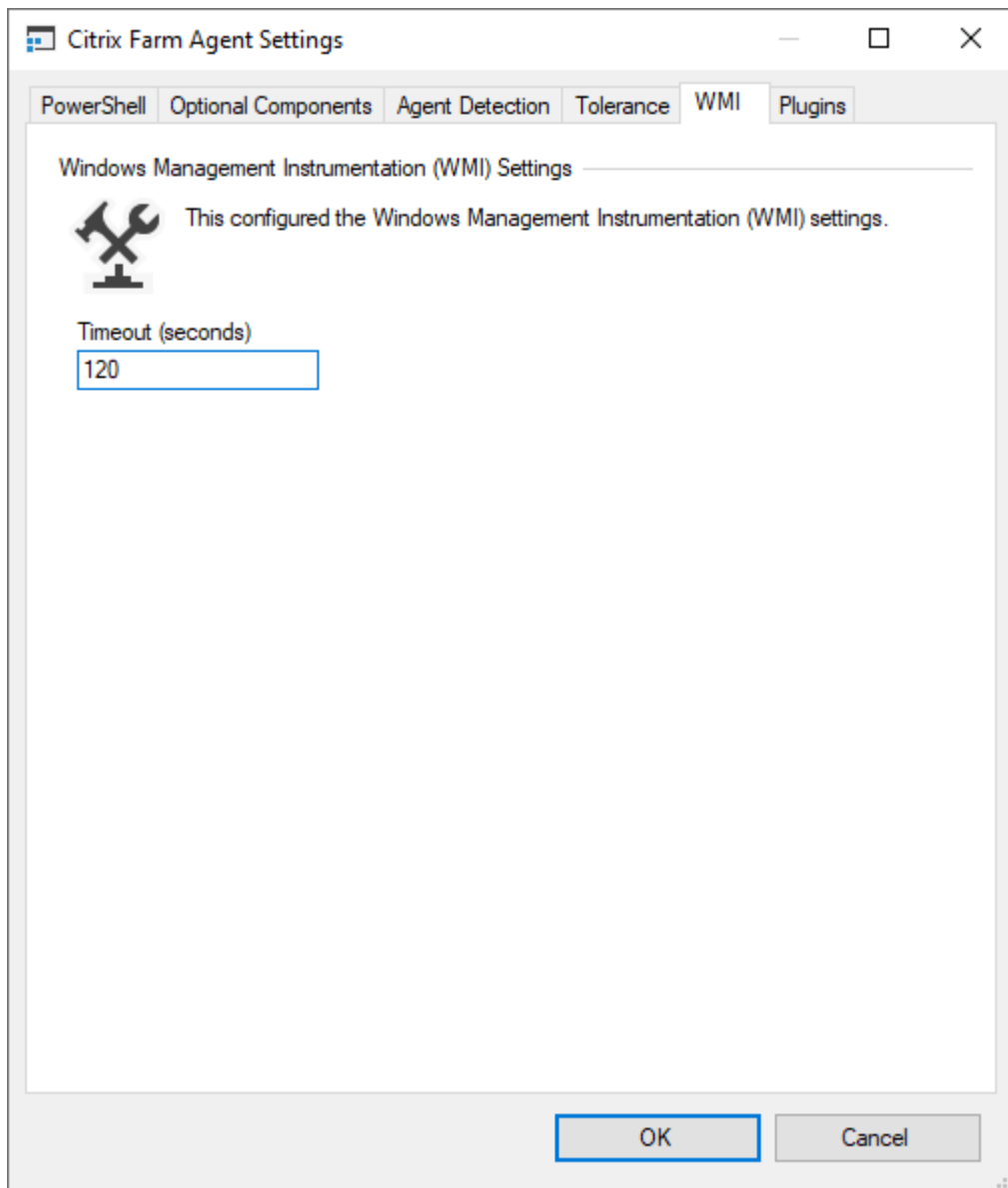


Invalid Load Balancing Policy Filters

Determines whether the scan should tolerate invalid load balancing policy filters such as invalid or deleted user accounts assigned to a policy.

For more information see the [Load balancing policies: Error resolving account](#) page.

WMI



WMI Timeout

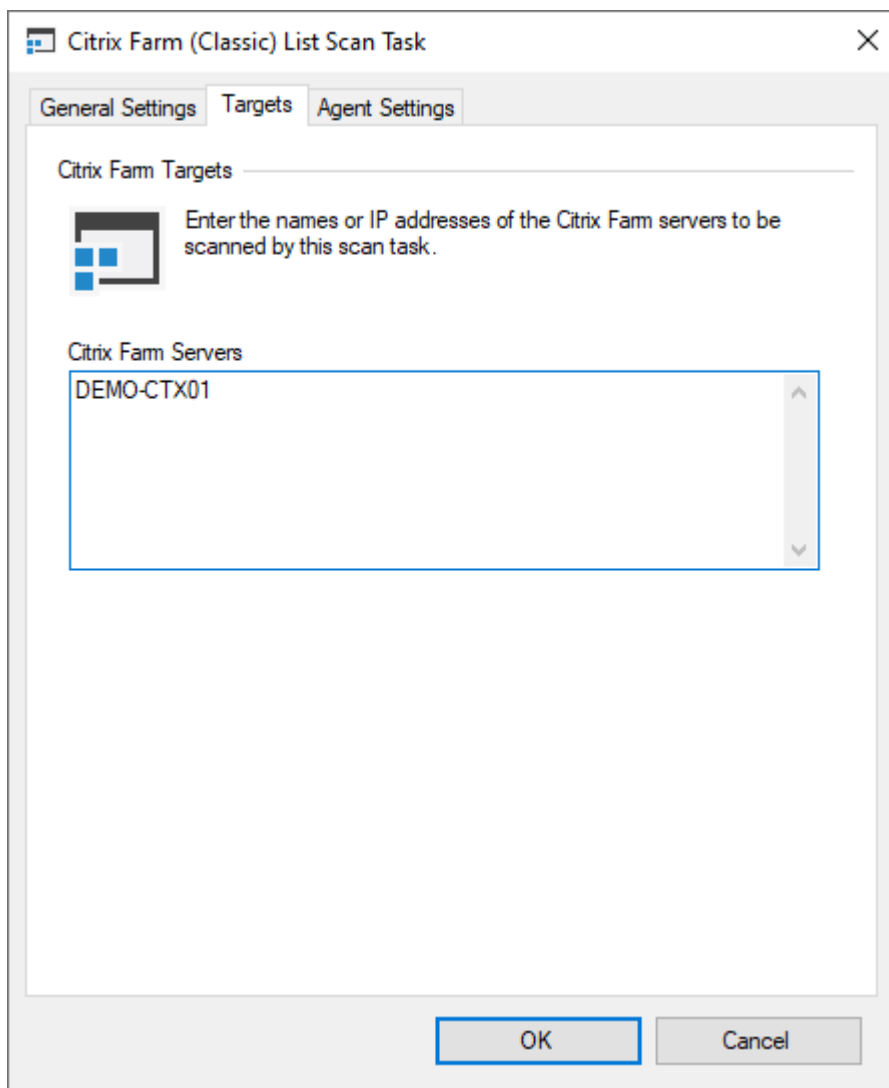
The timeout in seconds to use for WMI connections. This is only used when collecting the [optional component](#) host information, and a PowerShell connection cannot be made to the remote host.

Citrix Farm List Scan Task

The [Citrix farm](#) list scan task allows you to enter a list of Citrix servers participating in farms that you wish to scan. You need only specify the name of one server per farm.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Citrix XenApp farms](#).

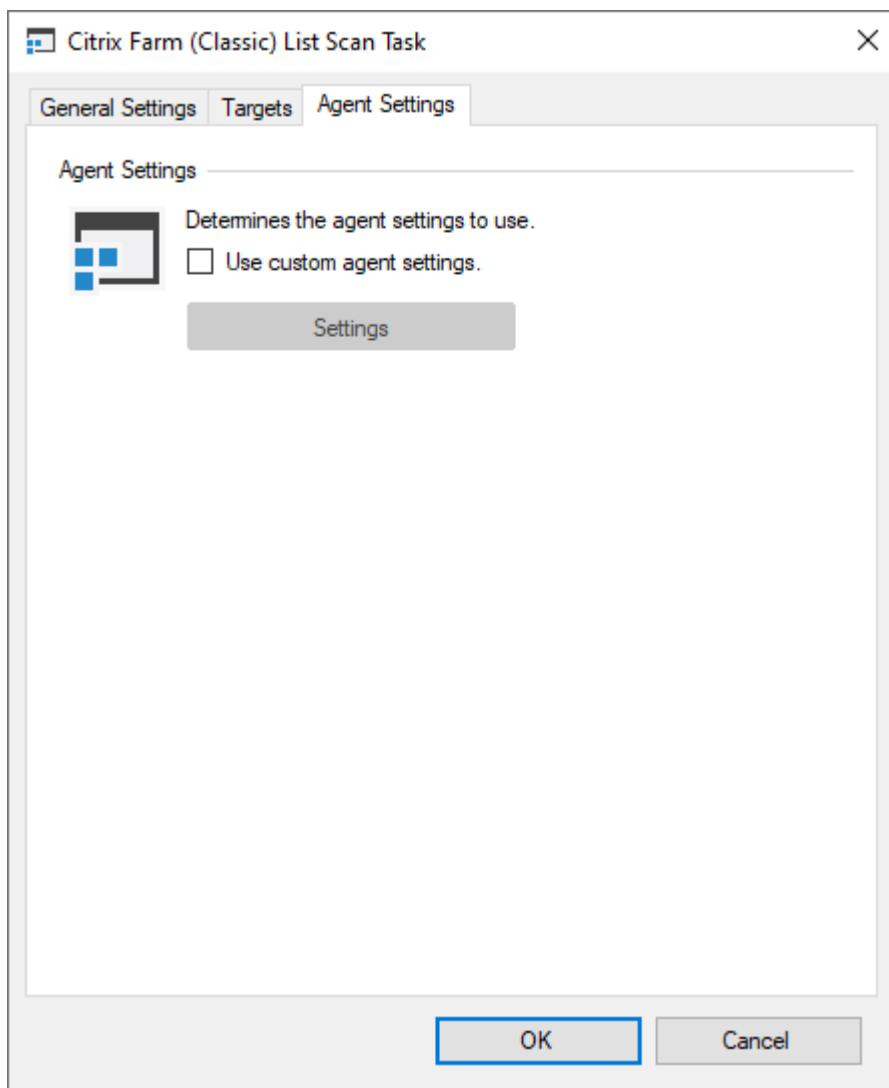
Targets



Citrix Farm Servers

The IP addresses, NetBIOS names, or fully qualified domain names of the Citrix Farm servers to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The [Citrix XenApp Farm](#) scan tasks are supported on the following platforms

- Citrix XenApp 6.5, Platinum Edition
- Citrix XenApp 6.5, Enterprise Edition
- Citrix XenApp 6.5, Advanced Edition
- Citrix XenApp 6.0, Platinum Edition
- Citrix XenApp 6.0, Enterprise Edition
- Citrix XenApp 6.0, Advanced Edition

Access Settings (PowerShell)

The scan tasks use Windows PowerShell Remoting to obtain information from a single server within the farm.

- Windows PowerShell 2.0 or above must be installed on the machine running the [XIA Configuration Client](#).
- Windows [PowerShell Remoting](#) must be [enabled](#) on the Citrix server even when installed on the same machine as the [XIA Configuration Client](#).
- Firewall access must allow access to the PowerShell Remoting (WinRM) port on the server.
- By default the XIA Configuration client service account (or the [custom credentials](#) in use) must have **Citrix View Only** or above rights to the farm, for more information see the following [page](#).

Windows Firewall

When using Windows Firewall with Advanced Security the following rules must be enabled.

- ✓ Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

Host Information

The [Citrix XenApp Farm](#) scan tasks are by default configured to collect [optional host information](#) such as manufacturer, and serial number from the host servers in the farm. This is by default collected using a direct [PowerShell remoting](#) connection to the hosts, however if this fails, a direct WMI connection will be attempted to the host servers.

- Please see the Access Settings (PowerShell) above for the PowerShell requirements for **each host** in the farm.

Host Information (WMI)

- Firewall access must allow access to the WMI ports on **each host** in the farm.
- By default, the [XIA Configuration Client service account](#) (or the [custom credentials](#) in use) must have administrator rights on the remote machine. This is a requirement for remote WMI access enforced by the operating system.

Host Information (WMI) - Windows Firewall

When using Windows Firewall with Advanced Security the following rules must be enabled.

- ✓ Windows Management Instrumentation (WMI-In)
This port allows the WMI queries directly.

Local Service

The [Citrix XenApp Farm](#) scan tasks do not support the [XIA Local Service](#).

Automatic Detection

- ✓ Citrix farm servers can be automatically detected and scanned by [Windows Machine Scan Tasks](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

0x80000007 Entry not found

Symptoms

When you scan a [Citrix XenApp Farm](#) you may see the error "0x80000007 Entry not found" - for example

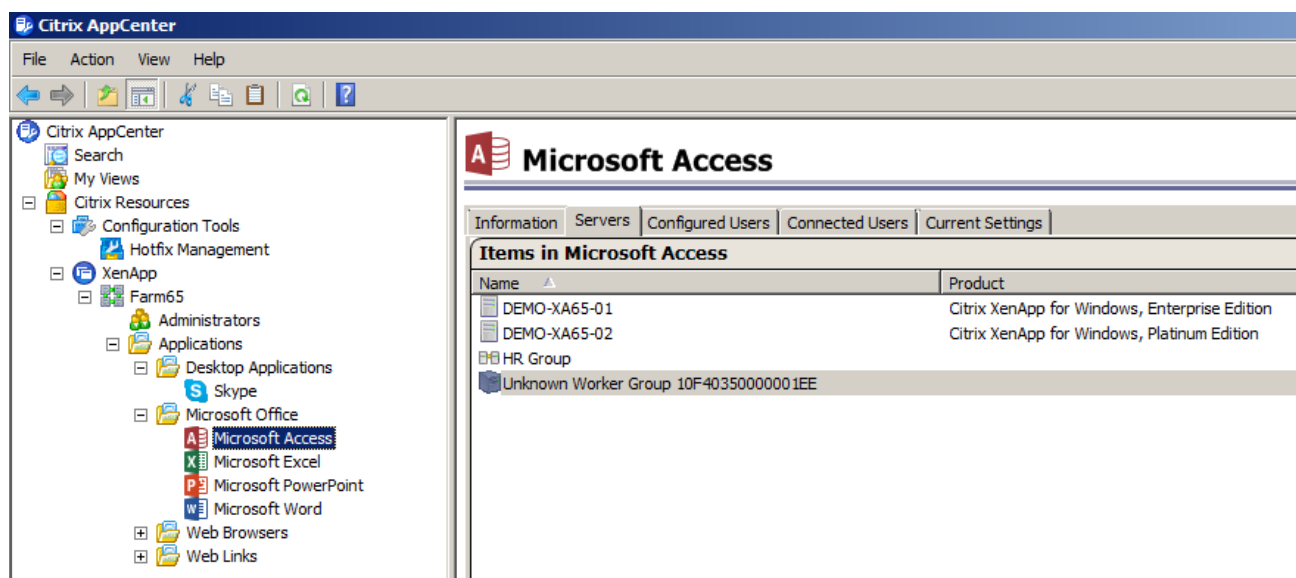
The Citrix XenApp farm agent encountered an exception when 'Reading **section**'. Error executing the command '*command*'. Cannot find *object* with id *objectidentifier* (0x80000007 Entry not found.).

Alternative errors may include

"Error getting data collector for zone *zonename* (0x802D0006)"

Cause

This error can be caused by objects that have become deleted from the Citrix Data Store but are still referenced by objects within the farm. When viewed in the Citrix AppCenter you see the object marked as "Unknown" - for example "Unknown Worker Group 10F403500000001EE".



Resolution

- Use the user interface to remove the corrupt objects

or

- Use the DSCHECK command to clean the Data Store. Ensure that you follow the guidance from Citrix when using support commands and have a full backup prior to executing these commands.
<http://support.citrix.com/article/CTX124406>

Access Denied Reading Zones

Symptoms

When you scan a [Citrix XenApp Farm](#) using either **View Only** or **Custom** credentials you may see the error

"The Citrix XenApp farm agent encountered an exception when 'Reading zones'. Access denied."

Cause

This error can be caused by an issue with Citrix XenApp 6.0 or 6.5.

Resolution

- To resolve the issue, ensure that the server is running the latest Citrix Hotfix Rollup pack. For Citrix XenApp 6.5 this issue was resolved in CTX136248 - "Hotfix Rollup Pack 2 for Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2".

or

- Alternatively, ensure the service account user performing the scan is configured as a Citrix administrator with **Full Admin** privilege.

Citrix commands must be executed at the Citrix server or using remoting.

Symptoms

When you scan a [Citrix XenApp Farm](#) you may see the error "Citrix commands must be executed at the Citrix server or using remoting. Make sure that your user account is a Citrix administrator and that the IMA service is started."

Cause

The user account being used to perform the scan does not have permissions to access the Citrix information.

Resolution

Within the Citrix management console ensure that the service account performing the scan is configured as a Citrix administrator with at least **View Only** privilege.



Administrators

Administrators | Information | Alerts

Citrix Administrator items in Administrators

Name	Privilege	Status
 DEMO-XA60-01\Administrators	View Only	Enabled

Could not load file or assembly 'System.Management.Automation'

Symptoms

When you scan a [Citrix XenApp Farm](#) you see the following error

"Could not load file or assembly 'System.Management.Automation, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35' or one of its dependencies. The system cannot find the file specified."

Cause

The [Citrix XenApp Farm Agent](#) uses Microsoft Windows PowerShell to gather information from the remote farm. The error is seen when Microsoft Windows PowerShell 2.0 or above is not installed on the machine running the [XIA Configuration Client](#).

Resolution

Install Windows PowerShell version 2.0 or above on the machine running the [XIA Configuration Client](#).

Error connecting to Citrix farm using Negotiate authentication

Symptoms

When scanning a [Citrix XenApp Farm](#) using [custom credentials](#) you may see the following error

The Citrix XenApp farm agent encountered an exception when 'Connecting to Citrix farm using Negotiate authentication'. Connecting to remote server failed with the following error message: The WinRM client cannot process the request. Default credentials with Negotiate over HTTP can be used only if the target machine is part of the TrustedHosts list or the Allow implicit credentials for Negotiate option is specified.

Cause

When scanning a [Citrix XenApp Farm](#) using [custom credentials](#) Negotiate authentication is used and the computer running the [XIA Configuration Client](#) must trust the remote machine before a remote PowerShell session can be established.

Resolution

For more information see the [Using Custom Credentials](#) section.

Error executing the command 'Get-XAFarm': The socket connection was aborted.

Symptoms

When scanning a server that is a member of [Citrix XenApp farm](#) you may see the following error

The Citrix XenApp farm agent encountered an exception when 'Reading general farm settings'. Error executing the command 'Get-XAFarm'. The socket connection was aborted. This could be caused by an error processing your message or a receive timeout being exceeded by the remote host, or an underlying network resource issue. Local socket timeout was '00:00:09.9960000'.

The value of the timeout displayed may differ.

Cause

This error can occur if the server being scanned is configured as [Session Host Only](#) and cannot communicate with a **Delivery Controller**.

Resolution

This error can safely be ignored as long as at least one server configured as a **Delivery Controller** is configured to be scanned.

- or -

If the scan must be conducted through the specified **Session Host Only** server complete the following steps

- Ensure that the **Citrix XenApp Command Remoting** service is running on the **Delivery Controller**.
- Ensure that the Citrix XenApp PowerShell remoting port (by default TCP/2513) is open on the **Delivery Controller**.

Load balancing policies: Error resolving account

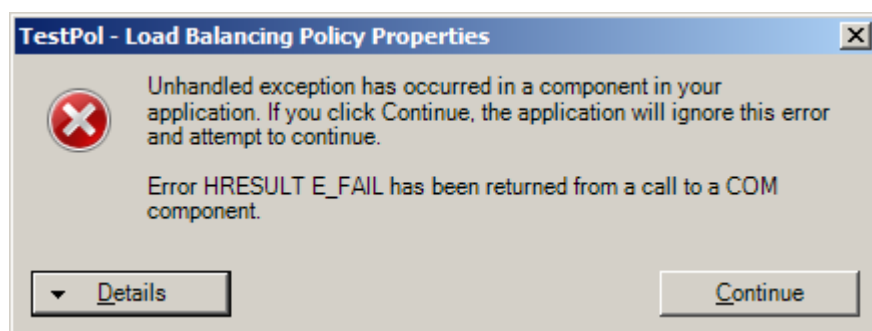
Symptoms

When you scan a [Citrix XenApp Farm](#) you may see the error when reading the load balancing policies.

"Error resolving account **Account GUID** (0x80130002)"

Cause

This error can occur when an invalid user account has been specified within the Filters > Users section of the load balancing policy. Viewing this in the Citrix management console may display the following error. An invalid user account may be caused by an account being assigned to the load balancing policy and subsequently being deleted.



Resolution

- Resolve the issue with the invalid user account in the load balancing policy.
- or
- Enable **Invalid Load Balancing Policy Filters** within the [tolerance settings](#).

Worker Group Organizational Units are not resolved

Symptoms

When you scan a [Citrix XenApp Farm](#) the organizational units assigned to a worker group may display in GUID format - for example "ad92cbab-3b86-4dea-bf83-a87d933de873".

Cause

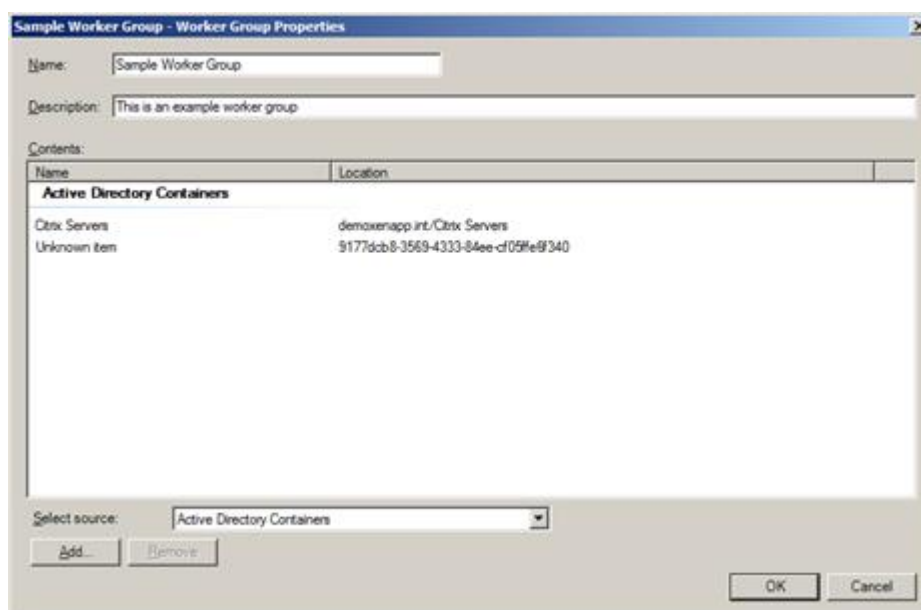
The Citrix XenApp PowerShell API returns the organizational units assigned to a worker group in GUID format. The [XIA Configuration Client](#) must communicate with Active Directory to determine the distinguished name of the organizational unit.

If there is an error the system will display the GUID in the results and the following error will be written to the [diagnostics trace log](#).

Error resolving the organizational unit with GUID '*GUID*' to the distinguished name.

Resolution

- Ensure that the organizational unit exists by viewing the worker group within the Citrix administrative tools.



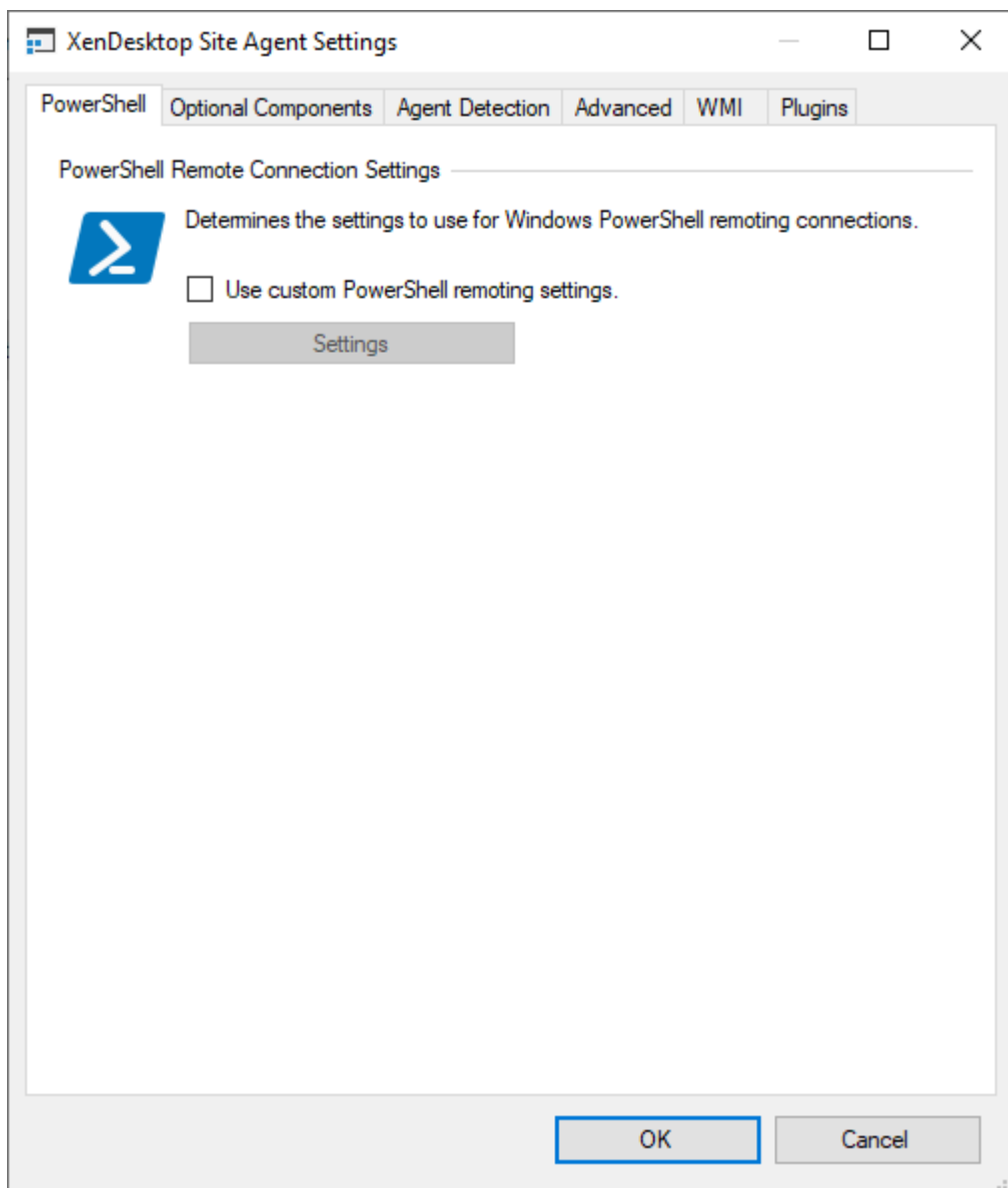
- If the organizational unit exists ensure that the [XIA Configuration Client](#) is able to communicate with Active Directory to resolve the organizational unit's GUID to its distinguished name.

Citrix XenDesktop Site

The Citrix XenDesktop Site scan tasks are able to document Citrix XenApp and XenDesktop (also known as [Citrix Virtual Apps and Desktops](#)) sites using [PowerShell remoting](#).

The data located by these tasks includes site configuration, applications, delivery groups, and machine catalogs.

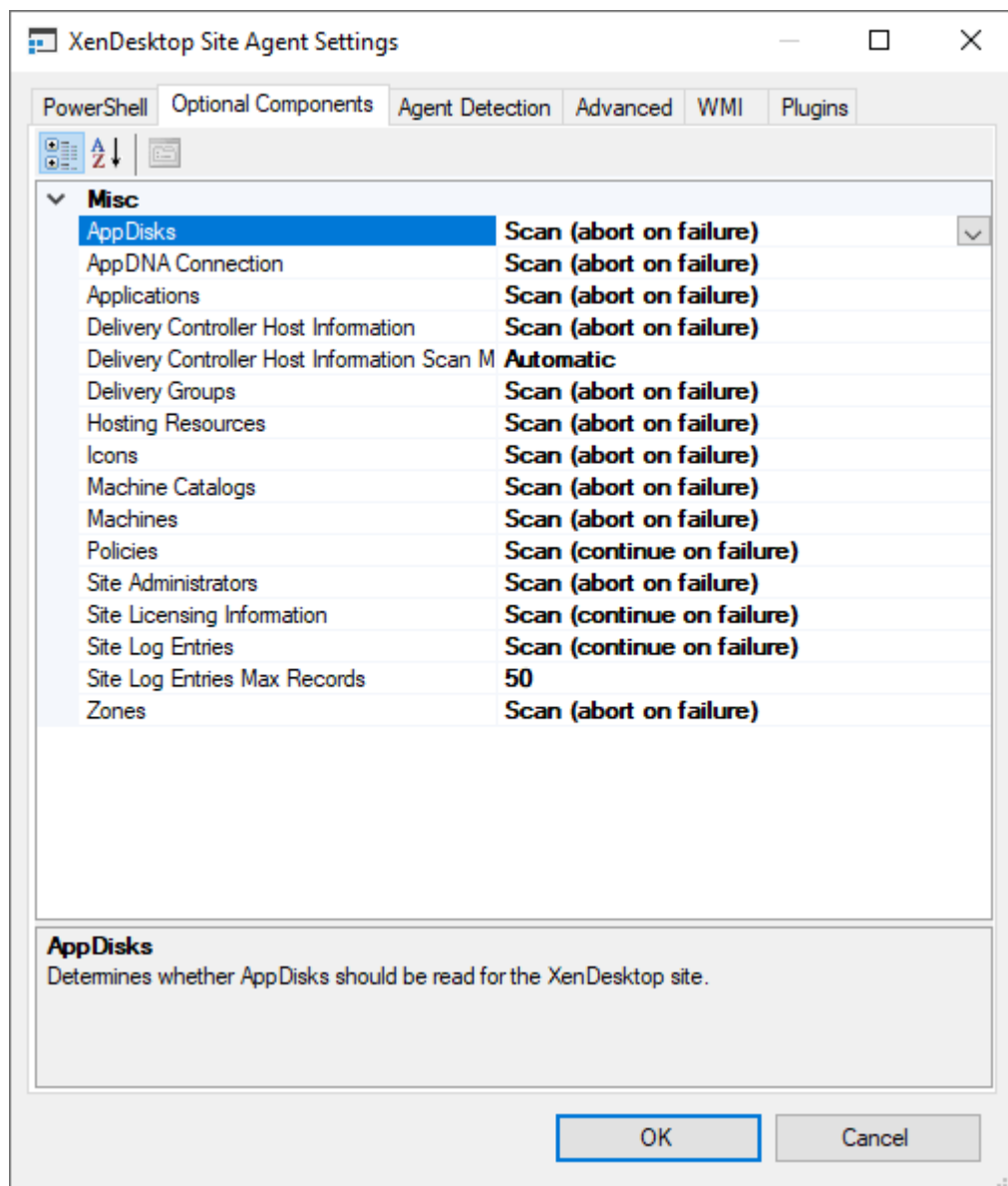
Agent Settings



PowerShell Remote Connection Settings

The [PowerShell connection settings](#) to use to connect to the remote machine.

Optional Components



AppDisks

Determines whether AppDisks should be read for the XenDesktop site.

AppDNA

Determines whether the connection details for AppDNA integration should be read for the XenDesktop site.

Applications

Determines whether applications should be read for the XenDesktop site.

Delivery Controller Host Information

Determines whether host information such as operating system name, manufacturer and model should be read from the delivery controller servers in the site. This requires a direct PowerShell remoting or WMI connection to be made to each host.

Delivery Controller Host Information Scan Method

Determines the scan method to use for connecting to each delivery controller directly to collect host information - Automatic, PowerShell or WMI. When set to Automatic the system will attempt to connect to each delivery controller using [PowerShell remoting](#), and if it fails will revert to a direct WMI connection.

Delivery Groups

Determines whether delivery groups should be read for the XenDesktop site.

Hosting Resources

Determines whether to read the hosting units (resources) configured for hypervisor (hosting) connections.

Icons

Determines whether to read the icons configured for items such as applications and delivery groups in the site.

Machine Catalogs

Determines whether machine catalogs should be read for the site.

Machines

Determines whether the machines providing the services should be read for the site.

Policies

Determines whether policies should be read from the site.

Site Administrators

Determines whether to read information about the administrators configured in the site.

Site Licensing Information

Determines whether licensing information should be read for the site.

Site Log Entries

Determines whether entries should be read from the site logging database. This setting only applies when the logging database is enabled for the site.

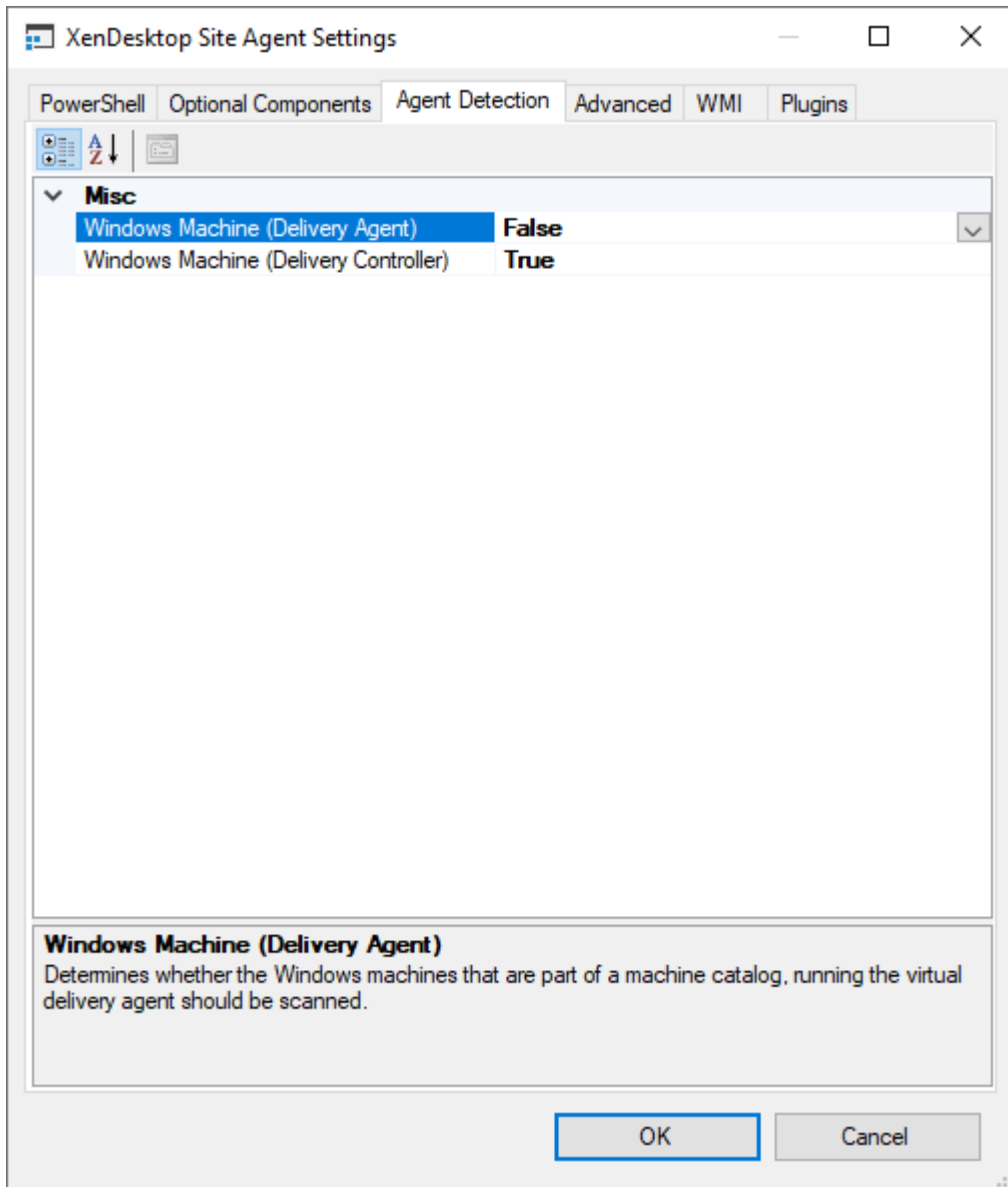
Site Log Entries Max Records

The maximum number of site log entries to read. This setting only applies when the site log entries are enabled.

Zones

Determines whether the Zones should be read for the XenDesktop site.

Agent Detection



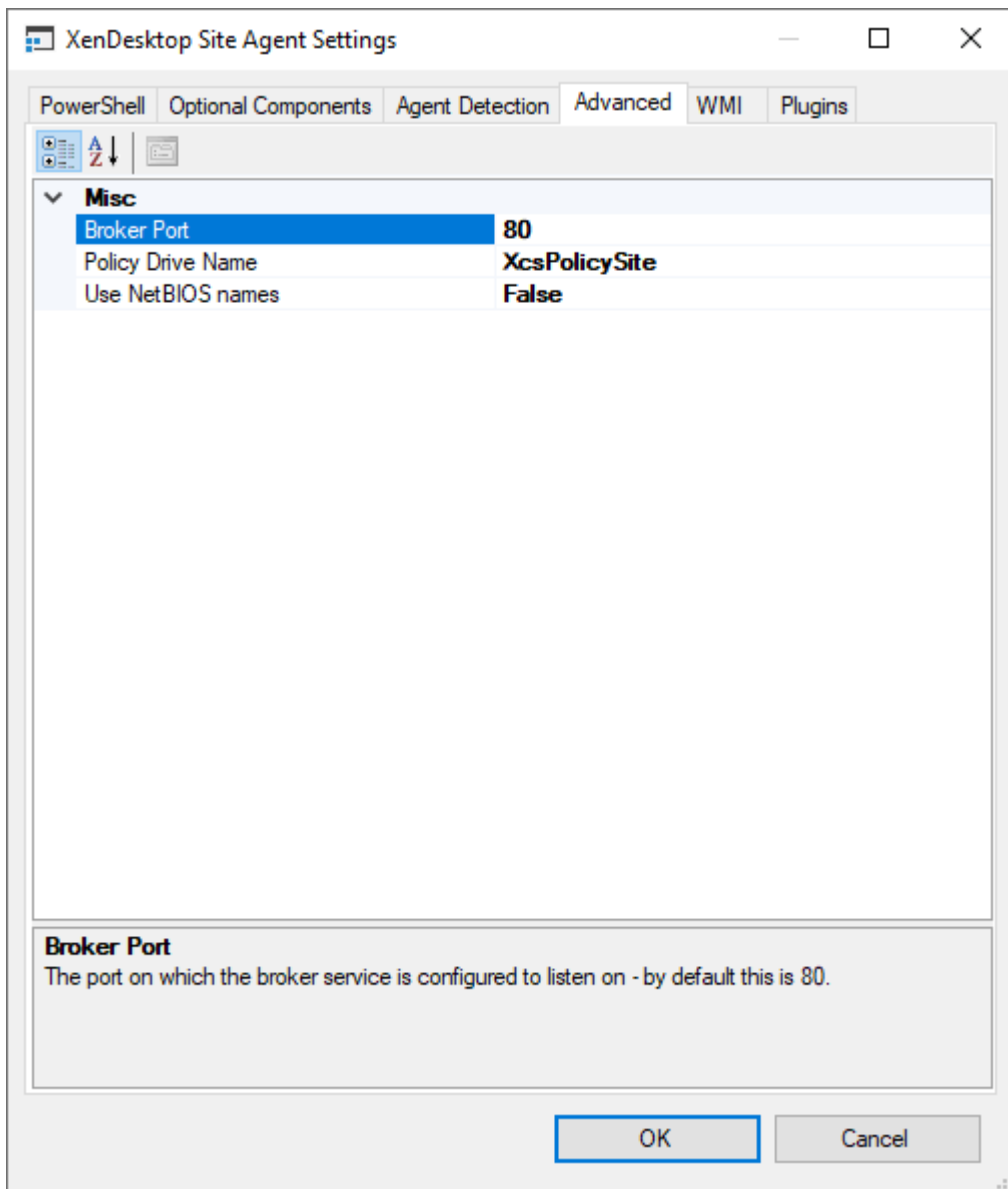
Windows Machine (Delivery Agent)

Determines whether to automatically launch a [Windows machine](#) scan agent against all machines running the Virtual Delivery Agent in the [Citrix XenDesktop Site](#). By default, this is false.

Windows Machine (Delivery Controller)

Determines whether to automatically launch a [Windows machine](#) scan agent against all servers acting as Delivery Controllers in the [Citrix XenDesktop Site](#). By default, this is true.

Advanced



Broker Port

The port on which the broker service is configured to listen on - by default this is 80.

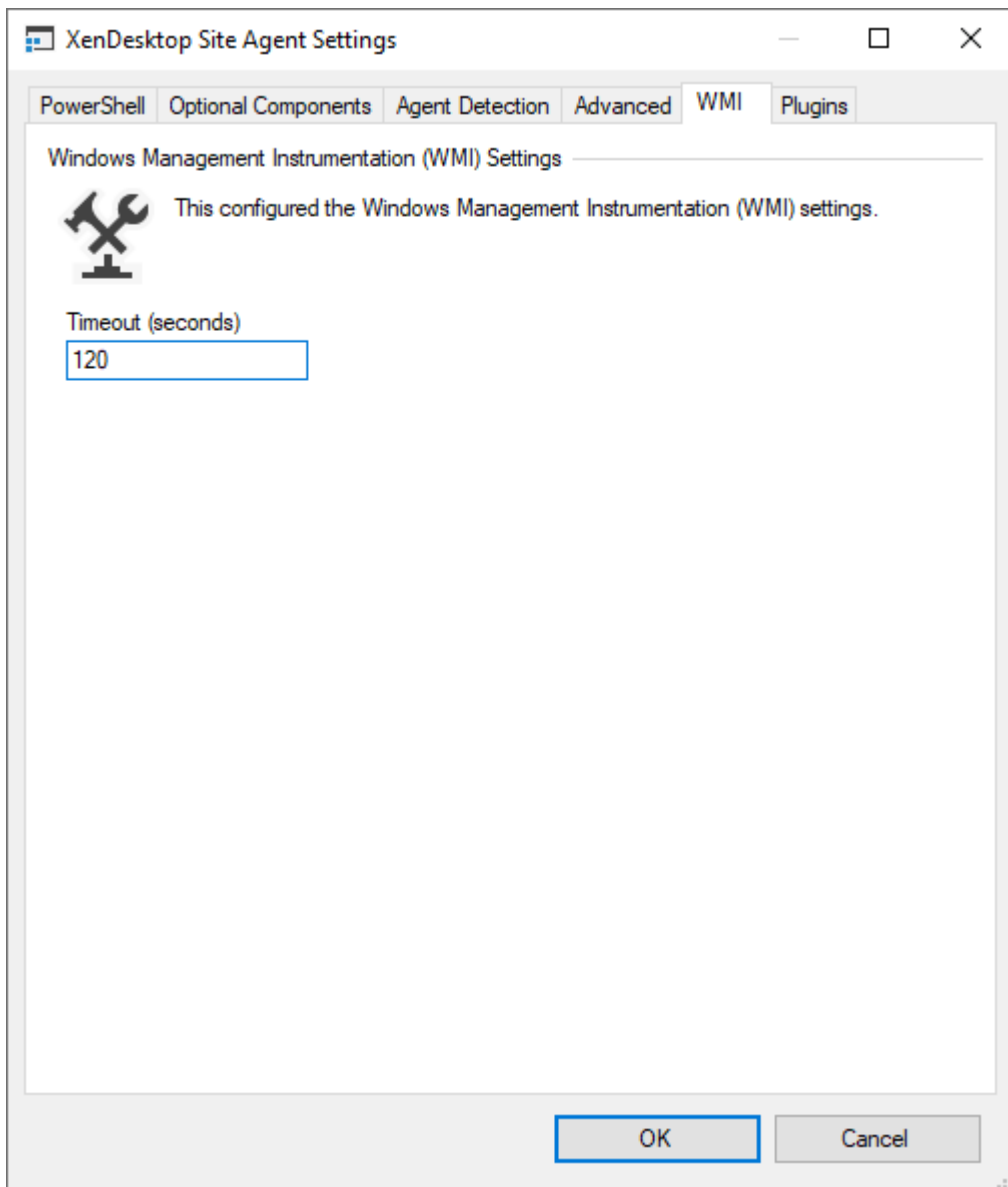
Policy Drive Name

The name of the temporary PowerShell drive name to use to access the site policies.

Use NetBIOS Names

Determine whether to use the NetBIOS names - for example "CORP-CTX01" when gathering host information and for agent detection. This setting does not apply when reading the site licensing information.

WMI



WMI Timeout

The timeout in seconds to use for WMI connections.

This is used when collecting the optional [delivery controller host information](#) using WMI if [PowerShell Remoting](#) is not available for these machines.

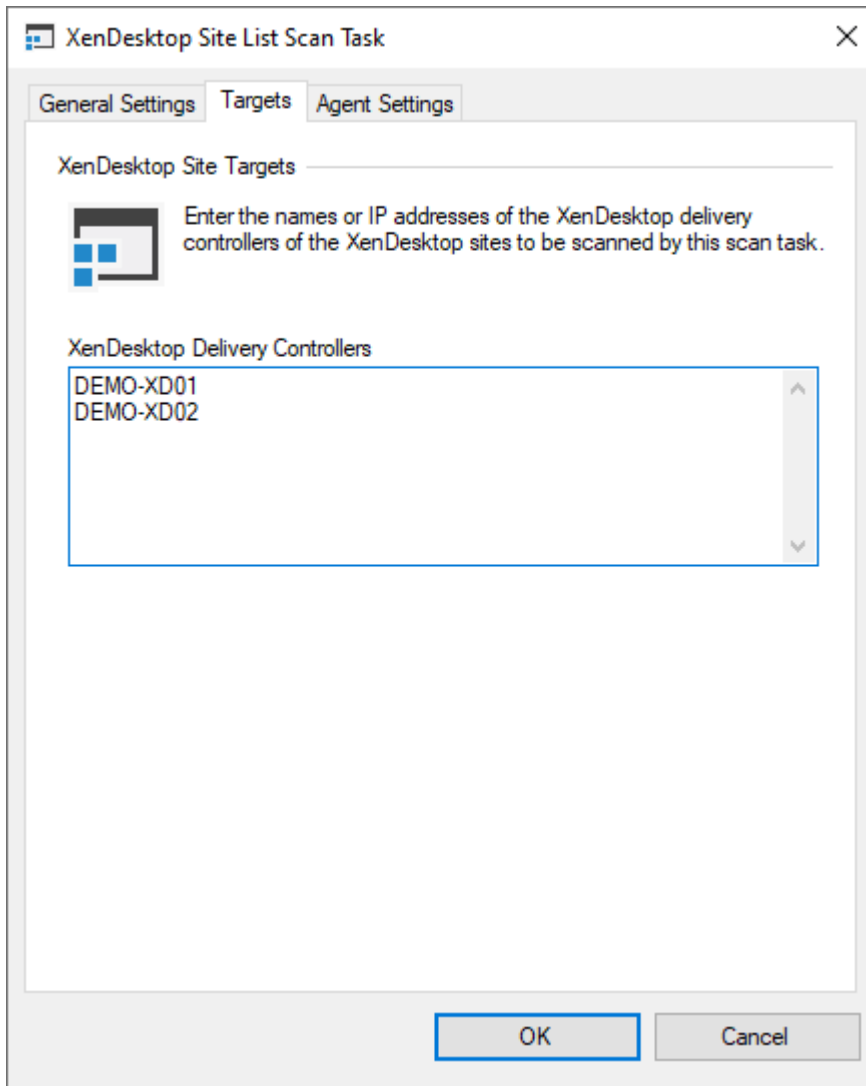
Citrix XenDesktop Site List Scan Task

The [Citrix XenDesktop Site](#) list scan task allows you to enter a list of Citrix Delivery Controller servers participating in sites that you wish to scan.

NOTE: You need only specify the name of one server per site.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Citrix XenDesktop sites](#).

Targets



The image shows a Windows-style dialog box titled "XenDesktop Site List Scan Task". It has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the dialog, there is a section titled "XenDesktop Site Targets" with a XenDesktop icon and a text box for entering names or IP addresses. Below this is a list box titled "XenDesktop Delivery Controllers" containing the entries "DEMO-XD01" and "DEMO-XD02". At the bottom of the dialog are "OK" and "Cancel" buttons.

XenDesktop Site List Scan Task

General Settings Targets Agent Settings

XenDesktop Site Targets

Enter the names or IP addresses of the XenDesktop delivery controllers of the XenDesktop sites to be scanned by this scan task.

XenDesktop Delivery Controllers

DEMO-XD01
DEMO-XD02

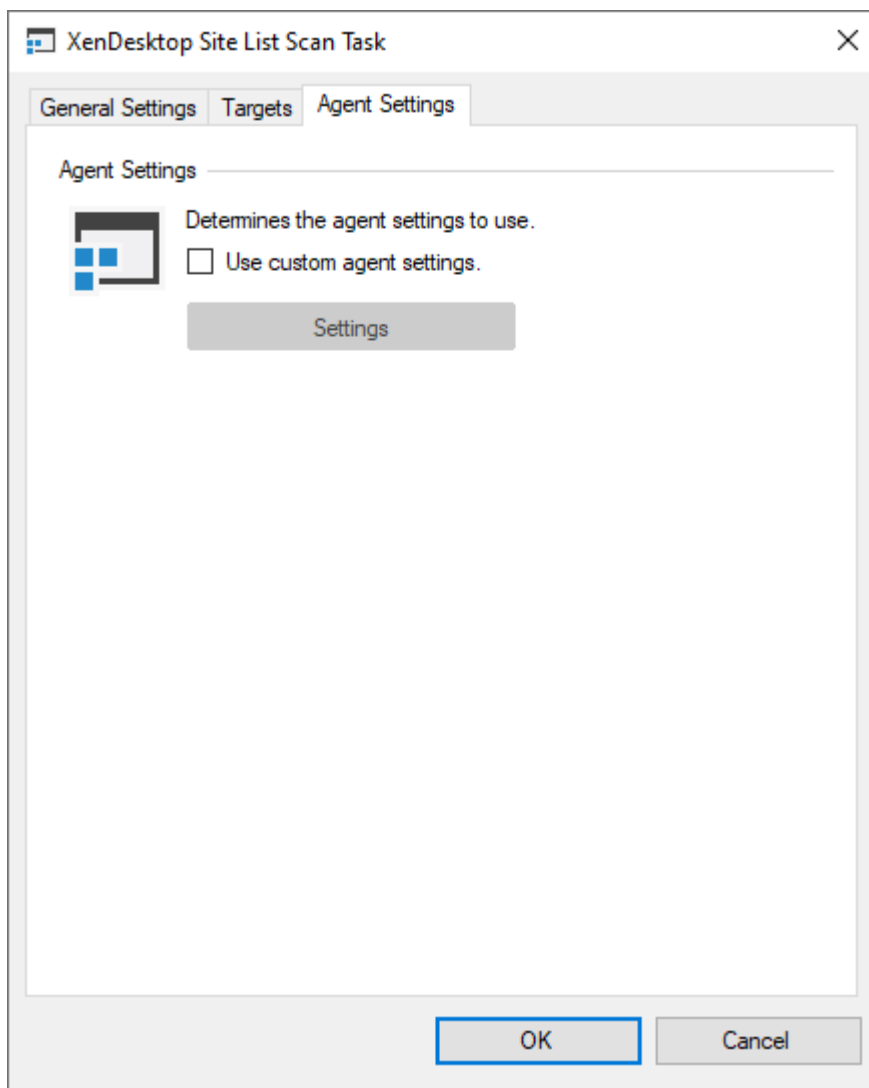
OK Cancel

XenDesktop Delivery Controllers

The IP addresses, NetBIOS names, or fully qualified domain names of the Citrix Delivery Controller servers to scan, one per line.

NOTE: You need only specify the name of one server per site.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The [Citrix XenDesktop site](#) scan tasks are supported on the following platforms

- Citrix Virtual Apps and Desktops 7 (*to version 2009*)
- Citrix XenApp / XenDesktop 7.x

Access Settings (PowerShell)

The scan tasks use [PowerShell remoting](#) to obtain information from a single delivery controller within the site and the license server.

- PowerShell 2.0 or above must be installed on the machine running the [XIA Configuration Client](#).
- [PowerShell remoting](#) must be enabled on the Citrix delivery controller even when installed on the same machine as the [XIA Configuration Client](#).
- The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) must have [Read Only Administrator](#) rights to the scope **All**.
- The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) must have **Read Only** rights within the **Licensing Administrators** section.
- The computer running the [XIA Configuration Client](#) service must be able to resolve and connect to the **license server** computer.

Windows Firewall

When using Windows Firewall with Advanced Security the following rules must be enabled.

NOTE: it is recommended that the PowerShell Remoting use a HTTPS connection.

Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

Host Information

The [Citrix XenDesktop Site](#) scan tasks are by default configured to collect [optional host information](#) such as manufacturer, and serial number from the delivery controllers in the site. This is by default collected using a direct [PowerShell remoting](#) connection to the delivery controllers, however if this fails, a direct WMI connection will be attempted to the delivery controllers.

- Please see the Access Settings (PowerShell) above for the PowerShell requirements for **each delivery controller** in the site.

Host Information (WMI)

- Firewall access must allow access to the WMI ports on **each delivery controller** in the site.
- By default, the [XIA Configuration Client service account](#) (or the [custom credentials](#) in use) must have administrator rights on the remote machine. This is a requirement for remote WMI access enforced by the operating system.

Host Information (WMI) - Windows Firewall

When using Windows Firewall with Advanced Security the following rules must be enabled.

Windows Management Instrumentation (WMI-In)

This port allows the WMI queries directly.

Local Service

The [Citrix XenDesktop Site](#) scan tasks do not support the [XIA Local Service](#).

Automatic Detection

 [Citrix XenDesktop Sites](#) can be automatically detected and scanned by [Windows Machine Scan Tasks](#).

Read Only Administrator Rights

The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) must have at least **Read Only Administrator** rights to the built in scope **All**.

This can be configured in Citrix Studio under **Configuration > Administrators**.

Edit Administrator

Administrator Name and Details

Name:

DEMOXENAPP\Administrator

Details:

Scope	Role
All	Read Only Administrator

Add...

Edit...

Delete

☒ Enable administrator

Clear check box to disable the administrator. No settings will be lost.

[Save full permissions report](#)

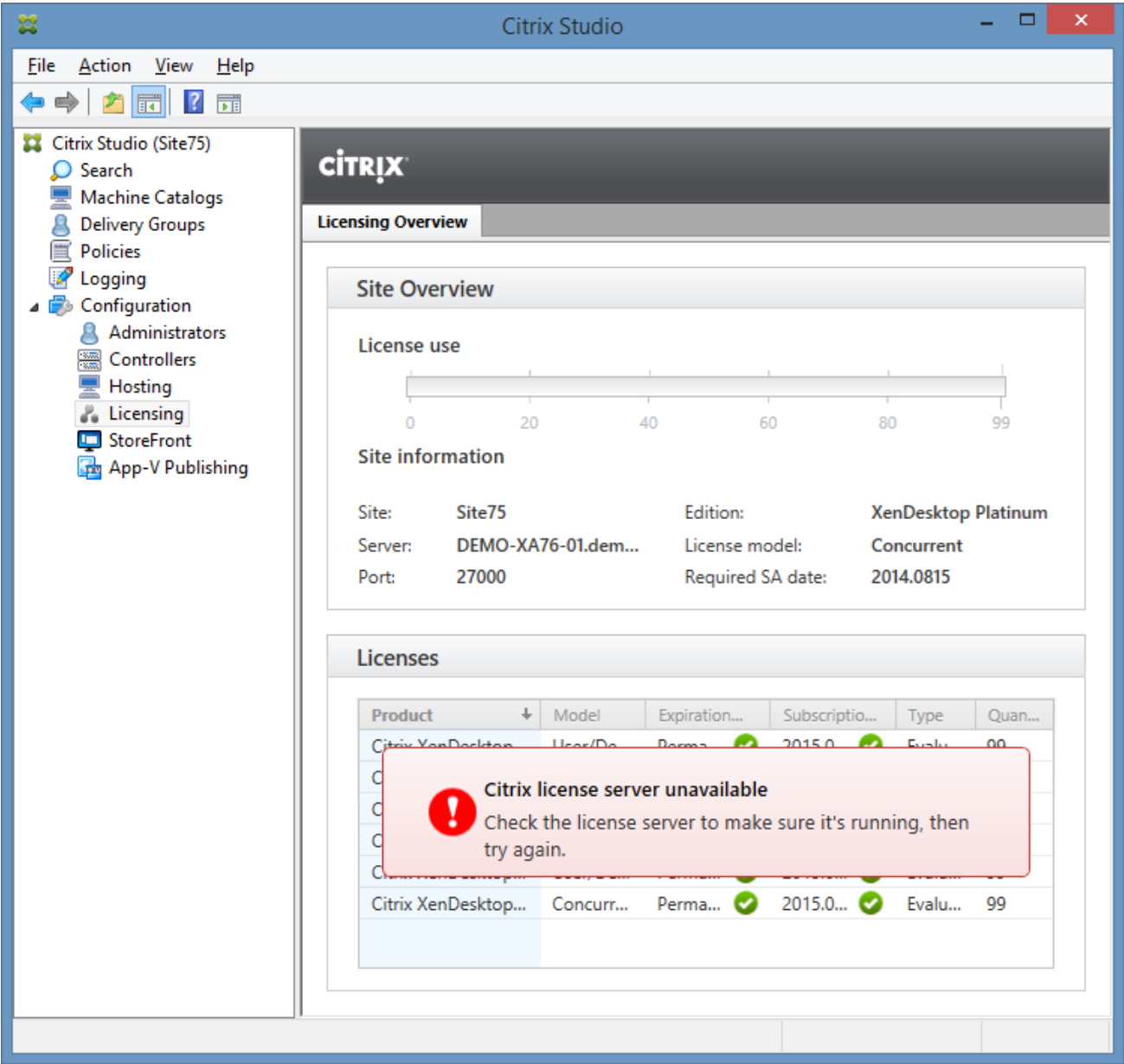
OK

Cancel

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

For all troubleshooting it is recommended that Citrix Studio is started on the delivery controller being scanned by the [Citrix XenDesktop Site](#) agent.



Could not load file or assembly 'System.Management.Automation'

Symptoms

When you scan a [Citrix XenDesktop Site](#) you see the following error

"Could not load file or assembly 'System.Management.Automation, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35' or one of its dependencies. The system cannot find the file specified."

Cause

The [Citrix XenDesktop Site Agent](#) uses Microsoft Windows PowerShell to gather information from the remote site. The error is seen when Microsoft Windows PowerShell 2.0 or above is not installed on the machine running the [XIA Configuration Client](#).

Resolution

Install Windows PowerShell version 2.0 or above on the machine running the [XIA Configuration Client](#).

Negotiate over HTTP error

Symptoms

When you scan a [Citrix XenDesktop Site](#) you see the following error

"The Citrix XenDesktop site agent encountered an exception when 'Connecting to the Citrix server using HTTP'. Connecting to remote server failed with the following error message: The WinRM client cannot process the request. Default credentials with Negotiate over HTTP can be used only if the target machine is part of the TrustedHosts list or the Allow implicit credentials for Negotiate option is specified. For more information, see the about_Remote_Troubleshooting Help topic."

Cause

The [Citrix XenDesktop Site Agent](#) uses Microsoft Windows PowerShell to gather information from the remote site. This error is seen when [custom credentials](#) are being used and the trusted hosts have not been configured for PowerShell.

Resolution

Follow the [Using Custom Credentials and PowerShell Remoting](#) instructions for the machine running the [XIA Configuration Client](#).

Permission to perform the operation was denied.

Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error 'Permission to perform the operation was denied.'

Cause

This can occur when the [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) do not have permissions required to the [Citrix XenDesktop Site](#).

Resolution

More information about the permissions required can be found in the [Requirements](#) and [Read Only Administrator Rights](#) sections.

The agent failed to scan the section 'Hosting Units'

Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error

The Citrix XenDesktop site agent encountered an exception when 'Reading resource '*name*' for hypervisor connection '*connection name*'. The agent failed to scan the section 'Hosting Units'. Error executing the command 'Get-Item'. Cannot find path 'XDHyp:\Connections*connection name**storagename*' because it does not exist.

Cause

This error can occur if the storage assigned to a resource has been renamed or deleted on the hypervisor.

CITRIX

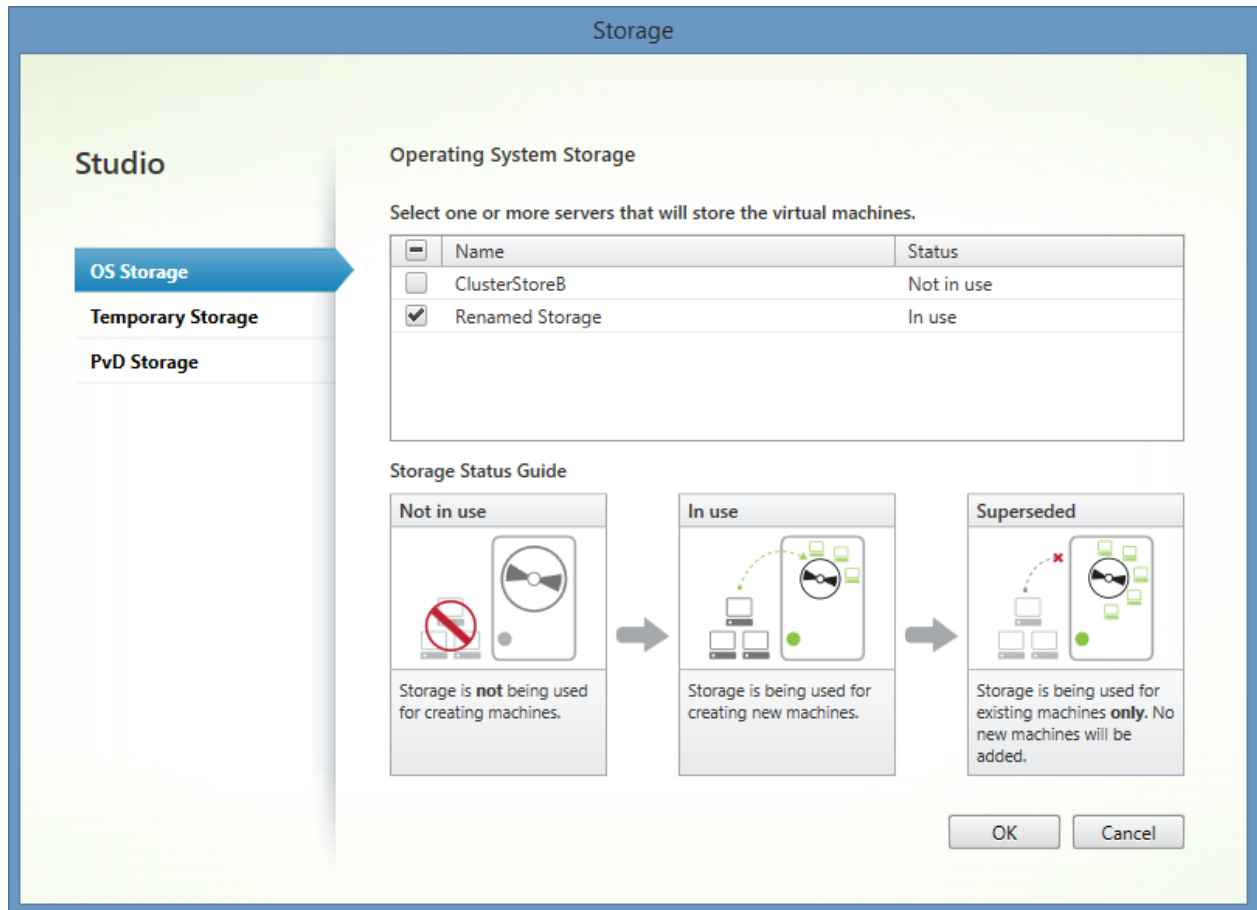
Name	Type	Address	State
vSphere Connection	VMware vSphere®	https://demo-vc51	Enabled
vSphere Resources			

The old or invalid storage name is displayed in the storage section.

Storage	
Standard storage	ClusterStoreA
Personal vDisk storage	ClusterStoreA
Temporary storage	ClusterStoreA

Resolution

- Refresh the storage view
- Right click the resources and select *Edit Storage*
- Confirm that the renamed, or valid storage is selected for each storage type and click OK.



- Or -

- Go to the [optional components](#) section within the [agent settings](#) and configure the *Hosting Resources* option as required.

The agent failed to scan the section 'Site Licensing Information'. CitrixLicensingVendorOrServiceDown

Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error "The agent failed to scan the section 'Site Licensing Information'. CitrixLicensingVendorOrServiceDown".

Cause

The configured Citrix XenDesktop license server is not configured correctly, or has failed.

Resolution

- Open the "Citrix License Administration Console" on the licensing server.
- Ensure that the vendor daemon is started and that licenses are available.

Concurrent Licenses

Vendor Daemon: CITRIX

Product	SA Date	In Use (Available)	Expiration	
▼ Citrix License Server Diagnostics License Server	2038.0101	0 (10000)	1-JAN-2038	System
▼ Citrix Start-up License Server	2038.0101	0 (10000)	PERMANENT	System

- or -

- Go to the [optional components](#) section within the [agent settings](#), and configure the *Site Licensing Information* option as required.

The agent failed to scan the section 'Site Licensing Information'.
CommunicationsError.

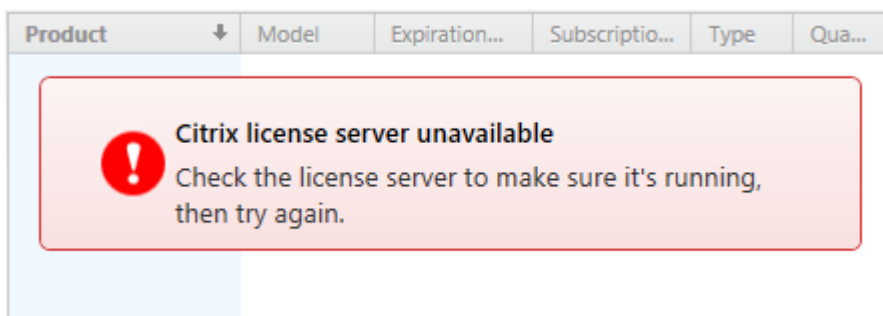
Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error "The agent failed to scan the section 'Site Licensing Information'. CommunicationsError".

Cause

The Citrix XenDesktop server being scanned cannot communicate with the Citrix Licensing server.

To validate the issue open Citrix Studio on the Citrix XenDesktop server being scanned and go to Configuration > Licensing.



Resolution

- Ensure the "Citrix Licensing" service is running on the licensing server.
- Ensure the "Citrix Web Services for Licensing" service is running on the license server.
- Follow the documentation provided with your version of Citrix XenDesktop for further troubleshooting,

Or

- Go to the [Optional Components](#) section within the [Agent Settings](#) and configure the **Site Licensing Information** option appropriately.

The agent failed to scan the section 'Site Licensing Information'. The server name cannot be resolved.

Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error

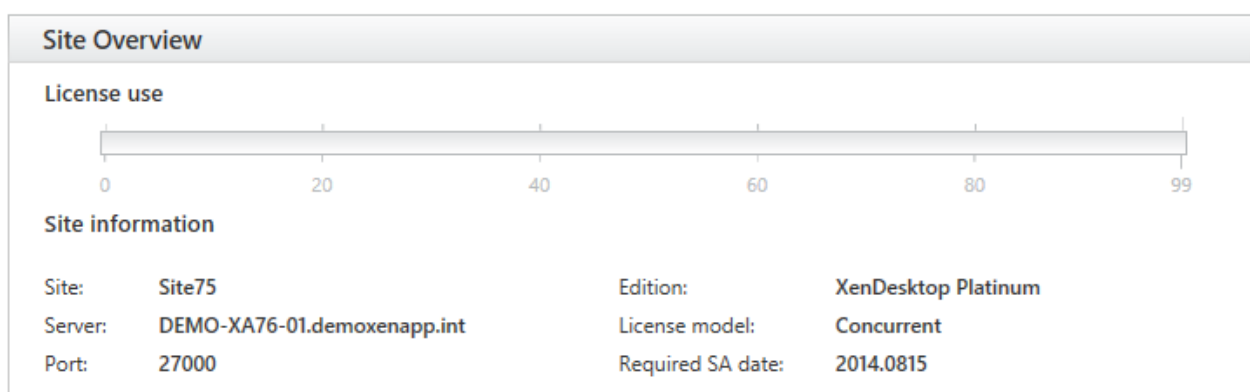
"The agent failed to scan the section 'Site Licensing Information'. Connecting to remote server failed with the following error message: The WinRM client cannot process the request because the server name cannot be resolved. For more information, see the [about_Remote_Troubleshooting](#) Help topic."

Cause

The computer running the [XIA Configuration Client](#) cannot resolve the name of the Citrix Licensing server.

Resolution

- Open Citrix Studio, and navigate to Configuration > Licensing



- Ensure that the computer running the [XIA Configuration Client](#) can resolve the specified **Server** name.

Or

- Go to the [Optional Components](#) section within the [Agent Settings](#) and configure the **Site Licensing Information** option appropriately.

The agent failed to scan the section 'Site Licensing Information'.

UserNotAuthorized

Symptoms

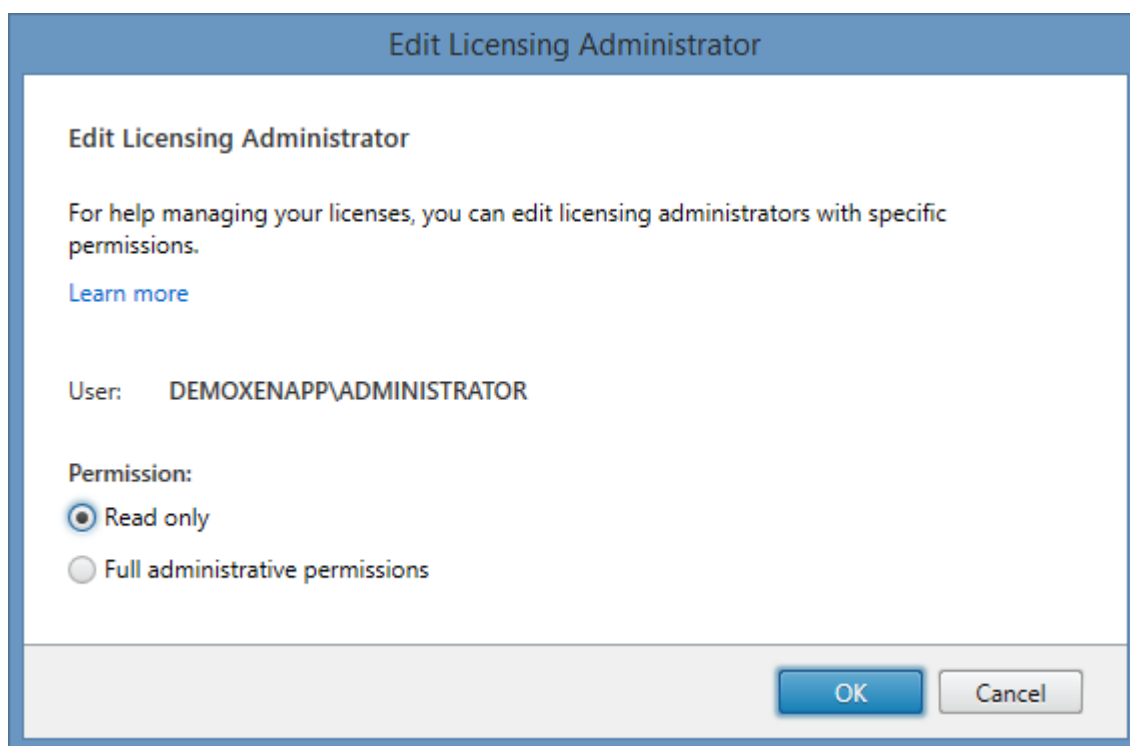
When you scan a [Citrix XenDesktop Site](#) you receive the error "The agent failed to scan the section 'Site Licensing Information'. UserNotAuthorized".

Cause

The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) do not have the minimum **Read Only** rights within the **Licensing Administrators** section as described in the [Requirements](#) section.

Resolution

- Within Citrix Studio go to Configuration > Licensing
- Ensure that the [XIA Configuration Client](#) service account (or the [custom credentials](#)) have the minimum **Read Only** rights.



Or

- Go to the [Optional Components](#) section within the [Agent Settings](#) and configure the **Site Licensing Information** option appropriately.

The Citrix Licensing PowerShell SnapIn 'Citrix.Licensing.Admin.V1' is not installed.

Symptoms

When you scan a [Citrix XenDesktop Site](#) you receive the error

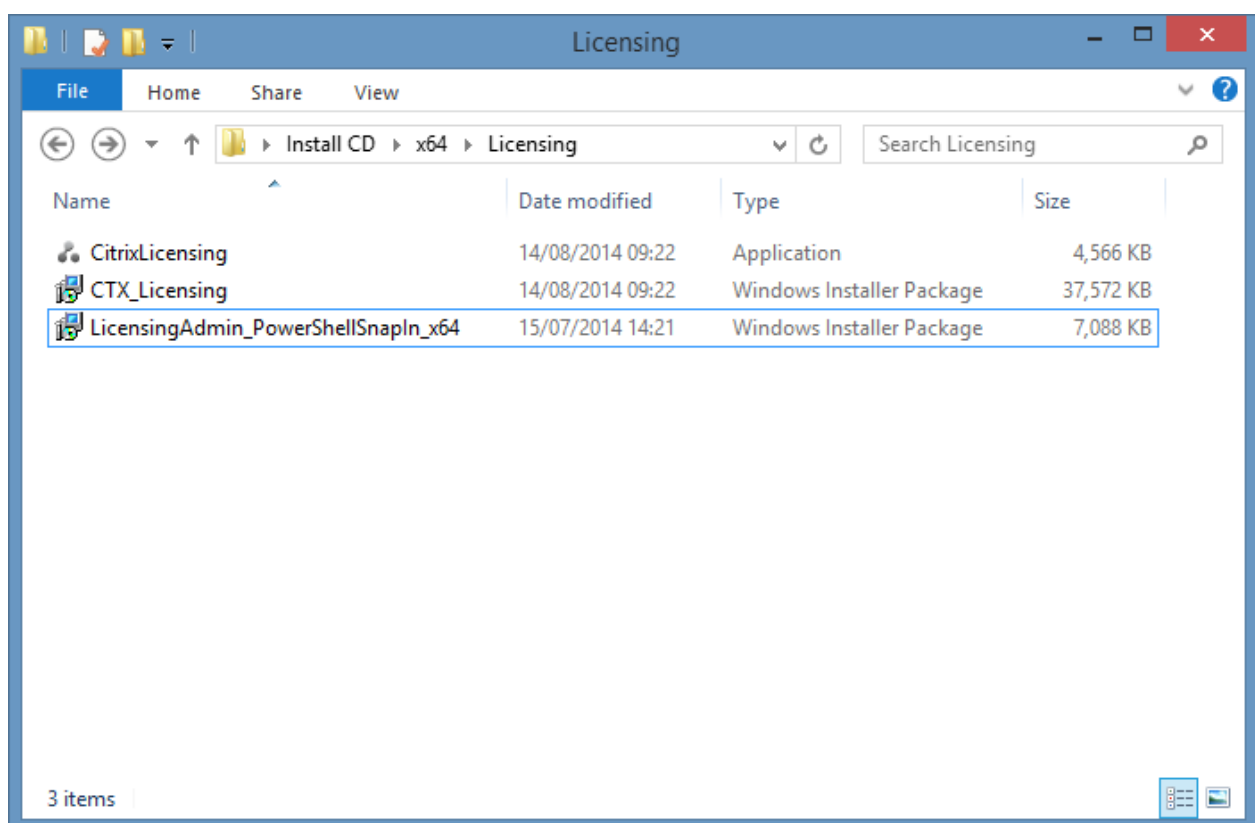
The agent failed to scan the section 'Site Licensing Information'. The Citrix Licensing PowerShell SnapIn 'Citrix.Licensing.Admin.V1' is not installed on the licensing server 'demo-xd-lic01'.

Cause

This can occur when the license server is installed on a dedicated machine but does not have the Citrix Licensing PowerShell SnapIn installed. The [Citrix XenDesktop Site Agent](#) connects directly to the license server to obtain information about available licenses and license administrators.

Resolution

- On the Citrix Licensing Server install the Citrix Licensing PowerShell SnapIn (LicensingAdmin_PowerShellSnapIn_x64.msi) found on the XenDesktop installation media.



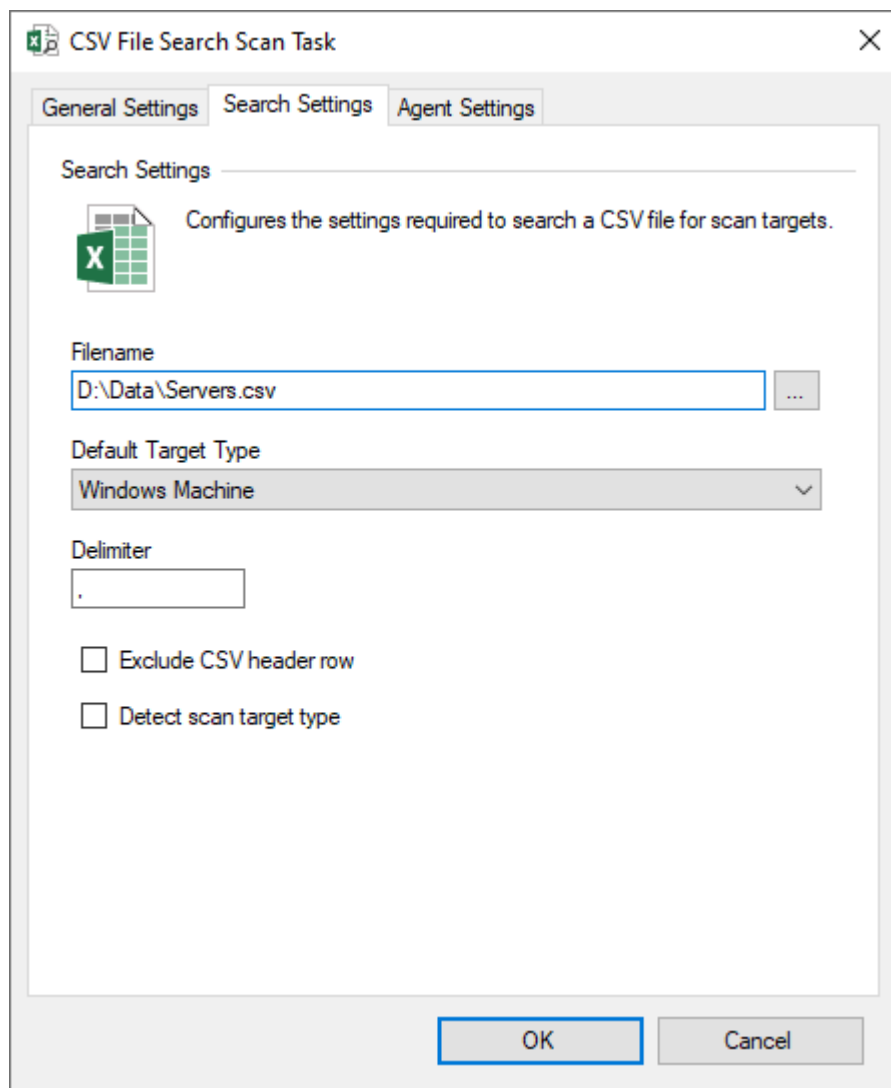
or

- Go to the [Optional Components](#) section within the [Agent Settings](#) and configure the **Site Licensing Information** option appropriately.

CSV File Search

The CSV file search [task](#) allows you to search a text file or CSV file for items to scan.

Search Settings



The screenshot shows a dialog box titled "CSV File Search Scan Task" with a close button (X) in the top right corner. It has three tabs: "General Settings", "Search Settings" (which is selected), and "Agent Settings". Below the tabs, the "Search Settings" section is titled "Search Settings" and includes a description: "Configures the settings required to search a CSV file for scan targets." with a small Excel icon. The settings include: a "Filename" text box containing "D:\Data\Servers.csv" with a browse button (...); a "Default Target Type" dropdown menu set to "Windows Machine"; a "Delimiter" text box containing a comma (,); and two checkboxes: "Exclude CSV header row" and "Detect scan target type", both of which are currently unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons.

Filename

The absolute path to the [CSV \(.csv\)](#) or [text file \(.txt\)](#). The filename may include environment variables, and reside on a UNC file share.

Default Target Type

The type of [item](#) to create if the [item type](#) is not specified within the file.

Delimiter

The delimiter used within the file, by default this is a comma. To use a tab delimiter the value `\t` should be used.

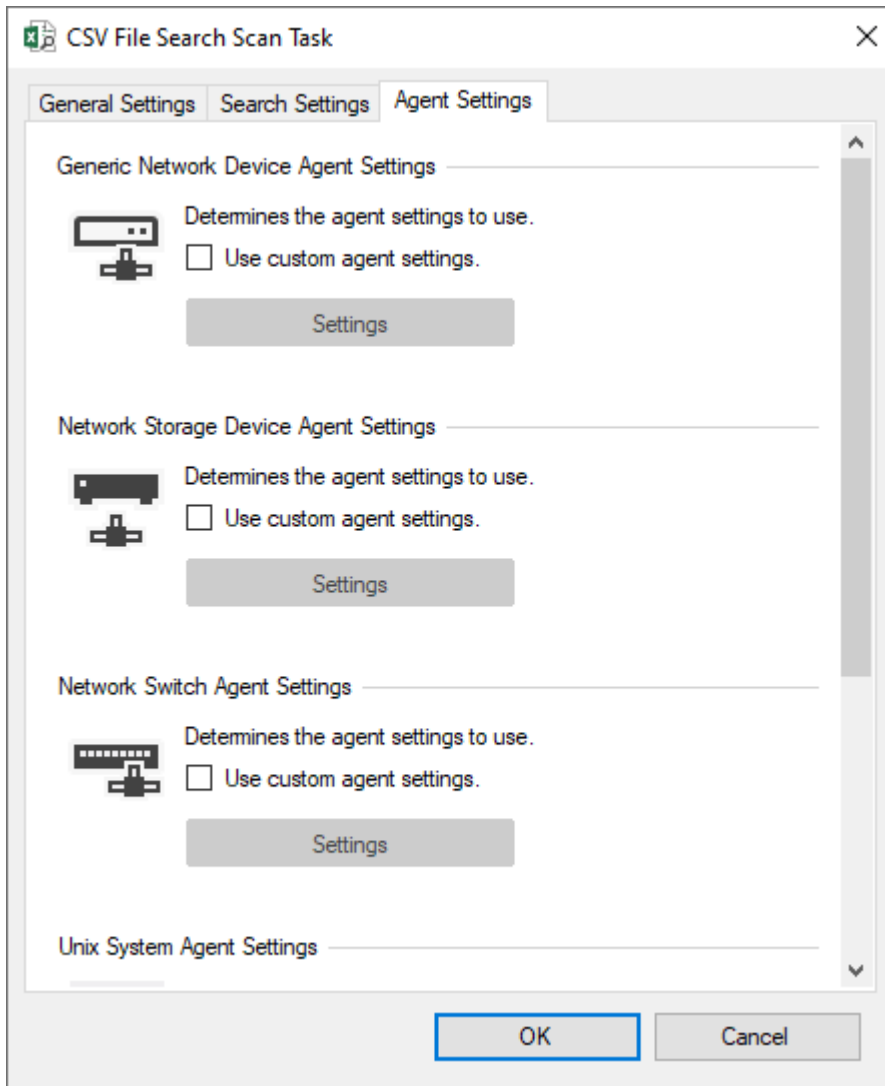
Exclude CSV header row

This box should be ticked if the file contains a header row which should be excluded.

Detect scan target type

Determines whether to read the type of [item](#) to create from within the file.

Agent Settings



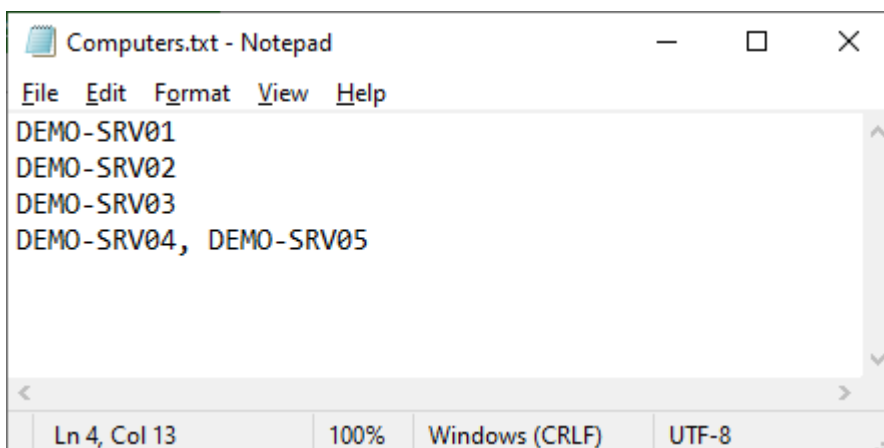
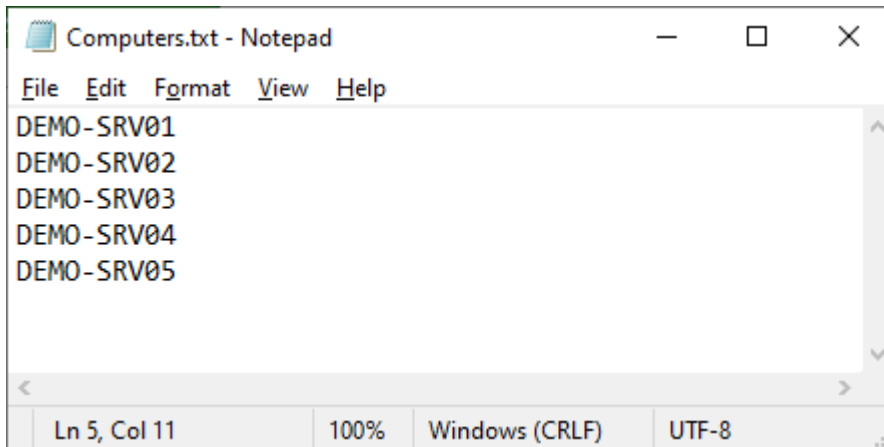
Use custom agent settings

Determines whether to use custom agent settings for the various [item type](#) detected by the search rather than the [default agent settings](#) for the [scan profile](#).

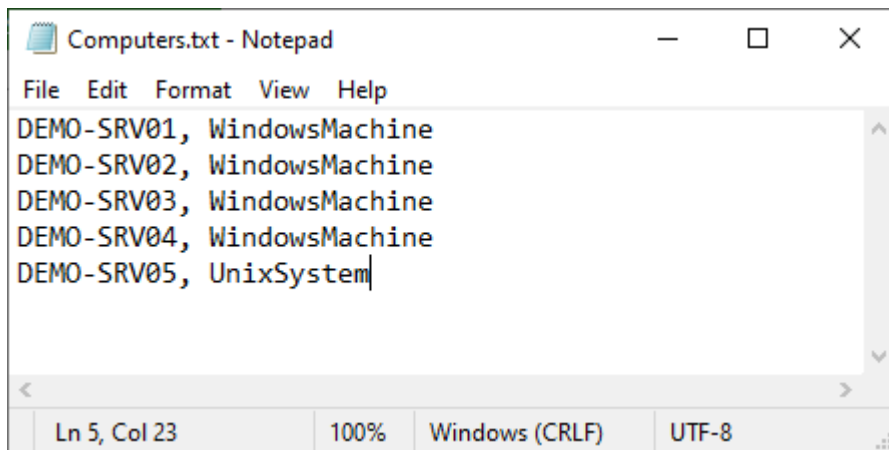
CSV File Format

The [CSV file search agent](#) can read a text file or CSV file for items to scan in the following formats.

When the [detect scan target type](#) setting is disabled in the [search settings](#), the item names can be entered either one per line, separated by the specified [delimiter](#), or a mixture of both. Detected items use the configured [default target type](#).



When the [detect scan target type](#) setting is enabled in the [search settings](#) the item names must be entered one per line and include the item type separated by the specified [delimiter](#).



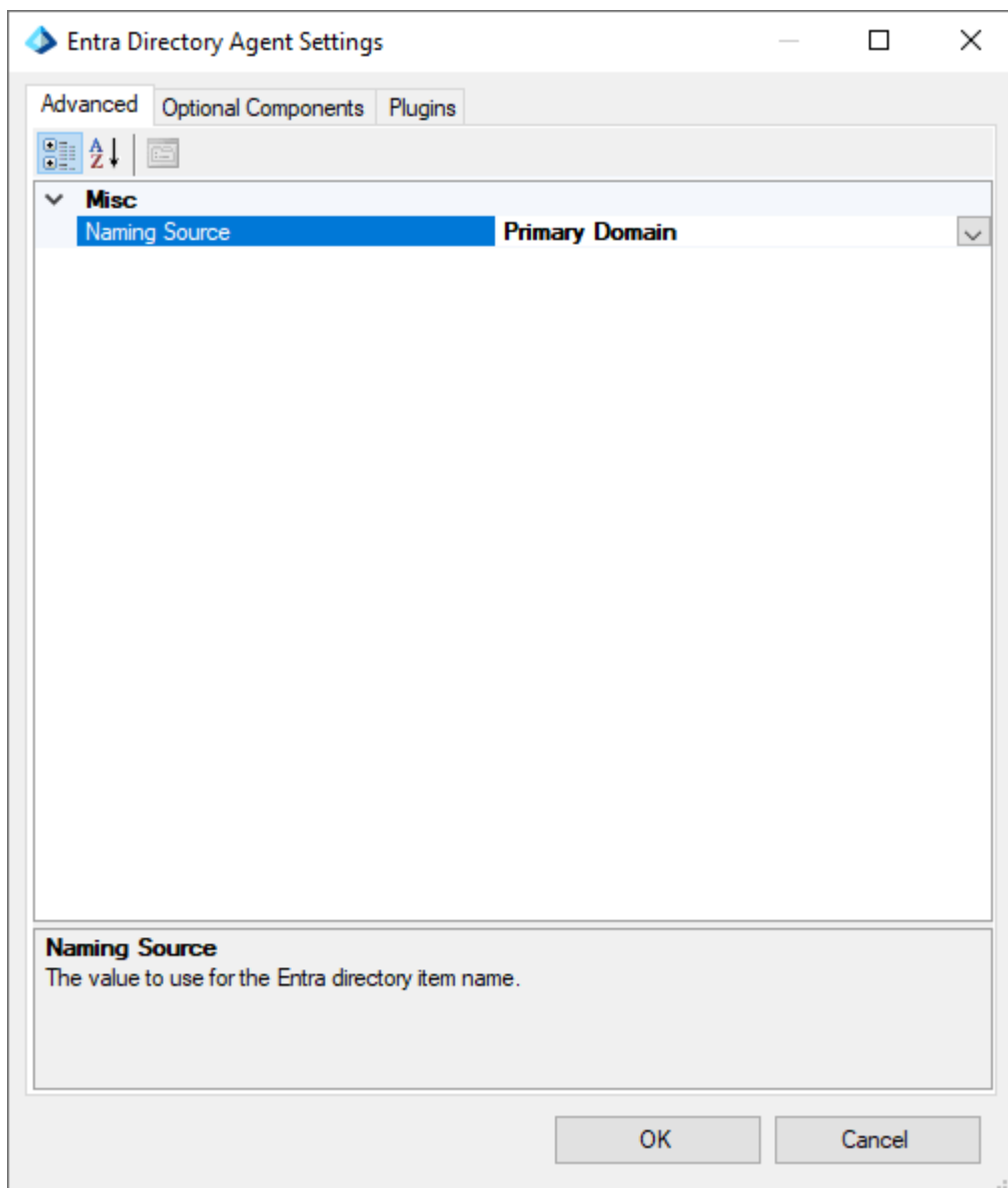
Entra Directory

Entra directory [scan tasks](#) are able to document an [Entra directory](#) also known as a tenant.

Agent Settings

This section describes the agent settings for the [Entra directory scan tasks](#).

Advanced

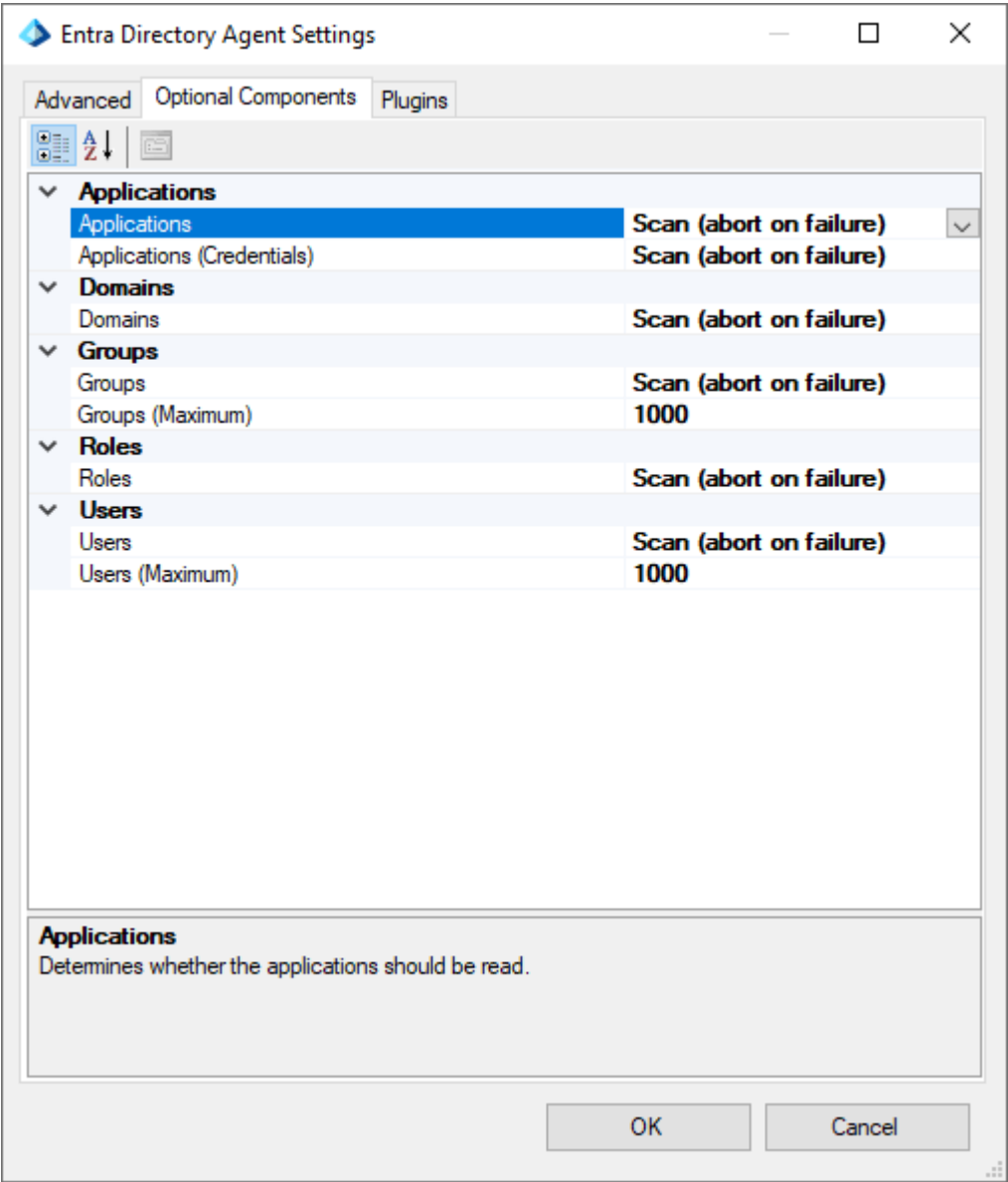


Naming Source

Determines the name to use for the [Entra Directory item](#).

- Primary Domain
- Organization Display Name

Optional Components



Applications

Determines whether applications are read for the Entra directory.

Applications (Credentials)

Determines whether credentials such as certificate and client secret information, are read for applications in the Entra directory.

Domains

Determines whether information about domains are read for the Entra directory.

Groups

Determines whether groups should be read for the Entra directory.

Groups (Maximum)

The maximum number of groups that the Entra directory can contain before the section is bypassed.

Roles

Determines whether roles are read for the Entra directory.

Users

Determines whether users should be read for the Entra directory.

Users (Maximum)

The maximum number of users that the Entra directory can contain before the section is bypassed.

Entra Directory Scan Task

The Entra Directory Scan Task allows an individual [Entra](#) directory to be scanned by the [XIA Configuration Client](#).

Connection Settings

The connection settings determines how to connect to the [Entra](#) directory.

Service Principal (Certificate)

This is the recommended authentication method.

Service Principal (Client Secret)

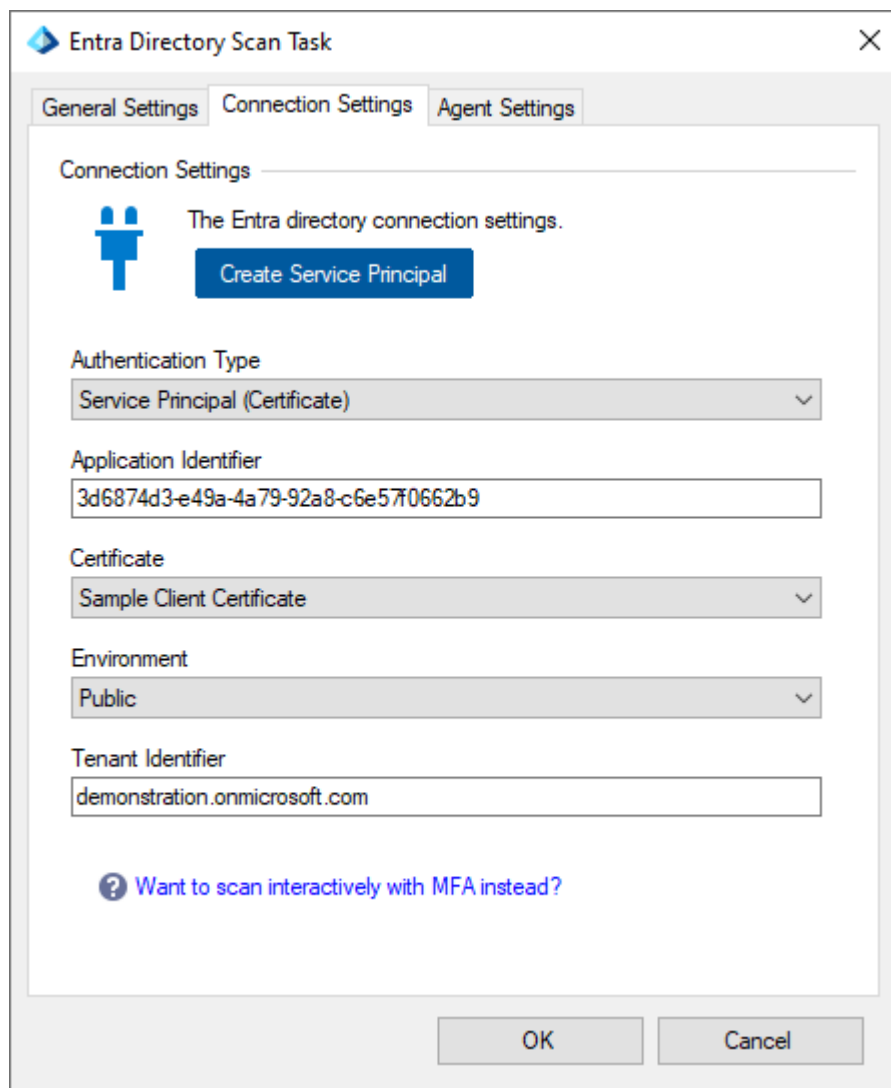
This method uses a client secret (password) for security - which is easier to share however is less secure than the certificate method.

Credentials (Deprecated)

This method uses a username and password and has been deprecated and is not recommended.

To scan interactivity instead using multi-factor authentication use the [Microsoft 365 Agent UI](#).

Service Principal (Certificate)



The screenshot shows the 'Entra Directory Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has three tabs: 'General Settings', 'Connection Settings', and 'Agent Settings'. The 'Connection Settings' tab contains the following fields and options:

- Connection Settings**: A section header with a blue plug icon and the text 'The Entra directory connection settings.' Below this is a blue button labeled 'Create Service Principal'.
- Authentication Type**: A dropdown menu with 'Service Principal (Certificate)' selected.
- Application Identifier**: A text box containing the GUID '3d6874d3-e49a-4a79-92a8-c6e57f0662b9'.
- Certificate**: A dropdown menu with 'Sample Client Certificate' selected.
- Environment**: A dropdown menu with 'Public' selected.
- Tenant Identifier**: A text box containing 'demonstration.onmicrosoft.com'.
- Footer**: A link that says '? Want to scan interactively with MFA instead?' and two buttons at the bottom: 'OK' and 'Cancel'.

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Certificate

The certificate to use for authentication. The certificate must be installed in the user store of the [XIA Configuration Client service account](#) and support client authentication.

Environment

The [environment](#) to connect to.

Tenant Identifier

The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Service Principal (Client Secret)

Entra Directory Scan Task

General Settings | Connection Settings | **Agent Settings**

Connection Settings

The Entra directory connection settings.

[Create Service Principal](#)

Authentication Type
Service Principal (Client Secret) ▾

Application Identifier
3d6874d3-e49a-4a79-92a8-c6e57f0662b9

Client Secret
●●●●●●●●●●●●●●●●

Environment
Public ▾

Tenant Identifier
demonstration.onmicrosoft.com

[? Want to scan interactively with MFA instead?](#)

OK Cancel

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Client Secret

The client secret (password) to use for authentication.

Environment

The [environment](#) to connect to.

Tenant Identifier

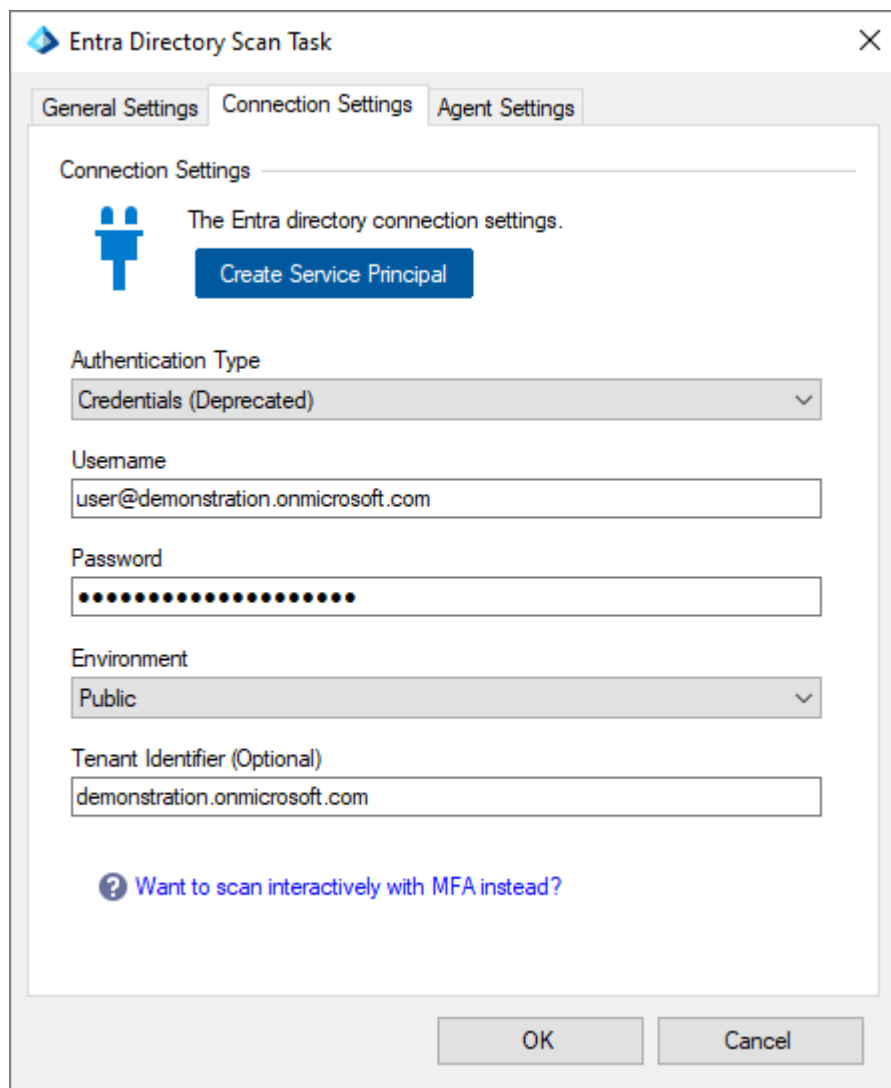
The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Credentials (Deprecated)



The screenshot shows a dialog box titled "Entra Directory Scan Task" with a close button (X) in the top right corner. It has three tabs: "General Settings", "Connection Settings" (which is selected), and "Agent Settings". The "Connection Settings" tab contains the following elements:

- A blue icon of a person with a plus sign.
- The text "The Entra directory connection settings."
- A blue button labeled "Create Service Principal".
- A label "Authentication Type" above a dropdown menu showing "Credentials (Deprecated)".
- A label "Username" above a text box containing "user@demostration.onmicrosoft.com".
- A label "Password" above a text box filled with black dots.
- A label "Environment" above a dropdown menu showing "Public".
- A label "Tenant Identifier (Optional)" above a text box containing "demostration.onmicrosoft.com".
- A link with a question mark icon: "Want to scan interactively with MFA instead?".
- At the bottom, "OK" and "Cancel" buttons.

Authentication Type

The authentication type is Credentials (Deprecated). This method is deprecated and not recommended.

It is recommended to use a [service principal with a certificate](#), or login interactively using multi-factor authentication using the [Microsoft 365 agent UI](#).

Username

The username of the account to use for login.

Password

The password of the user account.

Environment

The [environment](#) to connect to.

Tenant Identifier

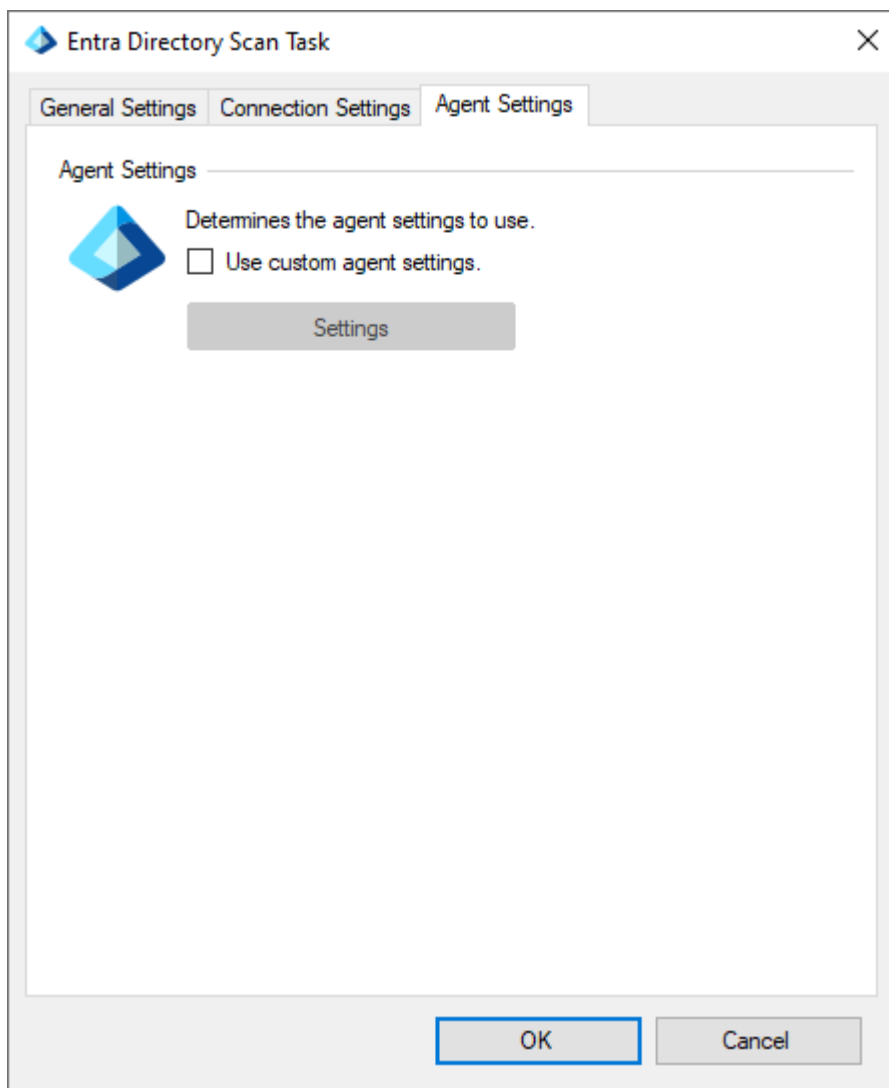
The name or identifier of the tenant (organization).

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will help automate the process of creating and configuring a [service principal with a certificate](#).

For more information see the [requirements](#) section.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

[Entra directory](#) scan tasks support scanning a [Microsoft Entra directory](#).

Windows Firewall Requirements

✔ The [Entra directory agent](#) must be able to connect to [Microsoft Graph](#) using HTTPS.

Access Settings

✔ The [Entra directory agent](#) must have [Global Reader](#) rights.

Local Service

⬇ [Entra directory](#) scan tasks do not support the [XIA Configuration Local Service](#).

Automatic Detection

✔ A [Microsoft Entra directory](#) can be automatically scanned by the [Microsoft 365 organization](#) scan task.

Service Principal Setup

Follow these steps to enable the [Entra directory agent](#) to access the [Entra directory](#) using a service principal.

[Service Principal \(Certificate\)](#)

[Service Principal \(Client Secret\)](#)

Service Principal (Certificate)

Follow these steps to enable the [Entra directory scan tasks](#) to access [Entra directory](#) using a service principal with certificate.

For more information see <https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal>

- Ensure that a client certificate and private key that supports client authentication is installed on the machine running the [XIA Configuration Client](#) and that the certificate is accessible to the [service account](#).

Issued To	Issued By	Expiration Date	Intended Purposes
 CSolutionsClient.org	MyRootCA	24/05/2031	Client Authentication, Server Authentication

- Export the public key of the client certificate in CER, PEM, or CRT format.
- Logon to the [Azure Portal](#) as a user account with the sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Server".
- For supported account types select *Accounts in this organizational directory only*
- Do not specify a Redirect URI.
- Click Register.
- Make a note of the following values

Application (client) ID
Directory (tenant) ID

- Go to Certificates & secrets > Certificates.
- Click Upload Certificate.

- Browse for the certificate and provide a description.

* Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

"ClientCert.cer" 

Description

XIA Configuration client certificate

- Copy and record the thumbprint.

Thumbprint	Description	Start date	Expires
BE4BCA8C388AF02EE1C50C3F5F74D6A34FE97DAF	XIA Configuration client certificate	5/24/2021	5/24/2031

- Go to Azure Active Directory > Roles and Administrators > Global reader.

Role	↑↓	Description	Type
  Global reader		Can read everything that a global administrator can, but ...	Built-in

- Click Add assignments and search for and select the service principal and click *Add*.

Search ⓘ

 XIA Configuration Server



XIA Configuration Server
fbf87ee4-cdb8-4e82-b4fd-0db0c8f9d315

Service Principal (Client Secret)

Follow these steps to enable the [Entra directory scan tasks](#) to access [Entra directory](#) using a service principal with a client secret.

For more information see <https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal>

- Logon to the [Azure Portal](#) as a user account with the sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Server".
- For supported account types select *Accounts in this organizational directory only*
- Do not specify a Redirect URI.
- Click Register.
- Make a note of the following values

Application (client) ID
Directory (tenant) ID

- Go to Certificates & secrets > Client secrets.
- Click *New Client Secret*.
- Enter a description and appropriate expiry, and click *Add*.

Add a client secret

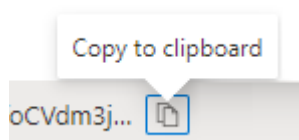
Description

XIA Configuration access

Expires

Recommended: 6 months

- Copy and record the client secret value. This value is only available at this point.



- Go to Azure Active Directory > Roles and Administrators > Global reader.

Role	↑↓	Description	Type
☒  Global reader		Can read everything that a global administrator can, but ...	Built-in

- Click Add assignments and search for and select the service principal and click *Add*.

Search ⓘ

 XIA Configuration Server
fbf87ee4-cdb8-4e82-b4fd-0db0c8f9d315

Troubleshooting

This section highlights the known issues for the [Entra Directory agent](#), and provides details of the solutions.

The client application is incorrect or not authorized

Symptoms

When you scan an [Entra Directory](#), you see the following error

The client application '*identifier*' is incorrect or not authorized.

Cause

This can occur if the application identifier has been specified incorrectly.

Resolution

Ensure that the correct application identifier has been specified.

Generic Network Device

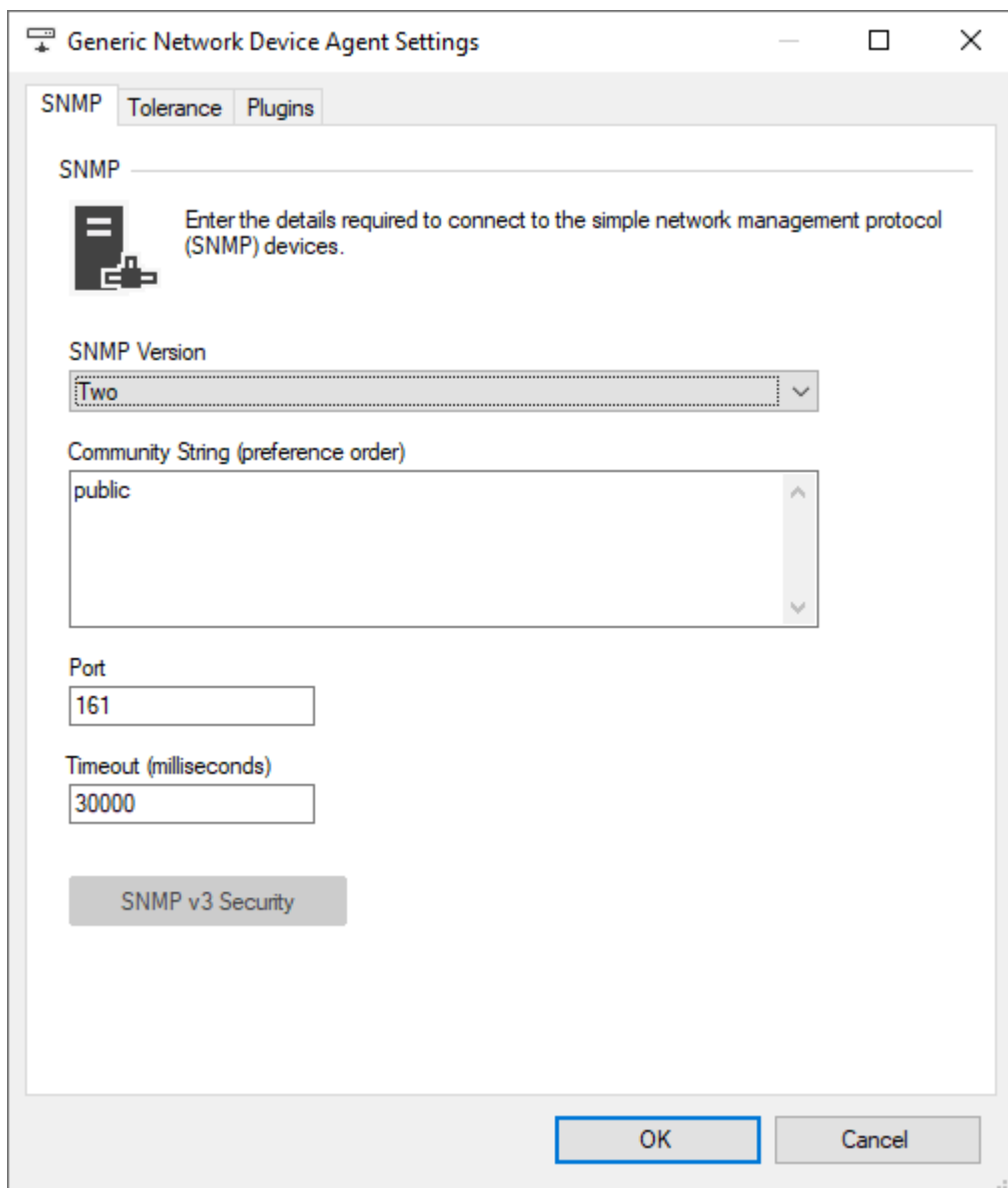
A generic network device is any SNMP enabled device that is not already documented by a dedicated agent. If an existing agent is already available - for example the [Network Switch](#) agent it is recommended that the dedicated agent is used.

Generic network devices can be detected using the [Network Device Search Scan Task](#) which is configured for generic network devices by default or manually using the [Generic Network Device List Scan Task](#).

The following information is collected by the agent:

- Name
- Description
- ARP cache
- Network Ports
- IP addresses
- Routing table

Agent Settings



The image shows a Windows-style dialog box titled "Generic Network Device Agent Settings". It has three tabs: "SNMP", "Tolerance", and "Plugins". The "SNMP" tab is selected. Inside the dialog, there is a section for "SNMP" with a sub-header "Enter the details required to connect to the simple network management protocol (SNMP) devices." Below this, there is a "SNMP Version" dropdown menu set to "Two". A "Community String (preference order)" text box contains the word "public". Below that, a "Port" text box contains "161" and a "Timeout (milliseconds)" text box contains "30000". At the bottom of the main content area is a button labeled "SNMP v3 Security". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Generic Network Device Agent Settings

SNMP Tolerance Plugins

SNMP

Enter the details required to connect to the simple network management protocol (SNMP) devices.

SNMP Version

Two

Community String (preference order)

public

Port

161

Timeout (milliseconds)

30000

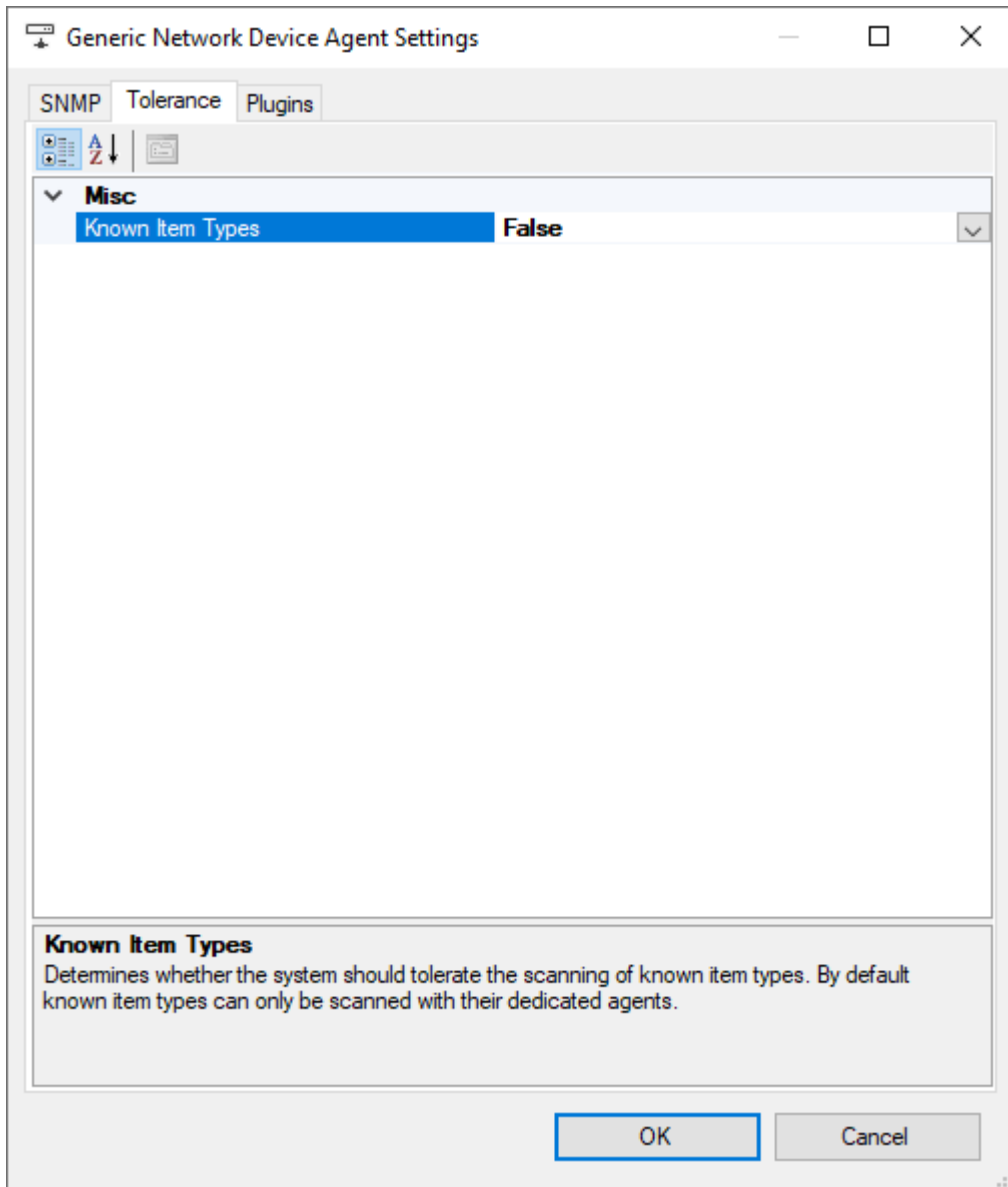
SNMP v3 Security

OK Cancel

SNMP

The [SNMP settings](#) for the [generic network device agent](#).

Tolerance



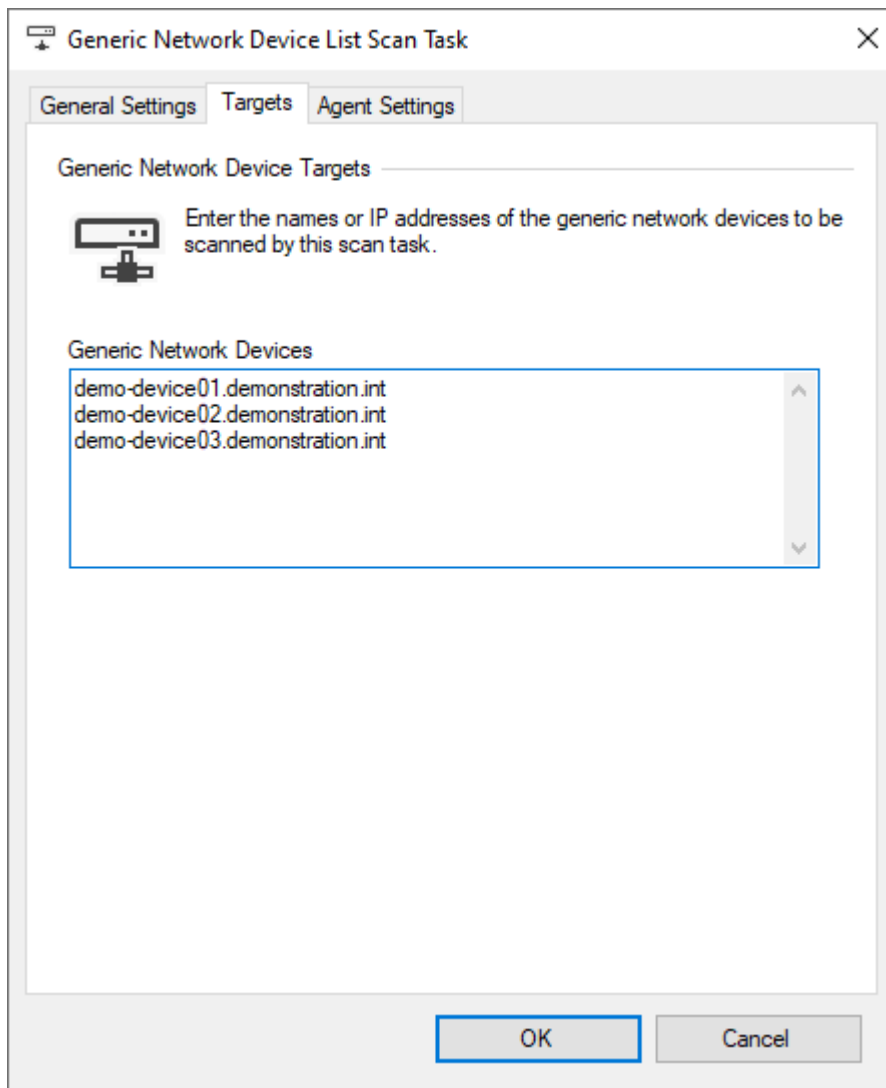
Known Item Types

Determines whether the [Generic Network Device Agent](#) should tolerate the scanning of devices for which a dedicated agent exists. When a dedicated agent exists for a device, for example the [Network Switch Agent](#), it is recommended that the dedicated agent is used as this will provide additional information.

Generic Network Device List Scan Task

The Generic Network Device List Scan Task allows you to enter a list of generic network devices that you wish to scan by either their hostname or IP address.

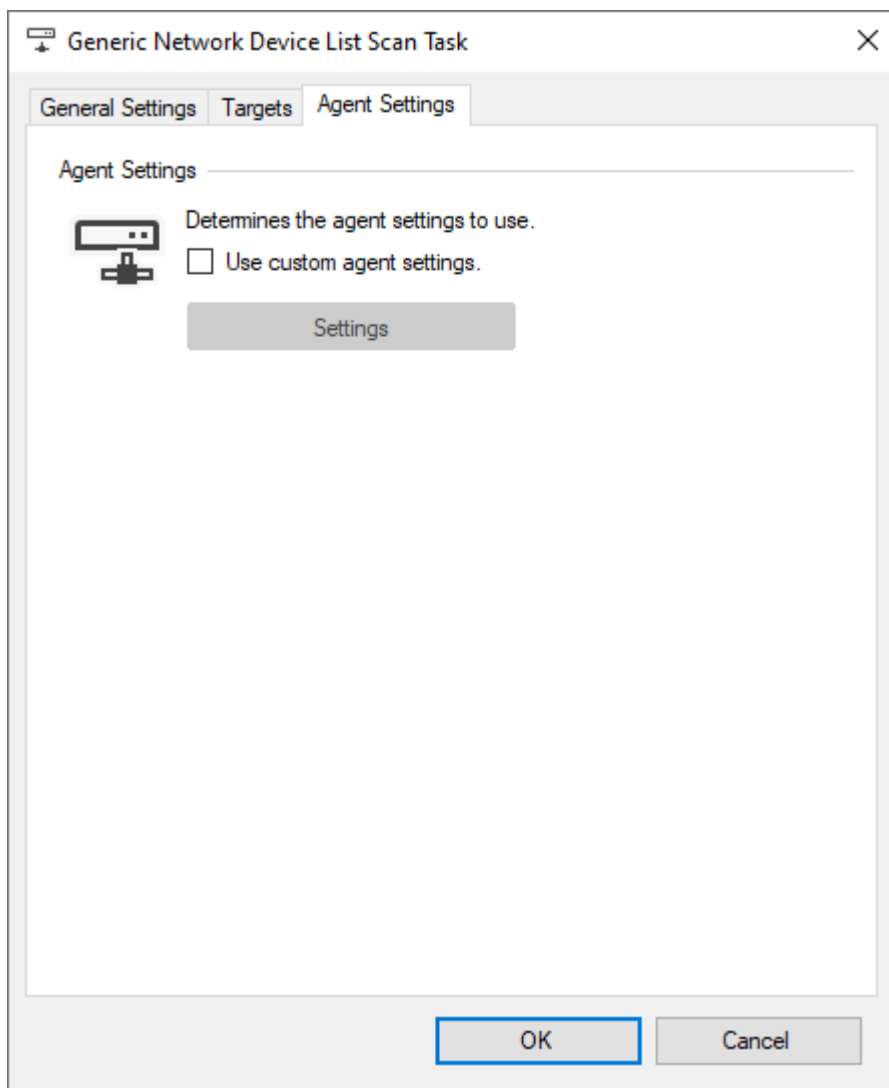
Targets



Generic Network Devices

The IP addresses, NetBIOS names, or fully qualified domain names of the generic network devices to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Item Identifiers

For more information about item identifiers please see the [Item Identifiers](#) section.

Primary Identifier

The device name.

Secondary Identifier

The device type's SNMP object identifier (OID).

Tertiary Identifier

Not used.

Requirements

Supported Target Systems

Any device that supports SNMP can be scanned using this agent.

Access Settings

The [Generic Network Device](#) agent uses SNMP to communicate with devices and has the following access requirements.

- Firewall access must allow access to the SNMP port on the device (by default port UDP/161).
- The [XIA Configuration Client](#) must be provided with a valid SNMP read community string within the [SNMP Settings](#).
- The device must be configured to allow the computer running the [XIA Configuration Client](#) to perform SNMP queries.

Local Service

The network device scan tasks do not support the local service.

Network Device Search Scan Task

Generic network devices can be automatically detected by the [Network Device Search Scan Task](#).

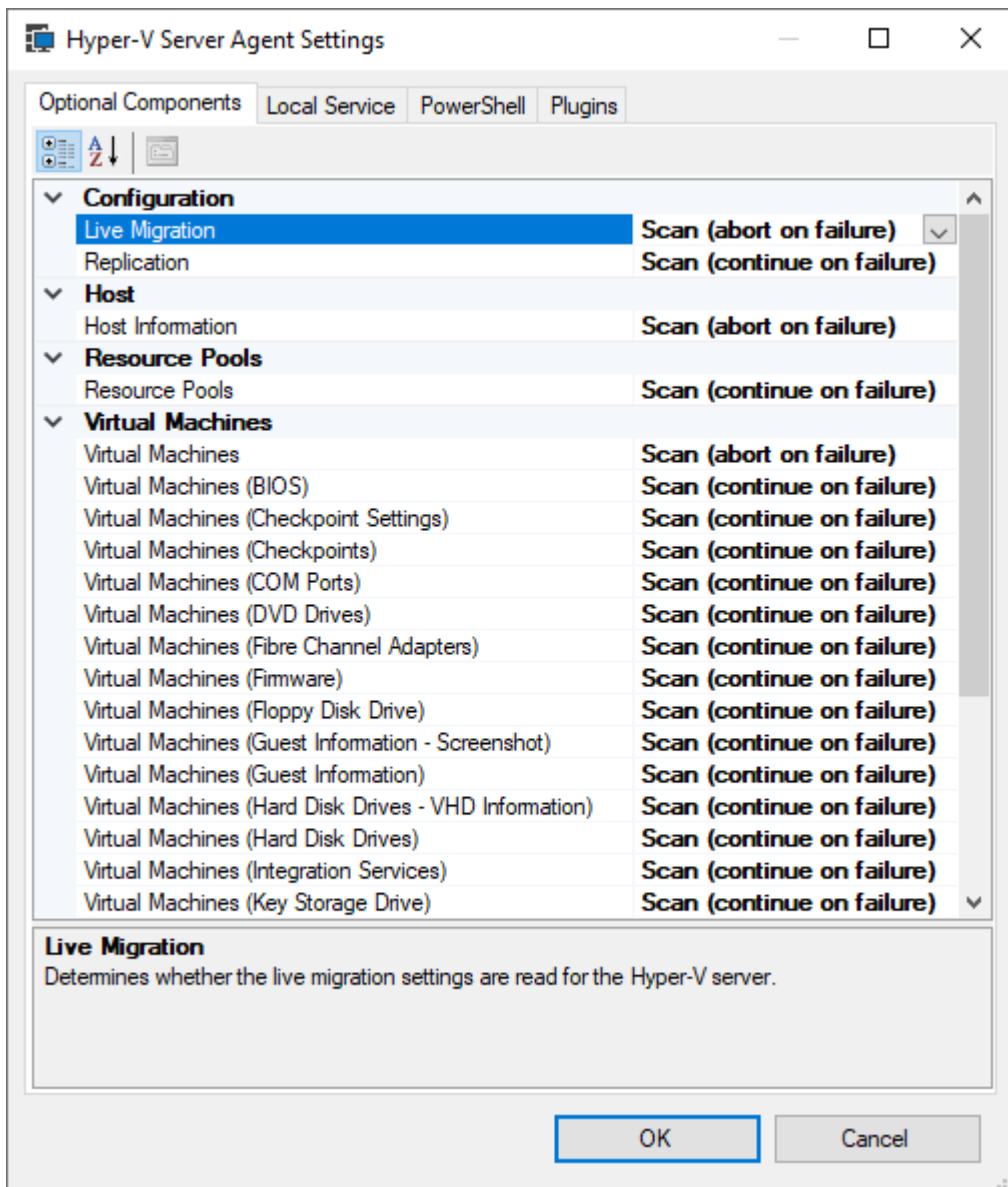
- Ensure the devices support and are configured for SNMP.
- Ensure the machine running the [XIA Configuration Client](#) is enabled as a manager within the device configuration. For more information see the documentation from your device manufacturer.
- Enter the subnet or IP address range in which the network switches reside in the [Network Device Search Scan Task](#).
- Ensure that Generic Network Devices are enabled within the **Agent Detection** tab.

Hyper-V Server

The Hyper-V Server [scan tasks](#) are able to document [Hyper-V Servers](#) running on [Windows Server 2012](#) and above and [Microsoft Azure Local](#) (Microsoft Azure Stack HCI) above using [PowerShell remoting](#).

The data located by these [scan tasks](#) include resource pools, server settings, virtual machines, and virtual switches.

Agent Settings



Configuration > Live Migration

Determines whether the live migration settings are read for the Hyper-V server.

Configuration > Replication

Determines whether the server replication settings are read for the Hyper-V server.

Host > Host Information

Determines whether the host information is read for the Hyper-V server.

Resource Pools > Resource Pools

Determines whether the resource pools are read for the Hyper-V server.

Virtual Machines > Virtual Machines

Determines whether the virtual machines are read for the Hyper-V server.

Virtual Machines > Virtual Machines (BIOS)

Determines whether the BIOS settings are read for generation 1 virtual machines.

Virtual Machines (Checkpoint Settings)

Determines whether the checkpoint settings are read for virtual machines.

Virtual Machines > Virtual Machines (Checkpoints)

Determines whether the checkpoints are read for virtual machines.

Virtual Machines > Virtual Machines (COM Ports)

Determines whether the COM ports are read for virtual machines. This only applies to Generation 1 virtual machines.

Virtual Machines > Virtual Machines (DVD Drives)

Determines whether the DVD drives are read for virtual machines.

Virtual Machines > Virtual Machines (Fibre Channel Adapters)

Determines whether the fibre channel adapters are read for virtual machines.

Virtual Machines > Virtual Machines (Firmware)

Determines whether the firmware settings are read for generation 2 virtual machines.

Virtual Machines > Virtual Machines (Floppy Disk Drive)

Determines whether the floppy disk drive is read for generation 1 virtual machines.

Virtual Machines > Virtual Machines (Guest Information - Screenshot)

Determines whether a screenshot is read as part of the guest information for virtual machines. The virtual machine must be powered on for this information to be available.

Virtual Machines > Virtual Machines (Guest Information)

Determines whether guest information is read for virtual machines. The virtual machine must be powered on for this information to be available.

Virtual Machines > Virtual Machines (Hard Disk Drives - VHD Information)

Determines whether the hard disk drive VHD information is read for virtual machines.

Virtual Machines > Virtual Machines (Hard Disk Drives)

Determines whether the hard disk drives are read for virtual machines.

Virtual Machines > Virtual Machines (Integration Services)

Determines whether the integration services settings are read for virtual machines.

Virtual Machines > Virtual Machines (Key Storage Drive)

Determines whether the key storage drive settings are read for virtual machines. This only applies to generation 1 virtual machines.

Virtual Machines > Virtual Machines (Memory)

Determines whether the memory settings are read for virtual machines.

Virtual Machines > Virtual Machines (Network Adapters)

Determines whether the network adapters are read for virtual machines.

Virtual Machines > Virtual Machines (Processor)

Determines whether the processor settings are read for virtual machines.

Virtual Machines > Virtual Machines (Security)

Determines whether the security settings are read for virtual machines. This only applies to Windows Server 2012 R2 and above.

Virtual Storage Area Networks > Virtual Storage Area Networks

Determines whether the virtual storage area networks are read for the Hyper-V server.

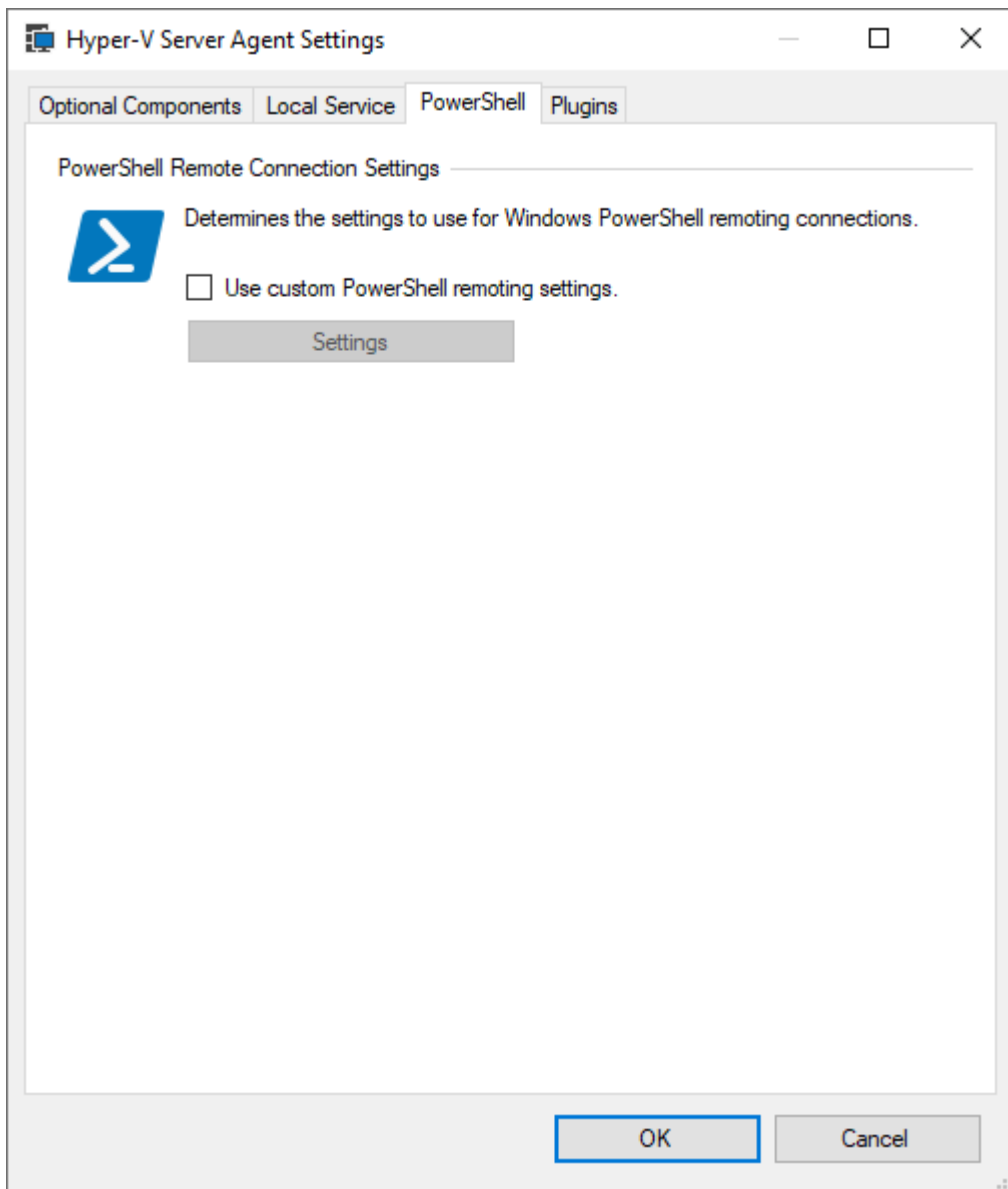
Virtual Switches > Virtual Switches

Determines whether the virtual switches are read for the Hyper-V server.

Virtual Switches > Virtual Switches (Extensions)

Determines whether the extensions are read for virtual switches.

PowerShell



Use custom PowerShell remoting settings

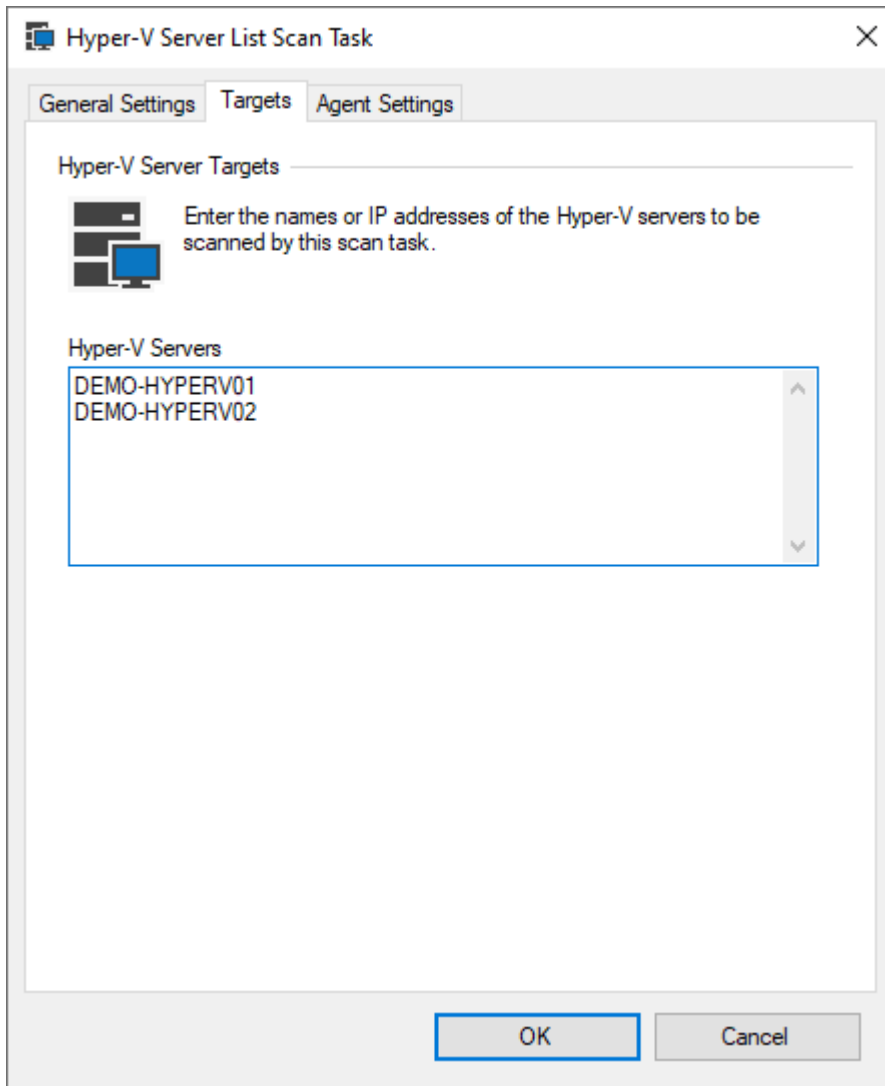
Determines whether to use custom [PowerShell connection settings](#).

Hyper-V List Scan Task

The Hyper-V Server list scan task allows you to enter a list of [Hyper-V Servers](#) you wish to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Hyper-V Servers](#).

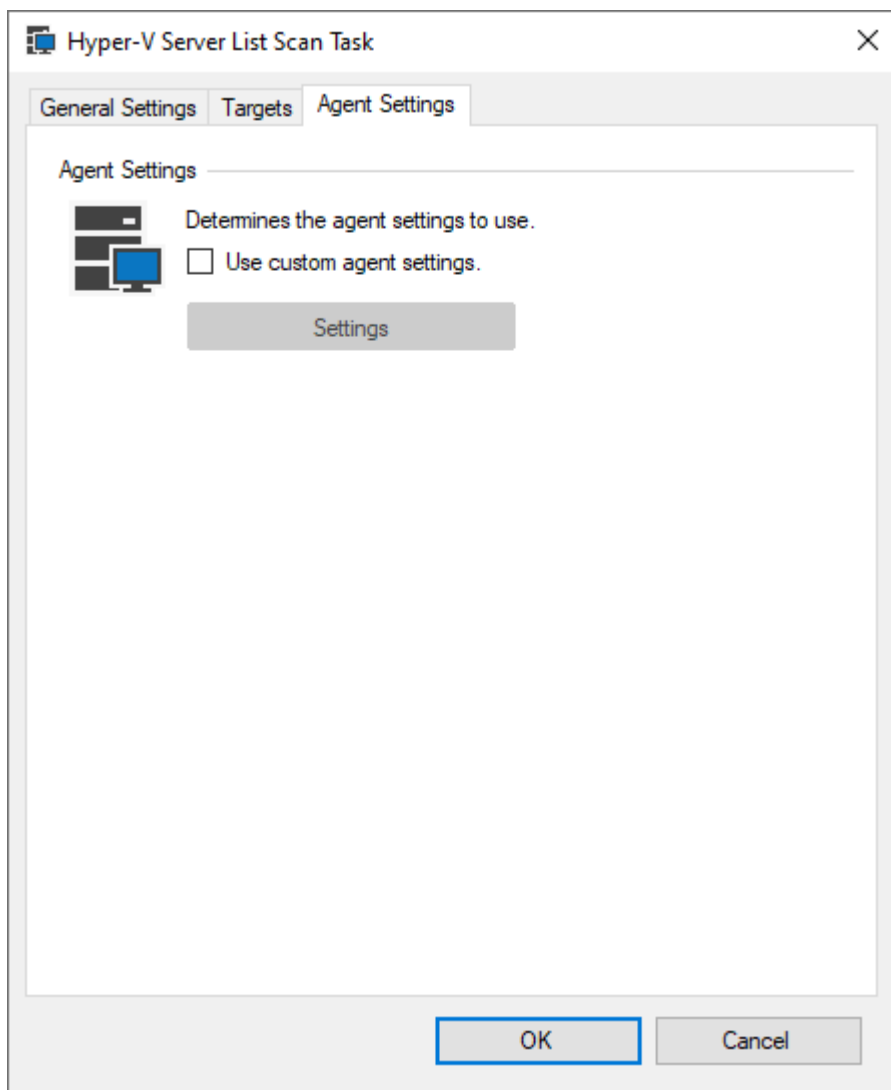
Targets



Hyper-V Servers

The IP addresses, NetBIOS names, or fully qualified domain names of the Hyper-V servers to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Server Target Systems

The [Hyper-V Server scan tasks](#) are supported on the following target server operating systems:

- Microsoft Azure Local (Microsoft Azure Stack HCI)
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Access Settings

The [Hyper-V Server scan tasks](#) use [PowerShell remoting](#) to obtain information remotely from [Hyper-V Servers](#).

- Firewall access must allow access to the [PowerShell remoting](#) ports on the remote machine
- The [XIA Configuration client service account](#) or [custom credentials](#) must have administrator rights on the remote machine.

Guest Information

To collect guest information such as the guest operating system, IP addresses and service pack, the [Hyper-V Integration Services](#) component must be installed and the virtual machine started with the guest operating system running.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✓ Windows Remote Management (HTTP-In)

Local Service

- ✓ The [Hyper-V Server scan tasks](#) support the [local service](#).

Automatic Detection

✔ [Hyper-V Servers](#) can be automatically detected and scanned by [Windows machine scan tasks](#).

Item Identifiers

For more information about item identifiers please see the [item identifiers](#) section.

Primary Identifier

The computer name.

Secondary Identifier

The computer serial number.

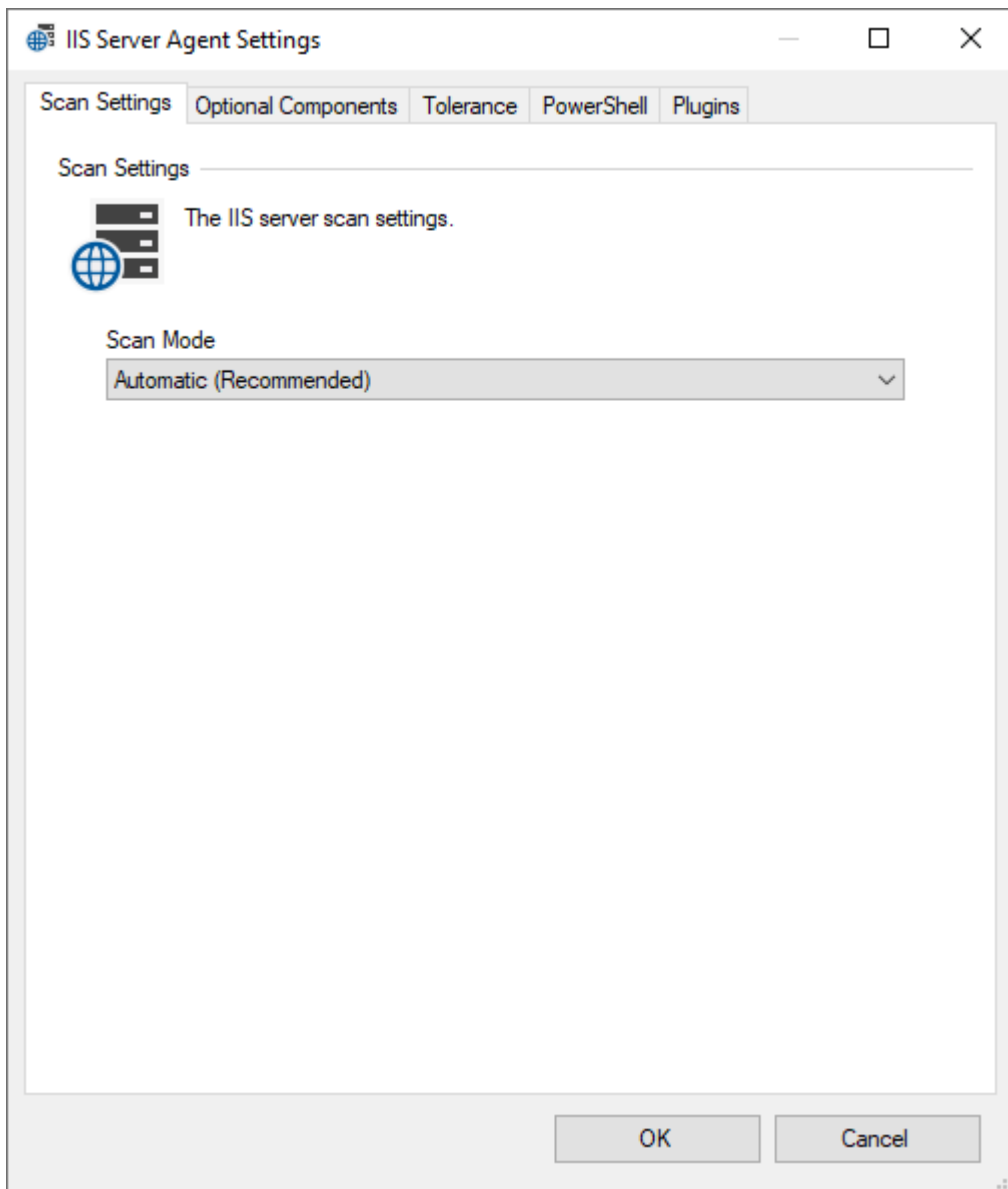
Tertiary Identifier

Not used.

IIS Server

The IIS server [scan tasks](#) are able to scan [Microsoft Internet Information Services \(IIS\) Servers](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).

Agent Settings

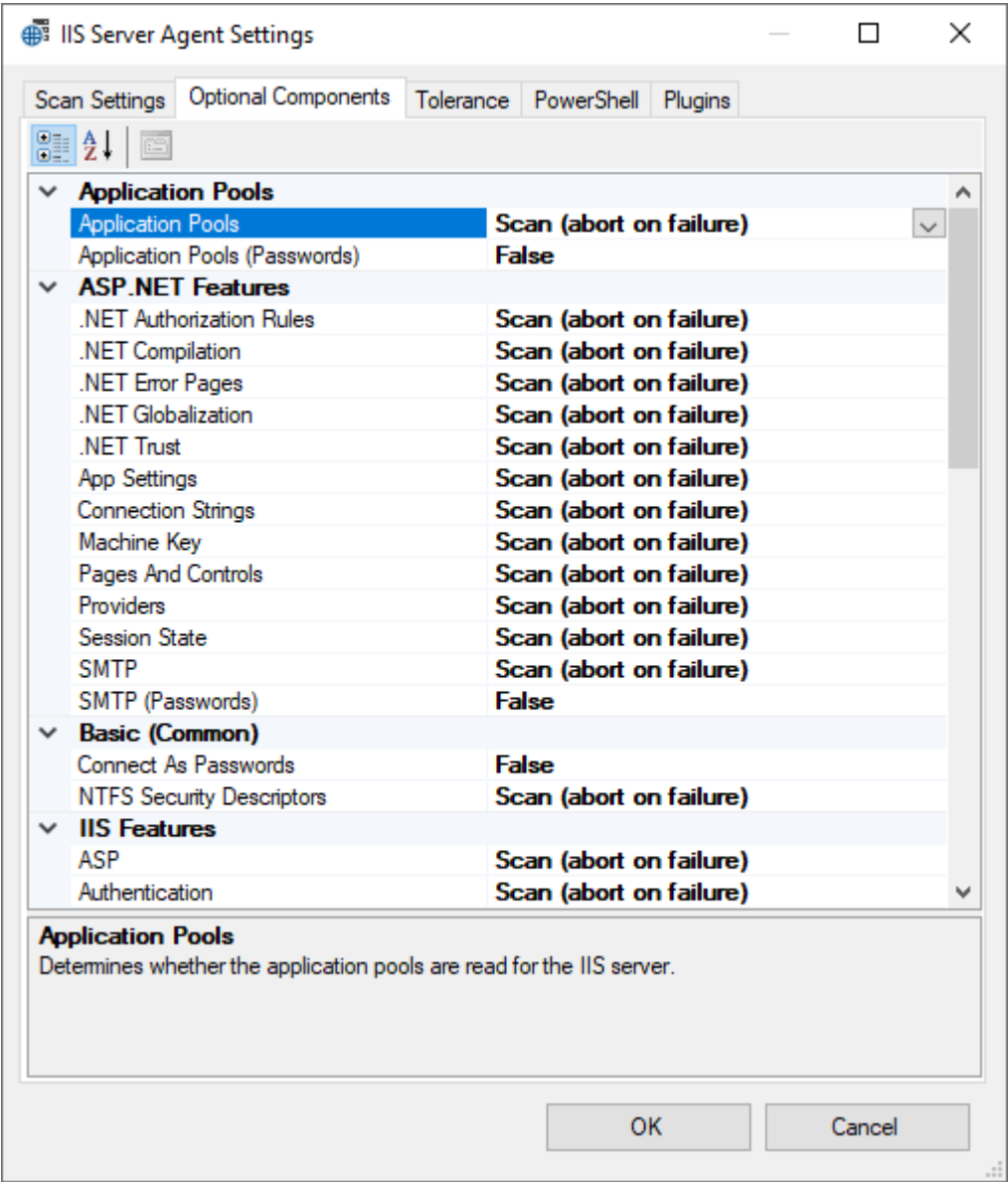


Scan Mode

Determines the scan mode for the agent.

- **Automatic (Recommended)**
The agent will automatically attempt to use the [IISAdministration PowerShell module](#) if available, otherwise the classic [WebAdministration](#) module will be used.
- **Modern Only**
The agent will use the [IISAdministration PowerShell module](#) if available, otherwise the scan will fail.
- **Classic Only**
The agent will use the classic [WebAdministration](#) module.

Optional Components



Application Pools > Application Pools
Determines whether the application pools are read for the IIS server.

Application Pools > Application Pools (Passwords)
Determines whether application pool passwords are read for the IIS server.

ASP.NET Features > .NET Compilation
Determines whether the .NET compilation settings are read.

ASP.NET Features > .NET Error Pages
Determines whether the .NET error pages are read.

ASP.NET Features > .NET Globalization
Determines whether the .NET globalization settings are read.

ASP.NET Features > .NET Trust

Determines whether the trust settings are read.

ASP.NET Features > App Settings

Determines whether the app settings are read.

ASP.NET Features > .NET Authorization Rules

Determines whether the .NET authorization rules are read.

ASP.NET Features > Connection Strings

Determines whether the connection strings are read.

ASP.NET Features > Machine Key

Determines whether the machine key settings are read.

ASP.NET Features > Pages And Controls

Determines whether the pages and controls settings are read.

ASP.NET Features > Providers

Determines whether the providers are read.

ASP.NET Features > Session State

Determines whether the session state settings are read.

ASP.NET Features > SMTP

Determines whether the SMTP settings are read.

ASP.NET Features > SMTP (Passwords)

Determines whether SMTP passwords are read for the IIS server.

Basic > Connect As Passwords

Determines whether the connect as passwords are read.

Basic > NTFS Security Descriptors

Determines whether NTFS security descriptors are read.

IIS Features > ASP

Determines whether the classic ASP settings are read.

IIS Features > Authentication

Determines whether the authentication are read.

IIS Features > Authentication (Passwords)

Determines whether the authentication passwords are read.

IIS Features > Authorization Rules

Determines whether the authorization rules are read.

IIS Features > CGI

Determines whether the CGI settings are read.

IIS Features > Default Documents

Determines whether the default documents are read.

IIS Features > Directory Browsing

Determines whether the directory browsing settings are read.

IIS Features > Dynamic Compression

Determines whether the dynamic compression settings are read.

IIS Features > Error Pages

Determines whether error pages are read.

IIS Features > Failed Request Tracing Rules

Determines whether the failed request tracing rules are read.

IIS Features > FastCGI Applications

Determines whether the FastCGI applications are read.

IIS Features > Handler Mappings

Determines whether the handler mappings are read.

IIS Features > HTTP Redirection

Determines whether the HTTP redirection settings are read.

IIS Features > HTTP Response Headers

Determines whether the HTTP response headers are read.

IIS Features > IP Restrictions

Determines whether the IP and domain restrictions are read.

IIS Features > ISAPI and CGI Restrictions

Determines whether the ISAPI and CGI restrictions are read.

IIS Features > ISAPI Filters

Determines whether the ISAPI filters are read.

IIS Features > Logging

Determines whether the logging settings are read.

IIS Features > MIME Types

Determines whether MIME types are read.

IIS Features > Modules

Determines whether modules are read.

IIS Features > Output Caching Rules

Determines whether the output caching rules are read.

IIS Features > Request Filtering

Determines whether the request filtering settings are read.

IIS Features > SSL Settings

Determines whether the SSL settings are read.

IIS Features > Static Compression

Determines whether the static compression settings are read.

IIS Features > WebDAV Authoring Rules

Determines whether the WebDAV authoring rules are read.

Management Features > Centralized Certificates

Determines whether the centralized certificates settings are read.

Management Features > Management Service

Determines whether the management service settings are read.

Management Features > Management Service (IIS Manager Users)

Determines whether the IIS manager users are read. This only applies when the modern scan method is used.

Management Features > Shared Configuration

Determines whether the shared configuration settings are read. This only applies when the modern scan method is used.

Server > Host Information

Determines whether the host information is read for the IIS server.

Server > Server Certificates

Determines whether the server certificates are to be read for the IIS server.

Server > Server Configuration

Determines whether the server configuration is to be read for the IIS server.

Sites > Sites

Determines whether the sites are read for the IIS server.

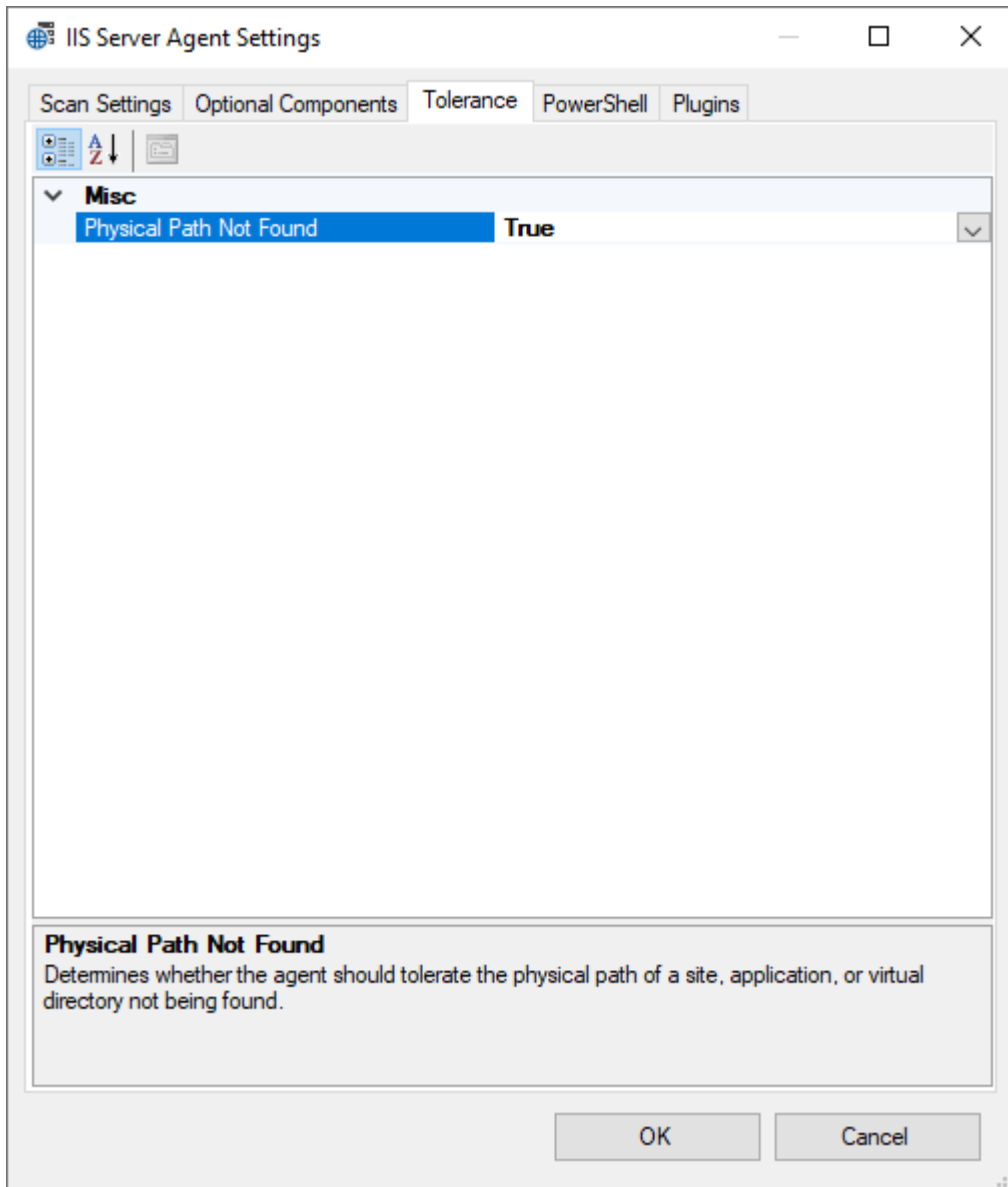
Sites > Sites (Applications)

Determines whether the applications are read for sites.

Sites > Sites (Virtual Directories)

Determines whether the virtual directories are read for sites.

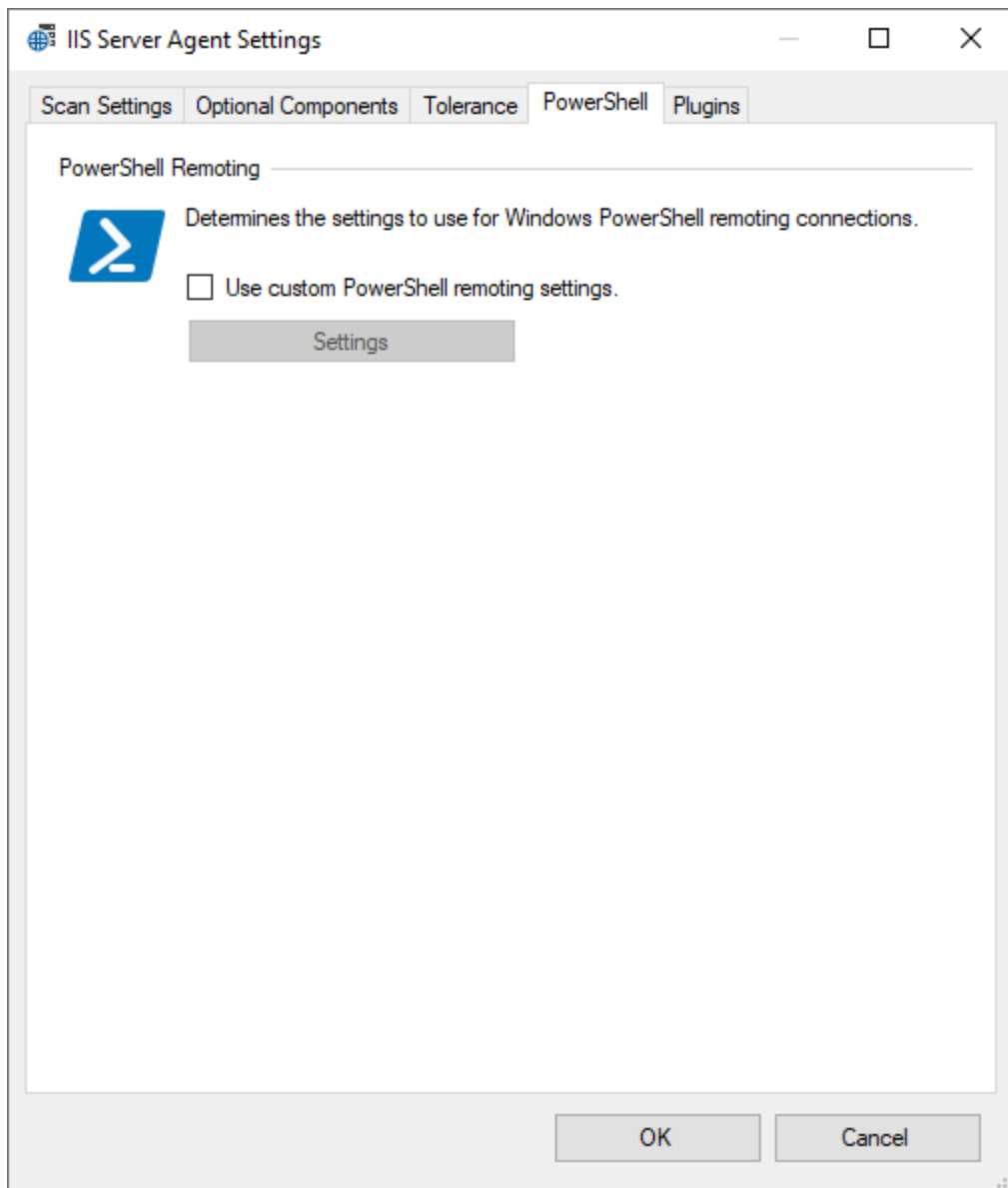
Tolerance



Physical Path Not Found

Determines whether the agent should tolerate the physical path of a site, application, or virtual directory not being found.

PowerShell



Use custom PowerShell remoting settings

Determines whether to use custom [PowerShell connection settings](#).

Requirements

Supported Server Target Systems

The [IIS server scan tasks](#) are supported on the following target server operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Supported Desktop Target Systems

The [IIS server scan tasks](#) are supported on the following target desktop operating systems:

- Windows 11
- Windows 10

IIS Administration PowerShell Module

By default the [IIS server scan tasks](#) will use [IISAdministration PowerShell module](#) if available, otherwise failing back to the older [WebAdministration PowerShell module](#).

The [IISAdministration PowerShell module](#) is included with Windows 10, Windows Server 2016, and above.

For Windows Server 2012, and Windows Server 2012 R2 it can be installed from the [PowerShell gallery](#).

<https://www.powershellgallery.com/packages/IISAdministration/1.1.0.0>

Access Settings

The [IIS server scan tasks](#) use [PowerShell remoting](#) to obtain information remotely from [IIS Servers](#).

- Firewall access must allow access to the [PowerShell remoting](#) ports on the remote machine
- The [XIA Configuration client service account](#) or [custom credentials](#) must have administrator rights on the remote machine.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✔ Windows Remote Management (HTTP-In)

Local Service

- ✔ The [IIS server scan tasks](#) support the [local service](#).

Automatic Detection

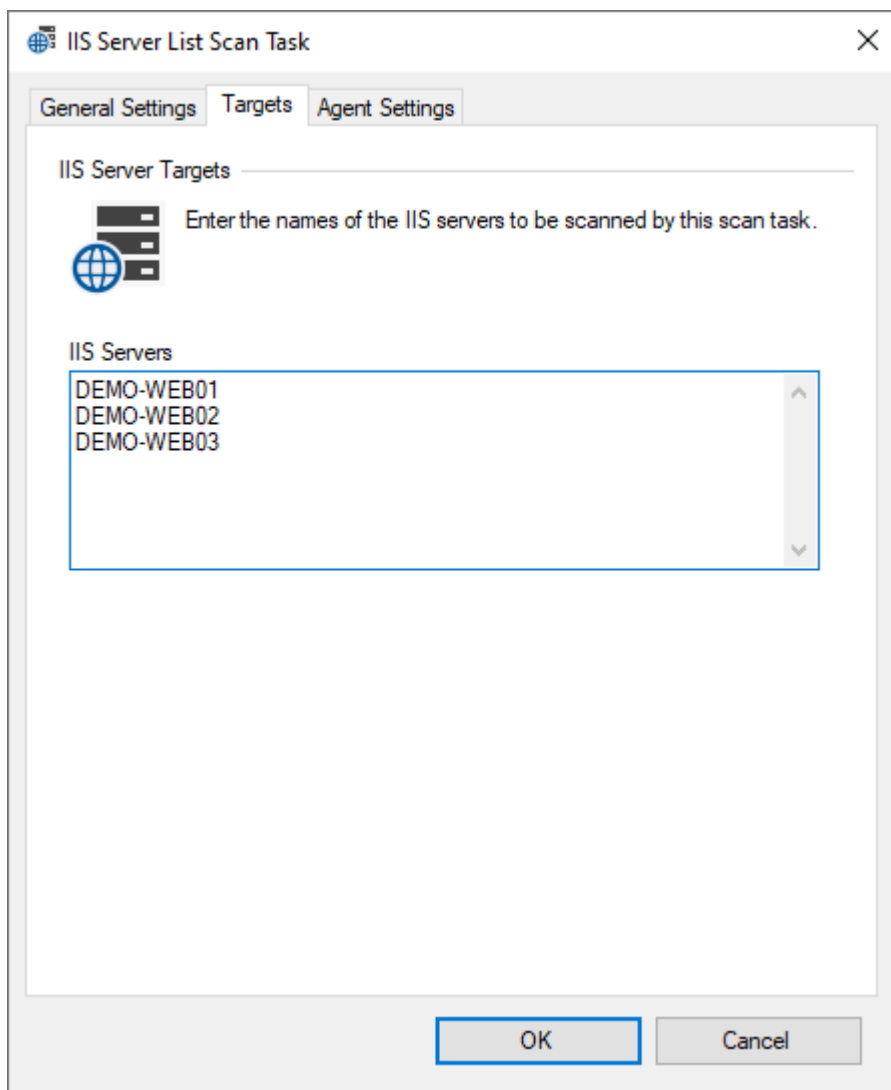
- ✔ [IIS servers](#) can be automatically detected and scanned by [Windows machine scan tasks](#).

IIS Server List Scan Task

The IIS Server list scan task allows you to enter a list of names or IP address of the [IIS servers](#) to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [IIS servers](#).

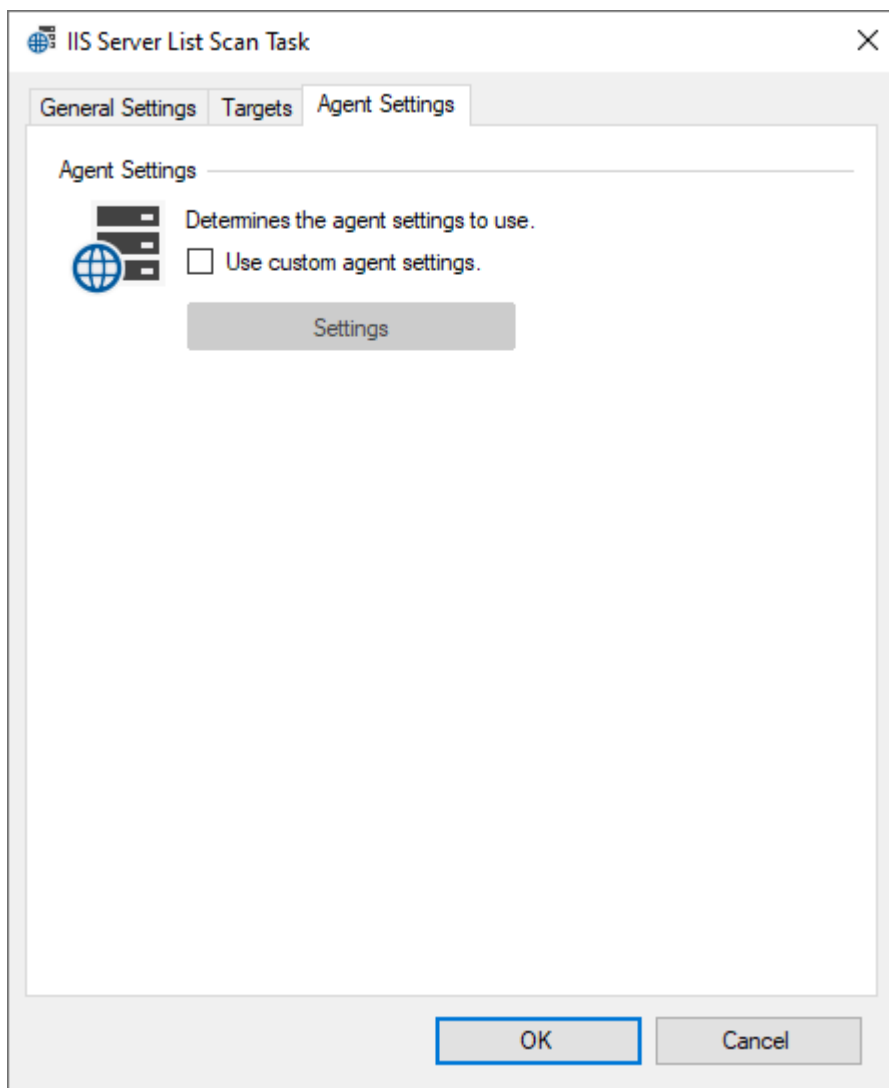
Targets



IIS Servers

The IP addresses, NetBIOS names, or fully qualified domain names of the [IIS servers](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Item Identifiers

For more information about item identifiers please see the [item identifiers](#) section.

Primary Identifier

The computer name.

Secondary Identifier

The computer serial number.

Tertiary Identifier

Not used.

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Error determining whether the physical path exists

Symptoms

When you scan an [IIS Server](#) that uses a UNC path for a site or virtual directory you may see the following.

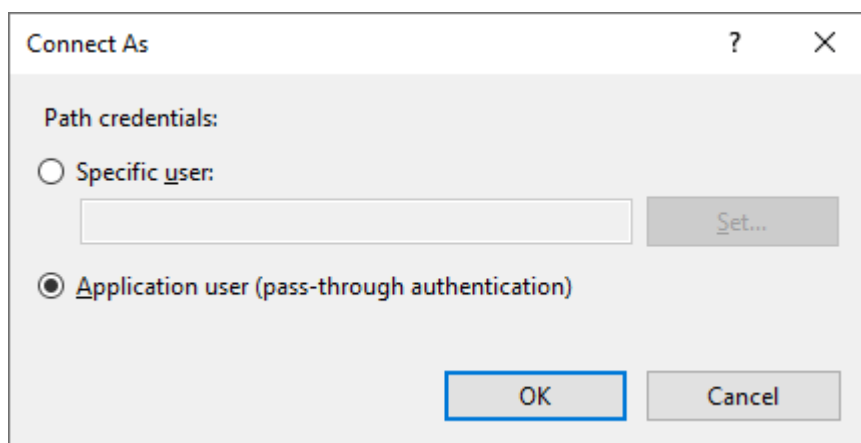
Error determining whether the physical path '*path*' exists for the virtual directory.

Access is denied

Cause

This error is caused by the authentication double hop issue under the following circumstances:

- The [IIS Server](#) that uses a UNC path for a site or virtual directory and that UNC path resides on a machine other than the [IIS Server](#) machine.
- The physical path credentials are set to "Application user (pass-through authentication).



- The [XIA Configuration Client](#) is installed on a separate machine to the machine running [IIS Server](#).

More Information

The authentication double hop issue refers to the fact that a connection is made from the machine (in this case the machine running the [XIA Configuration Client](#)) to a second machine running [IIS Server](#). When the PowerShell remoting connection then tries to connect to the machine where the UNC path is hosted the credentials are not permitted for this second hop.

For more information see the following article.

<https://learn.microsoft.com/powershell/scripting/security/remoting/ps-remoting-second-hop>

Resolution

- Configure the [optional components](#) to tolerate this issue.

- or -

- Configure the IIS server to use specific user credentials when accessing the UNC path.
WARNING: This change affects the security level.

- or -

- Install the [XIA Configuration Client](#) on the machine running the [IIS Server](#).

- or -

- Install the [XIA Configuration Local Service](#) on the machine running the [IIS Server](#).

- or -

- User Kerberos authentication for the scan and allow constrained Kerberos delegation.
<https://learn.microsoft.com/powershell/scripting/security/remoting/ps-remoting-second-hop>

NOTE: This is not compatible with [custom credentials](#).

Microsoft 365 Organization

The Microsoft 365 organization [scan tasks](#) provide a convenient way to scan multiple [Microsoft 365](#) services.

Microsoft 365 Organization Scan Task

The Microsoft 365 organization [scan tasks](#) provide a convenient way to scan multiple [Microsoft 365](#) services including:

- [Entra Directories](#)
- [Exchange Online Organizations](#)

Connection Settings

The connection settings determines how to connect to the [Microsoft 365](#) organization.

Service Principal (Certificate)

This is the recommended authentication method.

Service Principal (Client Secret)

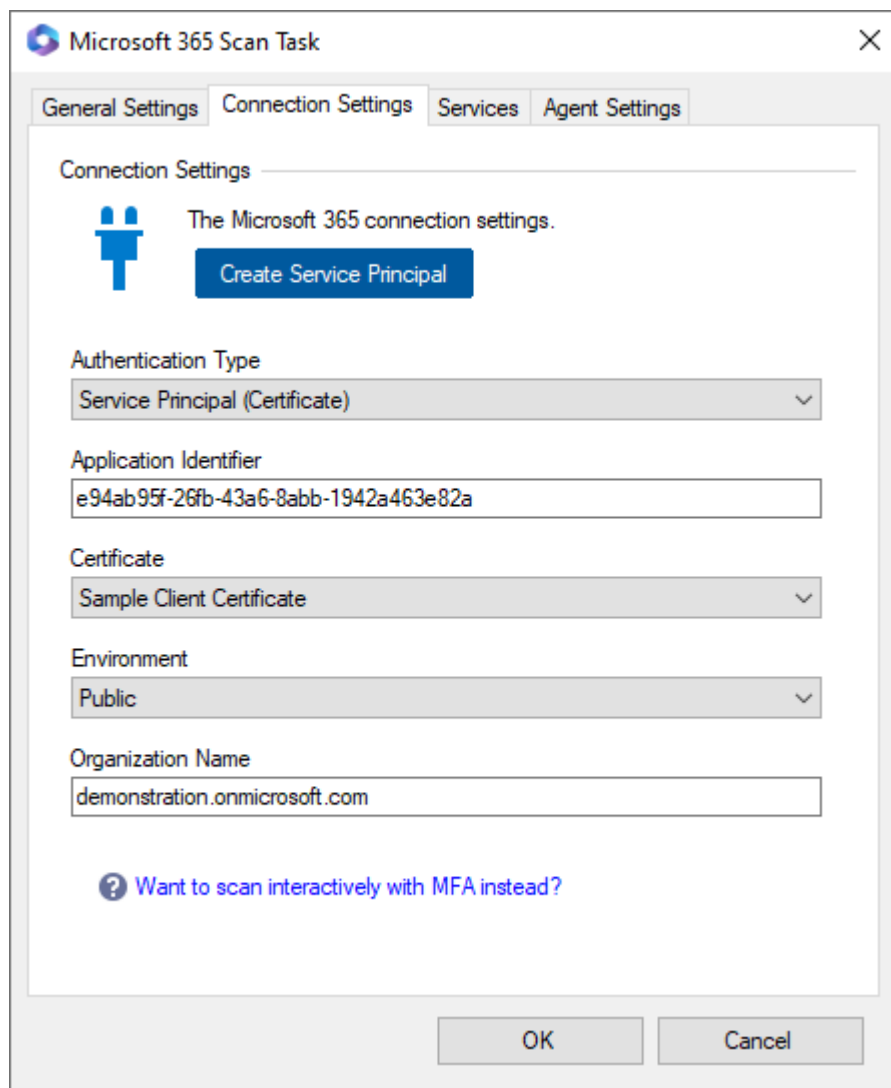
This method uses a client secret (password) for security - which is easier to share however is less secure than the certificate method.

Credentials (Deprecated)

This method uses a username and password and has been deprecated and is not recommended.

To scan interactivity instead using multi-factor authentication use the [Microsoft Online Agent UI](#).

Service Principal (Certificate)



The screenshot shows the 'Microsoft 365 Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'General Settings', 'Connection Settings', 'Services', and 'Agent Settings'. The 'Connection Settings' tab is active and contains the following elements:

- A blue plug icon and the text 'The Microsoft 365 connection settings.' with a blue 'Create Service Principal' button.
- An 'Authentication Type' dropdown menu set to 'Service Principal (Certificate)'.
- An 'Application Identifier' text box containing the GUID 'e94ab95f-26fb-43a6-8abb-1942a463e82a'.
- A 'Certificate' dropdown menu set to 'Sample Client Certificate'.
- An 'Environment' dropdown menu set to 'Public'.
- An 'Organization Name' text box containing 'demonstration.onmicrosoft.com'.
- A link with a question mark icon: '? Want to scan interactively with MFA instead?'.
- 'OK' and 'Cancel' buttons at the bottom.

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Certificate

The certificate to use for authentication. The certificate must be installed in the user store of the [XIA Configuration Client service account](#) and support client authentication.

Environment

The [environment](#) to connect to.

Organization Name

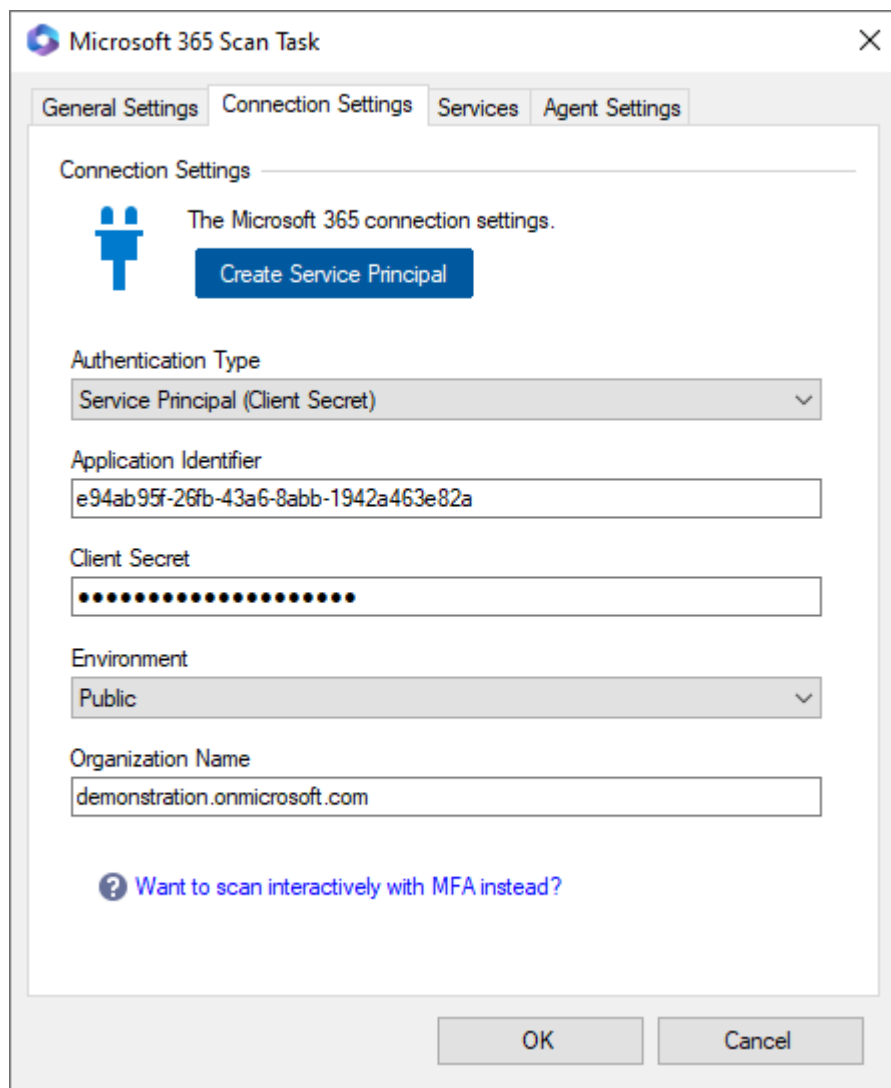
The name of the organization (tenant). The tenant identifier cannot be used as this is not compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Service Principal (Client Secret)



The screenshot shows the 'Microsoft 365 Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'General Settings', 'Connection Settings', 'Services', and 'Agent Settings'. The 'Connection Settings' tab is active and contains the following elements:

- A blue plug icon and the text 'The Microsoft 365 connection settings.' with a blue 'Create Service Principal' button.
- An 'Authentication Type' dropdown menu set to 'Service Principal (Client Secret)'.
- An 'Application Identifier' text box containing the GUID 'e94ab95f-26fb-43a6-8abb-1942a463e82a'.
- A 'Client Secret' text box filled with black dots.
- An 'Environment' dropdown menu set to 'Public'.
- An 'Organization Name' text box containing 'demonstration.onmicrosoft.com'.
- A link with a question mark icon: '? Want to scan interactively with MFA instead?'.
- 'OK' and 'Cancel' buttons at the bottom.

Authentication Type

The authentication type is Service Principal (Client Secret).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Client Secret

The client secret to use for authentication.

Environment

The [environment](#) to connect to.

Organization Name

The name of the organization (tenant). The tenant identifier cannot be used as this in not

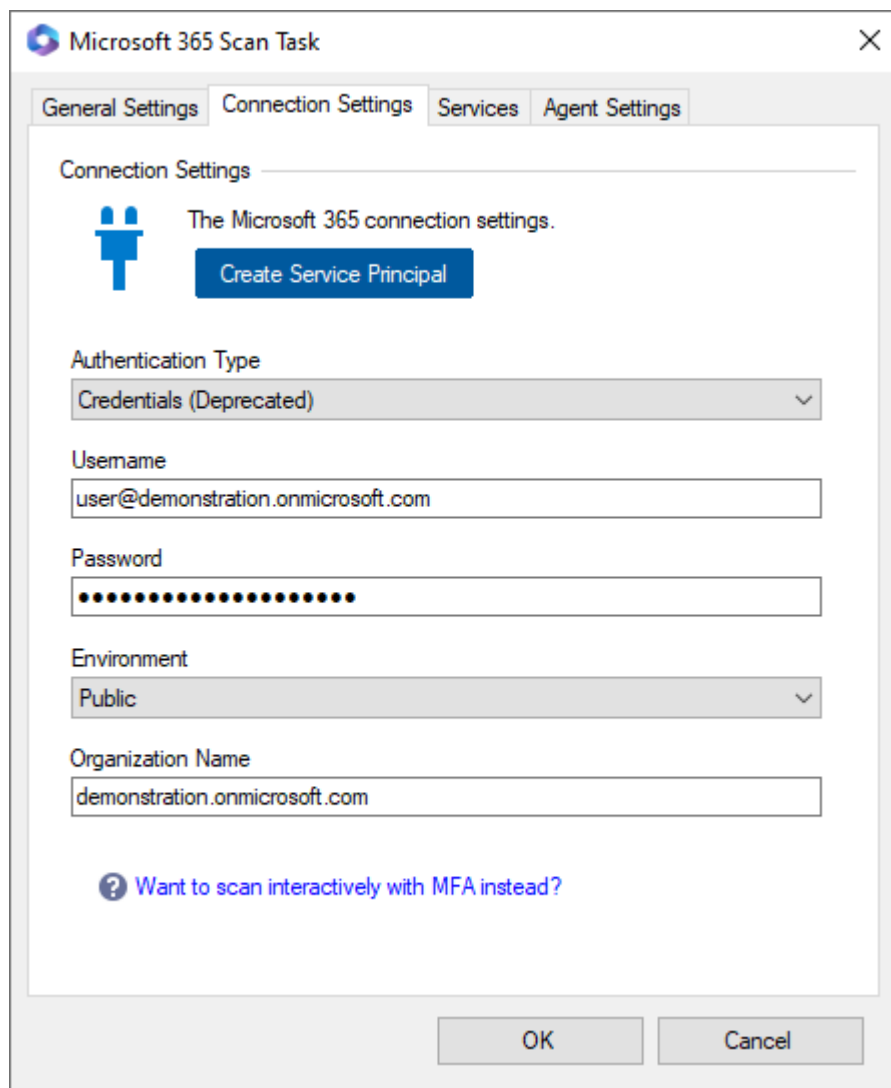
compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will create a new [service principal with certificate](#).

For more information see the [requirements](#) section.

Credentials (Deprecated)



The screenshot shows the 'Microsoft 365 Scan Task' dialog box with the 'Connection Settings' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'General Settings', 'Connection Settings', 'Services', and 'Agent Settings'. The 'Connection Settings' tab is active and contains the following elements:

- A blue icon of a person with a plus sign.
- The text 'The Microsoft 365 connection settings.'
- A blue button labeled 'Create Service Principal'.
- A label 'Authentication Type' above a dropdown menu showing 'Credentials (Deprecated)'.
- A label 'Username' above a text box containing 'user@ demonstration.onmicrosoft.com'.
- A label 'Password' above a text box filled with dots.
- A label 'Environment' above a dropdown menu showing 'Public'.
- A label 'Organization Name' above a text box containing 'demonstration.onmicrosoft.com'.
- A link with a question mark icon: '? Want to scan interactively with MFA instead?'.
- At the bottom, 'OK' and 'Cancel' buttons.

Authentication Type

The authentication type is Credentials (Deprecated). This method is deprecated and not recommended.

It is recommended to use a [service principal with a certificate](#), or login interactively using multi-factor authentication using the [Microsoft 365 agent UI](#).

Username

The username of the account to use for login.

Password

The password of the user account.

Environment

The [environment](#) to connect to.

Organization Name

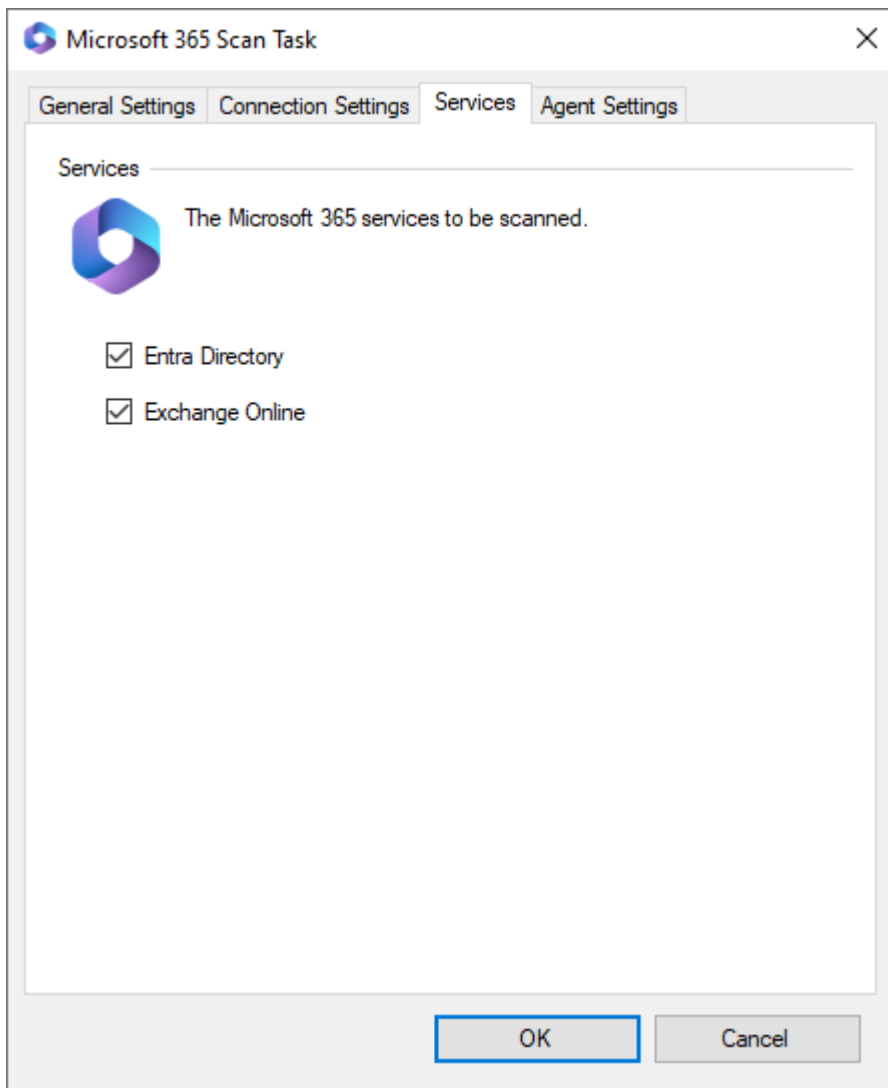
The name of the organization (tenant). The tenant identifier cannot be used as this is not compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will help automate the process of creating and configuring a [service principal with a certificate](#).

For more information see the [requirements](#) section.

Services



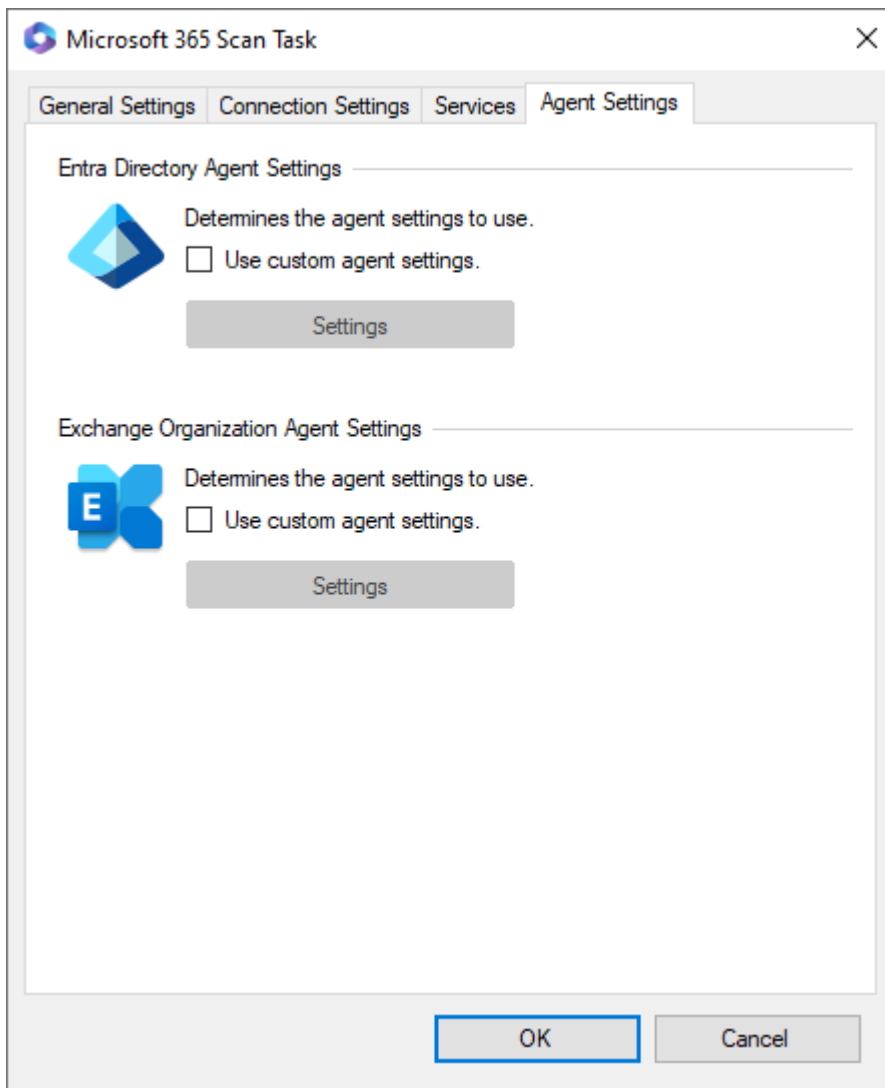
Entra Directory

Determines whether to scan the [Entra directory](#).

Exchange Online

Determines whether to scan the [Exchange Online organization](#).

Agent Settings



Entra Directory Agent Settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#) when scanning an [Entra directory](#).

Exchange Organization Agent Settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#) when scanning an [Exchange Online organization](#).

Requirements

The [Microsoft 365](#) organization [scan tasks](#) do not have their own requirements - for more information see the requirements of the supported [scan tasks](#):

Entra Directories

Please see the [Entra directory requirements](#).

Exchange Online

Please see the [Exchange Online requirements](#).

Microsoft DHCP Server

The Microsoft DHCP server [scan tasks](#) are able to document [Microsoft DHCP servers](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).

- Server Settings
 - Audit Log
 - Bindings
 - Database Settings
 - Dynamic DNS Credential
- Host Information
 - Operating System Name
 - Service Pack
 - Hardware Manufacturer
 - Hardware Model
 - Serial Number
 - Processors
- IPv4 Server
 - Failover Relationships
 - Filters
 - Policies
 - Predefined Options
 - Server Options
 - User and Vendor Classes
- IPv4 Multicast Scopes
 - Start IP Address

- End IP Address
- Lease Duration
- Description
- Address Pool
- Lifetime

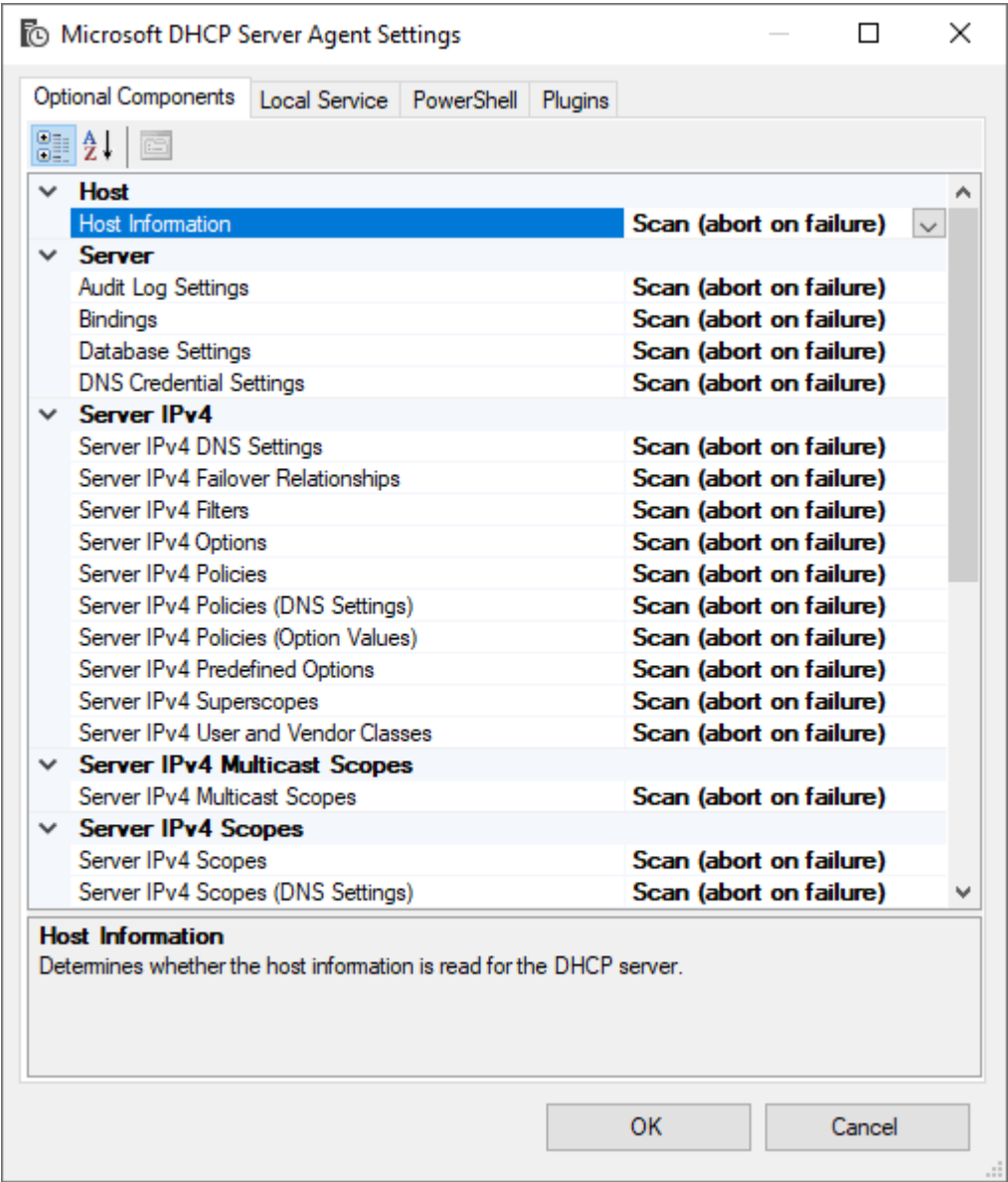
- IPv4 Scopes

- Lease Duration
- Description
- Scope Type
- DNS Settings
- Address Leases
- Address Pool
- Reservations
- Scope Options
- Superscope Name

- IPv6 Scopes

- Lease Duration
- Description
- Scope Type
- DNS Settings
- Address Leases
- Exclusions
- Reservations
- Scope Options

Agent Settings



Host Information

Determines whether the host information is read for the DHCP server.

Audit Log Settings

Determines whether the audit log settings information is read for the DHCP server.

Bindings

Determines whether the bindings are read for the DHCP server.

Database Settings

Determines whether the database settings information is read for the DHCP server.

DNS Credential Settings

Determines whether the DNS credential settings information is read for the DHCP server.

Server IPv4 DNS Settings

Determines whether the IPv4 server DNS settings are read for the DHCP server.

Server IPv4 Failover Relationships

Determines whether the IPv4 server failover relationships are read for the DHCP server.

Server IPv4 Filters

Determines whether the IPv4 server filters are read for the DHCP server.

Server IPv4 Options

Determines whether the IPv4 server options are read for the DHCP server.

Server IPv4 Policies

Determines whether the IPv4 server policies are read for the DHCP server.

Server IPv4 Policies (DNS Settings)

Determines whether the DNS settings are read for IPv4 server policies.

Server IPv4 Policies (Option Values)

Determines whether the option values are read for IPv4 server policies.

Server IPv4 Predefined Options

Determines whether the IPv4 predefined options are read for the DHCP server.

Server IPv4 Superscopes

Determines whether the IPv4 superscopes are read for the DHCP server.

Server IPv4 User and Vendor Classes

Determines whether the IPv4 user and vendor classes are read for the DHCP server.

Server IPv4 Multicast Scopes

Determines whether the IPv4 multicast scopes are read for the DHCP server.

Server IPv4 Scopes

Determines whether the IPv4 scopes are read for the DHCP server.

Server IPv4 Scopes (DNS Settings)

Determines whether the DNS settings are read for IPv4 scopes.

Server IPv4 Scopes (Leases)

Determines whether the leases are read for IPv4 scopes.

Server IPv4 Scopes (Reservation DNS Settings)

Determines whether the DNS settings are read for IPv4 reservations.

Server IPv4 Scopes (Reservation Option Values)

Determines whether the option values are read for IPv4 reservations.

Server IPv4 Scopes (Reservations)

Determines whether the reservations are read for IPv4 scopes.

Server IPv4 Scopes (Scope Options)

Determines whether the scope options are read for IPv4 scopes.

Server IPv6 DNS Settings

Determines whether the IPv6 server DNS settings are read for the DHCP server.

Server IPv6 Options

Determines whether the IPv6 server options are read for the DHCP server.

Server IPv6 Predefined Options

Determines whether the IPv6 predefined options are read for the DHCP server.

Server IPv6 User and Vendor Classes

Determines whether the IPv6 user and vendor classes are read for the DHCP server.

Server IPv6 Scopes

Determines whether the IPv6 scopes are read for the DHCP server.

Server IPv6 Scopes (DNS Settings)

Determines whether the DNS settings are read for IPv6 scopes.

Server IPv6 Scopes (Leases)

Determines whether the DNS settings are read for IPv6 scopes.

Server IPv6 Scopes (Reservation DNS Settings)

Determines whether the DNS settings are read for IPv6 reservations.

Server IPv6 Scopes (Reservation Option Values)

Determines whether the option values are read for IPv6 reservations.

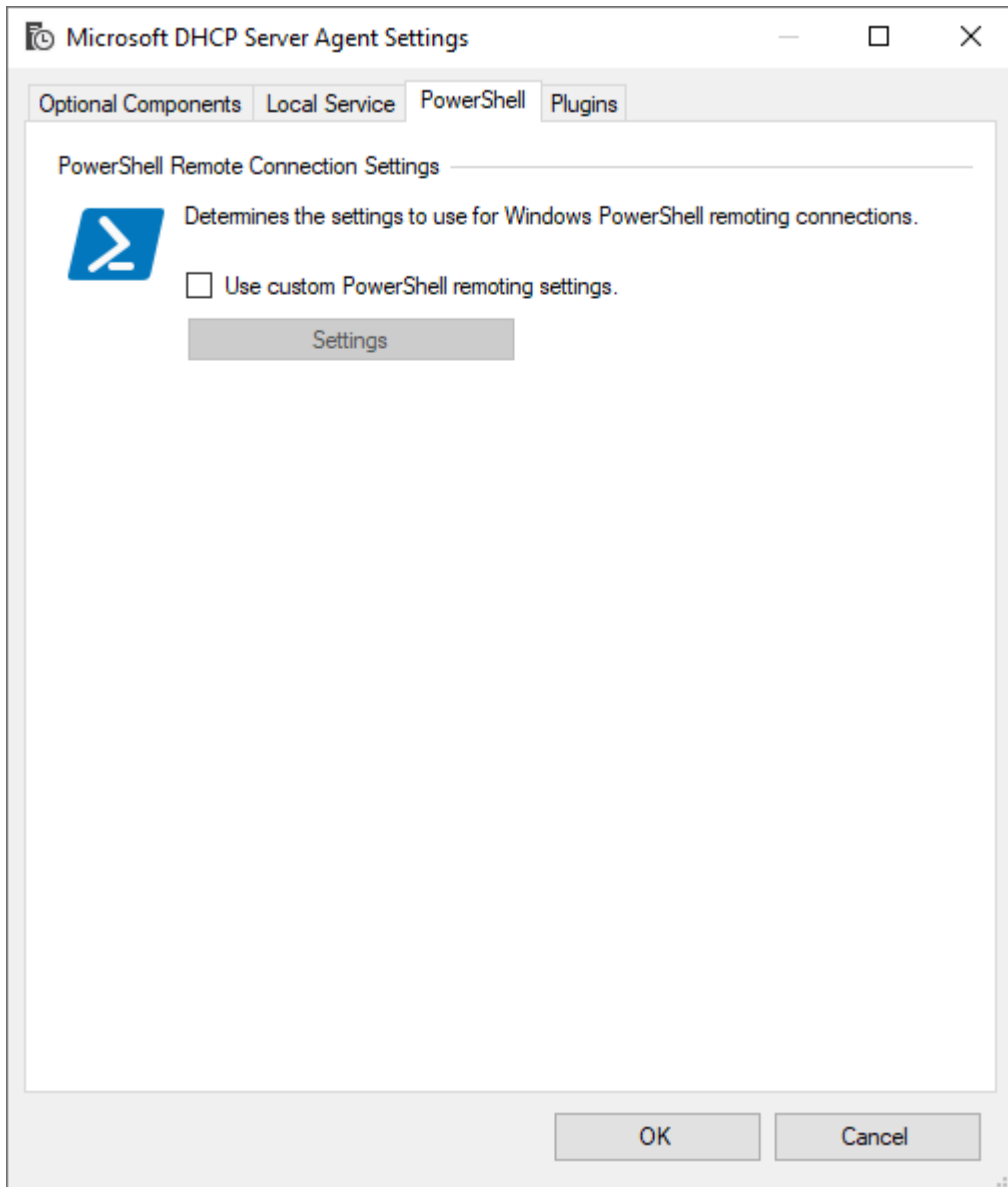
Server IPv6 Scopes (Reservations)

Determines whether the reservations are read for IPv6 scopes.

Server IPv6 Scopes (Scope Options)

Determines whether the scope options are read for IPv6 scopes.

PowerShell



Use custom PowerShell remoting settings

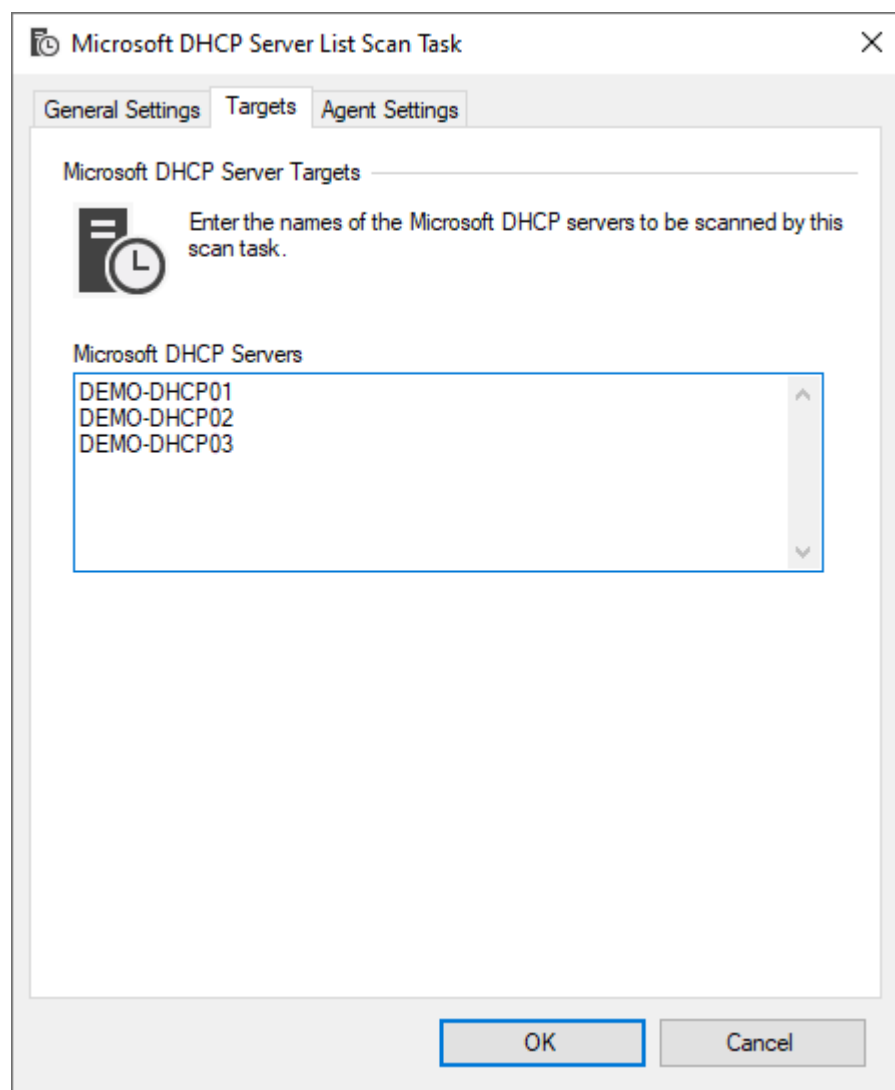
Determines whether to use custom [PowerShell connection settings](#).

Microsoft DHCP Server List Scan Task

The Microsoft DHCP Server list scan task allows you to enter a list of names or IP address of the [Microsoft DHCP servers](#) to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Microsoft DHCP servers](#).

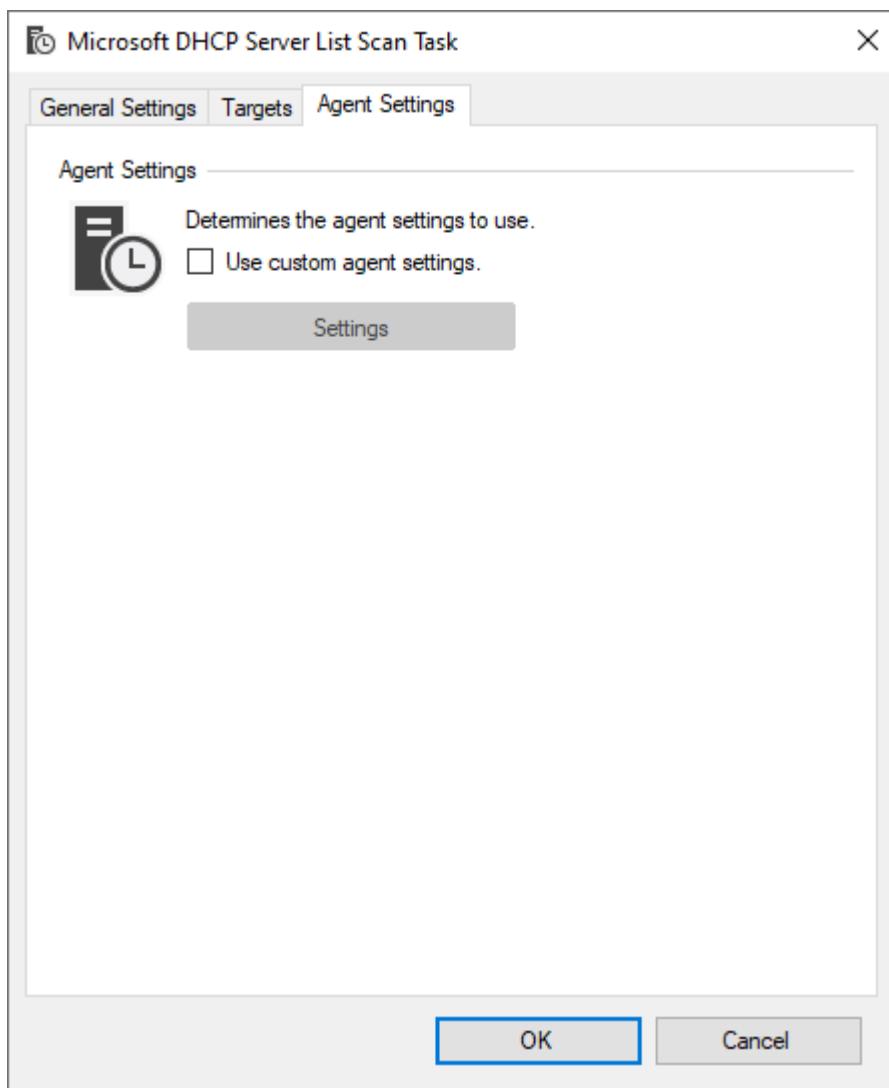
Targets



Microsoft DHCP Servers

The IP addresses, NetBIOS names, or fully qualified domain names of the [Microsoft DHCP servers](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Item Identifiers

For more information please see the [item identifiers](#) section.

Primary Identifier

The computer NetBIOS name.

Secondary Identifier

The computer serial number.

Tertiary Identifier

Not used

Requirements

Supported Target Systems

The [Microsoft DHCP server scan tasks](#) are supported on the following target operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Access Settings

The [Microsoft DHCP server scan tasks](#) use [PowerShell remoting](#) to obtain information remotely from [Microsoft DHCP servers](#).

- Firewall access must allow access to the [PowerShell remoting](#) ports on the remote machine
- The [XIA Configuration client service account](#) or [custom credentials](#) must have administrator rights on the remote machine.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✓ Windows Remote Management (HTTP-In)

Local Service

- ✓ The [Microsoft DHCP server scan tasks](#) support the [local service](#).

Automatic Detection

- ✓ [Microsoft DHCP servers](#) can be automatically detected and scanned by [Windows machine scan tasks](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

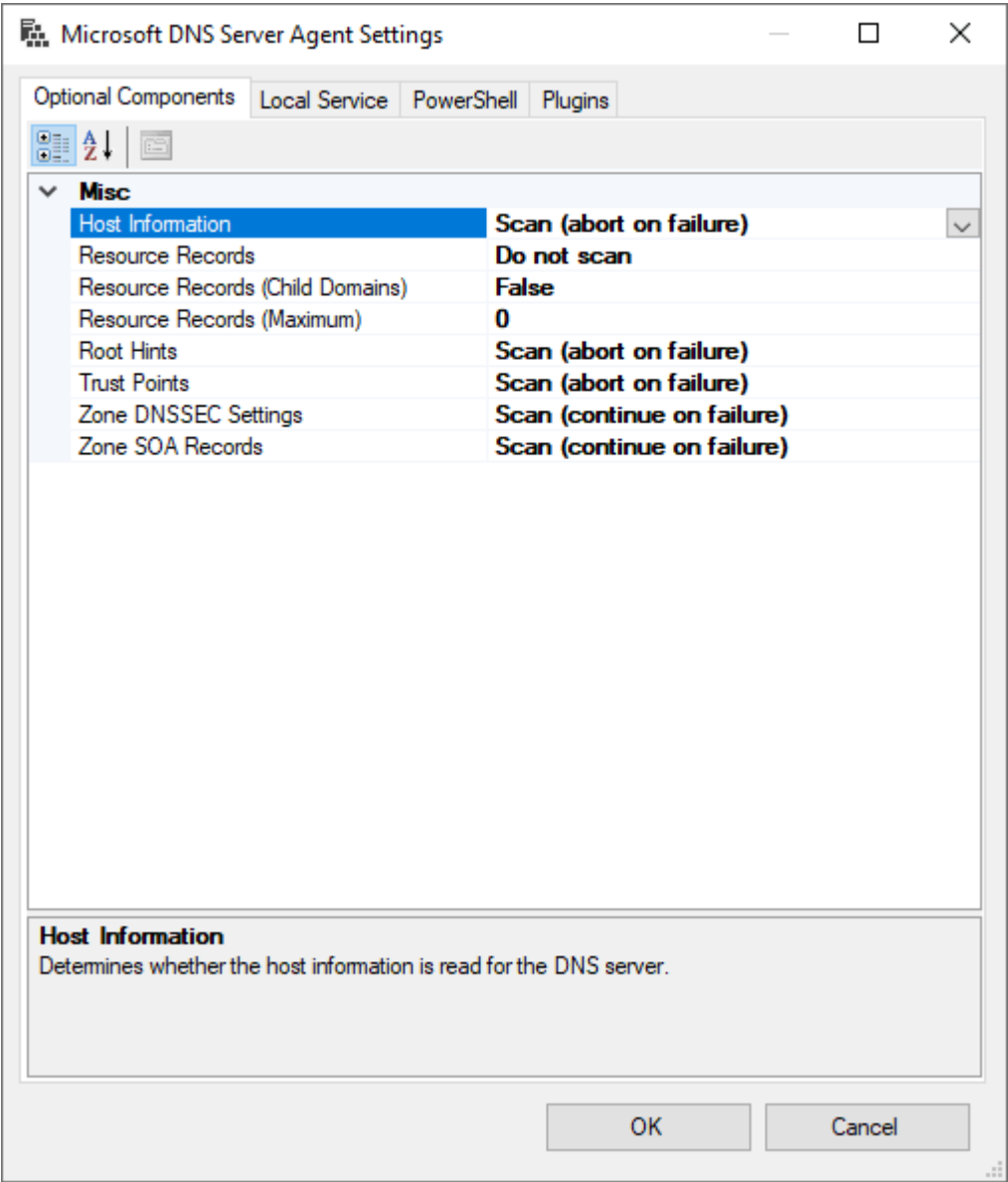
Microsoft DNS Server

The Microsoft DNS server [scan tasks](#) are able to document [Microsoft DNS servers](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).

- Server Configuration
 - Directory Settings
 - Diagnostics Settings
 - Forwarders
 - Global Names Zone Settings
 - Host Information
 - Recursion Settings
 - Root Hints
- Conditional Forwarders
- Trust Points
- Zones
 - Forward Lookup Zones
 - Reverse Lookup Zones
 - Stub Zones
 - Aging Settings
 - DNSSEC Settings
 - Name Servers
 - Notify Settings
 - Resource Records
 - SOA Record
 - Zone Status
 - Zone Transfers

- Zone Type

Agent Settings



Host Information

Determines whether the host information is read for the DNS server.

Resource Records

Determines whether to read the resource records for the zones.

Resource Records (Child Domains)

Determines whether resource records should be read for child domains.

Resource Records (Maximum)

The maximum number of resource records that can be documented for a zone. If the resource records option is enabled but the zone contains more resource records than the configured maximum value the section is bypassed and a [warning](#) is written to the [scan results](#).

Root Hints

Determines whether the root hints are read for the DNS server.

Trust Points

Determines whether the trust points are read for the DNS server.

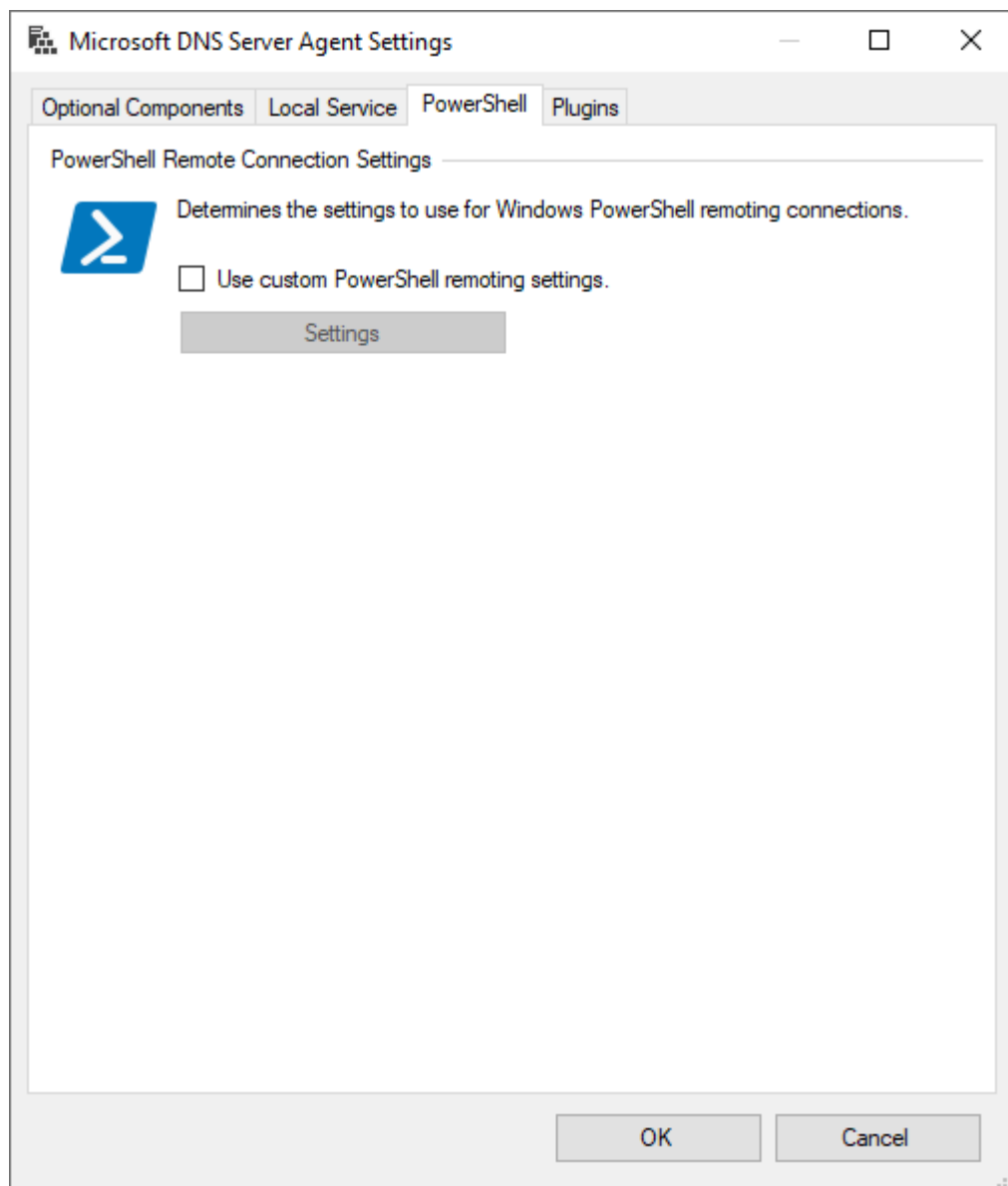
Zone DNSSEC Settings

Determines whether the DNSSEC settings is read for zones configured for the DNS server.

Zone SOA Records

Determines whether the SOA record for zones is read for the DNS server.

PowerShell



Use custom PowerShell remoting settings

Determines whether to use custom [PowerShell connection settings](#).

Item Identifiers

For more information please see the [item identifiers](#) section.

Primary Identifier

The computer NetBIOS name.

Secondary Identifier

The computer serial number.

Tertiary Identifier

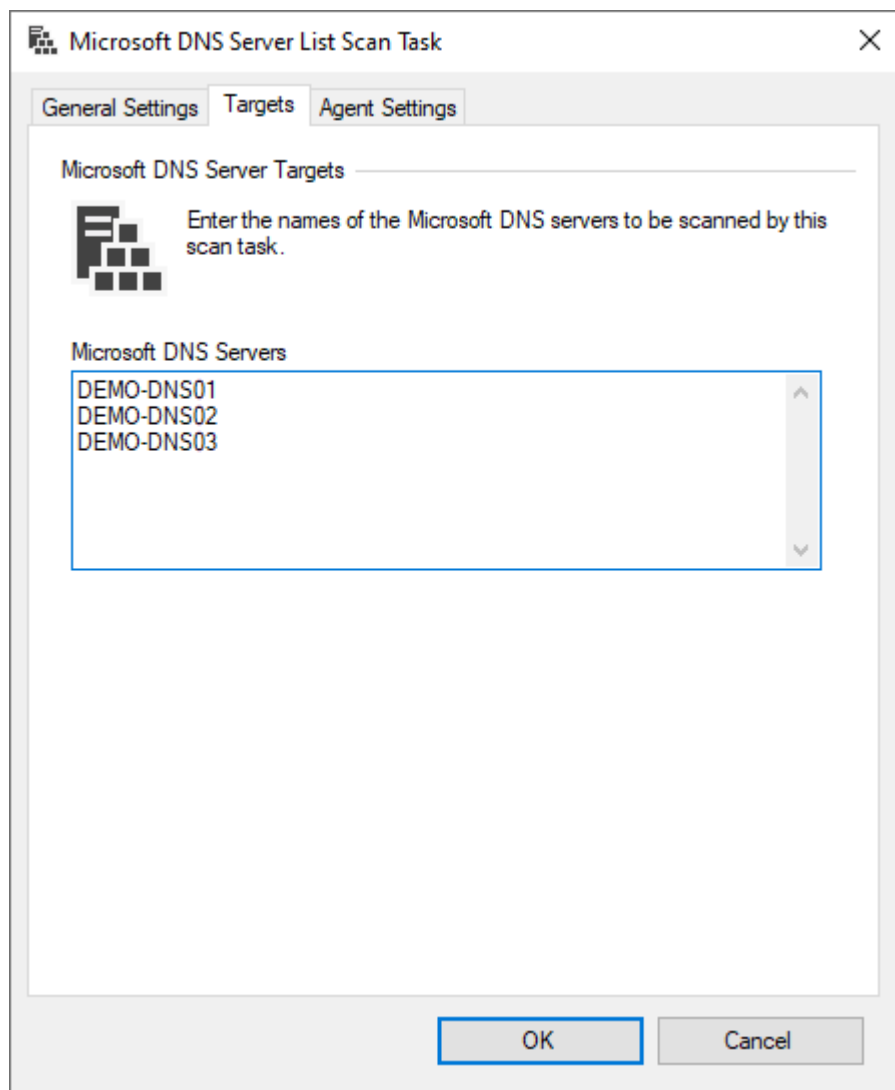
Not used

Microsoft DNS Server List Scan Task

The Microsoft DNS Server list scan task allows you to enter a list of names or IP address of the [Microsoft DNS servers](#) to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Microsoft DNS servers](#).

Targets

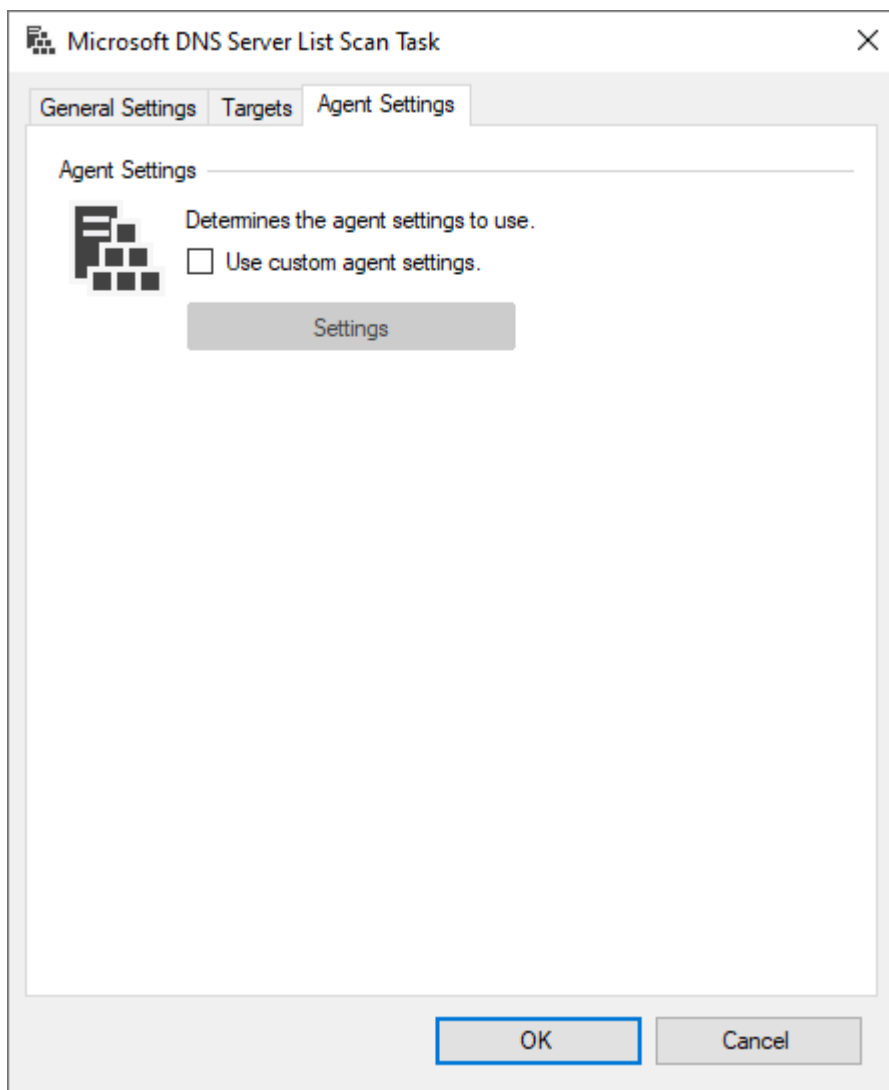


The screenshot shows a dialog box titled "Microsoft DNS Server List Scan Task" with a close button (X) in the top right corner. The dialog has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the "Targets" tab, there is a section titled "Microsoft DNS Server Targets" with a sub-header "Microsoft DNS Servers". Below this, there is a text area containing the following text: "Enter the names of the Microsoft DNS servers to be scanned by this scan task." Below the text area, there is a list box containing the following text: "DEMO-DNS01", "DEMO-DNS02", and "DEMO-DNS03". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Microsoft DNS Servers

The IP addresses, NetBIOS names, or fully qualified domain names of the [Microsoft DNS servers](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The [Microsoft DNS server scan tasks](#) are supported on the following target operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Access Settings

The [Microsoft DNS server scan tasks](#) use [PowerShell remoting](#) to obtain information remotely from [Microsoft DNS servers](#).

- Firewall access must allow access to the [PowerShell remoting](#) ports on the remote machine
- The [XIA Configuration client service account](#) or [custom credentials](#) must have administrator rights on the remote machine.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✓ Windows Remote Management (HTTP-In)

Local Service

- ✓ The [Microsoft DNS server scan tasks](#) support the [local service](#).

Automatic Detection

- ✓ [Microsoft DNS servers](#) can be automatically detected and scanned by [Windows machine scan tasks](#).

Troubleshooting

This section highlights the known issues for the [Microsoft DNS server agent](#), and provides details of the solutions.

Error executing PowerShell command 'Get-DnsServerRootHintDetails'

Symptoms

When you scan a [Microsoft DNS server](#), you see the following error

Error executing PowerShell command 'Get-DnsServerRootHintDetails'. No root hint found by *a.root-servers.net.* name server on *servername* server.

Cause

This can occur when the root hints data is corrupt on an Active Directory integrated [Microsoft DNS server](#) which is stored by default in the following location:

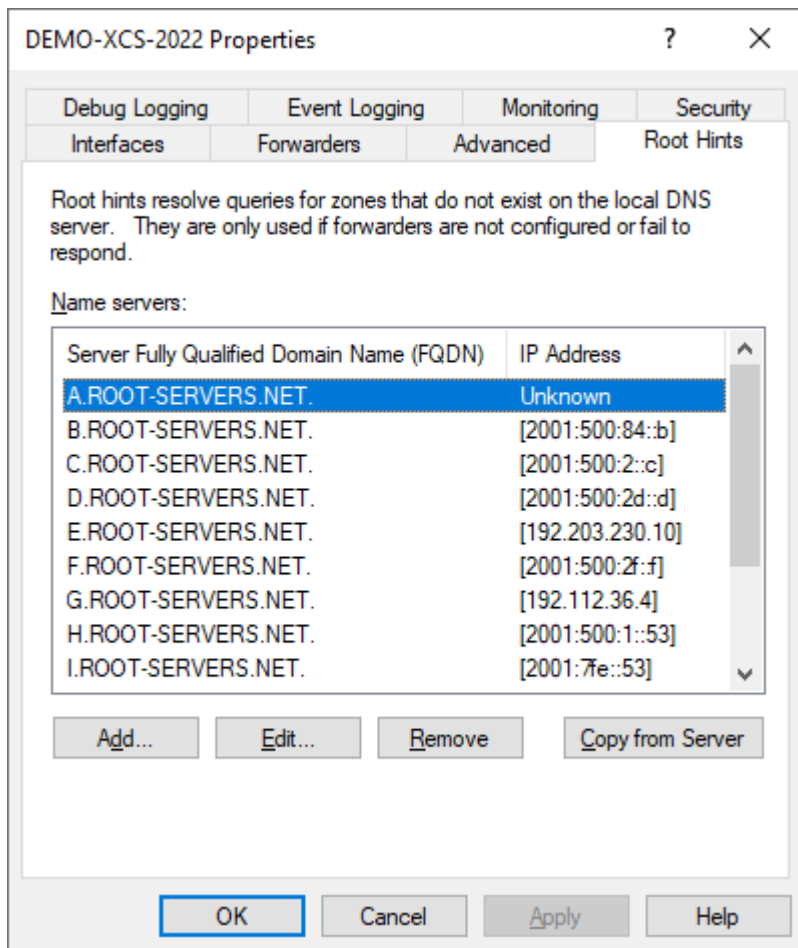
DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=*domain*,DC=*int*

If the [Microsoft DNS server](#) is not Active Directory integrated there may be an error in the cache.dns file which is by default found in the following location:

C:\Windows\System32\dns\cache.dns"

Resolution

Review the "Root Hints" section of the [Microsoft DNS server](#) Manager MMC and check for any "Unknown" values and correct as necessary.



Workaround

Set the "Root Hints" [optional component](#) to "Scan (continue on failure)".

Failed to enumerate the trust points

Symptoms

When you scan a [Microsoft DNS server](#), you see the following error

Error executing the command 'Get-DnsServerTrustPoint'. Failed to enumerate the trust points from the input server *servername*.

Cause

This can occur when the EnableDnsSec setting has been changed using the [Set-DnsServerSetting PowerShell cmdlet](#), but the DNS server service has not been restarted after making the change.

Resolution

Restart the DNS server service.

Trust Points: The remote procedure call failed

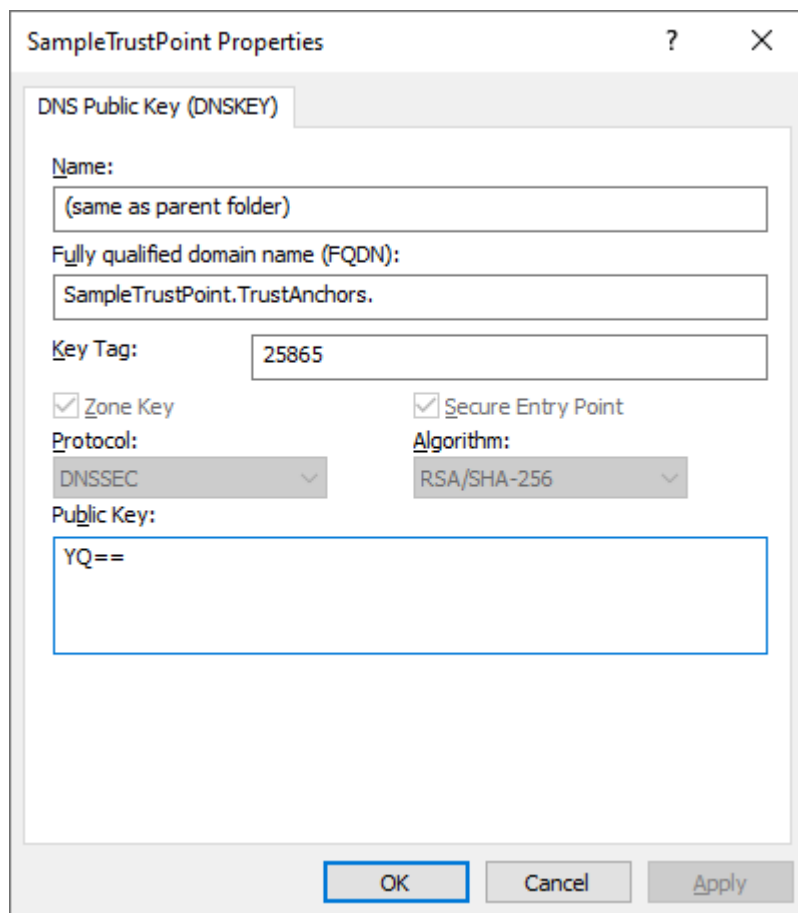
Symptoms

When you scan a [Microsoft DNS server](#), you see the following error

Error executing the command 'Get-DnsServerTrustAnchorDetails'. The remote procedure call failed.

Cause

This can occur when the public key assigned to a trust point is invalid.



The screenshot shows the 'SampleTrustPoint Properties' dialog box. It has a title bar with a question mark and a close button. The dialog is divided into two tabs: 'DNS Public Key (DNSKEY)' and 'Zone Data'. The 'DNS Public Key (DNSKEY)' tab is selected. Inside this tab, there are several fields and checkboxes. The 'Name' field contains '(same as parent folder)'. The 'Fully qualified domain name (FQDN)' field contains 'SampleTrustPoint.TrustAnchors.'. The 'Key Tag' field contains '25865'. There are two checkboxes: 'Zone Key' and 'Secure Entry Point', both of which are checked. Below these are two dropdown menus: 'Protocol' set to 'DNSSEC' and 'Algorithm' set to 'RSA/SHA-256'. At the bottom of the tab is a large text area labeled 'Public Key:' containing the text 'YQ=='. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Resolution

Correct the invalid public key.

Workaround

Set the "Trust Points" [optional component](#) to "Scan (continue on failure)".

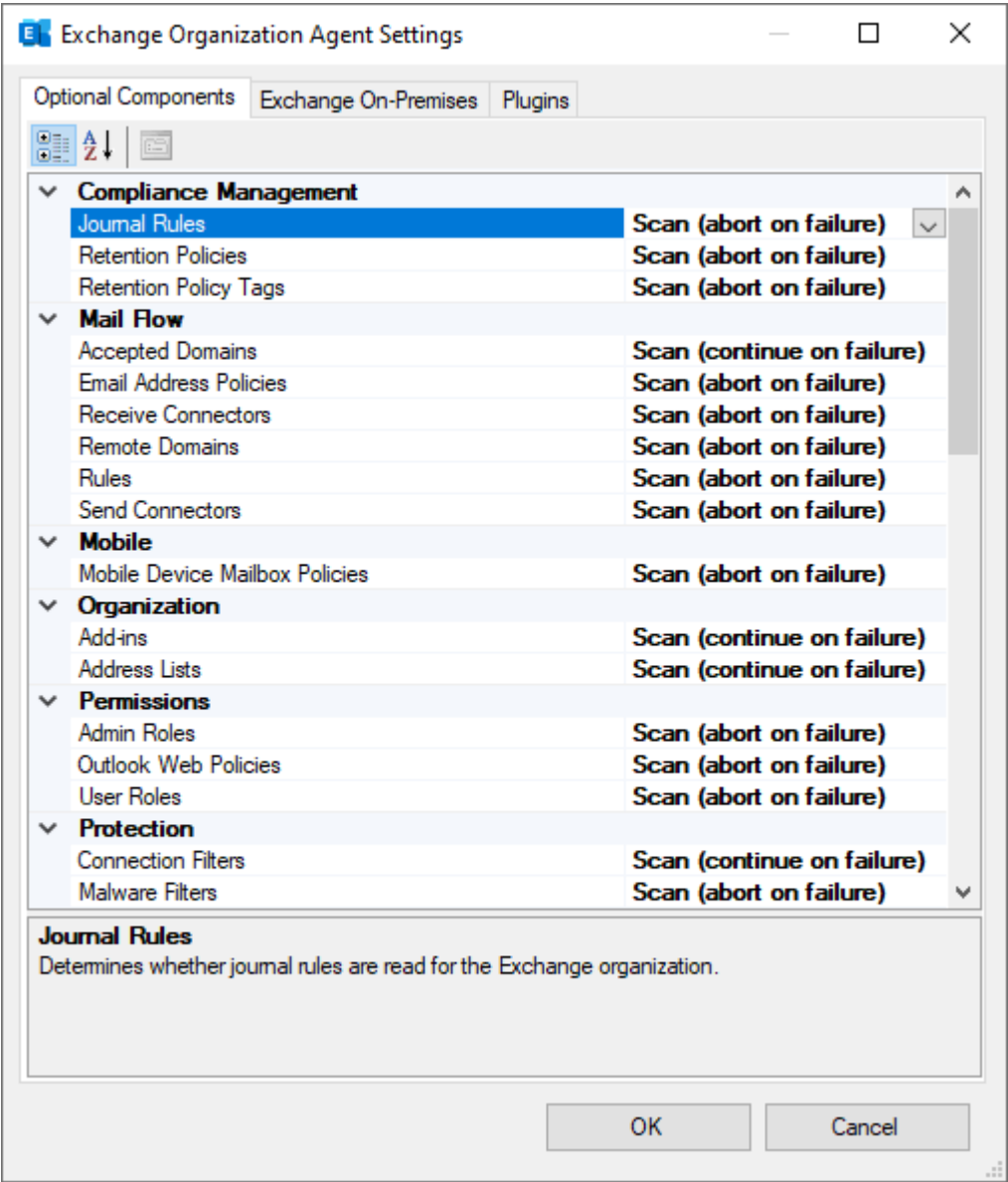
Microsoft Exchange Organization

Microsoft Exchange scan tasks are able to document both [Exchange Online](#) and Exchange On-Premises.

Agent Settings

This section describes the agent settings for the [Microsoft Exchange scan tasks](#).

Optional Components



Accepted Domains

Determines whether accepted domains are read for the Exchange organization. This setting also obtains information about whether DKIM is enabled for the domain on Exchange Online.

Add-ins

Determines whether add-ins are read for the Exchange organization.

Address Lists

Determines whether address lists are read for the Exchange organization. This setting only applies to Exchange On-Premises.

Admin Roles

Determines whether the role groups (admin roles) are read for the Exchange organization.

Connection Filters

Determines whether the hosted connection filters are read for the Exchange organization. This only applies to Exchange Online.

Database Availability Groups

Determines whether the database availability groups are read for the Exchange organization.

Database Availability Groups (Networks)

Determines whether the database availability group networks are read for the Exchange organization. A server within the database availability group must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Distribution Groups

Determines whether to read the standard distribution groups in the Exchange organization.

Dynamic Distribution Groups

Determines whether to read the dynamic distribution groups in the Exchange organization.

Email Address Policies

Determines whether email address policies are read for the Exchange organization.

Journal Rules

Determines whether journal rules are read for the Exchange organization.

Mailbox Databases

Determines whether the mailbox databases are read for the Exchange organization.

Mailbox Databases (Copies)

Determines whether the mailbox database copies are read for the Exchange organization. This only applies to Exchange On-Premises.

Mailbox Databases (Status)

Determines whether the status of mailbox databases are read for the Exchange organization. Each mailbox server hosting a mailbox database must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Mailboxes

Determines whether mailboxes will be read for the Exchange organization.

WARNING: This is disabled by default and is only recommended on small organizations as the size of the data gathered may become unmanageable.

Mailboxes (Statistics)

Determines whether mailbox statistics will be read for the Exchange organization. The server hosting the mailbox must be online and accessible at the time of the scan for this component to complete successfully.

Malware Filters

Determines whether malware filters are read for the Exchange organization.

Mobile Device Mailbox Policies

Determines whether mobile device mailbox policies are read for the Exchange organization.

Office 365 Groups

Determines whether the unified (Office 365) groups are read for the Exchange organization. This only applies to Exchange Online.

Outbound Spam Filters

Determines whether the outbound spam filters are read for the Exchange organization. This only applies to Exchange Online.

Outlook Web Policies

Determines whether Outlook web policies are read for the Exchange organization.

Public Folder Mailboxes

Determines whether public folder mailboxes are read for the Exchange organization.

Public Folders

Determines whether public folders are read for the Exchange organization.

Public Folders (Client Permissions)

Determines whether public folder client permissions are read for the Exchange organization.

Public Folders (Mail Settings)

Determines whether public folder mail settings are read for the Exchange organization.

Public Folders (Statistics)

Determines whether public folder statistics are read for the Exchange organization. The server

hosting the public folder must be online and accessible at the time of the scan for this component to complete successfully.

Receive Connectors

Determines whether receive connectors are read for the Exchange organization. This only applies to Exchange On-Premises.

Remote Domains

Determines whether remote domains should be read for the Exchange organization.

Retention Policies

Determines whether retention policies should be read for the Exchange organization.

Retention Policy Tags

Determines whether retention policy tags should be read for the Exchange organization.

Send Connectors

Determines whether send connectors are read for the Exchange organization. This only applies to Exchange On-Premises.

Servers

Determines whether the Exchange servers are read for the Exchange organization. This only applies to Exchange On-Premises.

Servers (Certificates)

Determines whether the certificate information of Exchange servers is read for the Exchange organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Servers (Client Access)

Determines whether the general Client Access information of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises.

Servers (Database Copies)

Determines whether the database copy information of Exchange servers is read for the Exchange organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Servers (Host Information)

Determines whether the host information of Exchange servers is read for the Exchange

organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Servers (IMAP)

Determines whether the IMAP information of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises.

Servers (Malware Filtering)

Determines whether the malware filtering information of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises, on Exchange Server 2013 and above.

Servers (Outlook Anywhere)

Determines whether the Outlook Anywhere information of Exchange servers is read for the Exchange organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Servers (POP3)

Determines whether the POP3 information of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises.

Servers (Status Information)

Determines whether the status information of Exchange servers is read for the Exchange organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Servers (Transport)

Determines whether the transport settings of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises, where the server is a hub transport server, or edge transport server.

Servers (Unified Messaging)

Determines whether the unified messaging (UM) information of Exchange servers is read for the Exchange organization. This only applies to Exchange On-Premises.

Servers (Virtual Directories)

Determines whether the virtual directory information of Exchange servers is read for the Exchange organization. Each server must be online and accessible at the time of the scan for this component to complete successfully. This only applies to Exchange On-Premises.

Spam Filters

Determines whether spam filters are read for the Exchange organization. This only applies to Exchange Online.

Transport (Mail Flow) Rules

Determines whether the transport (mail flow) rules are read for the Exchange organization.

Unified Messaging Auto Attendants

Determines whether the Unified Messaging auto attendants are read for the Exchange organization.

Unified Messaging Dial Plans

Determines whether the Unified Messaging (UM) dial plans are read for the Exchange organization.

Unified Messaging Hunt Groups

Determines whether the Unified Messaging hunt groups are read for the Exchange organization.

Unified Messaging IP Gateways

Determines whether the Unified Messaging (UM) IP gateways are read for the Exchange organization.

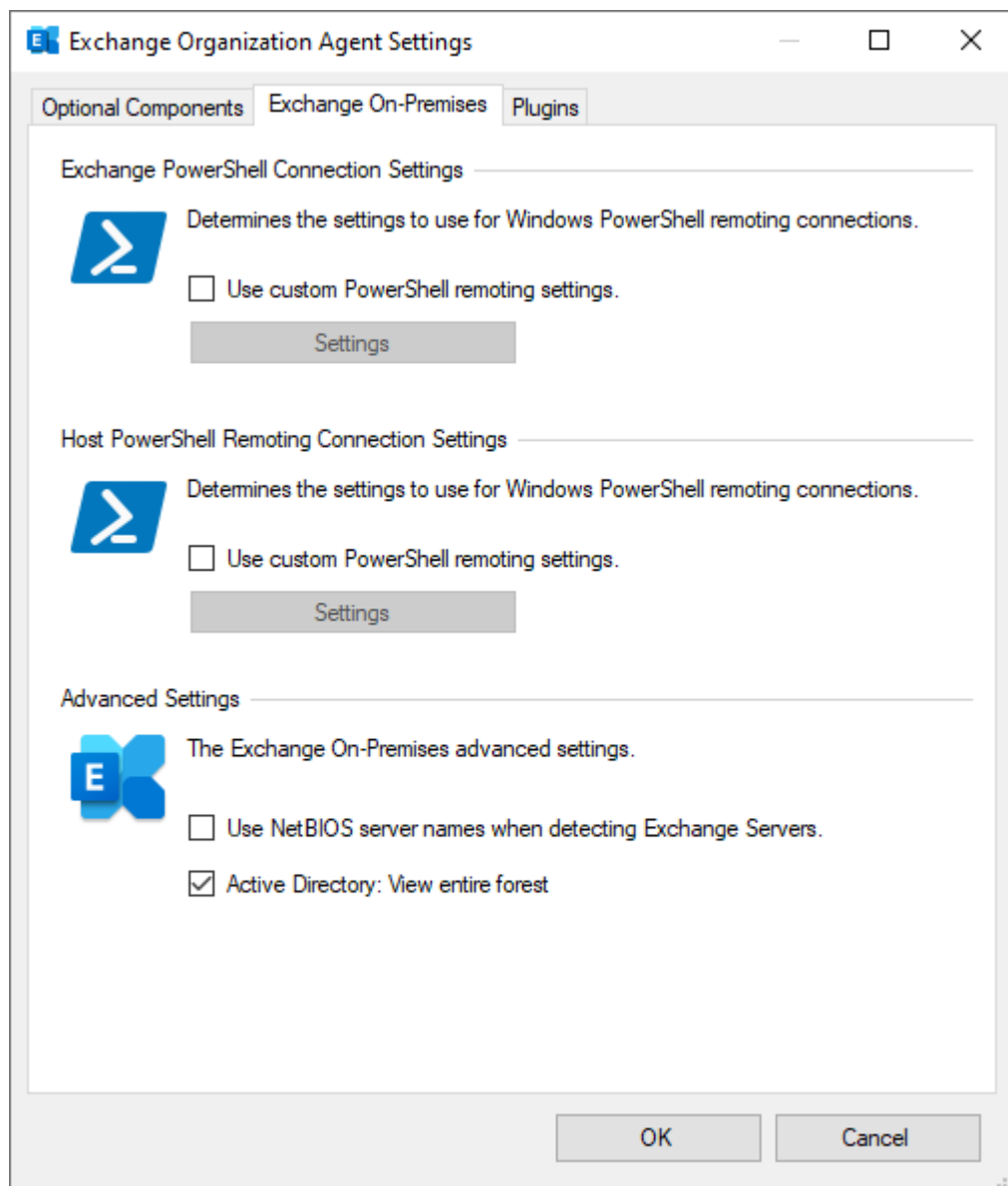
Unified Messaging Mailbox Policies

Determines whether the Unified Messaging (UM) mailbox policies are read for the Exchange organization.

User Roles

Determines whether the role assignment policies (user roles) are read for the Exchange organization.

On-Premises Settings



Exchange PowerShell Connection Settings

The [PowerShell connection settings](#) to use to connect to Exchange On-Premises.

Host PowerShell Remoting Connection Settings

The [PowerShell connection settings](#) to use to connect to each Exchange Server to obtain host information such as manufacturer and serial number.

Use NetBIOS server names when detecting Exchange Servers

Determines whether NetBIOS names should be used when automatically detecting and connecting to Exchange On-Premises servers.

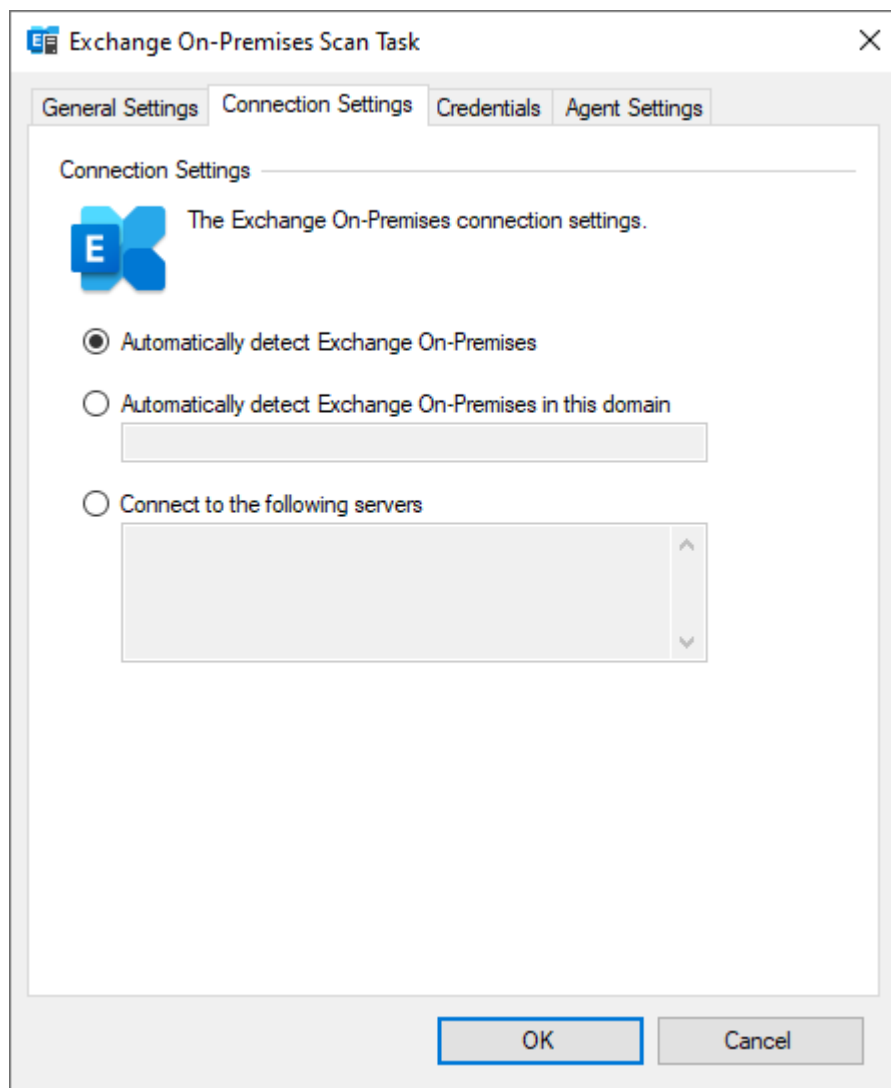
Active Directory: View entire forest

Determines whether all objects in the forest are viewed by the PowerShell session, for more information see the ViewEntireForest parameter of the [Set-ADServerSettings](#) cmdlet.

Exchange On-Premises Scan Task

The Exchange on-premises scan task allows you to scan on-premises Microsoft Exchange installations.

Connection Settings



Automatically detect Exchange On-Premises

The agent will automatically detect, and attempt to connect to Exchange Servers in the forest of which the computer running the [XIA Configuration Client](#) is a member. Server connections are attempted in order of Exchange version number, highest first.

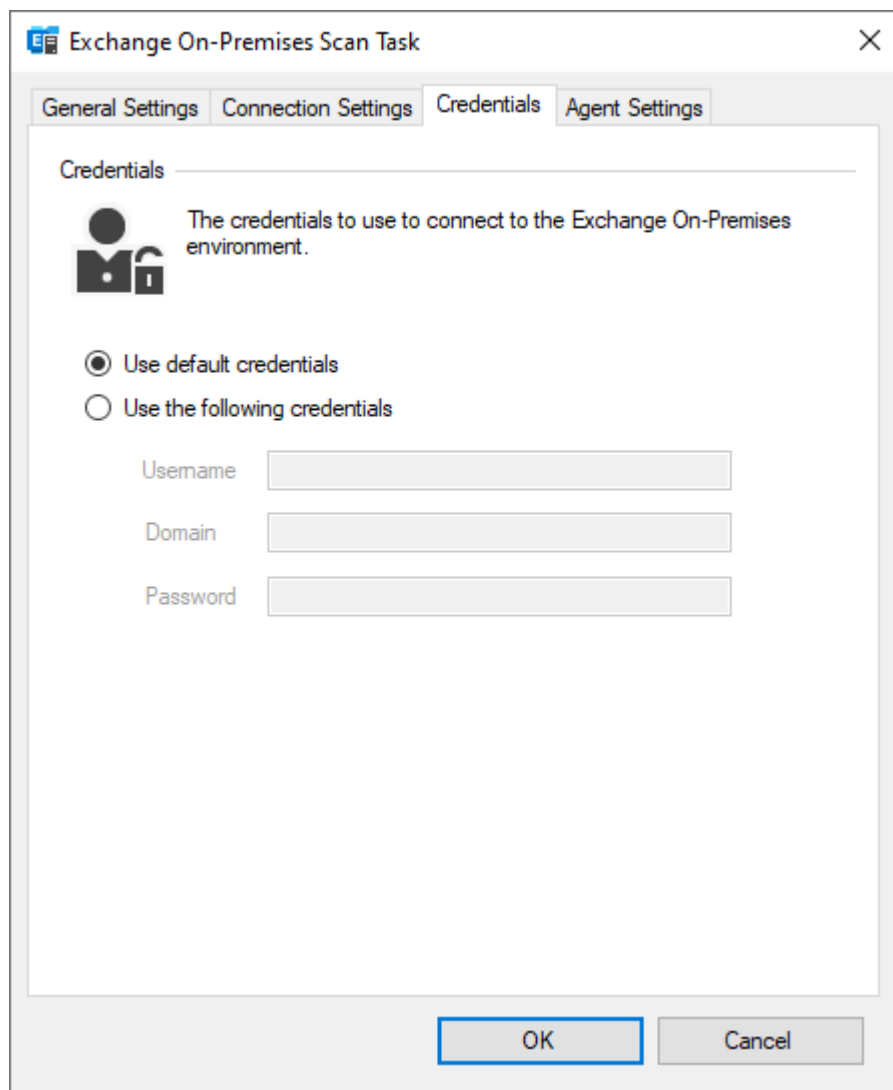
Automatically detect Exchange On-Premises in this domain

The agent will automatically detect, and attempt to connect to Exchange Servers in the parent forest of the specified domain. Server connections are attempted in order of Exchange version number, highest first.

Connect to the following servers

The agent will attempt to connect to the Exchange Servers specified. Server connections are attempted in the order specified.

Credentials



The image shows a screenshot of the 'Exchange On-Premises Scan Task' dialog box, specifically the 'Credentials' tab. The dialog has four tabs: 'General Settings', 'Connection Settings', 'Credentials', and 'Agent Settings'. The 'Credentials' tab is active, showing a section titled 'Credentials' with a description: 'The credentials to use to connect to the Exchange On-Premises environment.' Below this, there are two radio button options: 'Use default credentials' (which is selected) and 'Use the following credentials'. Under the second option, there are three text input fields labeled 'Username', 'Domain', and 'Password'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Use Default Credentials

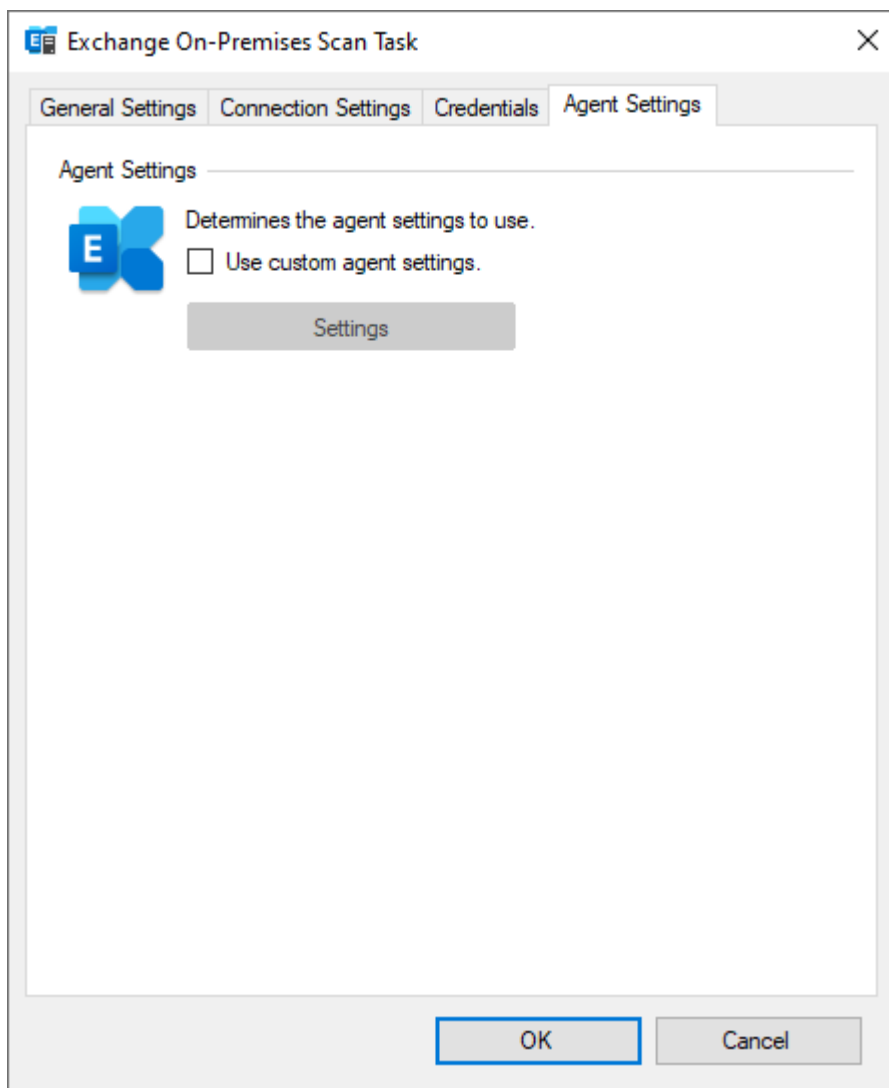
The current credentials of the [service account](#), or [custom credentials](#) if applicable will be used to connect to the Exchange organization.

Use Specific Credentials

The specified credentials will be used to connect to the Exchange organization. The account must have the [View-Only Organization Management](#) or greater [admin role](#) to the Exchange organization.

NOTE: The credentials are used to make a connection to the Exchange organization, and are not used to collect [server host information](#).

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Exchange Online Scan Task

The Exchange Online scan task allows you to scan cloud based [Exchange Online](#) organizations.

Connection Settings

The connection settings determines how to connect to the [Exchange Online](#) organization.

Service Principal (Certificate)

This is the recommended authentication method.

Service Principal (Client Secret)

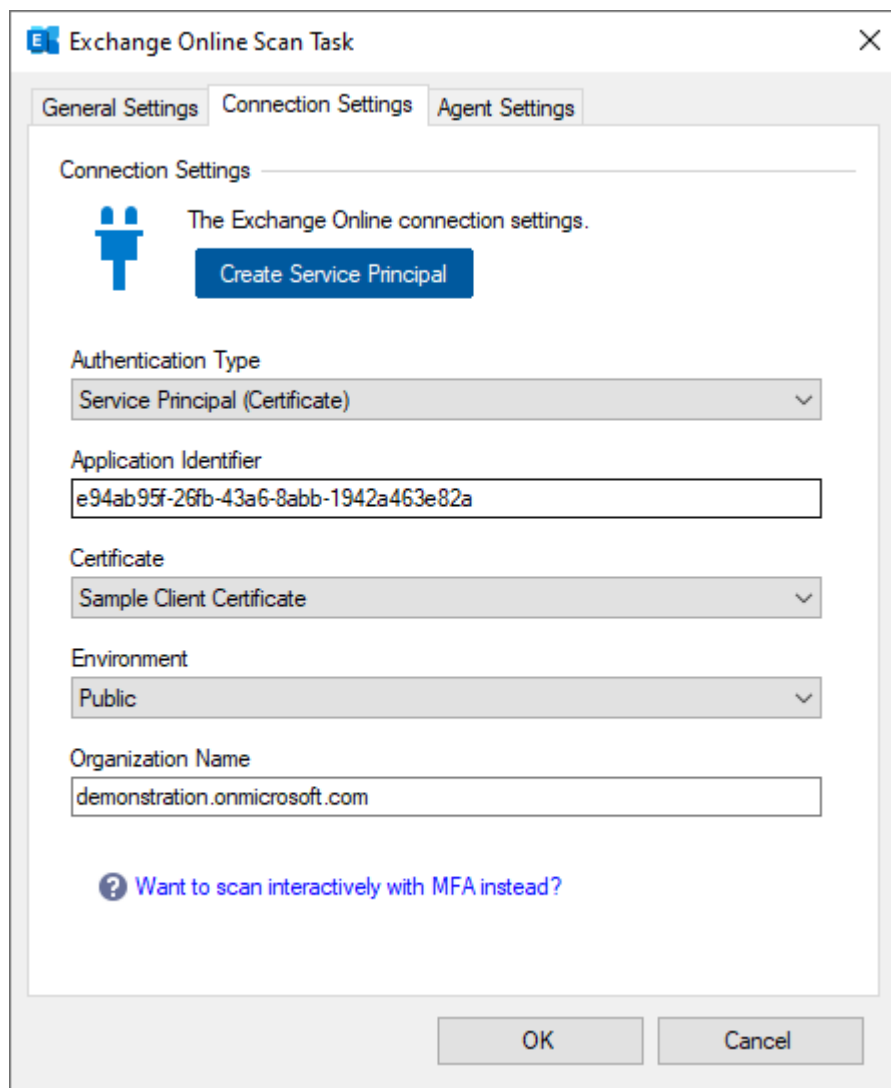
This method uses a client secret (password) for security - which is easier to share however is less secure than the certificate method.

Credentials (Deprecated)

This method uses a username and password and has been deprecated and is not recommended.

To scan interactivity instead using multi-factor authentication use the [Microsoft 365 Agent UI](#).

Service Principal (Certificate)



The dialog box is titled "Exchange Online Scan Task" and has three tabs: "General Settings", "Connection Settings", and "Agent Settings". The "Connection Settings" tab is selected. It contains a blue icon of a person with a plus sign, the text "The Exchange Online connection settings.", and a blue button labeled "Create Service Principal". Below this are several fields: "Authentication Type" with a dropdown menu showing "Service Principal (Certificate)", "Application Identifier" with a text box containing "e94ab95f-26fb-43a6-8abb-1942a463e82a", "Certificate" with a dropdown menu showing "Sample Client Certificate", "Environment" with a dropdown menu showing "Public", and "Organization Name" with a text box containing "demonstration.onmicrosoft.com". At the bottom left is a link with a question mark icon that says "Want to scan interactively with MFA instead?". At the bottom right are "OK" and "Cancel" buttons.

Authentication Type

The authentication type is Service Principal (Certificate).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Certificate

The certificate to use for authentication. The certificate must be installed in the user store of the [XIA Configuration Client service account](#) and support client authentication.

Environment

The [environment](#) to connect to.

Organization Name

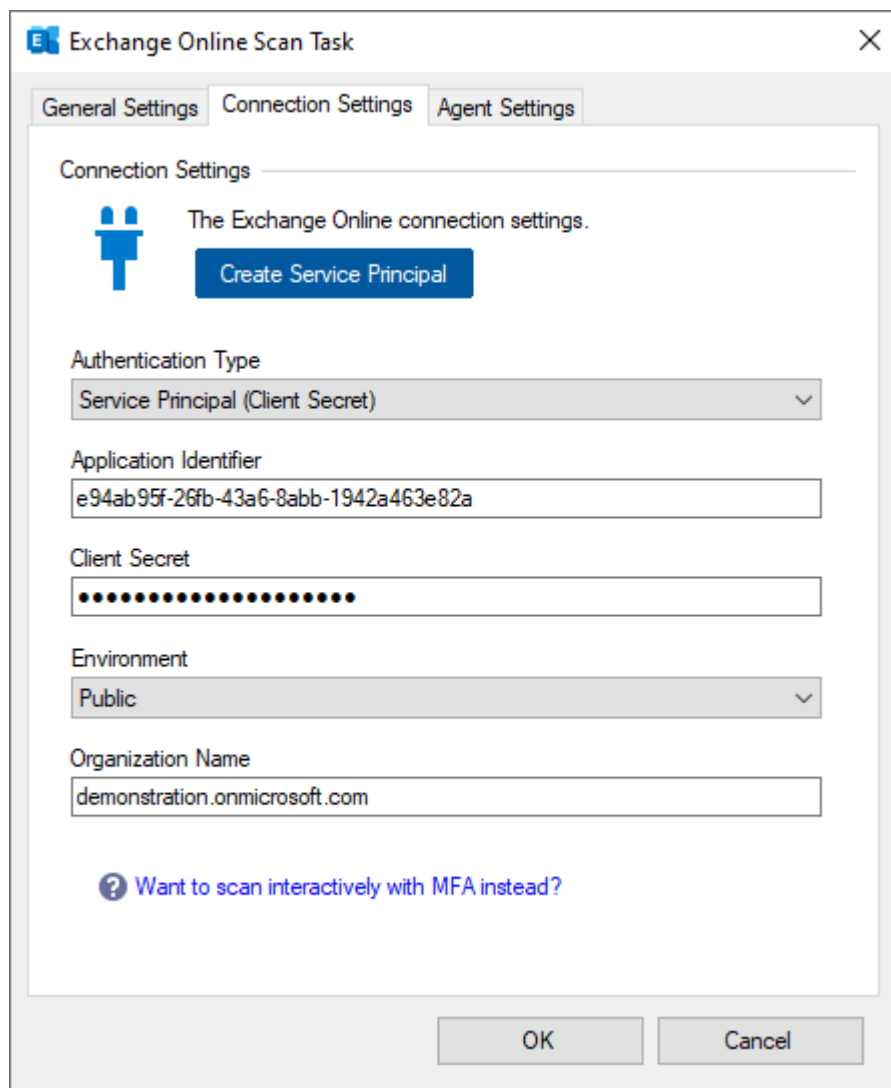
The name of the organization (tenant). The tenant identifier cannot be used as this is not compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#).

For more information see the [requirements](#) section.

Service Principal (Client Secret)



The dialog box is titled "Exchange Online Scan Task" and has three tabs: "General Settings", "Connection Settings", and "Agent Settings". The "Connection Settings" tab is selected. It contains a blue icon of a person with a plus sign, the text "The Exchange Online connection settings.", and a blue button labeled "Create Service Principal". Below this are several input fields: "Authentication Type" (a dropdown menu showing "Service Principal (Client Secret)"), "Application Identifier" (a text box containing "e94ab95f-26fb-43a6-8abb-1942a463e82a"), "Client Secret" (a text box filled with dots), "Environment" (a dropdown menu showing "Public"), and "Organization Name" (a text box containing "demonstration.onmicrosoft.com"). At the bottom left is a link with a question mark icon that says "Want to scan interactively with MFA instead?". At the bottom right are "OK" and "Cancel" buttons.

Authentication Type

The authentication type is Service Principal (Client Secret).

Application Identifier

The identifier of the [Entra](#) application to use for authentication in [GUID](#) format.

Client Secret

The client secret to use for authentication.

Environment

The [environment](#) to connect to.

Organization Name

The name of the organization (tenant). The tenant identifier cannot be used as this in not

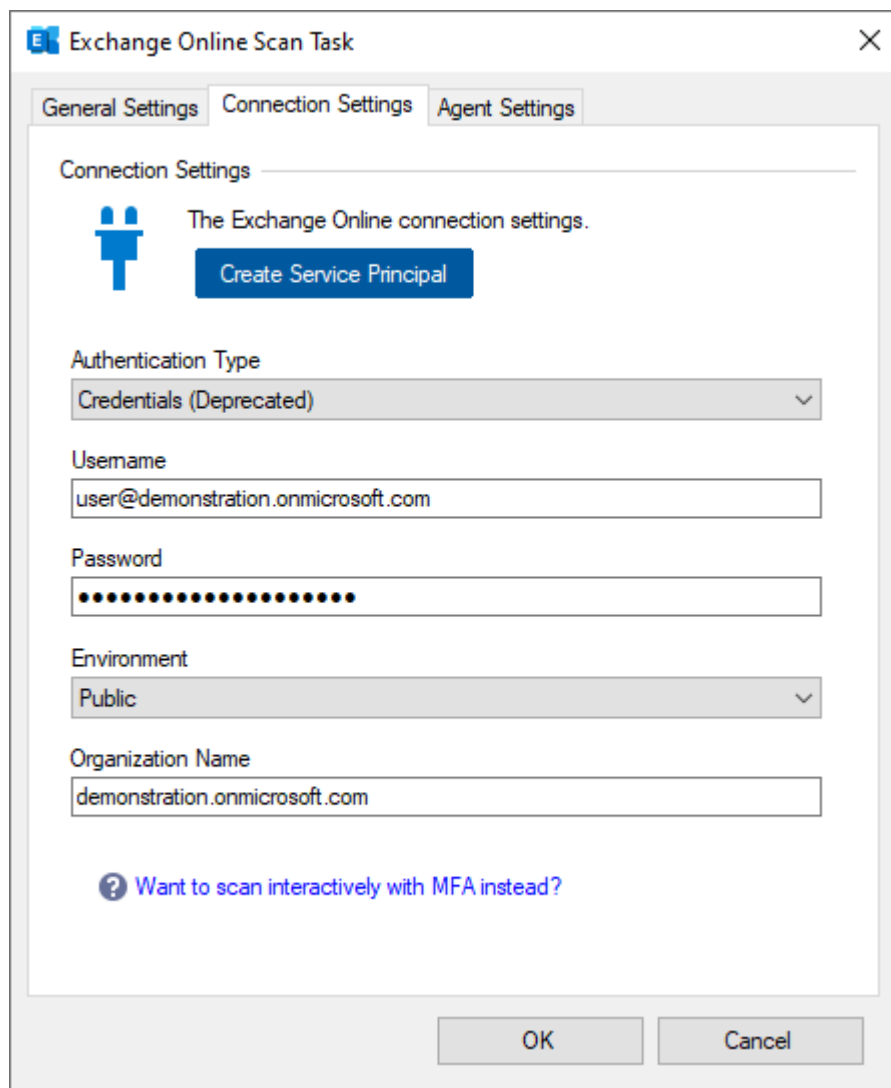
compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will create a new [service principal with certificate](#).

For more information see the [requirements](#) section.

Credentials (Deprecated)



The image shows a Windows-style dialog box titled "Exchange Online Scan Task". It has three tabs: "General Settings", "Connection Settings", and "Agent Settings". The "Connection Settings" tab is selected. Inside this tab, there is a blue icon of a person and the text "The Exchange Online connection settings." Below this is a blue button labeled "Create Service Principal". Further down, there are several fields: "Authentication Type" is a dropdown menu showing "Credentials (Deprecated)"; "Username" is a text box containing "user@ demonstration.onmicrosoft.com"; "Password" is a text box filled with dots; "Environment" is a dropdown menu showing "Public"; and "Organization Name" is a text box containing "demonstration.onmicrosoft.com". At the bottom of the dialog, there are "OK" and "Cancel" buttons. A link with a question mark icon says "Want to scan interactively with MFA instead?"

Authentication Type

The authentication type is Credentials (Deprecated). This method is deprecated and not recommended.

It is recommended to use a [service principal with a certificate](#), or login interactively using multi-factor authentication using the [Microsoft 365 agent UI](#).

Username

The username of the account to use for login.

Password

The password of the user account.

Environment

The [environment](#) to connect to.

Organization Name

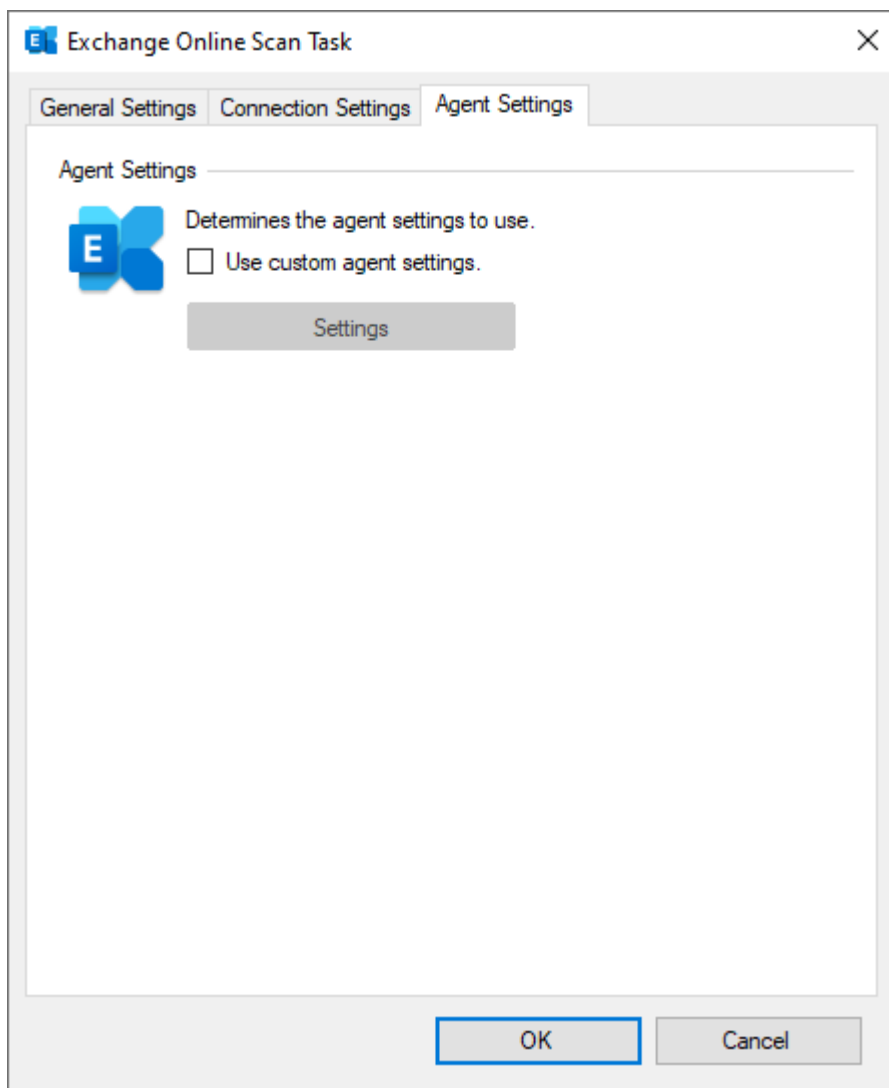
The name of the organization (tenant). The tenant identifier cannot be used as this is not compatible with the [Exchange Online organization](#) scan tasks.

Create Service Principal

Launches the [Microsoft service principal creation tool](#). This will help automate the process of creating and configuring a [service principal with a certificate](#).

For more information see the [requirements](#) section.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

[Microsoft Exchange](#) scan tasks are supported on the following Exchange versions. Some features may not be supported on all versions.

- Microsoft Exchange Online
- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013

Windows Firewall Requirements

Please see the [Exchange Online](#) or [Exchange On-Premises](#) requirements.

Access Settings

Please see the [Exchange Online](#) or [Exchange On-Premises](#) requirements.

Local Service

 [Microsoft Exchange](#) scan tasks do not support the [XIA Configuration Local Service](#).

Automatic Detection

 [Microsoft Exchange](#) On-Premises organizations can be automatically detected within the forest.

Exchange Online Requirements

Windows Firewall Requirements

✔ The [Microsoft Exchange Organization agent](#) must be able to connect to Exchange Online using HTTPS.

Exchange Online PowerShell Cmdlets

The Exchange Online PowerShell cmdlets must be installed on the machine running the [XIA Configuration Client](#) or [Exchange Online Agent UI](#).

For more information see the [Installing Exchange Online PowerShell Cmdlets](#) section.

Service Principal (Certificate)

When scanning using the [XIA Configuration Client](#) a service principal with certificate authentication must be configured. For more information see the [Service Principal \(Certificate\)](#) section.

Alternatively, the [Exchange Online Agent UI](#) can be used for interactive, multi-factor authentication.

Required Permissions

The service principal or user account used for the connection must have the following permissions.

- Global Reader (in Entra ID)
- Address Lists (to read address lists and global address lists)
- E-Mail Address Policies (to read e-mail address policies)
- Mail Recipients (to read the assigned "send as" permissions)
- View-Only Configuration

Service Principal Setup

Follow these steps to enable the [Microsoft Exchange Organization agent](#) to access [Exchange Online](#) using a service principal.

[Service Principal \(Certificate\)](#)

[Service Principal \(Client Secret\)](#)

Service Principal (Certificate)

Follow these steps to enable the [Microsoft Exchange Organization agent](#) to access [Exchange Online](#) using a service principal with a certificate.

For more information see

<https://learn.microsoft.com/powershell/exchange/app-only-auth-powershell-v2>

- Ensure that a client certificate and private key that supports client authentication is installed on the machine running the [XIA Configuration Client](#) and that the certificate is accessible to the [service account](#).

Issued To	Issued By	Expiration Date	Intended Purposes
 CSolutionsClient.org	MyRootCA	24/05/2031	Client Authentication, Server Authentication

- Export the public key of the client certificate in CER, PEM, or CRT format.
- Logon to the [Azure Portal](#) as a user account with sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Exchange".
- For supported account types select
Accounts in this organizational directory only
- Do not specify a Redirect URI.
- Click Register.
- Go to API Permissions
- Click Add a permission > APIs my organization uses > Office 365 Exchange Online
- Select Application Permissions when prompted
- Select Exchange.ManageAsApp

Select permissions expand all

Exchange.ManageAsApp
×

	Permission	Admin consent required
▼ Exchange (1)		
☒	Exchange.ManageAsApp ⓘ Manage Exchange As Application	Yes

- Click the Add permissions button
- Click the Grant admin consent link

✔ Grant admin consent for CENTREL Solutions
- Go to Certificates & secrets > Certificates.
- Click Upload Certificate.
- Browse for the certificate and provide a description.

* Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

"ClientCert.cer"
📁

Description

XIA Configuration client certificate

- Click the Add button.
- Click Overview > *Application Name* under the "Managed application in local directory" header.

Managed application in local directory
[XIA Configuration Exchange](#)

- Make a note of the **Application ID** and **Object ID**.

Properties

XC

Name ⓘ

XIA Configuration Exchange 

Application ID ⓘ

441c6c13-def5-468d-92cb-... 

Object ID ⓘ

0295b269-877d-4248-8ad3... 

- Goto Microsoft Entra ID > Roles and administrators > Global Reader
- Select Add assignments and search for the service principal that was created - for example "XIA Configuration Exchange" and click Add.

Add assignments

 Try changing or adding filters if you don't see what you're looking for.

Search ⓘ

 XIA Configuration Exchange 

All

Users

Enterprise applications

	Name	Type	Details
	 XIA Configuration Exchange	Enterprise ap...	441c6c13-def5-468d-92cb-efc598352d82

- On a machine with the [Exchange Online PowerShell cmdlets](#) installed open PowerShell and connect to [Exchange Online](#) interactively using appropriate credentials.

Connect-ExchangeOnline

- Execute the following command to create a corresponding Service Principal in [Exchange Online](#) using the **Application ID** and **Object ID** noted above.

```
New-ServicePrincipal -AppId "00000000-0000-0000-0000-000000000000" -ObjectId "00000000-0000-0000-0000-000000000000" -DisplayName "XIA Configuration Exchange"
```

- Execute the following commands to assign the required [management role assignments](#) using the **Application ID** noted above.

```
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "Address  
Lists"  
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "E-Mail  
Address Policies"  
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "Mail  
Recipients"  
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "View-  
Only Configuration"
```

Service Principal (Client Secret)

Follow these steps to enable the [Microsoft Exchange Organization agent](#) to access [Exchange Online](#) using a service principal with client secret.

For more information see <https://learn.microsoft.com/powershell/exchange/app-only-auth-powershell-v2>

- Logon to the [Azure Portal](#) as a user account with sufficient permissions.
- Go to Microsoft Entra ID > App Registrations > New Registration.
- Enter an appropriate name for the application - for example "XIA Configuration Exchange".
- For supported account types select *Accounts in this organizational directory only*
- Do not specify a Redirect URI.
- Click Register.
- Go to API Permissions
- Click Add a permission > APIs my organization uses > Office 365 Exchange Online
- Select Application Permissions when prompted
- Select Exchange.ManageAsApp

Select permissions expand all

Exchange.ManageAsApp

Permission	Admin consent required
Exchange (1)	
☒ Exchange.ManageAsApp ⓘ Manage Exchange As Application	Yes

- Click the Add permissions button
- Click the Grant admin consent link

✓ Grant admin consent for CENTREL Solutions

- Go to Certificates & secrets > Client secrets.
- Click the New Client Secret button.

+ New client secret

- Enter a description and the expiry for the client secret.

Add a client secret



Description

XIA Configuration Exchange Client Secret

Expires

Recommended: 180 days (6 months)



- Click the copy button next to the value for the client secret and make a note of this value. This value is only available at this point.

XIA Configuration Exchange Client Secret

27/03/2024

KmP8Q~Rq1PD.jKDUw3QRxx6LULVbf7s...



- Click Overview > *Application Name* under the "Managed application in local directory" header.

Managed application in local directory

[XIA Configuration Exchange](#)

- Make a note of the **Application ID** and **Object ID**.

Properties

XC

Name ⓘ

XIA Configuration Exchange



Application ID ⓘ

441c6c13-def5-468d-92cb-...



Object ID ⓘ

0295b269-877d-4248-8ad3...



- Goto Microsoft Entra ID > Roles and administrators > Global Reader
- Select Add assignments and search for the service principal that was created - for example "XIA Configuration Exchange" and click Add.

Add assignments

 Try changing or adding filters if you don't see what you're looking for.

Search 

 XIA Configuration Exchange 

All Users Enterprise applications

	Name	Type	Details
 	XIA Configuration Exchange	Enterprise ap...	441c6c13-def5-468d-92cb-efc598352d82

- On a machine with the [Exchange Online PowerShell cmdlets](#) installed open PowerShell and connect to [Exchange Online](#) interactively using appropriate credentials.

Connect-ExchangeOnline

- Execute the following command to create a corresponding Service Principal in [Exchange Online](#) using the **Application ID** and **Object ID** noted above.

```
New-ServicePrincipal -AppId "00000000-0000-0000-0000-000000000000" -ObjectId "00000000-0000-0000-0000-000000000000" -DisplayName "XIA Configuration Exchange"
```

- Execute the following commands to assign the required [management role assignments](#) using the **Application ID** noted above.

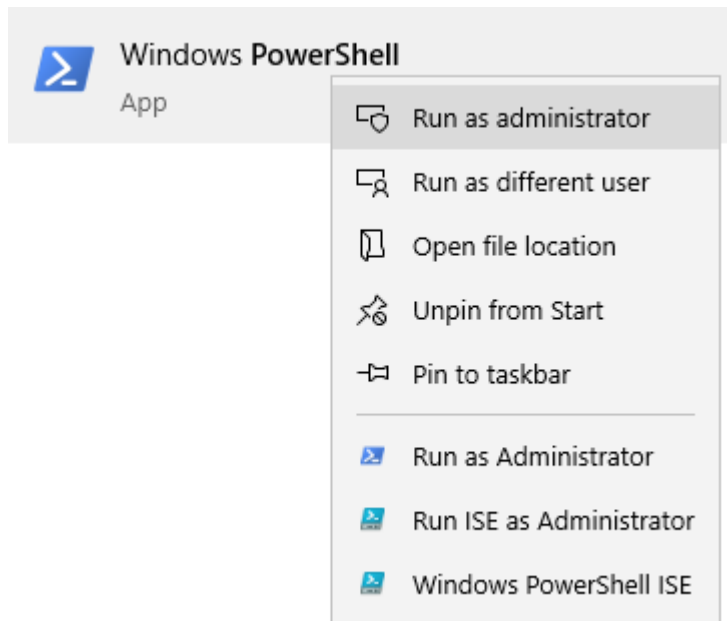
```
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "Address Lists"
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "E-Mail Address Policies"
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "Mail Recipients"
New-ManagementRoleAssignment -App "00000000-0000-0000-0000-000000000000" -Role "View-Only Configuration"
```

Installing Exchange Online PowerShell Cmdlets

The [Exchange Online PowerShell cmdlets](#) must be installed onto the computer running the [XIA Configuration Client](#).

NOTE: The tools can be automatically installed using the [Install Exchange Online PowerShell Cmdlets](#) option on the [tools menu](#) of the [Exchange Online Agent UI](#).

- Start [Windows PowerShell](#) as an Administrator



- Set the remote execution policy with the [Set-ExecutionPolicy](#) cmdlet.
`Set-ExecutionPolicy RemoteSigned -Force;`
- Install the latest NuGet package provider using the [Install-PackageProvider](#) cmdlet.
`Install-PackageProvider -Name NuGet -Force;`
- Allow the PowerShell gallery repository to be trusted with the [Set-PSRepository](#) cmdlet.
`Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted;`
- Install the latest PowerShellGet module using the [Install-Module](#) cmdlet.
`Install-Module -Name PowerShellGet -Force;`
- Install the [Exchange Online PowerShell cmdlets](#) using the [Install-Module](#) cmdlet.
`Install-Module -Name ExchangeOnline -Force -AllowClobber;`

NOTE: If you see the following error "WARNING: Unable to download the list of available providers. Check your internet connection" please review [this section](#).

Exchange On-Premises Requirements

Windows Firewall Requirements

- The [Microsoft Exchange organization agent](#) must be able to connect to the Exchange organization using Exchange PowerShell over HTTP or HTTPS.
- To obtain [optional](#) host information such as manufacturer and serial number, the [service account](#) or [custom credentials](#) must have access to connect to each host using [PowerShell remoting](#), by default this is TCP/5985.

Access Settings

- The [service account](#) or [custom credentials](#) must have the [View-Only Organization Management](#) or greater [admin role](#) to the Exchange organization.
- **NOTE:** Microsoft Exchange Server does not support [managed service accounts](#).
- To obtain [optional](#) host information such as manufacturer and serial number, the [service account](#) or [custom credentials](#) must have permissions to connect to each host using [PowerShell remoting](#).

Managed Service Provider Exchange Online Best Practice

Managed service providers (MSPs) typically have a single [XIA Configuration Server](#) installation and one or more [XIA Configuration Client](#) installations in each customer environment.

This allows a single managed repository of technical information whilst allowing the [XIA Configuration Client](#) to be installed behind each customer's firewall and configured with credentials appropriate for the customer environment.

As a cloud based solution the [Exchange Online scan tasks](#) can either be executed by the [XIA Configuration Client](#) installed in each customer environment, or directly from the MSP environment. The following compares the two options.

Customer Environment

- The [Exchange Online scan task](#) must be configured for the [XIA Configuration Client](#) in each customer environment.
- The customer retains control of their [connection credentials](#), and these [credentials](#) must be updated in each customer environment when they are changed.
- [Item creation rules](#) are used when data is sent to the [XIA Configuration Server](#).

Managed Service Provider Environment

- An [Exchange Online scan task](#) must be configured for each customer with the appropriate [connection credentials](#) within the [XIA Configuration Client](#) within the managed service provider's environment.

 Scan Tasks Configures the tasks that will be performed by this scan profile. Start Scan Profile			
Display Name	Status	Type	
 Customer 1	Enabled	Exchange Online	
 Customer 2	Enabled	Exchange Online	
 Customer 3	Enabled	Exchange Online	

- The managed service provider retains control of all connection credentials.
- As the same [XIA Configuration Client](#) is used for all scans, [item creation rules](#) created for the customer are not used when data is sent to the [XIA Configuration Server](#). Therefore the managed service provider must move the [Microsoft Exchange Organization](#) item to the appropriate [container](#) or [customer](#) when it is created.

Troubleshooting

This section highlights the known issues for the [Microsoft Exchange agent](#), and provides details of the solutions.

Could not connect to any Exchange server

Symptoms

When you scan an [Exchange On-Premises organization](#) you see the following error
Error when 'Connecting to Exchange On-Premises'. Could not connect to any Exchange server in the organization.

Cause

By default the [Exchange organization agent](#) will automatically detect and connect to Exchange servers in order of version, with newer versions first.

Resolution

Review the [scan result details](#), and check the [warnings](#) tab for information relating to connection failures for each Exchange server.

Error executing PowerShell command 'Connect-ExchangeOnline'. Unauthorized

Symptoms

When you scan an [Exchange Online](#) organization using the [Microsoft Exchange Organization agent](#), you see the following error

Error executing PowerShell command 'Connect-ExchangeOnline'. Unauthorized

Cause

This can occur when the service principal has not been configured correctly in [Exchange Online](#).

Resolution

Follow the steps in the [Service Principal \(Certificate\)](#) section.

Error when reading add-ins. {Account name} isn't a mailbox user

Symptoms

When you scan an [Exchange On-Premises organization](#) you see the following error
Error when 'Reading add-ins'. Error executing the command 'Get-App'. The specified mailbox "*mailbox name*" doesn't exist. Reason: *mailbox name* isn't a mailbox user.

Cause

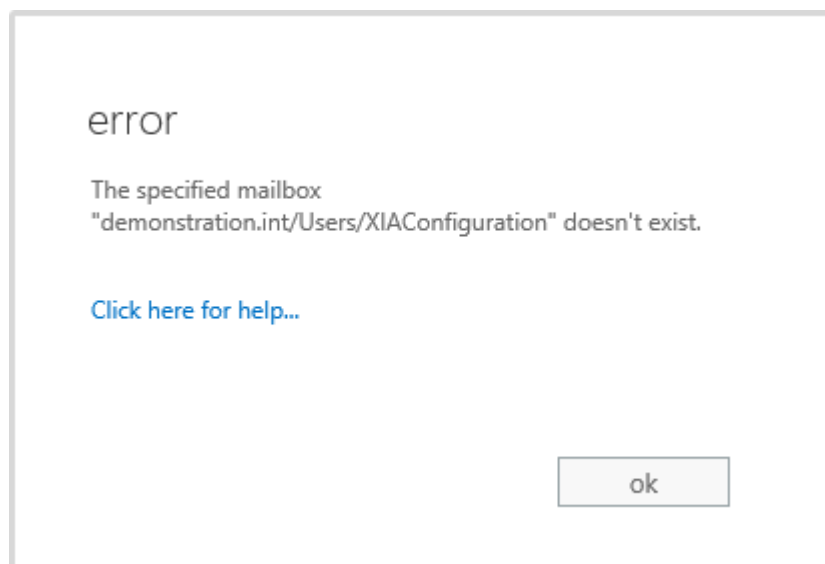
The account performing the scan must be associated with an Exchange mailbox in order to execute the [Get-App](#) cmdlet.

Resolution

Ensure that the [service account](#) (or [custom credentials](#) if in use), has an associated Exchange mailbox.

More Information

The error can be replicated within the Exchange Admin Center.



Kerberos authentication cannot be used

Symptoms

When you scan an [Exchange On-Premises organization](#) you see the following error

The Exchange PowerShell connection is configured to use Kerberos authentication; however, this machine is a member of a workgroup. Please provide the custom credentials in the Exchange On-Premises scan task.

Cause

Implicit Kerberos authentication cannot be used when the computer running the XIA Configuration Client machine is on a workgroup, rather than being domain joined. This is common when using the [technician license](#) and the computer running the [XIA Configuration Client](#) is separate from the environment being scanned.

Resolution

Manually configure the [credentials](#) for the [Exchange on-premises scan task](#).

The local computer is not joined to a domain

Symptoms

When you scan a [Microsoft Exchange organization](#), and the computer running the [XIA Configuration Client](#) is on a workgroup you see the following error

Error when 'Detecting Exchange servers'. The local computer is not joined to a domain or the domain cannot be contacted.

Cause

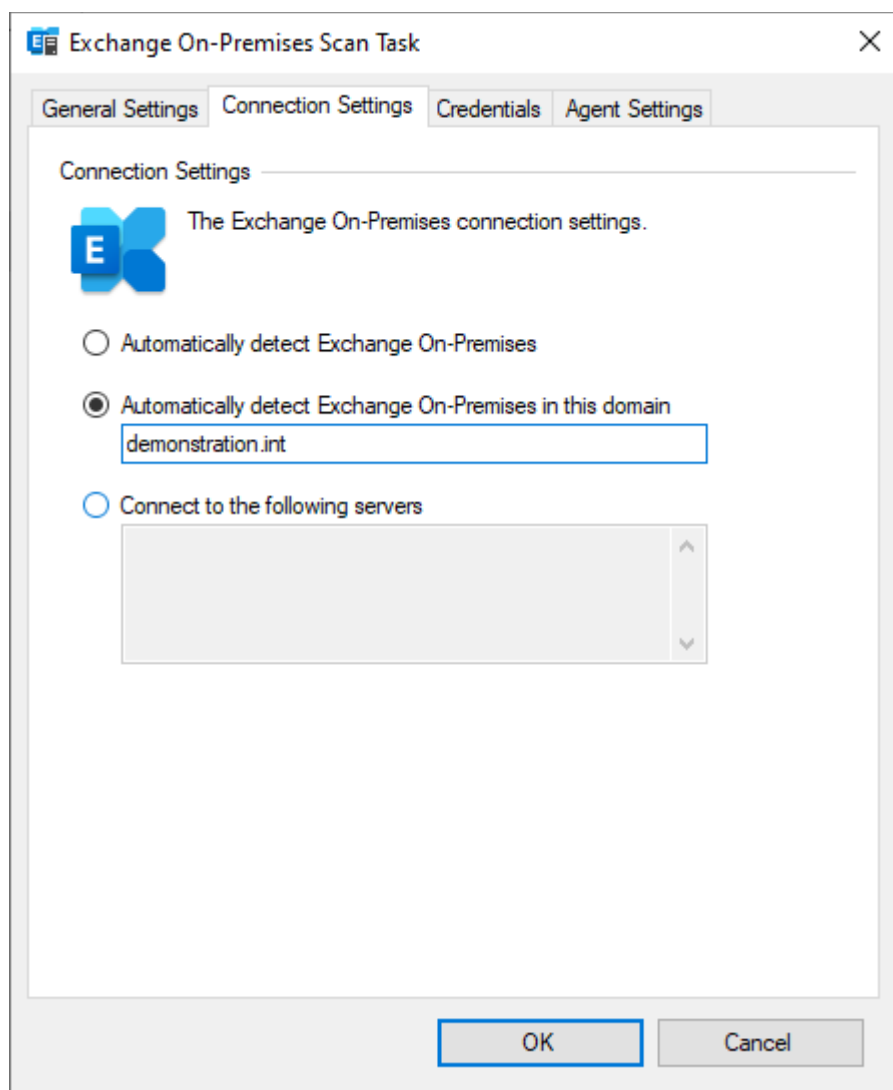
This behaviour is by design, by default the system will automatically connect to the domain that the computer running the [XIA Configuration Client](#) is a member of.

More Information

This is common when using the [technician license](#) and the computer running the [XIA Configuration Client](#) is separate from the environment being scanned.

Resolution

Configure the [connection settings](#), select the *automatically detect Exchange On-Premises in this domain* option, and enter the name of the domain or forest in which to search for Exchange servers.



The operation couldn't be performed because 'account name\$' couldn't be found

Symptoms

When you scan an [Exchange On-Premises organization](#) you see the following error
The operation couldn't be performed because '*domain\account\$*' couldn't be found.

Cause

The error can occur when using a [managed service account](#) to scan the [Exchange On-Premises organization](#) as [managed service accounts](#) are not supported by [Microsoft](#) for use with [Exchange On-Premises](#).

Resolution

Use alternative [credentials](#) to scan the [Exchange On-Premises organization](#).

The term is not recognized as the name of a cmdlet

Symptoms

When you scan a [Microsoft Exchange organization](#), you see the following error

The term '*cmdlet name*' is not recognized as the name of a cmdlet, function, script file, or operable program.

Cause

The account performing the scan does not have the appropriate permissions.

More Information

When connecting to Microsoft Exchange using PowerShell remoting only the cmdlets to which you have permission are made available.

Resolution

Ensure that the [service account](#) (or [custom credentials](#) if in use), has the permissions described in the [requirements](#) section.

The user isn't assigned to any management roles

Symptoms

When you scan an [Exchange Online](#) organization using the [Microsoft Exchange Organization agent](#), you see the following error

Error executing PowerShell command 'Connect-ExchangeOnline'. The user "userid" isn't assigned to any management roles.

Cause

This can occur when the service principal has not been configured correctly in [Exchange Online](#) and has not been assigned any management roles.

Resolution

Follow the steps in the [Service Principal \(Certificate\)](#) section.

Your account isn't enabled for Remote PowerShell

Symptoms

When you scan an [Exchange On-Premises organization](#) using the [Microsoft Exchange Organization agent](#), you see the error "Could not connect to any Exchange server" and the following warnings are seen.

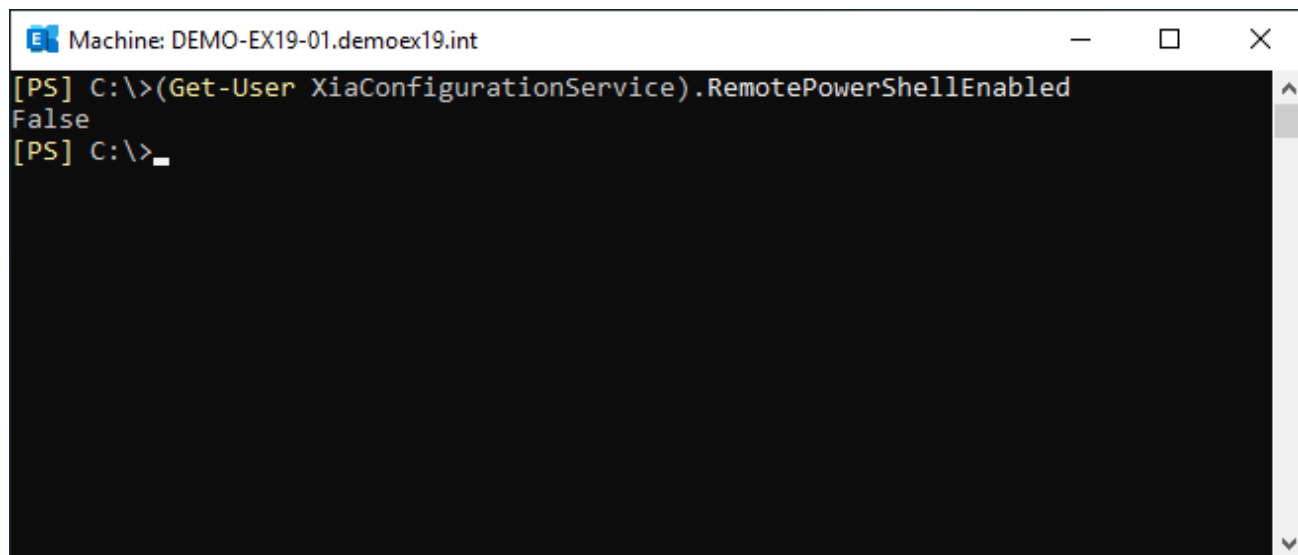
Your attempt to connect to this Exchange server was denied because your account isn't enabled for Remote PowerShell.

Cause

This can occur when the [service account](#) does not have the "RemotePowerShellEnabled" setting enabled.

To validate this open the [Exchange Management Shell](#) and run the [Get-User cmdlet](#) replacing the [service account](#) name as required.

`(Get-User XiaConfigurationService).RemotePowerShellEnabled`

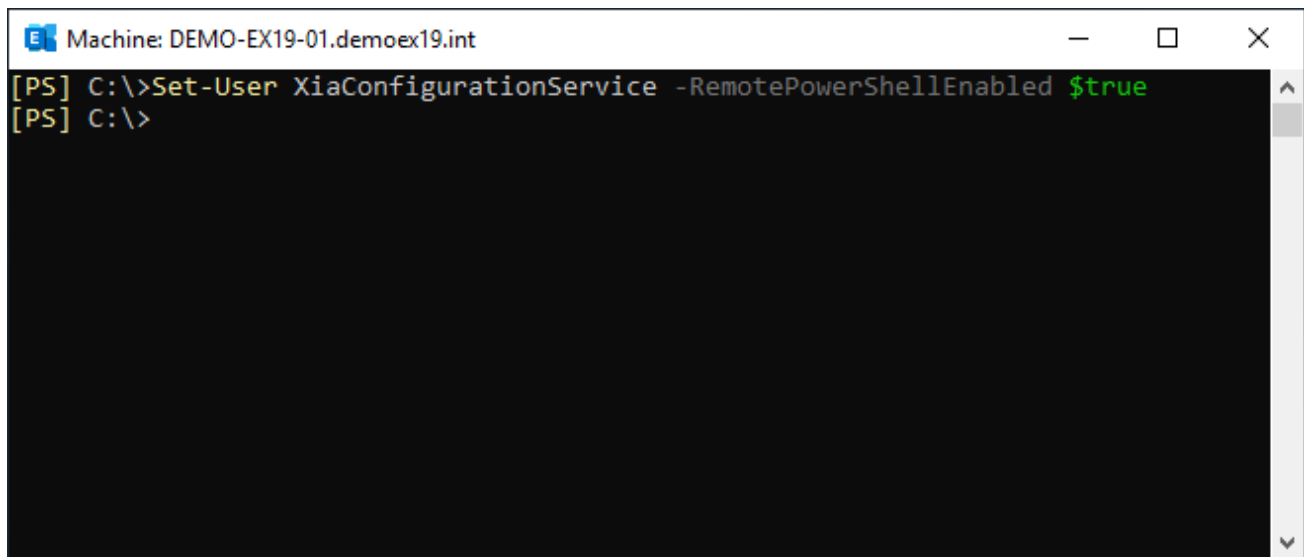


```
Machine: DEMO-EX19-01.demoex19.int
[PS] C:\>(Get-User XiaConfigurationService).RemotePowerShellEnabled
False
[PS] C:\>_
```

Resolution

To set the "RemotePowerShellEnabled" setting open the [Exchange Management Shell](#) and use the [Set-User cmdlet](#) replacing the [service account](#) name as required.

`Set-User XiaConfigurationService -RemotePowerShellEnabled $true`



A screenshot of a PowerShell terminal window. The title bar at the top reads "Machine: DEMO-EX19-01.demoex19.int" and includes standard window controls (minimize, maximize, close). The terminal content shows two lines of text: the first line is a PowerShell command "[PS] C:\>Set-User XiaConfigurationService -RemotePowerShellEnabled \$true" where "\$true" is highlighted in green; the second line is the prompt "[PS] C:\>". A vertical scrollbar is visible on the right side of the terminal area.

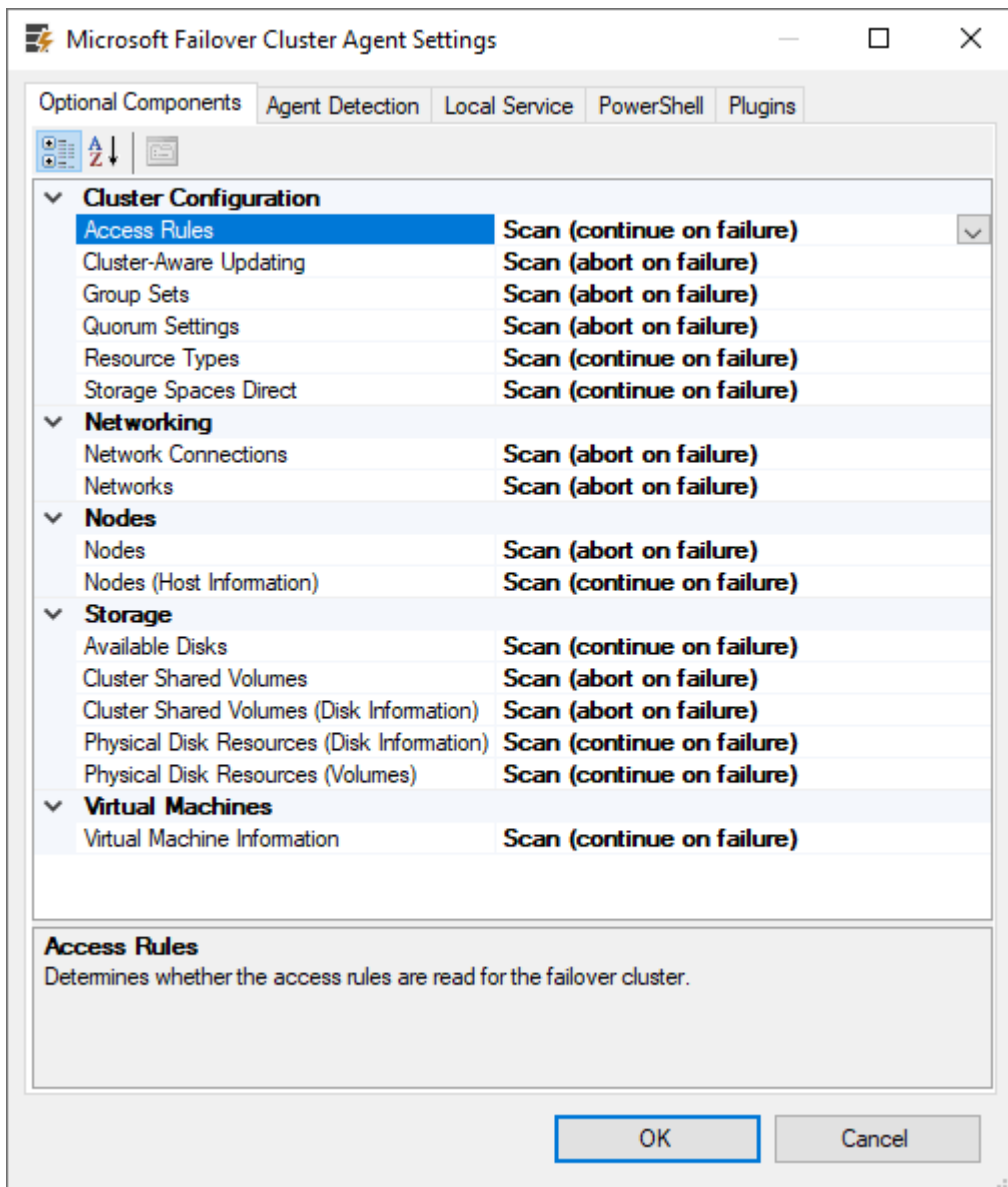
```
[PS] C:\>Set-User XiaConfigurationService -RemotePowerShellEnabled $true
[PS] C:\>
```

Microsoft Failover Cluster

The Microsoft failover cluster [scan tasks](#) are able to document the [Microsoft failover clusters](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).

The data located by these [scan tasks](#) include cluster configuration, quorum, roles, and storage.

Agent Settings



Cluster Configuration > Access Rules

Determines whether the access rules are read for the failover cluster.

Cluster Configuration > Cluster-Aware Updating

Determines whether the cluster-aware updating settings are read for the failover cluster.

Cluster Configuration > Group Sets

Determines whether the group sets are read for the failover cluster. This only applies to Windows Server 2016 and above.

Cluster Configuration > Quorum Settings

Determines whether the quorum settings are read for the failover cluster.

Cluster Configuration > Resource Types

Determines whether the resource types are read for the failover cluster.

Cluster Configuration > Storage Spaces Direct

Determines whether the Storage Spaces Direct configuration is read for the failover cluster. This only applies to Azure Local (Azure Stack HCI), Windows Server 2016 Datacenter Edition and above.

Networking > Network Interfaces

Determines whether the network interfaces are read for the Microsoft failover cluster.

Networking > Networks

Determines whether the networks are read for the Microsoft failover cluster.

Nodes > Nodes

Determines whether the nodes are read for the Microsoft failover cluster.

Nodes > Nodes (Host Information)

Determines whether the host information is read for nodes in the failover cluster.

Storage > Available Disks

Determines whether the available disks are read for the failover cluster.

Storage > Cluster Shared Volumes

Determines whether the cluster shared volumes are read for the failover cluster.

Storage > Cluster Shared Volumes (Disk Information)

Determines whether disk information is read for the cluster shared volumes.

Storage > Physical Disk Resources (Disk Information)

Determines whether disk information is read for physical disk resources.

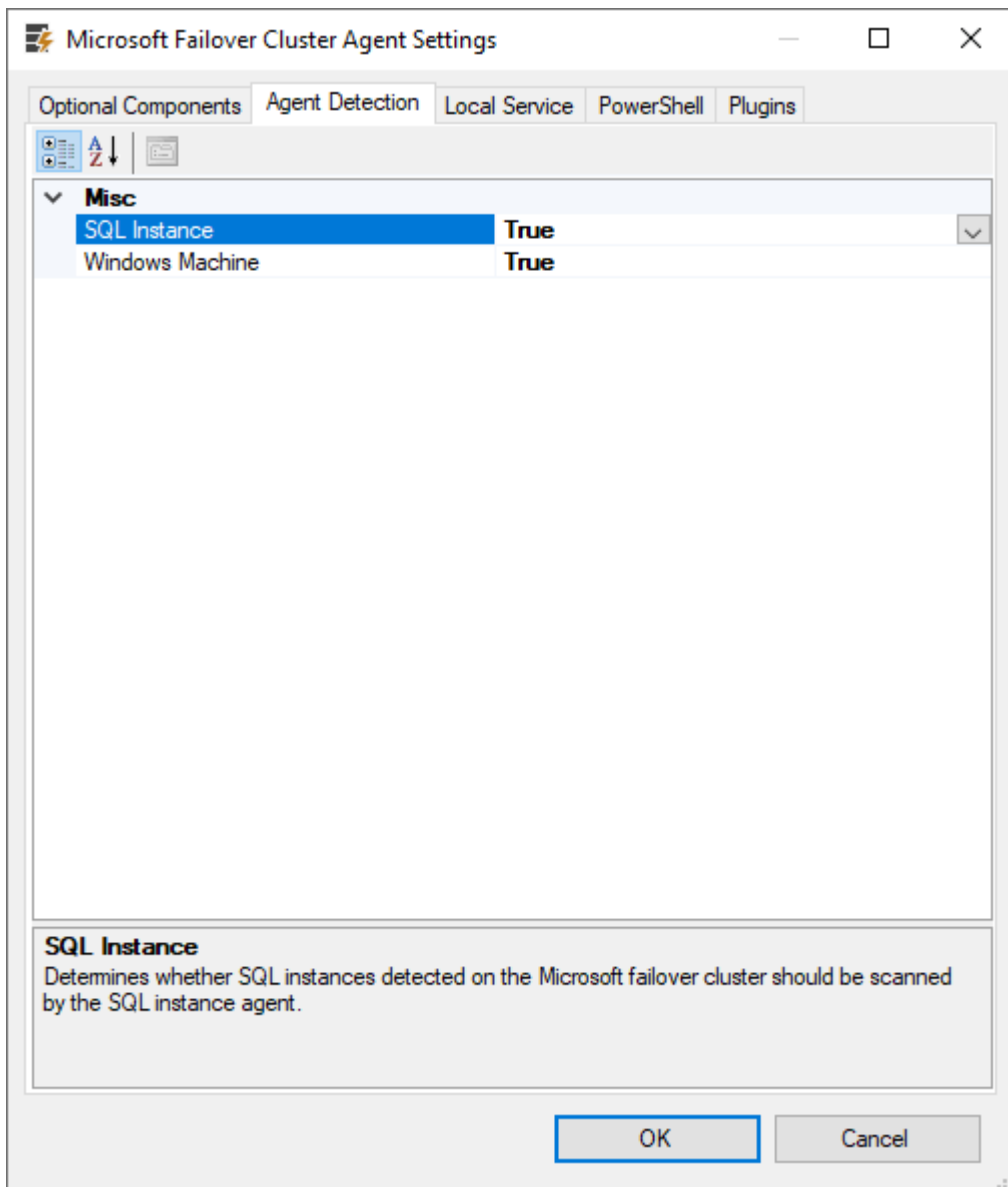
Storage > Physical Disk Resources (Volumes)

Determines whether volumes information is read for physical disk resources.

Virtual Machines > Virtual Machine Information

Determines whether additional information is read for the virtual machines in the failover cluster.

Agent Detection



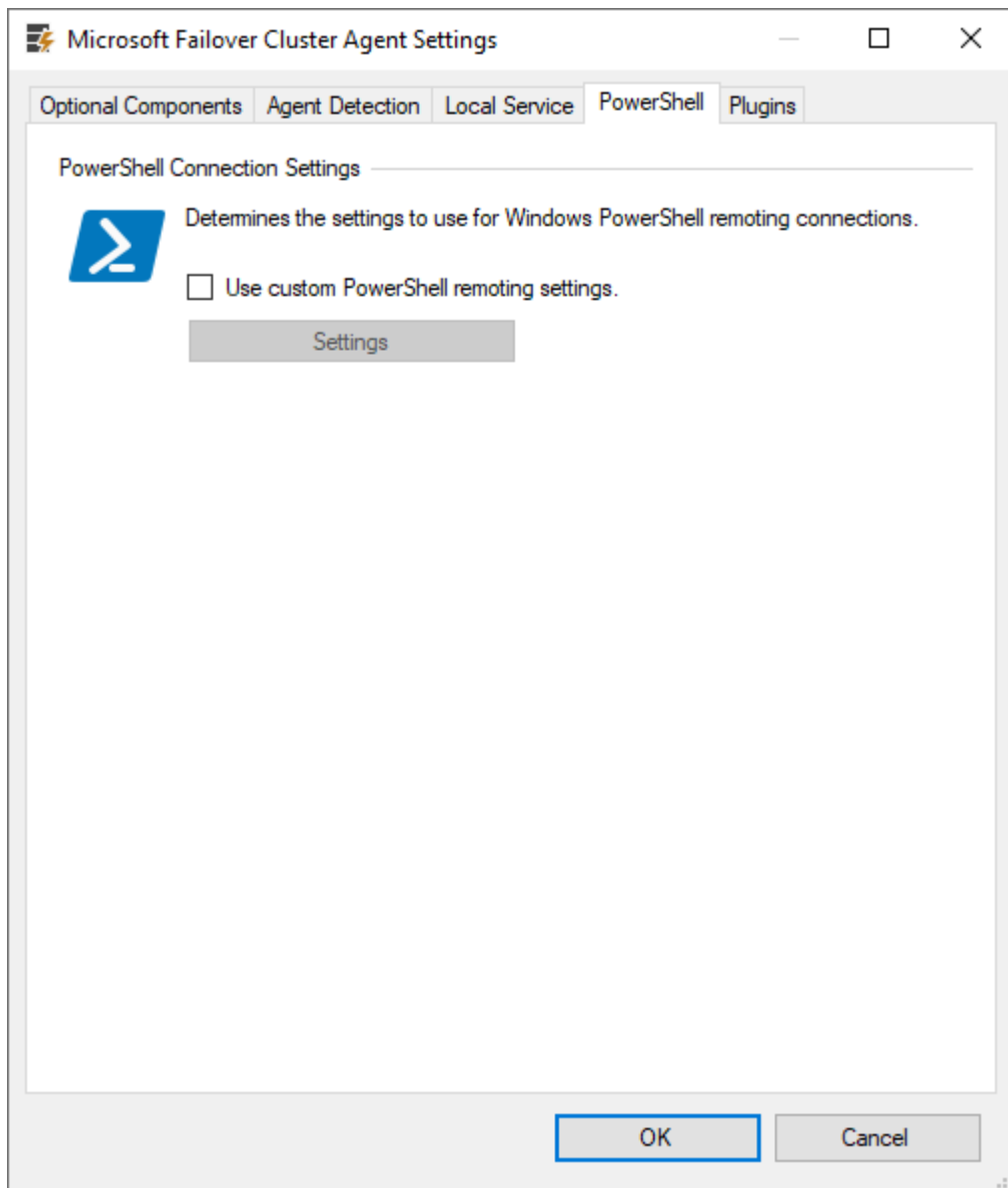
SQL Instance

Determines whether to automatically launch a [SQL instance scan](#) against all SQL instances running on the cluster.

Windows Machine

Determines whether to automatically launch a [Windows machine scan](#) against all nodes of the Microsoft cluster.

PowerShell



Use custom PowerShell remoting settings

Determines whether to use custom [PowerShell connection settings](#).

Item Identifiers

For more information please see the [item identifiers](#) section.

Primary Identifier

The cluster name.

Secondary Identifier

The [Active Directory domain](#) name if the cluster is a member of a domain.

Tertiary Identifier

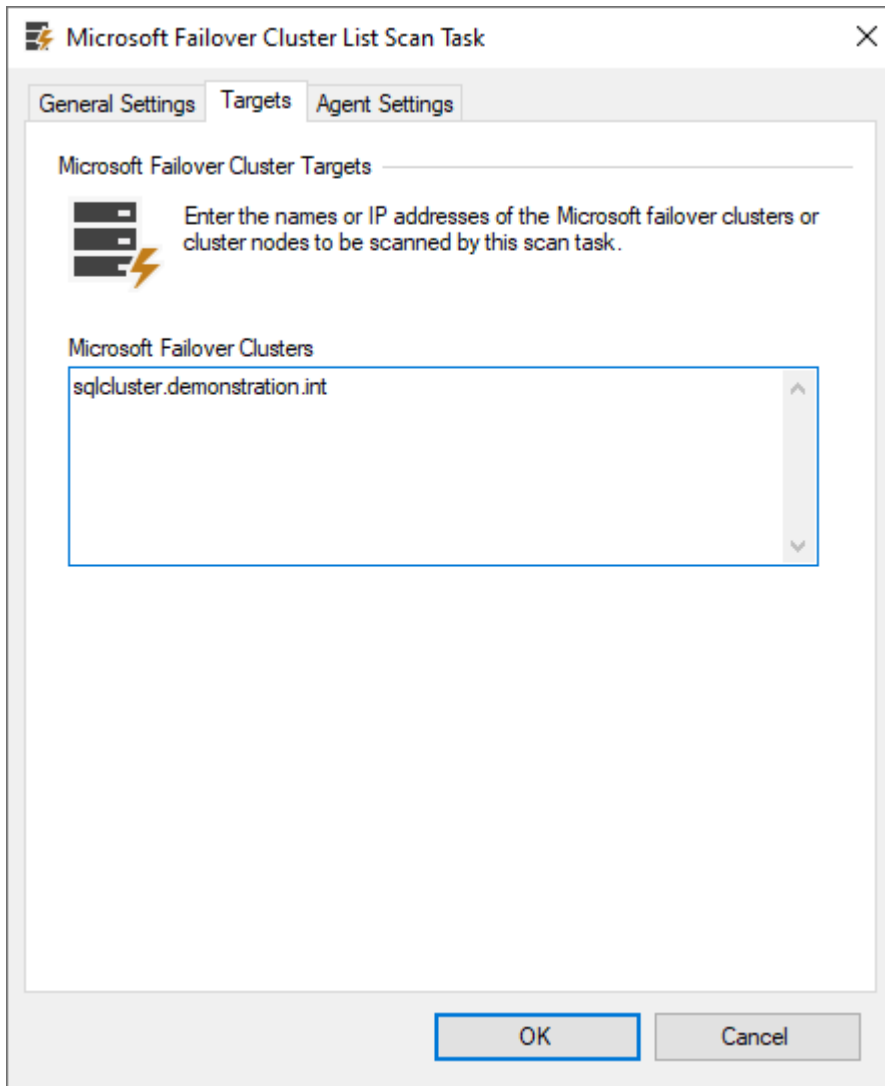
Not used

Microsoft Failover Cluster List Scan Task

The Microsoft failover cluster list scan task allows you to enter a list of names or IP address of the [Microsoft failover clusters](#) to scan. The names or IP address of a specific node can also be used.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Microsoft failover clusters](#) running on [Windows machines](#).

Targets



The screenshot shows a dialog box titled "Microsoft Failover Cluster List Scan Task" with a close button (X) in the top right corner. The dialog has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the "Targets" tab, there is a section titled "Microsoft Failover Cluster Targets" with a sub-header "Microsoft Failover Clusters". Below this, there is a text area containing the text "sqlcluster.demonstration.int". To the left of the text area is an icon representing a server rack with a lightning bolt. Below the text area are "OK" and "Cancel" buttons.

Microsoft Failover Cluster List Scan Task

General Settings Targets Agent Settings

Microsoft Failover Cluster Targets

Enter the names or IP addresses of the Microsoft failover clusters or cluster nodes to be scanned by this scan task.

Microsoft Failover Clusters

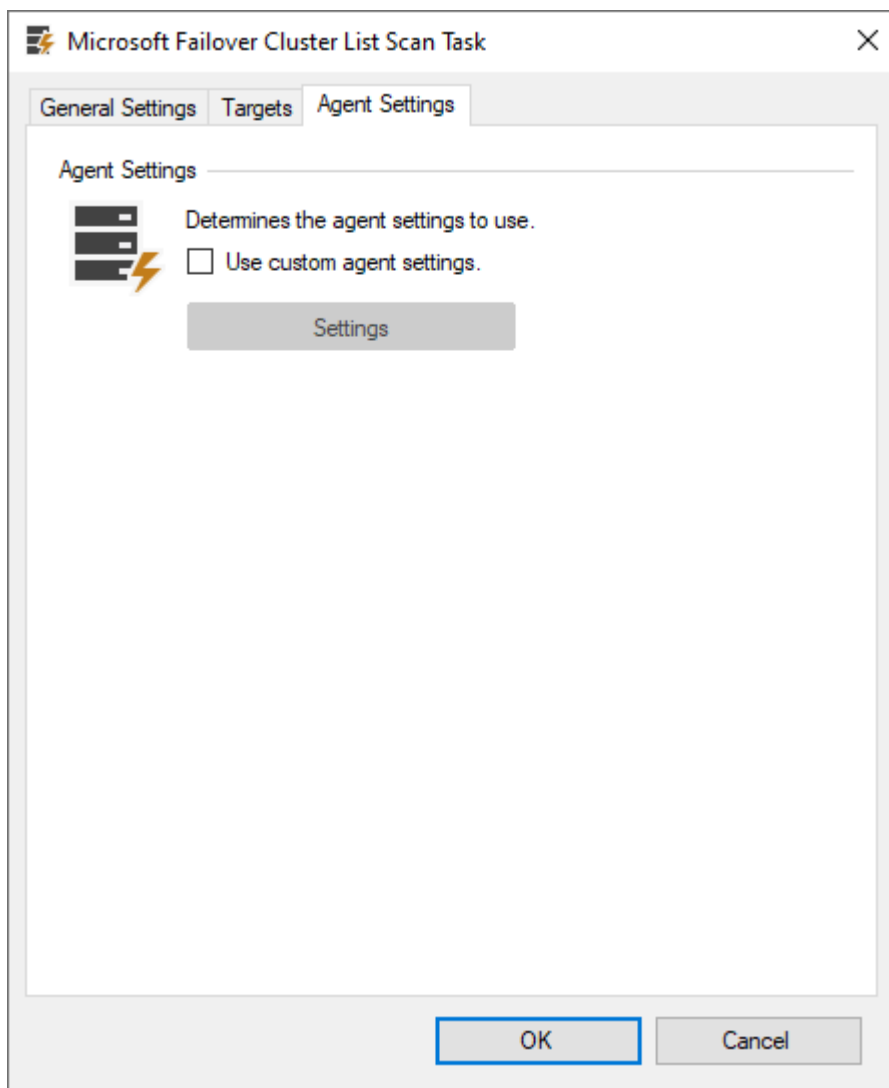
sqlcluster.demonstration.int

OK Cancel

Microsoft Failover Clusters

The IP addresses, NetBIOS names, or fully qualified domain names of the [Microsoft failover clusters](#) or cluster nodes to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The Microsoft failover cluster scan tasks are supported on the following operating systems:

- Azure Local (Azure Stack HCI)
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Access Settings

The [Microsoft failover cluster scan tasks](#) use [PowerShell remoting](#) to obtain information remotely from [Microsoft failover clusters](#).

- Firewall access must allow access to the [PowerShell remoting](#) ports on the remote machine
- The [XIA Configuration client service account](#) or [custom credentials](#) must have administrator rights on the remote machine.

Windows Firewall

When using [Windows Firewall with Advanced Security](#) the following rules must be enabled.

- ✔ Windows Remote Management (HTTP-In)

Local Service

- 📌 The [Microsoft failover cluster scan tasks](#) support the [local service](#).

Automatic Detection

- ✔ [Microsoft failover clusters](#) can be automatically detected and scanned by [Windows machine scan tasks](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Microsoft Network Load Balancing Cluster

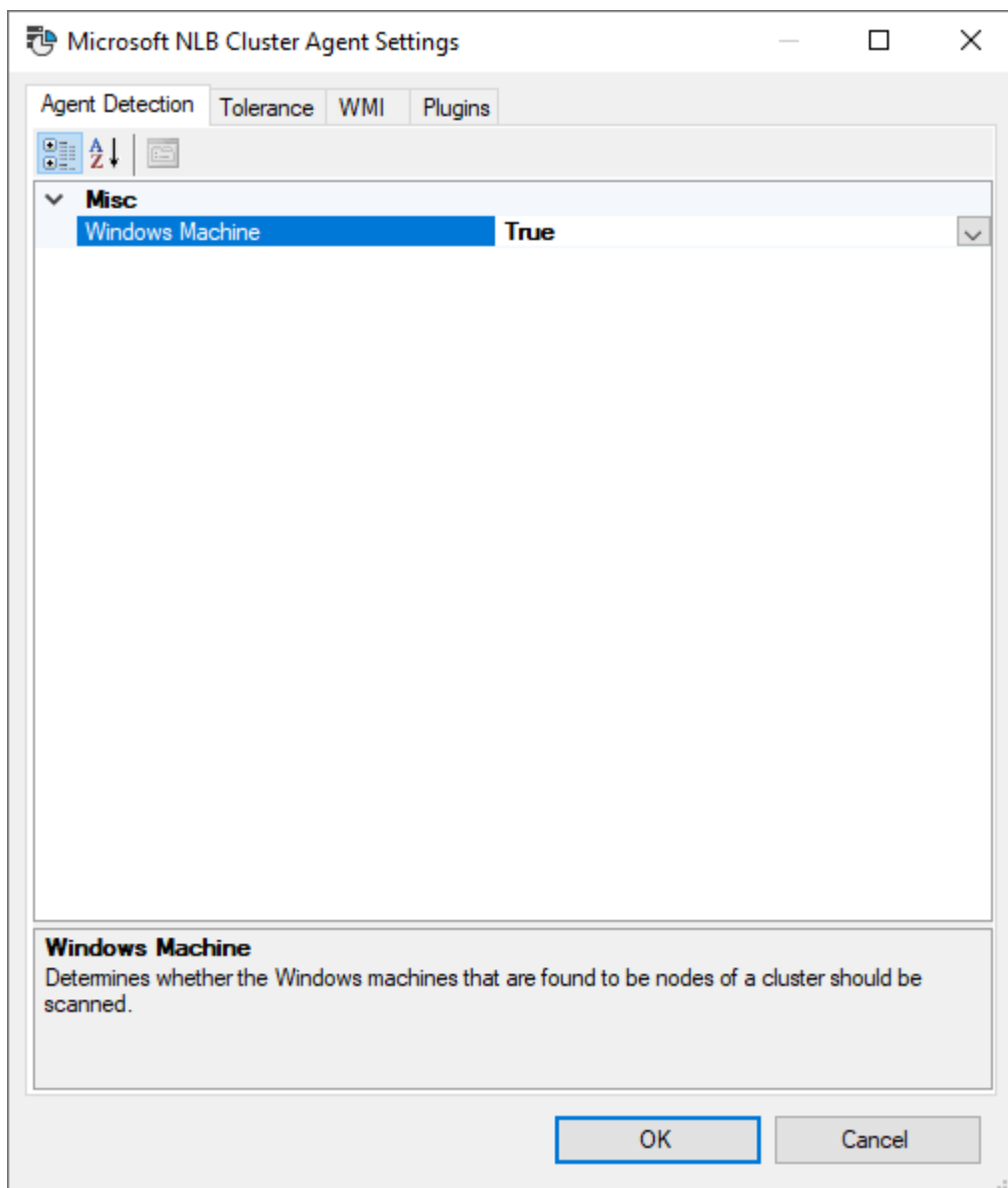
Microsoft [network load balancing](#) (NLB) increases the availability and scalability of Internet server applications such as web, FTP, firewall and proxy.

For information about Microsoft failover clustering support see the [Microsoft failover cluster](#) section.

Microsoft network load balancing cluster scan tasks are able to document NLB clusters running on Windows Server 2003 and above and provide the following information.

- Cluster name
- Cluster network addresses
- Cluster operation mode
- Host name
- Host operating system, model, serial number and manufacturer
- Host priority
- Host network addresses
- Host initial state
- Port rules

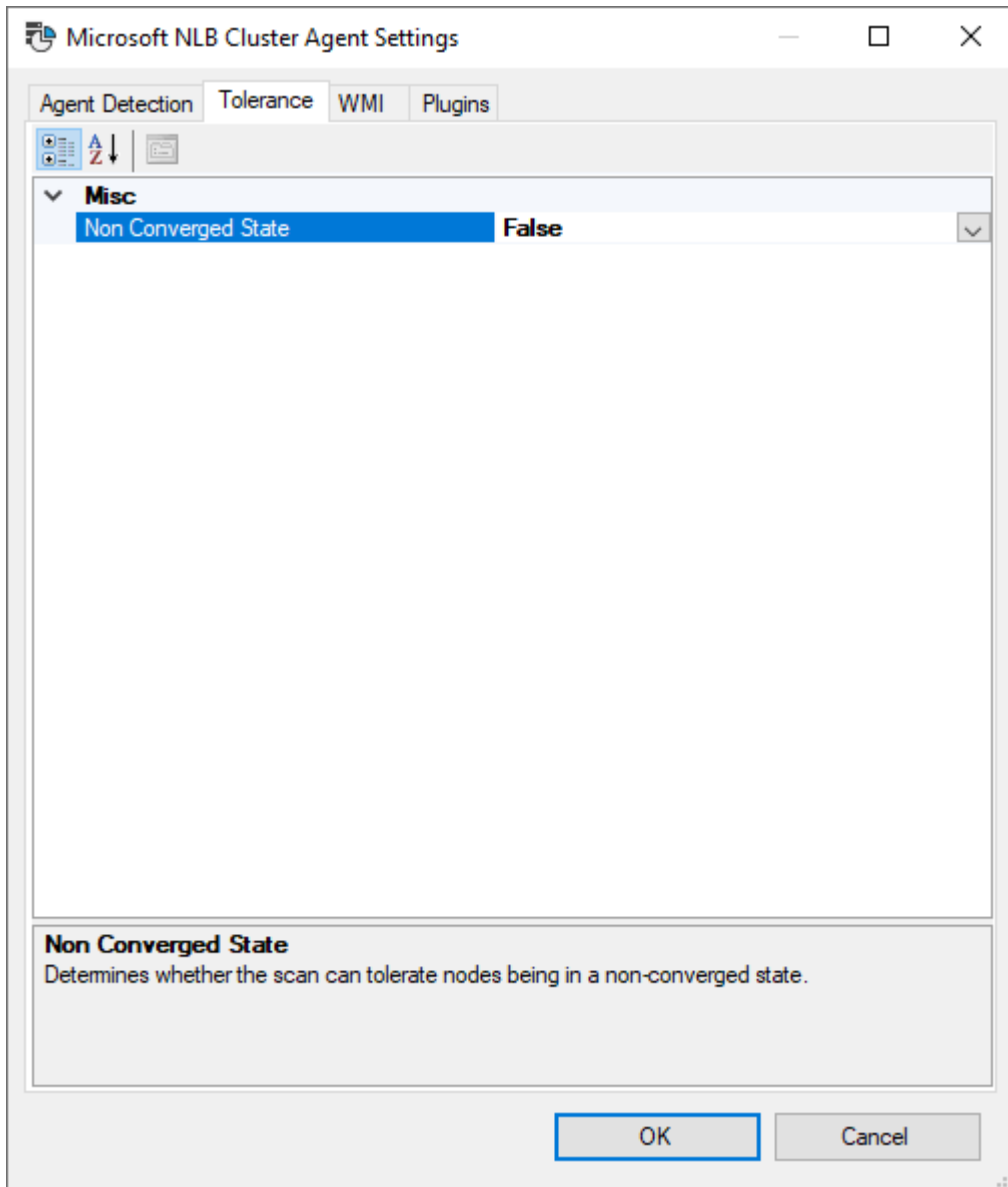
Agent Settings



Windows Machine

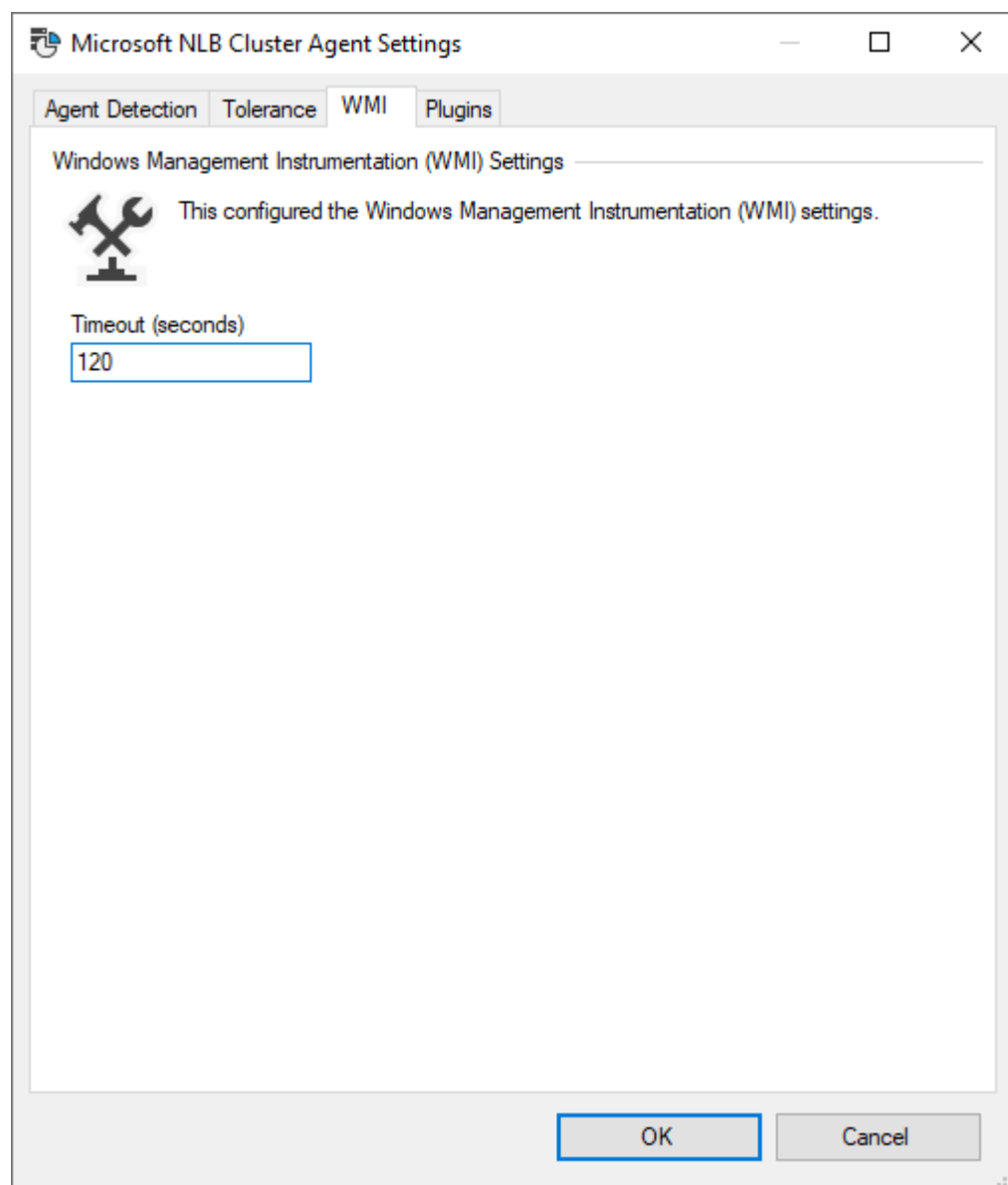
Determines whether to automatically launch a Windows machine scan agent against all nodes of the [Microsoft network load balancing cluster](#). By default, this is true.

Tolerance



Non Converged State

Determines whether the scan should tolerate and proceed if any of the nodes in the cluster is found to be in a non-converged state. Enabling this option may lead to inconsistent or incomplete information being reported by the [network load balancing cluster](#).

**WMI Timeout**

The timeout in seconds to use for WMI connections.

Item Identifiers

For more information about item identifiers please see the [Item Identifiers](#) section.

Primary Identifier

The cluster name.

Secondary Identifier

Not used.

Tertiary Identifier

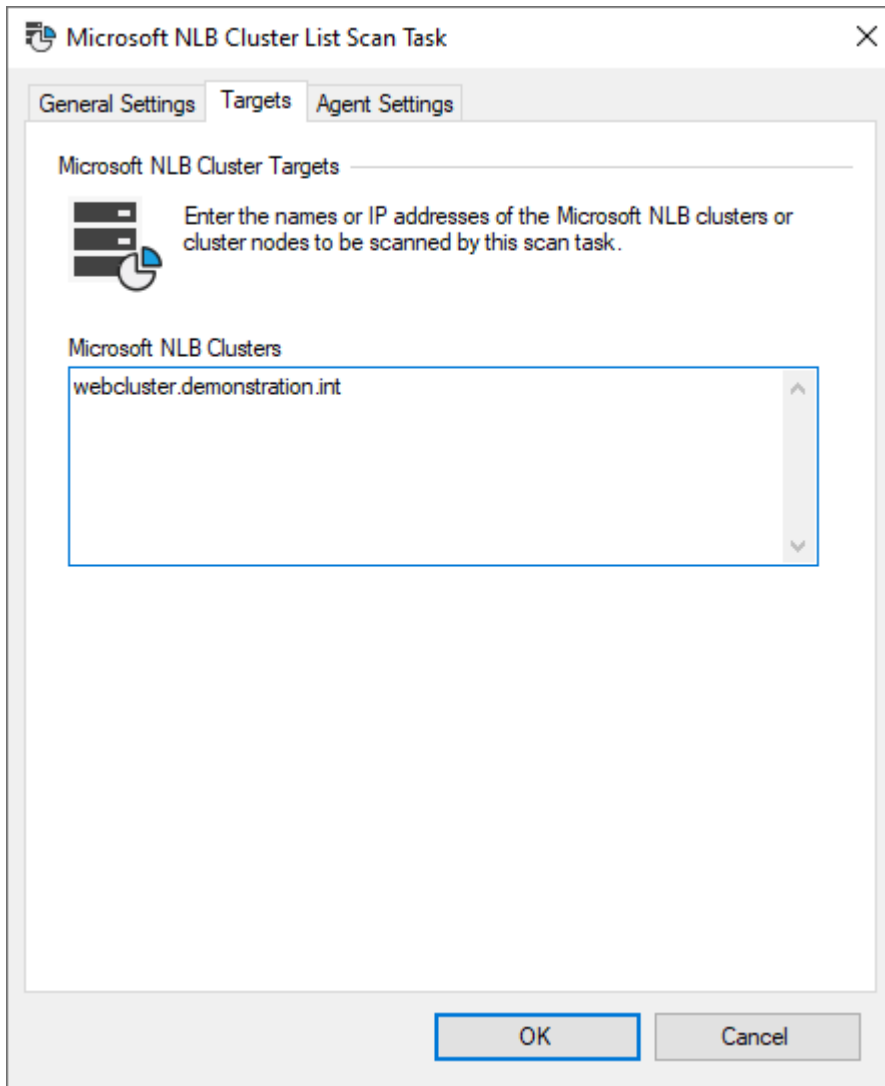
Not used.

Microsoft Network Load Balancing Cluster List Scan Task

The Microsoft network load balancing cluster list task allows you to enter a list of Microsoft network load balancing (NLB) cluster or node names that you wish to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [Microsoft network load balancing clusters](#).

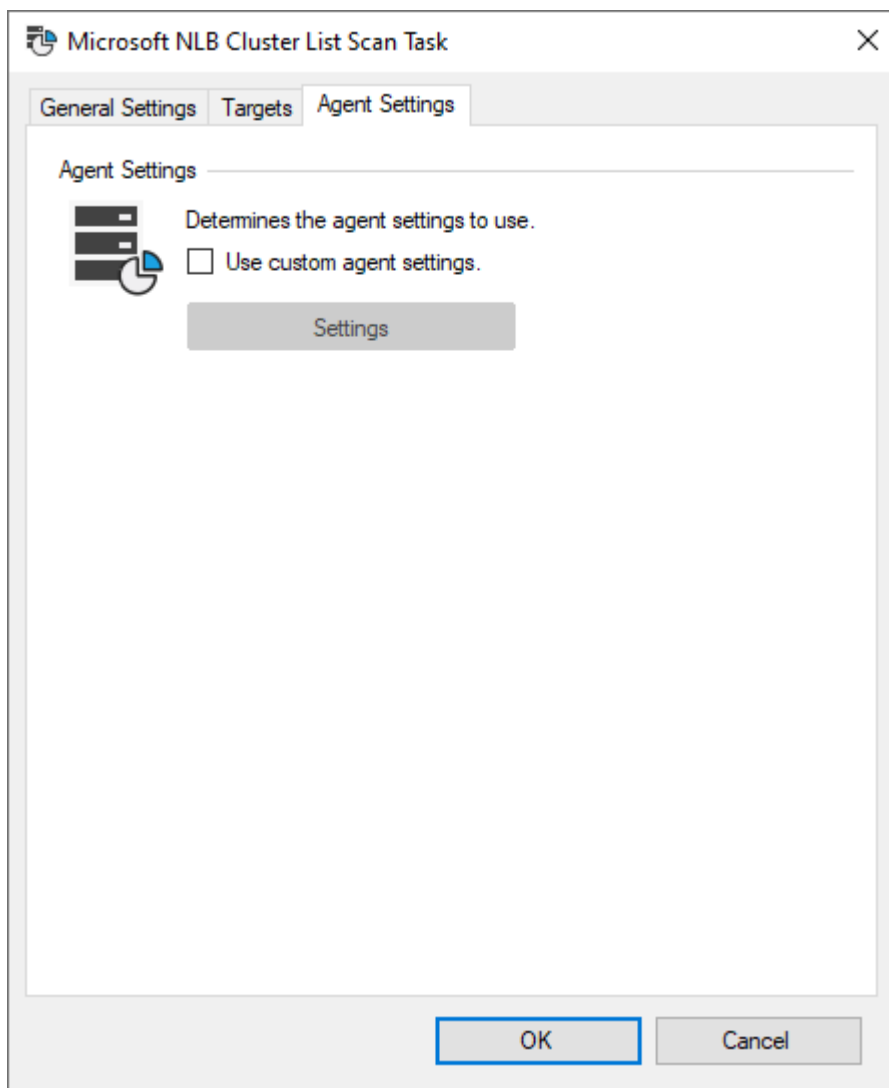
Targets



Microsoft Failover Clusters

The IP addresses, NetBIOS names, or fully qualified domain names of the [Microsoft network load balancing clusters](#) or cluster nodes to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Requirements

Supported Target Systems

The Microsoft network load balancing cluster scan tasks are supported on the following operating systems

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 2008 R2
- Windows 2008
- Windows 2003

Access Settings

The scan tasks use WMI to obtain information remotely from Microsoft network load balancing clusters.

- Firewall access must allow access to the WMI ports on **each** node in the cluster.
- The computer running the [XIA Configuration Client](#) must be able to resolve the fully qualified domain name of the network load balancing cluster.
- By default, the XIA Configuration client service account must have administrator rights on the remote machine (*this is a requirement for remote WMI access enforced by the operating system*)

Windows Firewall

When using Windows Firewall with Advanced Security the following rules must be enabled.

- ✔ Windows Management Instrumentation (WMI-In)
This port allows the WMI queries directly.

Local Service

- ⚠ The Microsoft [network load balancing cluster](#) scan tasks do not support the [XIA Local Service](#).

Automatic Detection

- ✔ Cluster nodes can be automatically detected and scanned by [Windows Machine Scan Tasks](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Ensure remote control is enabled for the cluster

Symptoms

When you scan a [Microsoft Network Load Balancing Cluster](#) running on Windows 2003 you receive the error

"No clusters were found, for Windows 2003 server you must ensure that remote control is enabled for the cluster."

Cause

For **Windows 2003 only (later versions do not require this change)** the remote control settings must be enabled for the cluster to enable information about the cluster to be presented to WMI. <https://msdn.microsoft.com/en-us/library/aa371001%28v=vs.85%29.aspx>

Resolution

Review the security requirements of enabling remote control for a [Microsoft Network Load Balancing Cluster](#) within the Microsoft documentation before proceeding.

- Tick the "Allow remote control" checkbox
- Enter the remote password
- Confirm the password
- Click OK
- Wait for cluster convergence
- Run the scan again

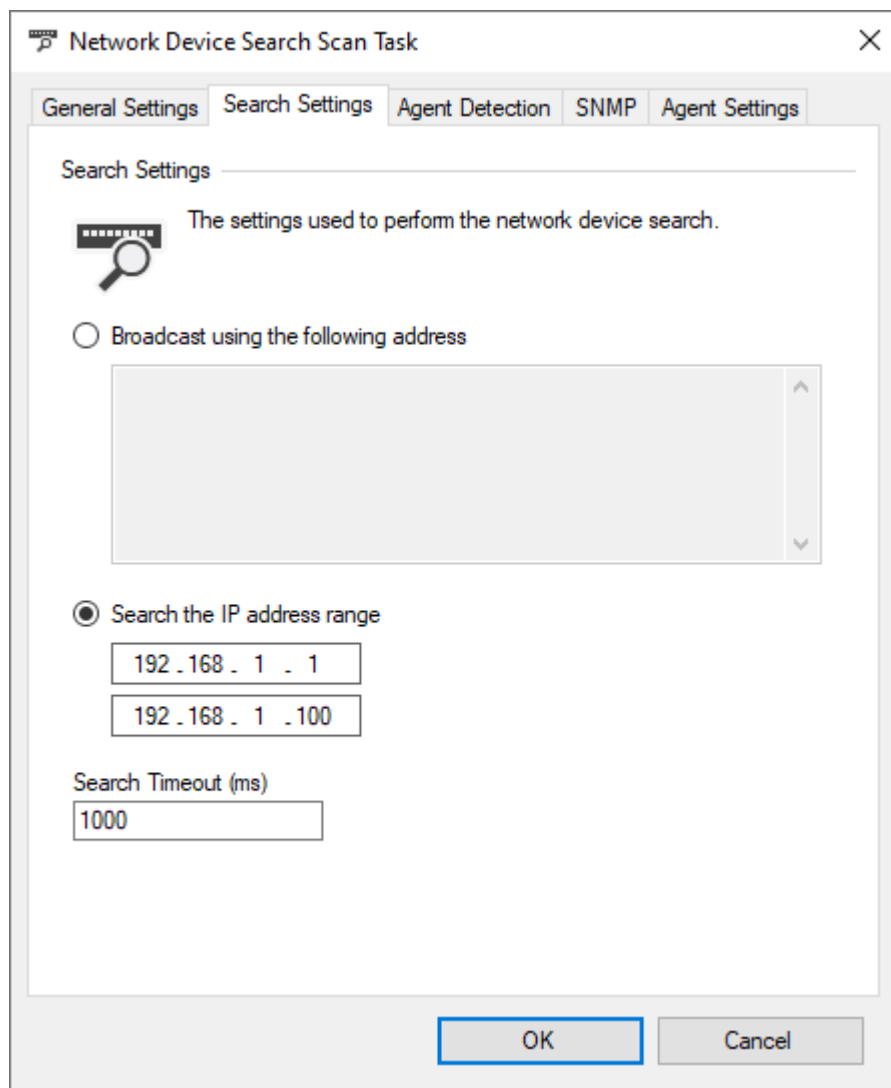
The screenshot shows the 'Cluster Properties' dialog box with the 'Cluster Parameters' tab selected. The 'Cluster IP configuration' section contains the following fields: IP address (192.168.89.240), Subnet mask (255.255.255.0), Full Internet name (cluster2k3.demonstratio), and Network address (03-bf-c0-a8-59-f0). The 'Cluster operation mode' section has three radio buttons: Unicast (selected), Multicast, and IGMP multicast. The 'Allow remote control' checkbox is checked. Below it, the 'Remote password' and 'Confirm password' fields are both masked with asterisks. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Cluster Properties	
Cluster Parameters Cluster IP Addresses Port Rules	
Cluster IP configuration	
IP address:	192 . 168 . 89 . 240
Subnet mask:	255 . 255 . 255 . 0
Full Internet name:	cluster2k3.demonstratio
Network address:	03-bf-c0-a8-59-f0
Cluster operation mode	
☐ Unicast	☒ Multicast
☐ IGMP multicast	
☒ Allow remote control	
Remote password:	*****
Confirm password:	*****
OK Cancel Help	

Network Device Search Scan Task

The network device search scan task is able to locate SNMP manageable network devices such as network switches found within an IP address range or over a broadcast address.

Search Settings



The screenshot shows a dialog box titled "Network Device Search Scan Task" with a close button (X) in the top right corner. The dialog has four tabs: "General Settings", "Search Settings" (which is selected), "Agent Detection", "SNMP", and "Agent Settings". The "Search Settings" tab contains the following elements:

- A section header "Search Settings" with a magnifying glass icon and the text "The settings used to perform the network device search."
- A radio button labeled "Broadcast using the following address" which is currently unselected. Below it is a large, empty text area for specifying a broadcast address.
- A radio button labeled "Search the IP address range" which is currently selected. Below it are two text boxes for specifying an IP range: the first contains "192 . 168 . 1 . 1" and the second contains "192 . 168 . 1 . 100".
- A label "Search Timeout (ms)" followed by a text box containing the value "1000".
- At the bottom right, there are two buttons: "OK" and "Cancel".

Broadcast using the following address

Send a broadcast message to the specified IPv4 broadcast address. The network must be configured to allow these broadcast messages.

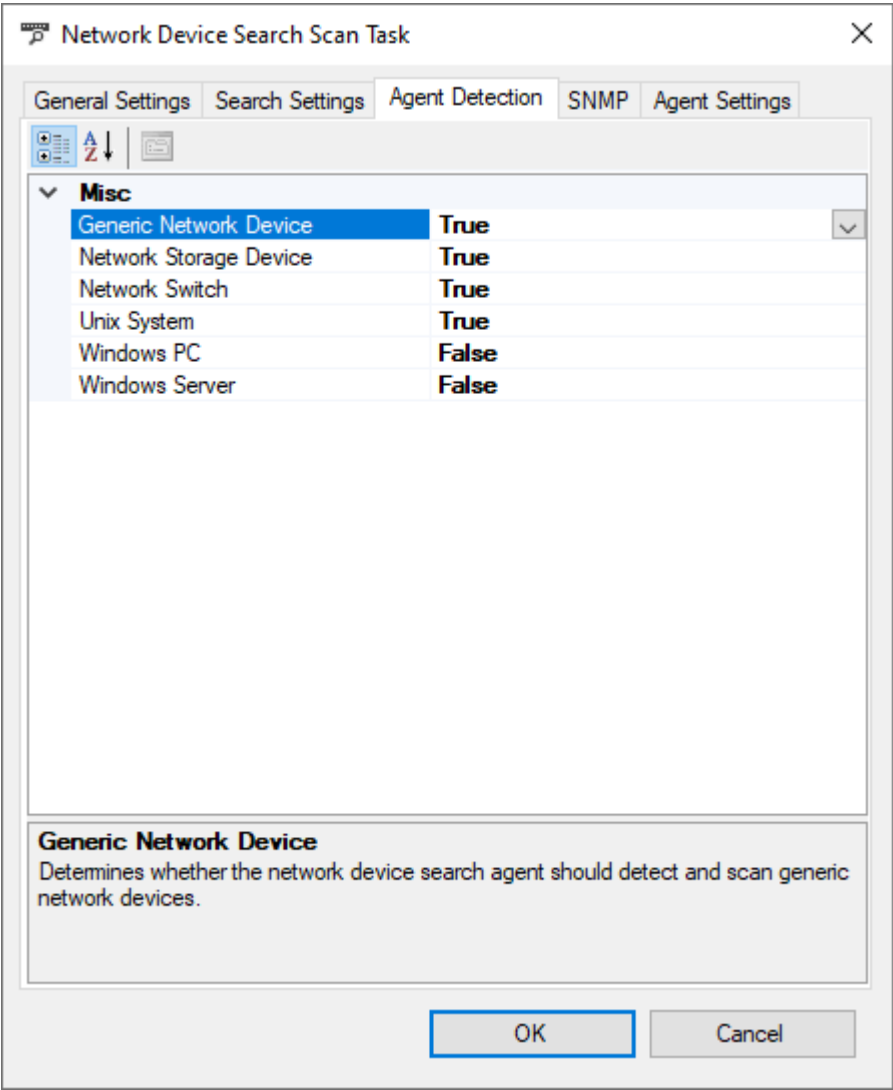
Search the IP address range

The IPv4 address range to search.

Poll Timeout

The polling timeout in milliseconds.

Agent Detection



Generic Network Device

Determines whether [generic network devices](#) should be detected.

Network Storage Device

Determines whether [network storage devices](#) should be detected.

Network Switch

Determines whether [network switches](#) should be detected.

Unix System

Determines whether [Unix and Linux systems](#) should be detected.

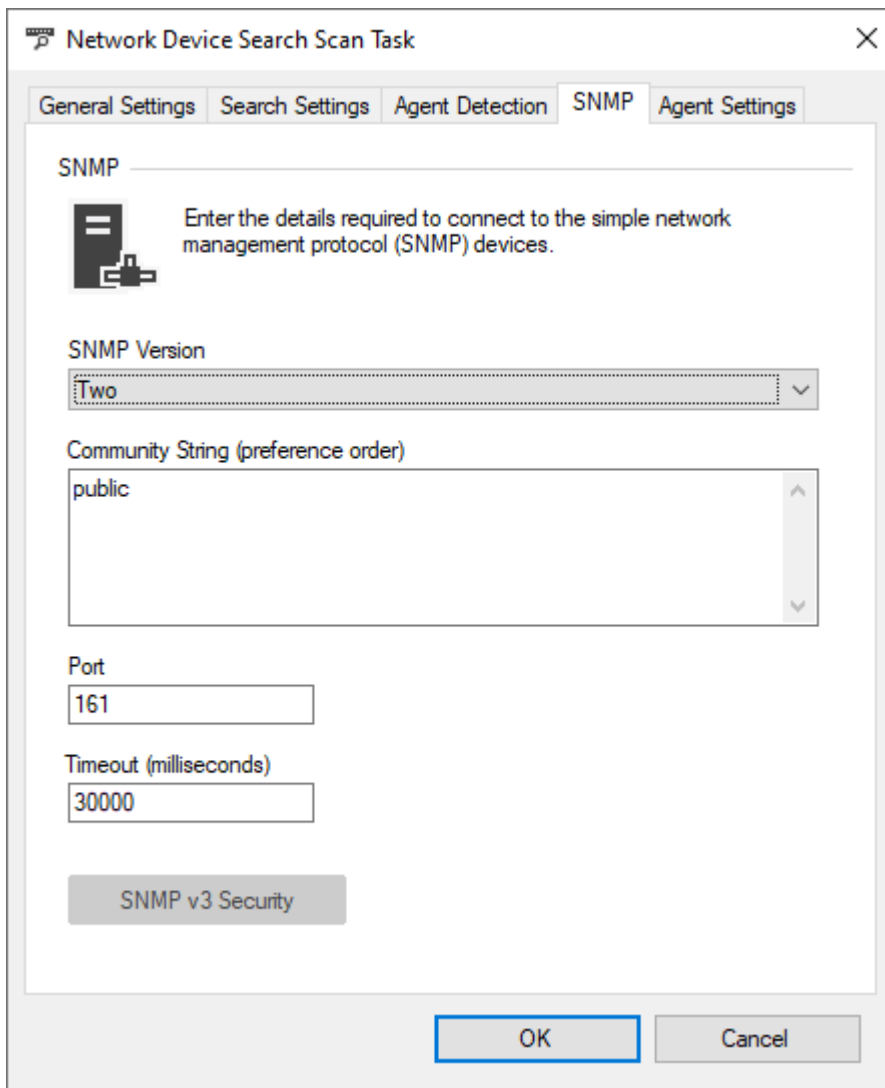
Windows PC

Determines whether [Windows PCs](#) should be detected.

Windows Server

Determines whether [Windows servers](#) should be detected.

SNMP



The image shows a dialog box titled "Network Device Search Scan Task" with a close button (X) in the top right corner. The dialog has five tabs: "General Settings", "Search Settings", "Agent Detection", "SNMP", and "Agent Settings". The "SNMP" tab is currently selected. Inside the tab, there is a section header "SNMP" followed by an icon of a server and a lock, and a text instruction: "Enter the details required to connect to the simple network management protocol (SNMP) devices." Below this, there are four input fields: "SNMP Version" (a dropdown menu showing "Two"), "Community String (preference order)" (a text box containing "public"), "Port" (a text box containing "161"), and "Timeout (milliseconds)" (a text box containing "30000"). At the bottom of the tab area is a button labeled "SNMP v3 Security". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Network Device Search Scan Task

General Settings Search Settings Agent Detection **SNMP** Agent Settings

SNMP

Enter the details required to connect to the simple network management protocol (SNMP) devices.

SNMP Version

Two

Community String (preference order)

public

Port

161

Timeout (milliseconds)

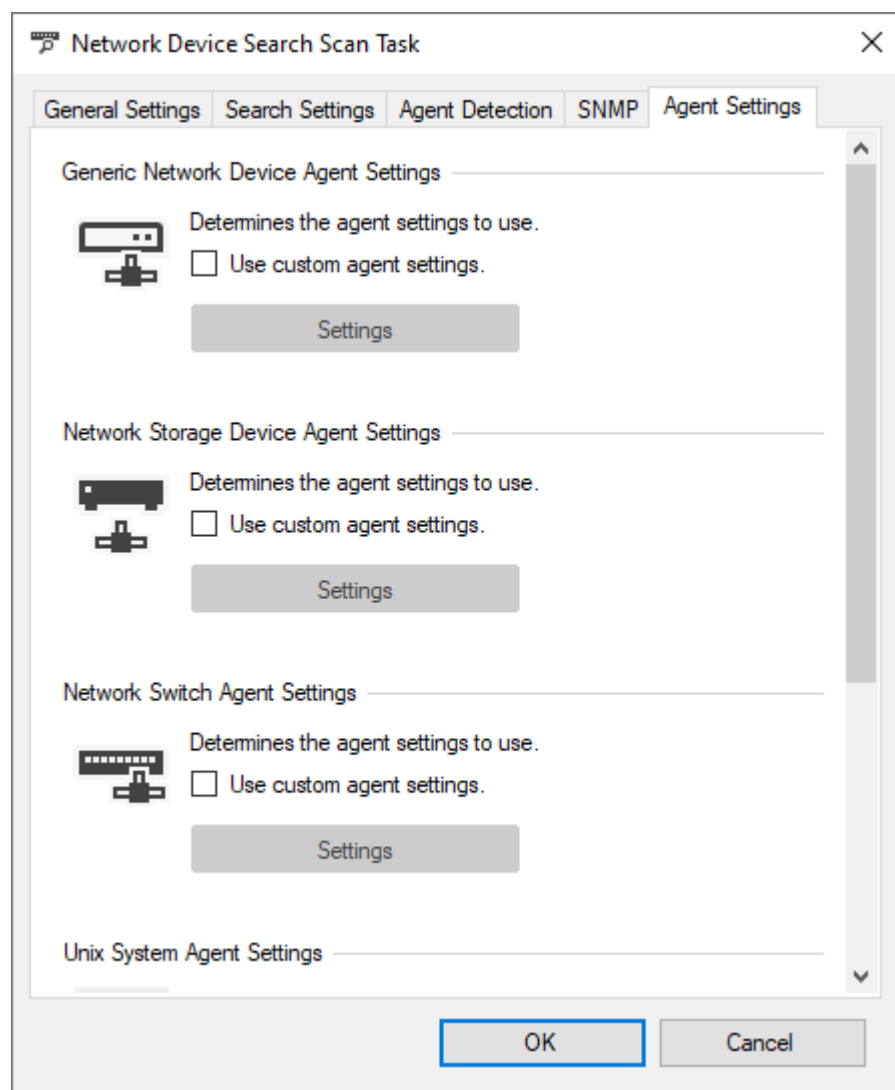
30000

SNMP v3 Security

OK Cancel

Determines the [SNMP settings](#) to use for the search.

Agent Settings



Use custom agent settings

Determines whether to use custom agent settings for the items detected by the search rather than the [default agent settings](#) for the [scan profile](#).

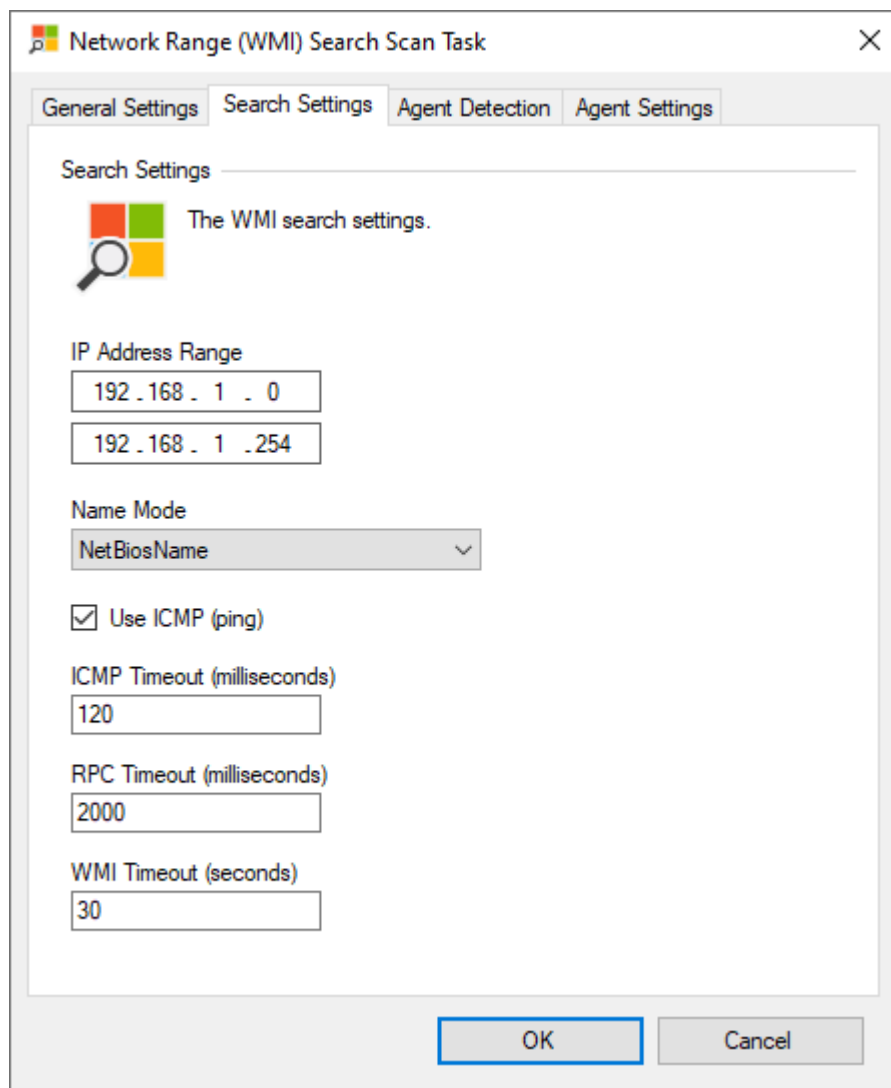
Network Range Search (WMI)

The Network Range Search task allows you to search a range of IP addresses for Windows workstations and servers to document.

Unlike the [Network Device Search Scan Task](#) connections are made to the machines using WMI ([Windows Management Instrumentation](#)) and therefore SNMP is not required to be installed on the remote machine.

NOTE: This search task is typically used in a workgroup scenario. When using Active Directory, the recommended method for detecting Windows workstations and servers is the [Active Directory Search](#) agent.

Search Settings



The screenshot shows a Windows-style dialog box titled "Network Range (WMI) Search Scan Task". It has four tabs: "General Settings", "Search Settings" (which is selected), "Agent Detection", and "Agent Settings". The "Search Settings" tab contains the following elements:

- A sub-header "Search Settings" with a magnifying glass icon and the text "The WMI search settings."
- An "IP Address Range" section with two text boxes: the first contains "192 . 168 . 1 . 0" and the second contains "192 . 168 . 1 . 254".
- A "Name Mode" dropdown menu currently set to "NetBiosName".
- A checked checkbox labeled "Use ICMP (ping)".
- An "ICMP Timeout (milliseconds)" text box containing the value "120".
- An "RPC Timeout (milliseconds)" text box containing the value "2000".
- A "WMI Timeout (seconds)" text box containing the value "30".
- At the bottom right, there are "OK" and "Cancel" buttons.

IP Address Range

The range of IP addresses that should be scanned.

Use ICMP (ping)

Determines whether each address in the range should be pinged to determine whether the machine is online and accessible on the network. This increases the speed of the search however should be disabled if ICMP communications are blocked by a firewall.

ICMP Timeout

The ping timeout in milliseconds after which the machine is determined to be offline.

RPC Timeout

The RPC connection timeout in milliseconds after which the machine is determined to be offline.

WMI Timeout

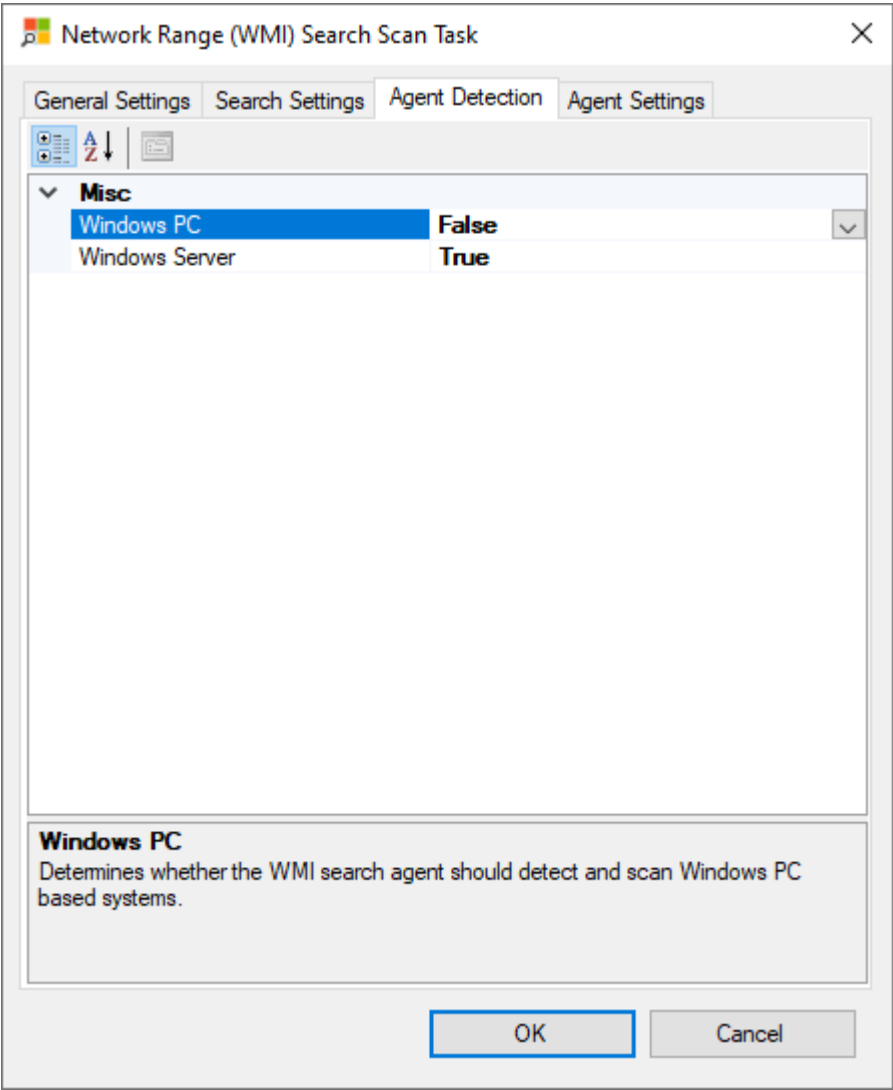
The WMI connection timeout in seconds after which the machine is determined to be offline.

Name Mode

The name that is used for connections to the remote machine by the [Windows Machine](#) agent. By default, the computer (NetBIOS) name is used. Valid values are

- Address
- NetBIOS Name
- Fully Qualified Domain Name

Agent Detection



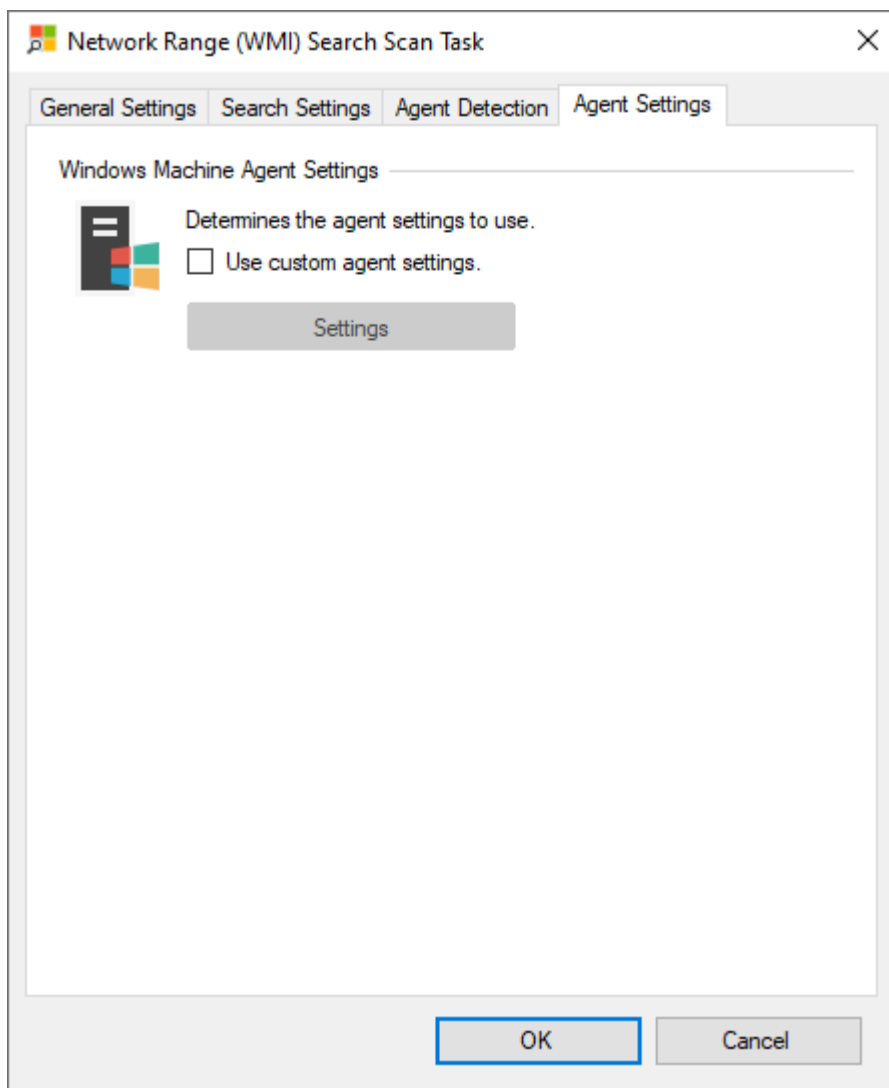
Windows PC

Determines whether to automatically launch a Windows machine scan agent against all Windows PCs detected by the search of the network range. By default, this is false.

Windows Server

Determines whether to automatically launch a Windows machine scan agent against all Windows servers detected by the search of the network range. By default, this is true.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) for the [Windows machines](#) detected by the search rather than the [default agent settings](#) for the [scan profile](#).

Network Storage Device

A network storage device is used to provide storage, typically to servers, over a Fibre Channel (FC) or Ethernet (iSCSI) network.

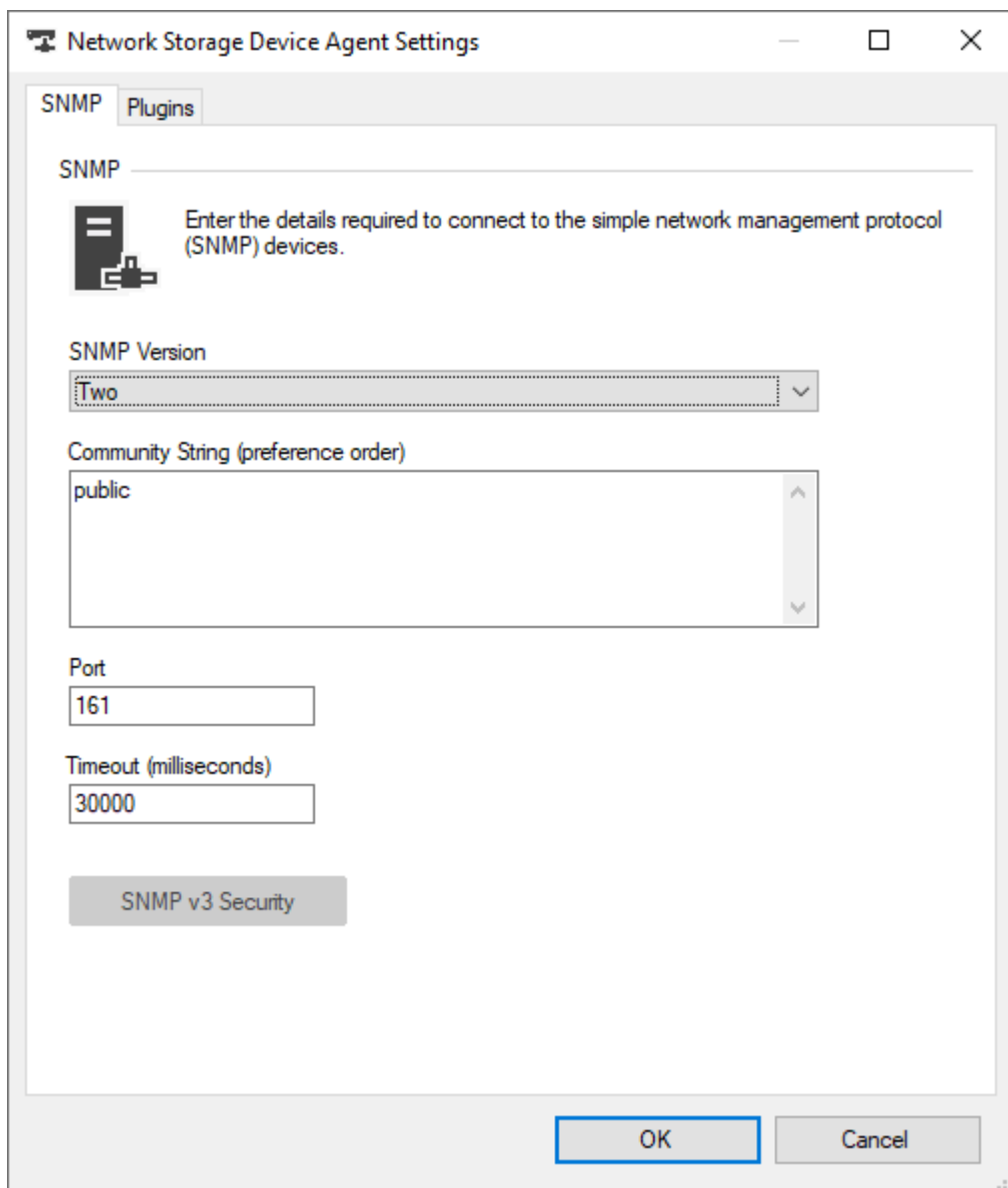
Network storage device tasks are able to document devices from various manufacturers including

- Hewlett-Packard
- NetApp

The following information is collected by the agent, however dependent on the capabilities of the device certain information may not be available.

- Name
- Description
- ARP cache
- Network Ports
- IP addresses
- Routing table
- Serial number
- Model
- Firmware
- Software Version
- Product Number

Agent Settings



The image shows a Windows-style dialog box titled "Network Storage Device Agent Settings". It has two tabs: "SNMP" and "Plugins", with "SNMP" selected. Below the tabs, there is a section for "SNMP" with a sub-header "Enter the details required to connect to the simple network management protocol (SNMP) devices." and a small icon of a server. The settings include: "SNMP Version" set to "Two" in a dropdown menu; "Community String (preference order)" set to "public" in a text box; "Port" set to "161" in a text box; and "Timeout (milliseconds)" set to "30000" in a text box. There is a button labeled "SNMP v3 Security". At the bottom right are "OK" and "Cancel" buttons.

Network Storage Device Agent Settings

SNMP Plugins

SNMP

Enter the details required to connect to the simple network management protocol (SNMP) devices.

SNMP Version

Two

Community String (preference order)

public

Port

161

Timeout (milliseconds)

30000

SNMP v3 Security

OK Cancel

SNMP

The [SNMP settings](#) for the [network storage device agent](#).

Requirements

Supported Target Systems

The following manufacturers are currently supported

- Hewlett-Packard
- NetApp

Access Settings

The network storage device agent uses SNMP to communicate with the devices and has the following access requirements.

- Firewall access must allow access to the SNMP port on the device (typically port 161).
- The XIA Configuration client must be provided with an SNMP read community string valid for the device.
- The storage device must be configured to allow the computer running the [XIA Configuration Client](#) to perform SNMP queries. Please see the documentation provided with your device for more information.

Local Service

 The [network storage device](#) scan tasks do not support the local service.

Network Storage Device Search Task

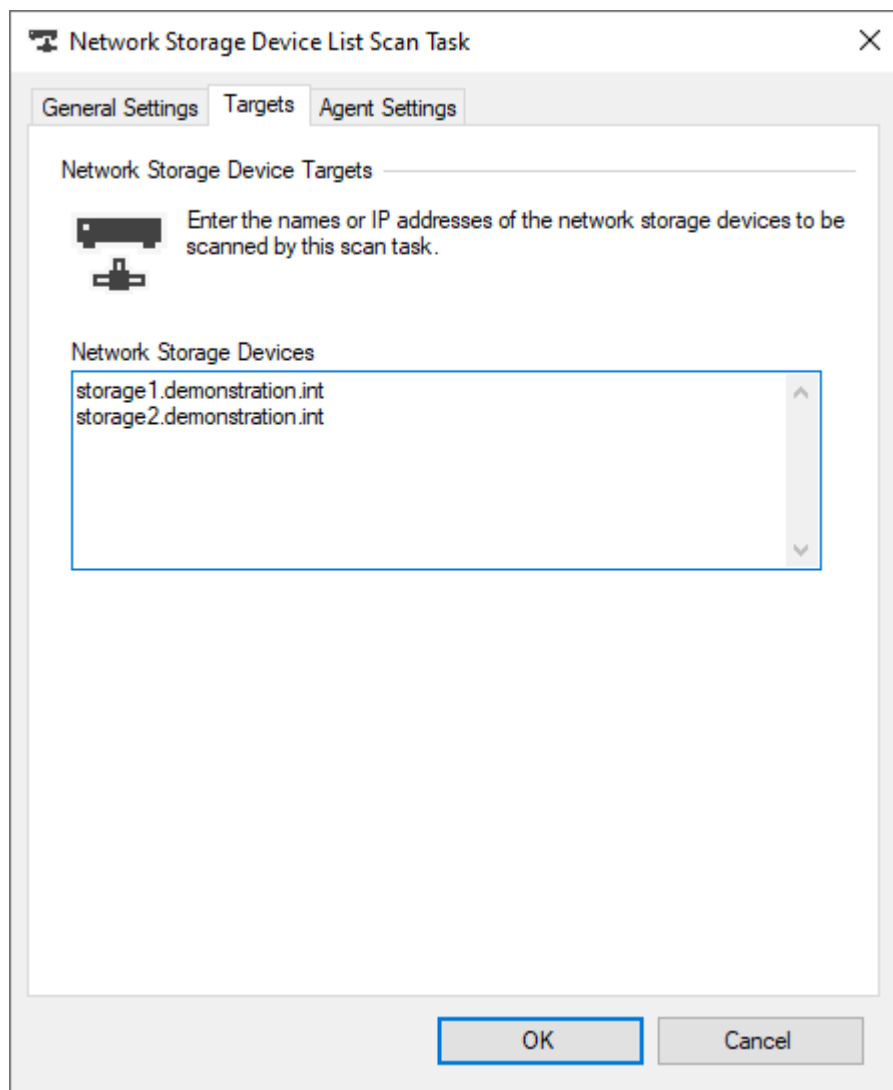
Network storage devices can be detected automatically using the [Network Device Search Scan Task](#).

- Ensure the network storage devices support, and are configured for SNMP.
- Ensure the machine running the [XIA Configuration Client](#) is enabled as a manager within the switch configuration. For more information see the documentation from your storage device manufacturer.
- Enter the subnet or IP address range in which the network switches reside in the [Network Device Search Scan Task](#).
- Ensure that **Network Storage Devices** are enabled within the **Agent Detection** tab.

Network Storage Device List Scan Task

The network storage device list scan task allows you to enter a list of [supported](#) network storage devices that you wish to scan.

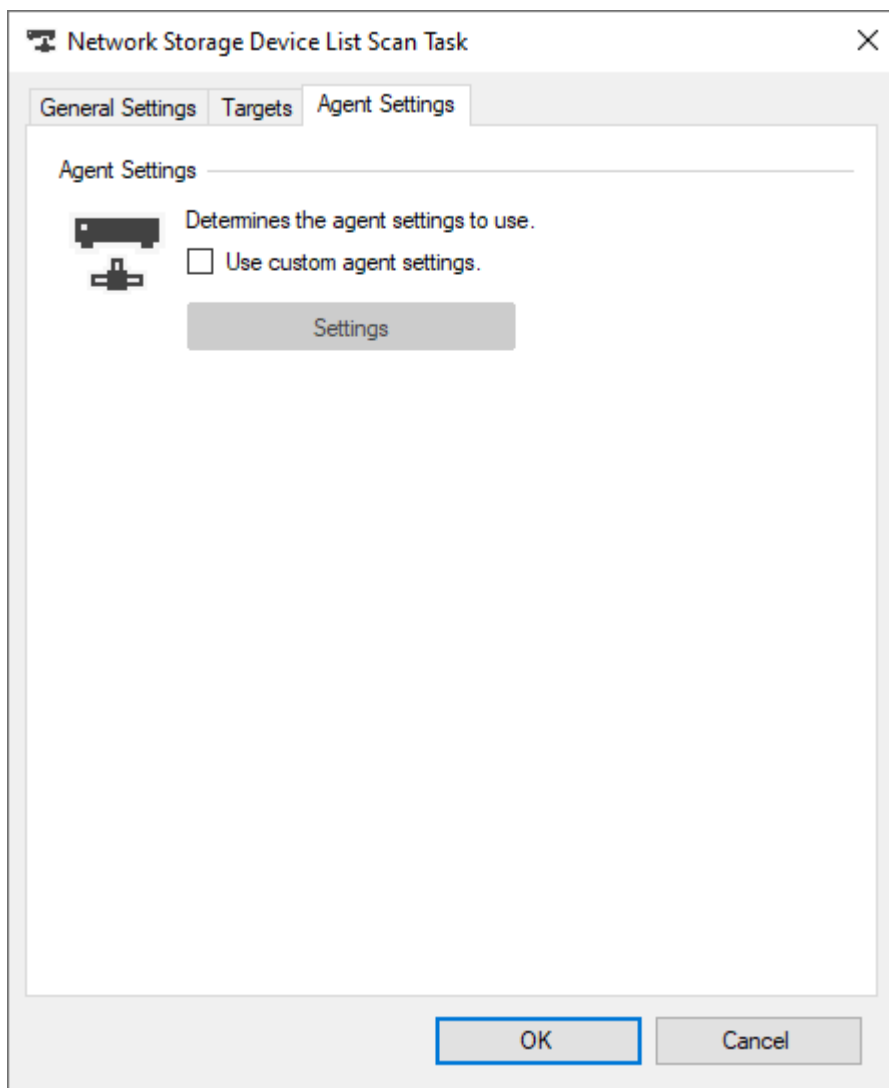
Targets



Network Storage Devices

The IP addresses or fully qualified domain names of the [network storage devices](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Item Identifiers

For more information about item identifiers please see the [Item Identifiers](#) section.

Primary Identifier

The primary identifier is the name of the device

Secondary Identifier

The serial number of the device

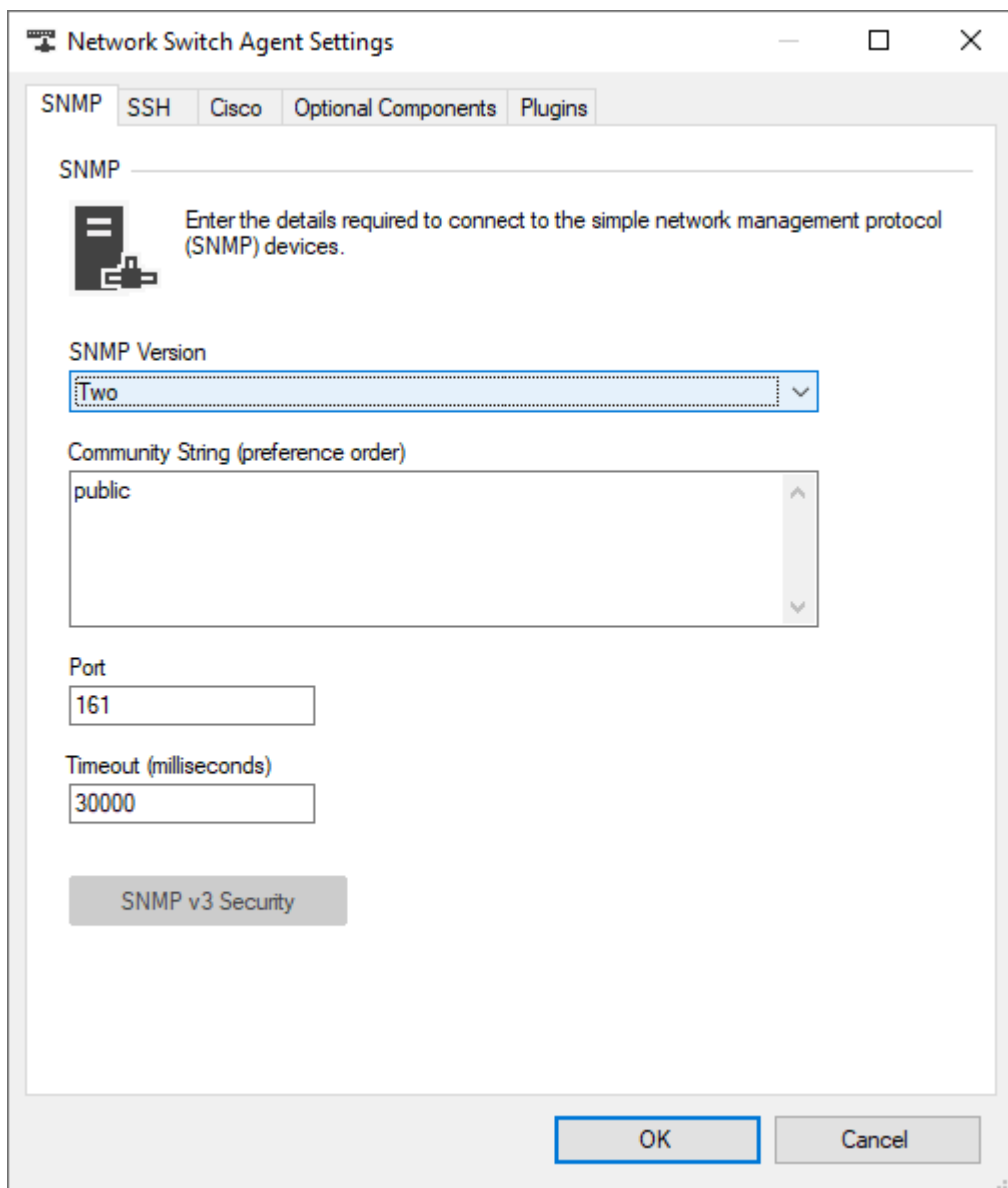
Tertiary Identifier

Not used

Network Switch

Network switch tasks are able to document network switches from various manufacturers that support [SNMP](#) management. To understand the capabilities of your network equipment please refer the documentation provided by your switch manufacturer.

Agent Settings



The image shows a Windows-style dialog box titled "Network Switch Agent Settings". It has a tabbed interface with tabs for "SNMP", "SSH", "Cisco", "Optional Components", and "Plugins". The "SNMP" tab is selected. Inside the tab, there is a header "SNMP" with a sub-header "Enter the details required to connect to the simple network management protocol (SNMP) devices." Below this, there are several input fields: "SNMP Version" is a dropdown menu currently showing "Two"; "Community String (preference order)" is a text box containing "public"; "Port" is a text box containing "161"; and "Timeout (milliseconds)" is a text box containing "30000". There is also a button labeled "SNMP v3 Security". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Network Switch Agent Settings

SNMP SSH Cisco Optional Components Plugins

SNMP

Enter the details required to connect to the simple network management protocol (SNMP) devices.

SNMP Version

Two

Community String (preference order)

public

Port

161

Timeout (milliseconds)

30000

SNMP v3 Security

OK Cancel

SNMP

The [SNMP settings](#) for the [network switch](#) agent.

SSH

Network Switch Agent Settings

SNMPSSHCiscoOptional ComponentsPlugins

SSH Settings



Enter the details required to connect to the secure shell (SSH) server.

☒ Enable SSH Connection

Username

admin

Password

••••••••••••••••

Port

22

Timeout

60000

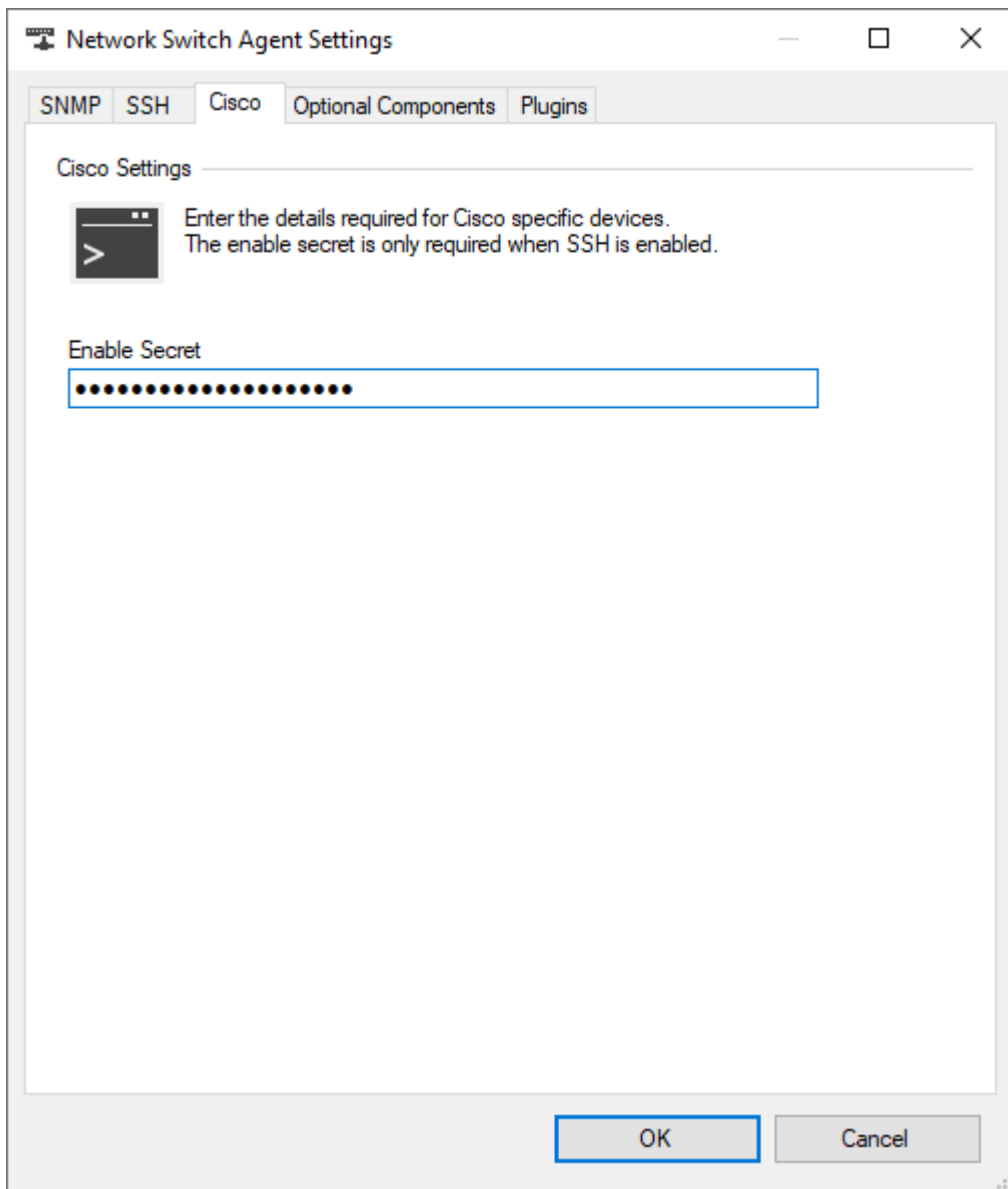
Advanced Settings

OK

Cancel

SSH

The **SSH settings** for the **network switch** agent.

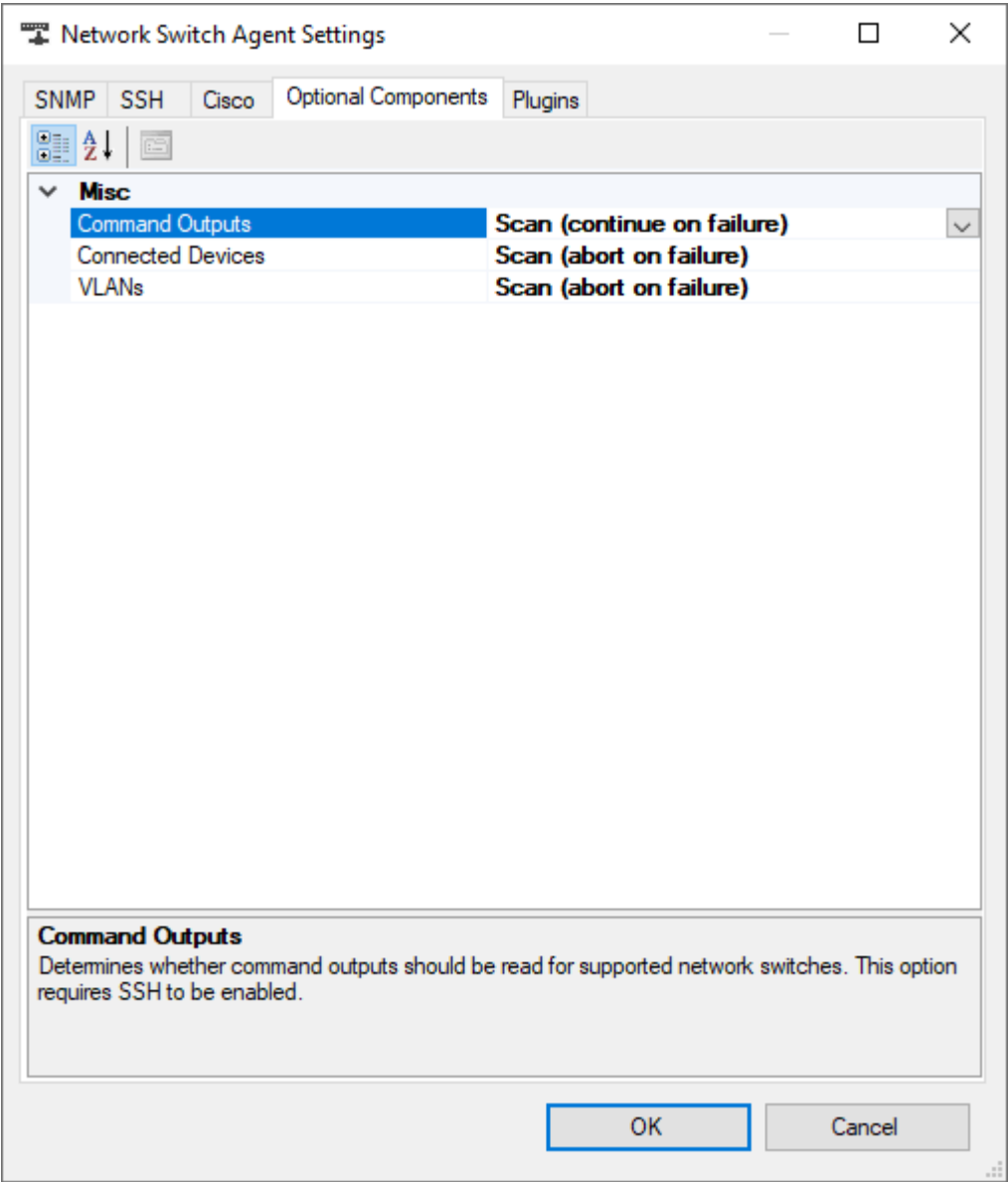


The image shows a Windows-style dialog box titled "Network Switch Agent Settings". It has five tabs: "SNMP", "SSH", "Cisco" (which is selected), "Optional Components", and "Plugins". The "Cisco" tab contains a section titled "Cisco Settings" with a terminal icon and the text: "Enter the details required for Cisco specific devices. The enable secret is only required when SSH is enabled." Below this is a label "Enable Secret" followed by a text input field filled with 20 black dots. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Cisco Enable Secret

The enable secret password to allow privileged access to Cisco [network switches](#).

Optional Components



Command Outputs

Determines whether [command outputs](#) should be read for supported [network switches](#). This option requires [SSH](#) to be enabled and configured.

Connected Devices

Determines whether [connected devices](#) should be read for [network switches](#).

VLANs

Determines whether [VLANs](#) should be read for supported [network switches](#).

Command Outputs

Command outputs read the output from commands executed on supported [network switches](#) using [secure shell \(SSH\)](#).

This option requires [SSH](#) to be enabled and configured.

Cisco

- Running Configuration (*show running-config*)
- Flash (*show flash*)
- Hardware (*show hardware*)

Hewlett Packard

- Running Configuration (*show running-config*)
- Flash (*show flash*)

Additional commands may be executed using [agent plugins](#), for more information see the [network switch command outputs](#) SDK example.

Connected Devices

The connected devices option reads the MAC address of the devices connected to [network switches](#) using [SNMP](#).

The device must support the dot1dBasePortTable table in BRIDGE-MIB.

 Cisco switches will only display connected devices on the default VLAN if the [VLANs optional component](#) is not read.

 Cisco switches will only display connected devices on the default VLAN when using [SNMP](#) version 3 if contexts are not configured. No error message will be displayed.

VLANs

Determines whether virtual LANs (VLANs) should be read for supported [network switches](#) using [SNMP](#).

This is only supported for Cisco [network switches](#) that support CISCO-VTP-MIB, or other manufacturers that support Q-BRIDGE-MIB.

Requirements

Supported Target Systems

The basic switch information can be obtained from any [SNMP](#) manageable network switch that supports the use of RFC1213-MIB and BRIDGE-MIB.

Additional information can be obtained from the following manufacturers:

- Cisco
- Hewlett-Packard
- Allied Telesis
- 3Com

Access Settings

The network switch agent uses [SNMP](#) to communicate with network devices and has the following access requirements.

- Firewall access must allow access to the [SNMP](#) port on the device which is by default UDP/161.
- A read community string must be provided in the [SNMP settings](#).
- The [network switch](#) must have the computer running [XIA Configuration Client](#) configured as an allowed manager. Please see the documentation provided with your [network switch](#) for more information.
- Certain [optional components](#) require [SSH](#) to be enabled and configured.

Local Service

 The [network switch](#) scan tasks do not support the [local service](#).

Network Device Search Scan Task

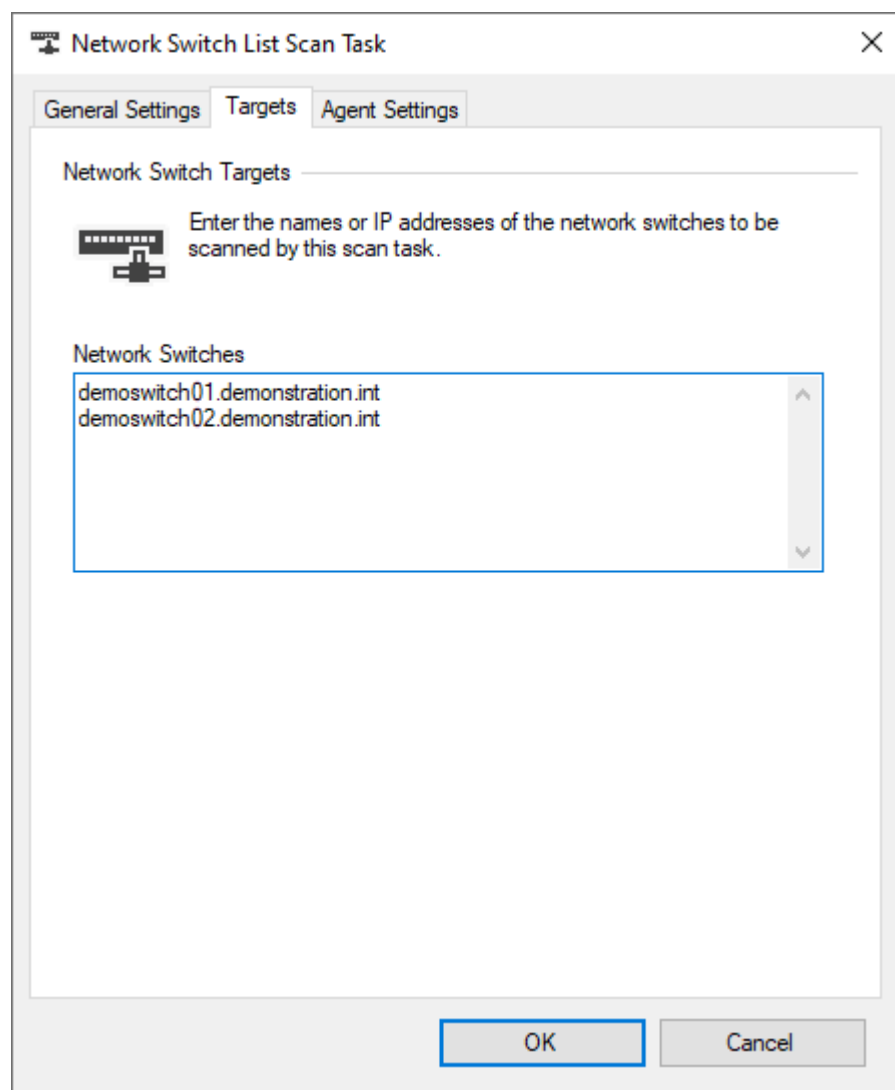
[Network switches](#) can be detected automatically using the [network device search scan task](#).

- Ensure that the [network switches](#) are configured for [SNMP](#).
- Ensure that the [network switches](#) have the computer running [XIA Configuration Client](#) configured as an allowed manager.
- Enter the subnet or IP address range in which the [network switches](#) reside in the [network device search scan task](#).
- Ensure that [network switches](#) are enabled within the agent detection tab.

Network Switch List Scan Task

The network switch list task allows you to enter a list of [network switches](#) that you wish to scan by either their hostname or IP address.

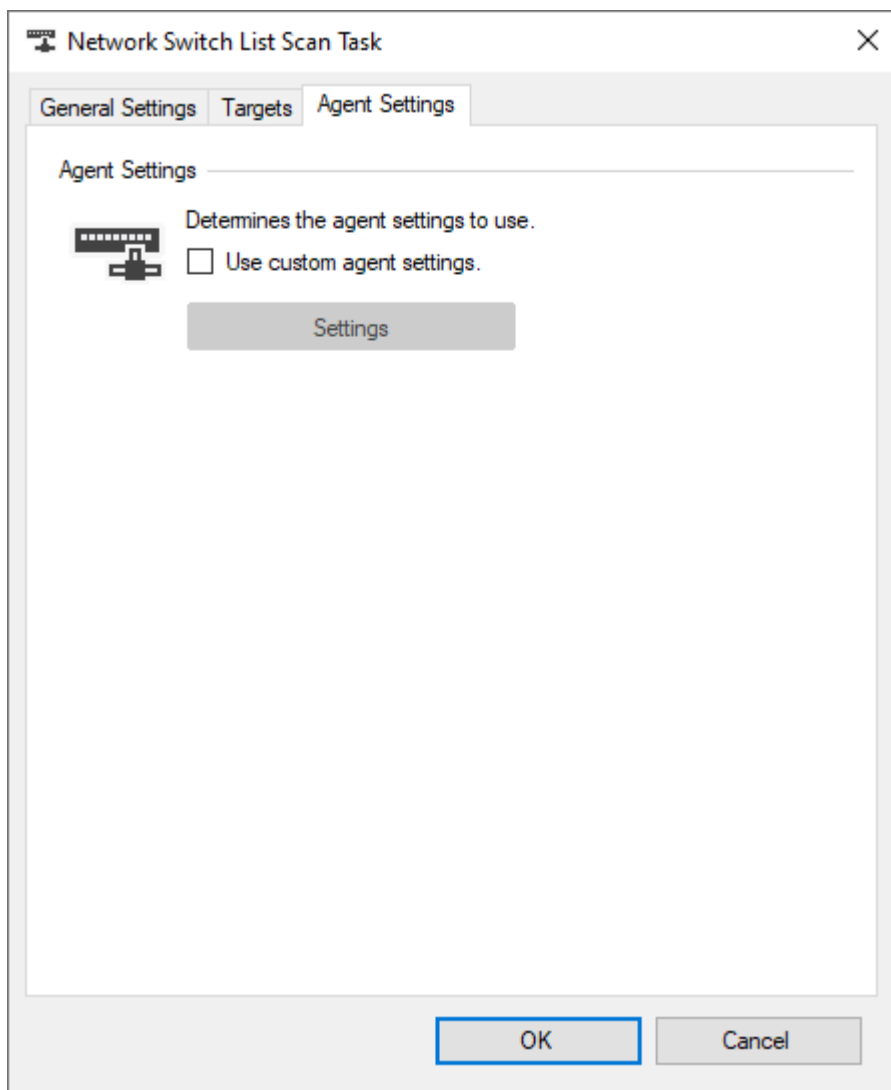
Targets



Network Storage Devices

The IP addresses or fully qualified domain names of the [network switches](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Item Identifiers

For more information about item identifiers please see the [item identifiers](#) section.

Primary Identifier

The primary identifier is the MAC address of the switch - for example "00-50-56-9B-00-06"

Secondary Identifier

Not used

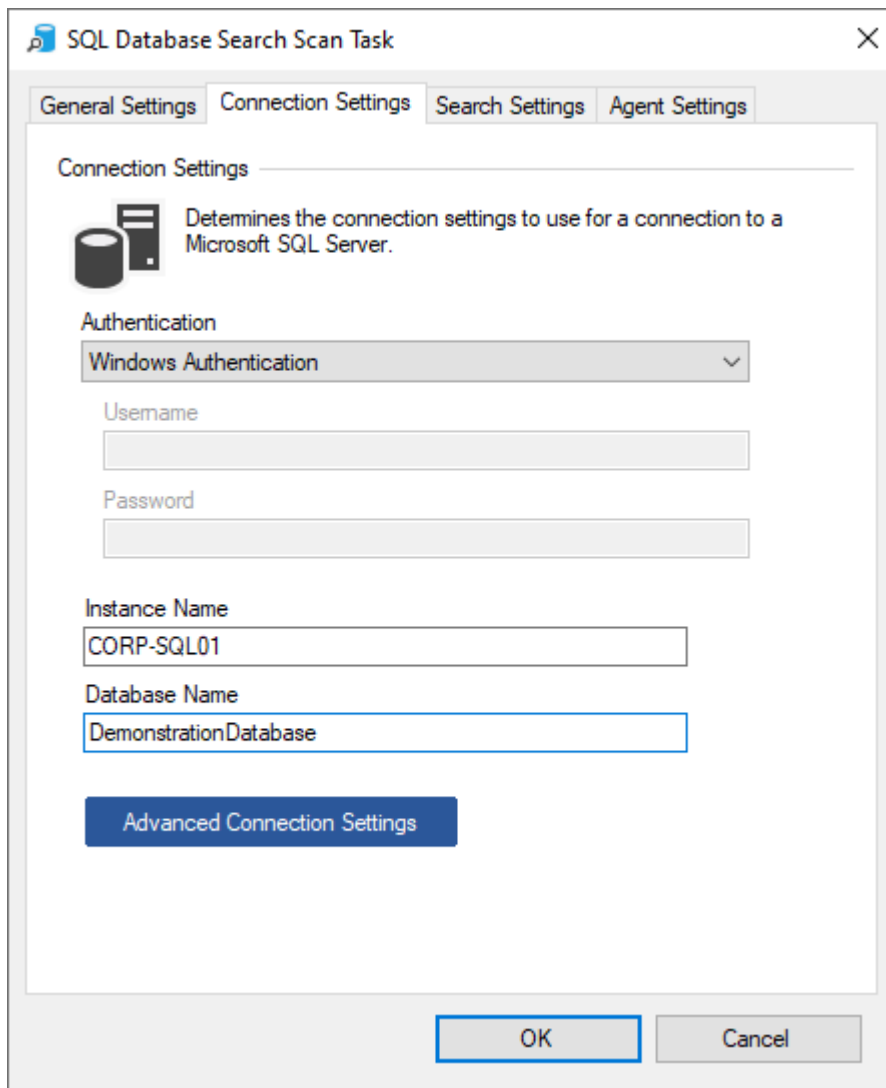
Tertiary Identifier

Not used

SQL Database Search

The SQL database search [task](#) allows you to search a Microsoft SQL database for items to scan.

Connection Settings



The screenshot shows a dialog box titled "SQL Database Search Scan Task" with a close button (X) in the top right corner. It has four tabs: "General Settings", "Connection Settings" (which is selected), "Search Settings", and "Agent Settings". The "Connection Settings" tab contains a description: "Determines the connection settings to use for a connection to a Microsoft SQL Server." Below this is an "Authentication" section with a dropdown menu set to "Windows Authentication". There are text input fields for "Username" and "Password". Below these are fields for "Instance Name" (containing "CORP-SQL01") and "Database Name" (containing "DemonstrationDatabase"). A blue button labeled "Advanced Connection Settings" is located below the database name field. At the bottom of the dialog are "OK" and "Cancel" buttons.

Authentication

Determines the type of [authentication](#) to use.

- Azure Active Directory Password
- Azure Active Directory Integrated
- Windows Authentication
- SQL Password

Username

The username to use when Azure Active Directory Password or SQL password is selected as the authentication type.

Password

The password to use when Azure Active Directory Password or SQL password is selected as the authentication type.

Instance Name

The name of the SQL instance to connect to.

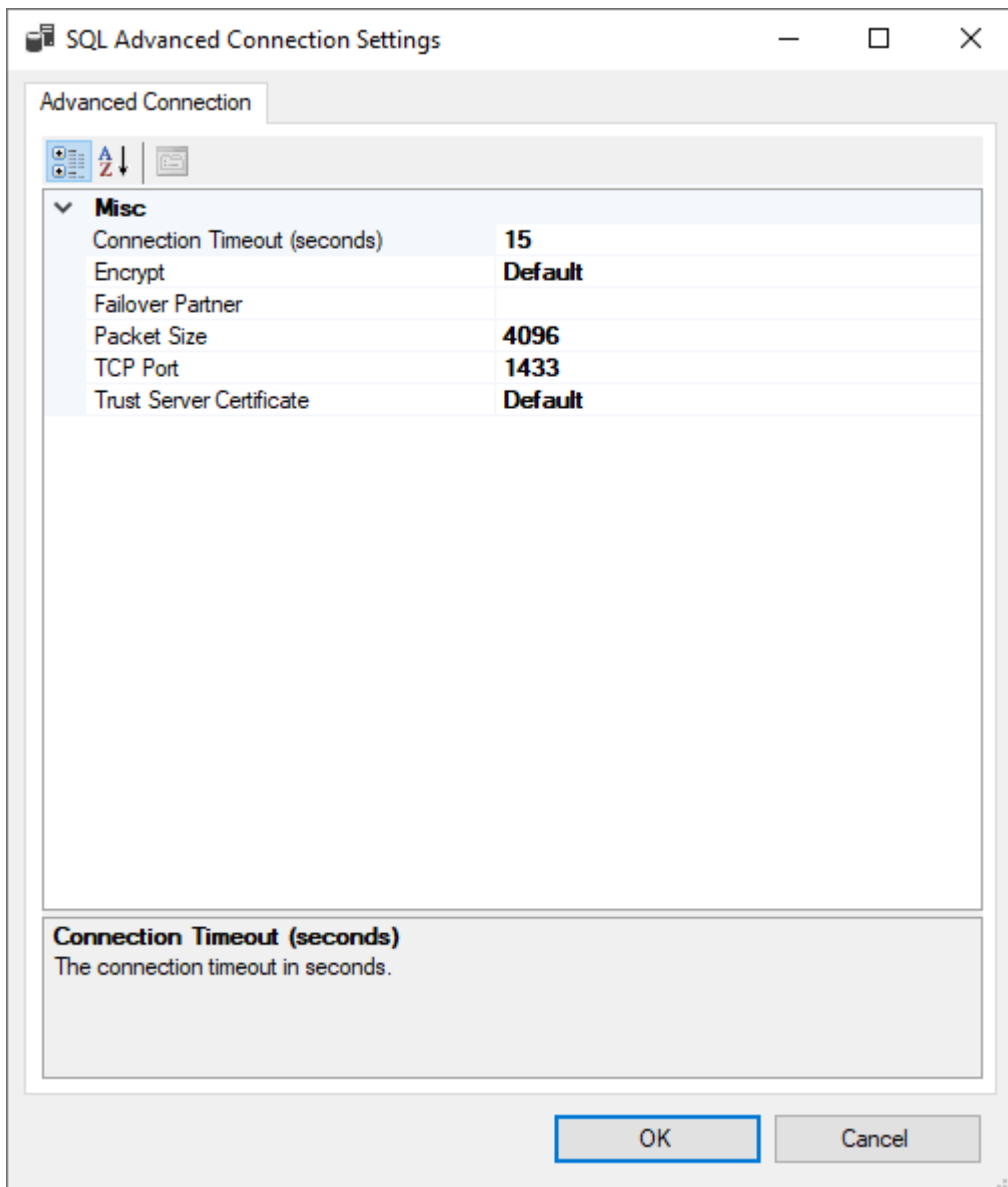
Database Name

The name of the database from which to read the item names.

Advanced Connection Settings

Displays the [advanced connection settings](#) dialog.

Advanced Connection Settings



Connection Timeout (Seconds)

The connection timeout in seconds.

Encrypt

Determines whether to encrypt the connection.

Failover Partner

The name of the failover partner if required.

Packet Size

The size of the network packets used to communicate with an instance of SQL server in bytes.

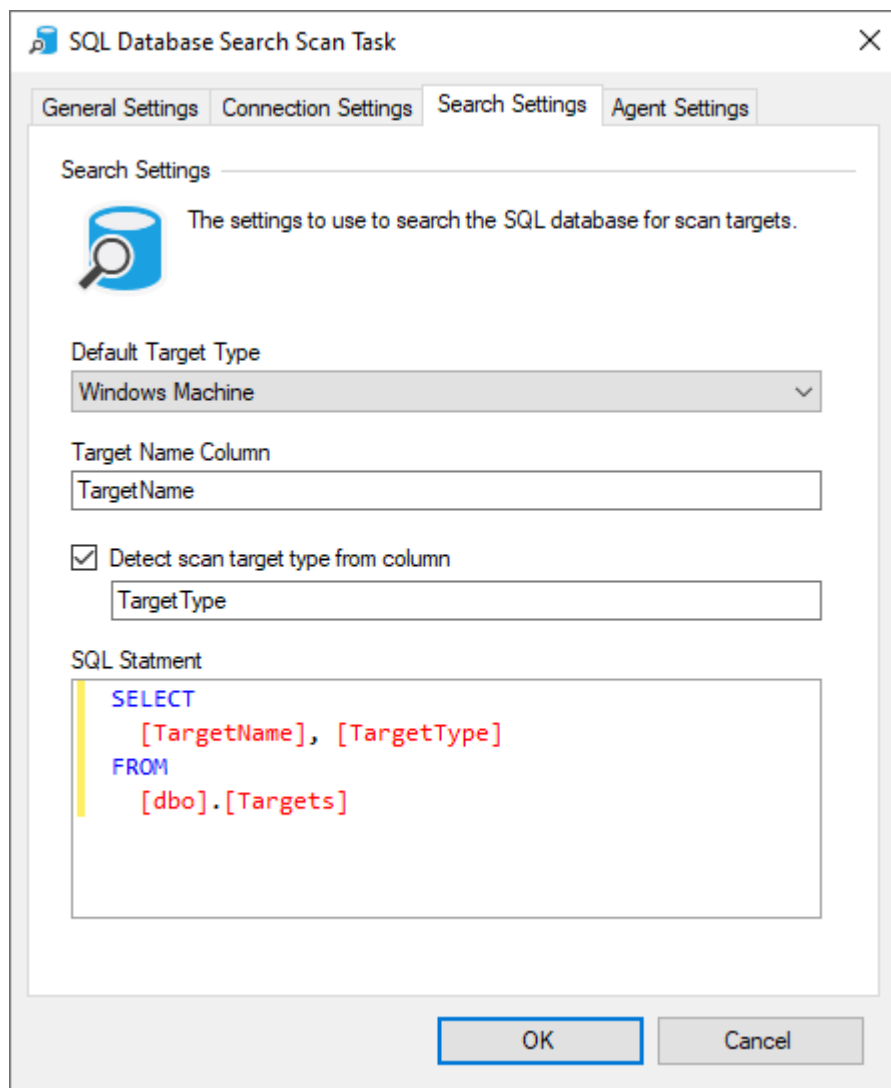
TCP Port

The TCP port to connect to - by default this is 1433.

Trust Server Certificate

Determines whether the client trusts the server certificate.

Search Settings



The screenshot shows the 'SQL Database Search Scan Task' dialog box with the 'Search Settings' tab selected. The dialog has four tabs: 'General Settings', 'Connection Settings', 'Search Settings', and 'Agent Settings'. The 'Search Settings' tab contains the following fields and options:

- Search Settings**: A section header with a magnifying glass icon and the text 'The settings to use to search the SQL database for scan targets.'
- Default Target Type**: A dropdown menu currently set to 'Windows Machine'.
- Target Name Column**: A text input field containing 'TargetName'.
- Detect scan target type from column**: A checked checkbox with a corresponding text input field containing 'TargetType'.
- SQL Statment**: A text area containing the following SQL query:

```
SELECT
    [TargetName], [TargetType]
FROM
    [dbo].[Targets]
```

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Default Target Type

The type of [item](#) to create if the [item type](#) is not specified within the database.

Target Name Column

The name of the database column returned from the SQL statement from which to read the target names.

Detect scan target type

Determines whether to read the type of [item](#) to create from within the database.

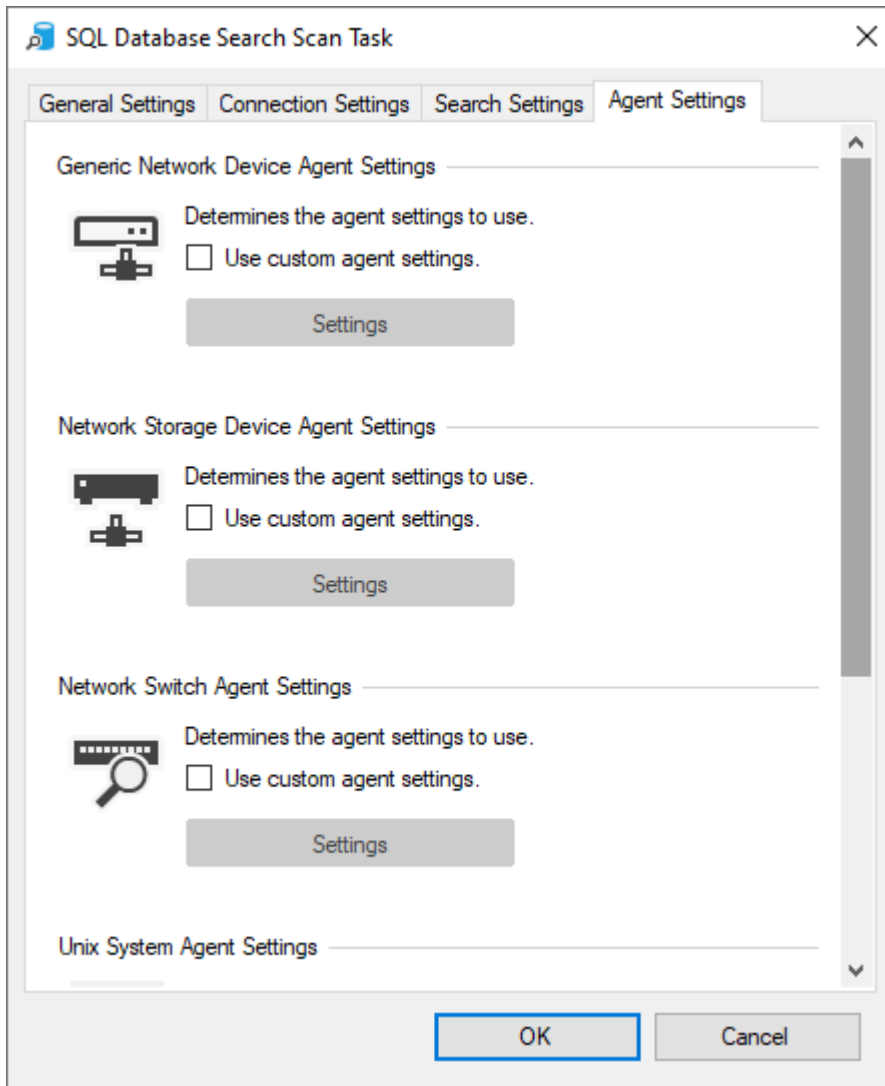
Target Type Column

The name of the database column returned from the SQL statement from which to read the target [item types](#).

SQL Statement

The T-SQL statement to execute to obtain the targets.

Agent Settings



Use custom agent settings

Determines whether to use custom agent settings for the various [item type](#) detected by the search rather than the [default agent settings](#) for the [scan profile](#).

SQL Instance

The [SQL Instance agent](#) is able to document both [Microsoft SQL Server](#) on-premises installations and Microsoft Azure SQL databases¹.

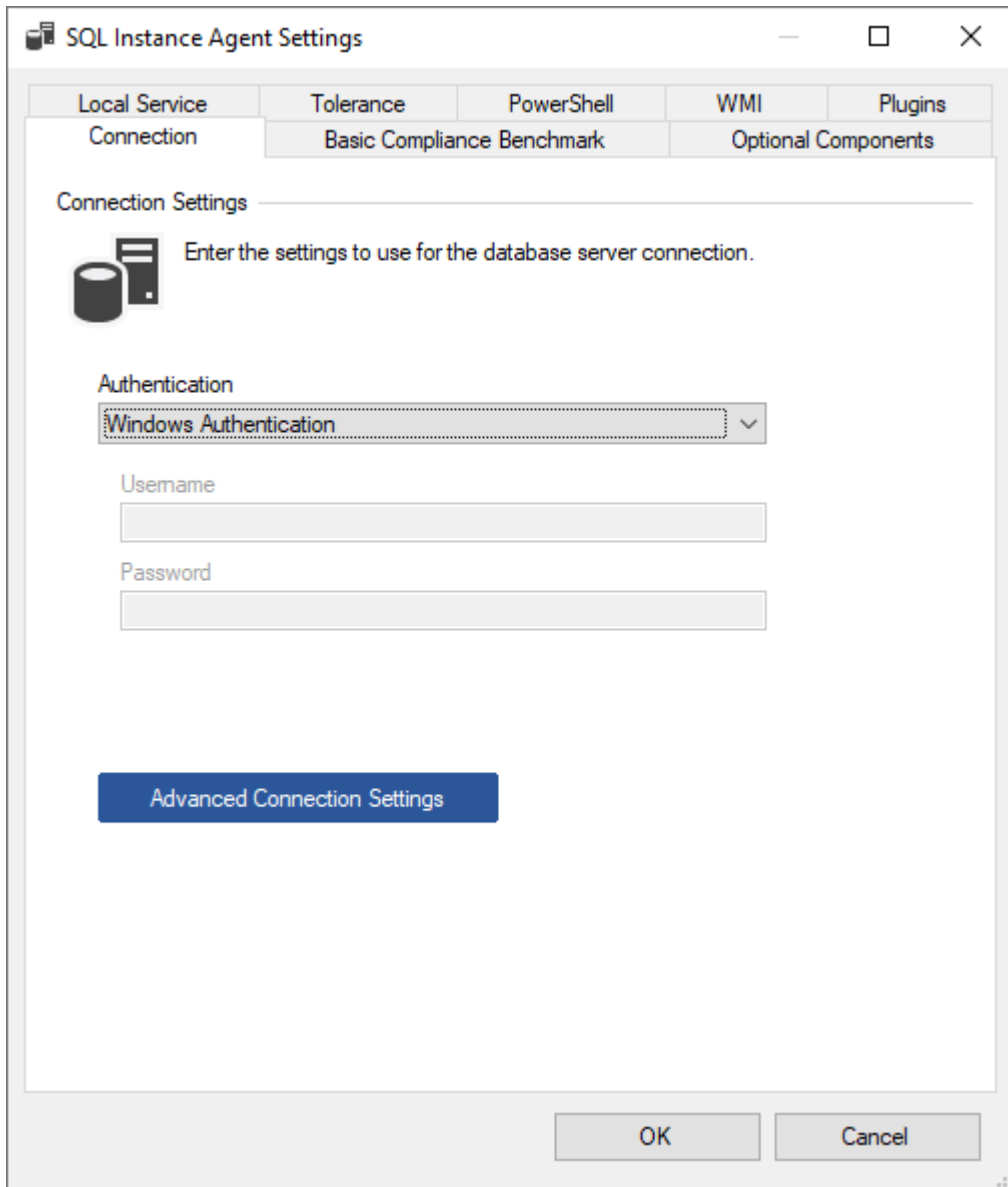
The data located by these tasks includes the following information types:

- Always On High Availability
- Databases
 - Assemblies
 - Database Options
 - Files and Filegroups
 - Stored Procedures
 - Tables
 - Table Columns
 - Table Foreign Keys
 - Triggers
 - User Defined Functions
- Host Information
- Management Settings
 - Database Mail Accounts
 - Resource Governor Settings
- Security Settings
 - Credentials
 - Cryptographic Providers
 - Logins
 - Server Roles
- Server Objects

- Backup Devices
 - Endpoints
- Server Properties
- SQL Server Agent
 - Alerts
 - Jobs
 - Operators
 - Proxies

¹ Some information is only available for Microsoft SQL Server on-premises installations.

Agent Settings



SQL Instance Agent Settings

Local Service Connection | Tolerance | PowerShell | WMI | Plugins

Basic Compliance Benchmark | Optional Components

Connection Settings

Enter the settings to use for the database server connection.

Authentication

Windows Authentication

Username

Password

Advanced Connection Settings

OK Cancel

Authentication

Determines the type of [authentication](#) to use.

- Azure Active Directory Password
- Azure Active Directory Integrated
- Windows Authentication
- SQL Password

Username

The username to use when Azure Active Directory Password or SQL password is selected as the authentication type.

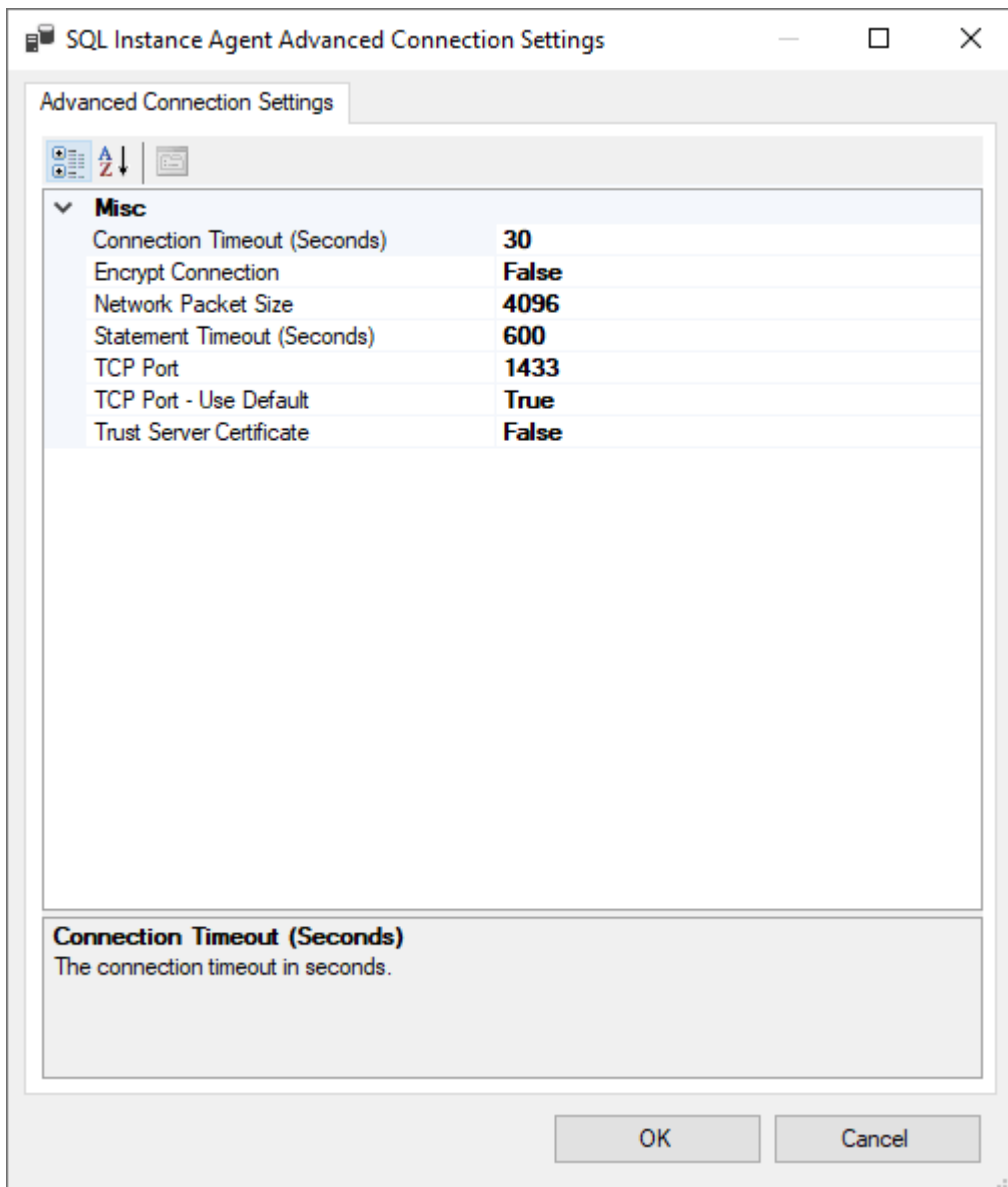
Password

The password to use when Azure Active Directory Password or SQL password is selected as the authentication type.

Advanced Connection Settings

Displays the [advanced connection settings](#) dialog.

Advanced Connection Settings



Connection Timeout (Seconds)

The connection timeout in seconds.

Encrypt Connection

Determines whether to encrypt the connection.

Network Packet Size

The size of the network packets used to communicate with an instance of SQL server in bytes.

Statement Timeout (Seconds)

The number of seconds that a statement is attempted to be sent to the server before it fails. By default this is 600 seconds.

TCP Port

The TCP port to connect to - by default this is 1433. This setting only applies when TCP Port - Use Default is set to false.

TCP Port - Use Default

Determines whether to use the default TCP port 1433 when connecting to the SQL instance.

Trust Server Certificate

Determines whether the client trusts the server certificate.

Basic Compliance Benchmark

The [SQL basic compliance benchmark](#) provides a simple overview of the security settings against simple security best practices for on-premises installations of [SQL instances](#) and should be used for guidance only as this does not guarantee a secure system. Users should fully investigate the consequences of any security configuration changes prior to making them.

Name

SQL Basic Compliance Benchmark

Unique Identifier

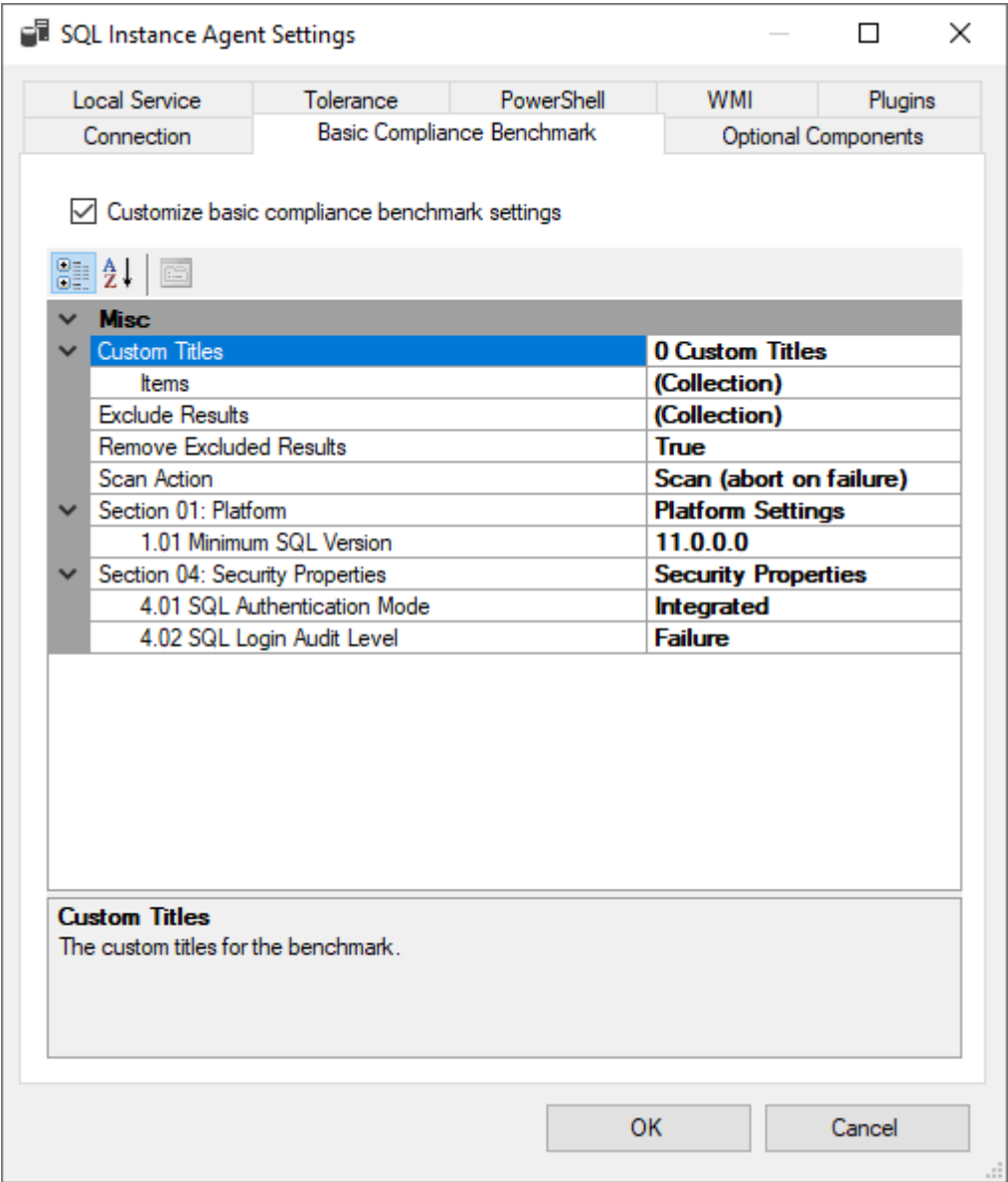
a8a61a13-798e-407b-9cfa-25e6ac76c31d

Provider

CENTREL Solutions Ltd

Benchmark Settings

The [SQL Instance Basic Compliance Benchmark](#) has the following configurable options



Use Basic Compliance Benchmark Custom Settings

Determines whether the custom settings should be configured for the Windows machine [Basic Compliance Benchmark](#).

Custom Titles

Determines the [custom text](#) to use for compliance benchmark titles.

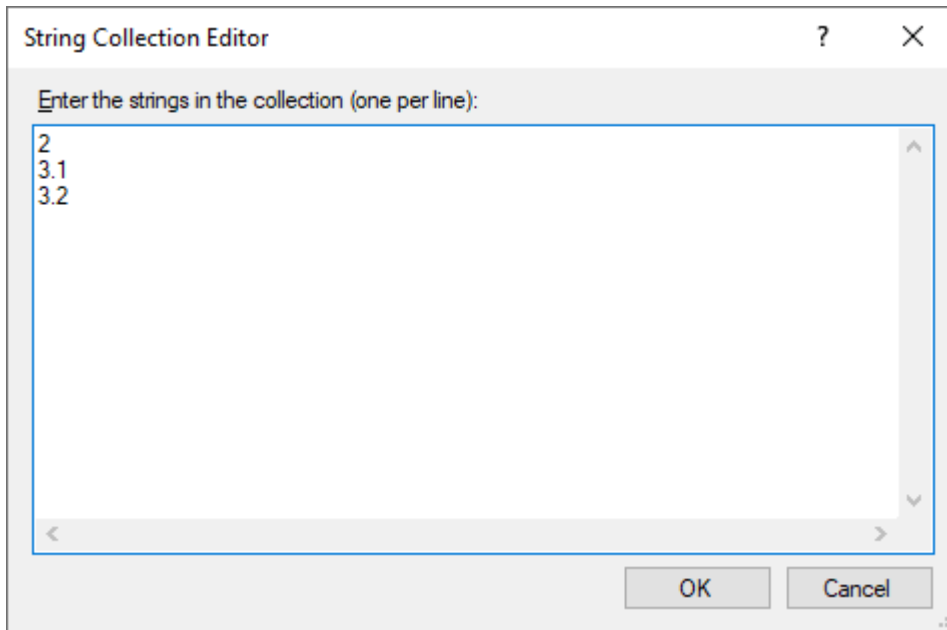
Remove Excluded Results

Determines whether results that are excluded (for example by configuration or because the results do not apply to the target platform) should be removed from the result set.

Exclude Results

The results that should be excluded from the benchmark test - this can include the reference

numbers of individual tests as well as the reference numbers of entire sections.



Scan Action *

The action that should be performed for this optional component.

* **NOTE:** the option "Scan (abort on failure)" refers to the inability of the [XIA Configuration Client](#) to perform the benchmark test, rather than sections of the benchmark failing compliance.

Section 1: Platform

1.01 Minimum SQL Version

Determines the minimum version of SQL Server.

Section 4: Security Properties

4.01 SQL Authentication Mode

Determines the desired SQL authentication mode.

Unknown: This value is not valid for benchmarks.

Integrated: Windows Authentication Mode.

Mixed: SQL Server And Windows Authentication Mode.

4.02 SQL Login Audit Level

Determines the desired SQL login audit level.

Unknown: This value is not valid for benchmarks.

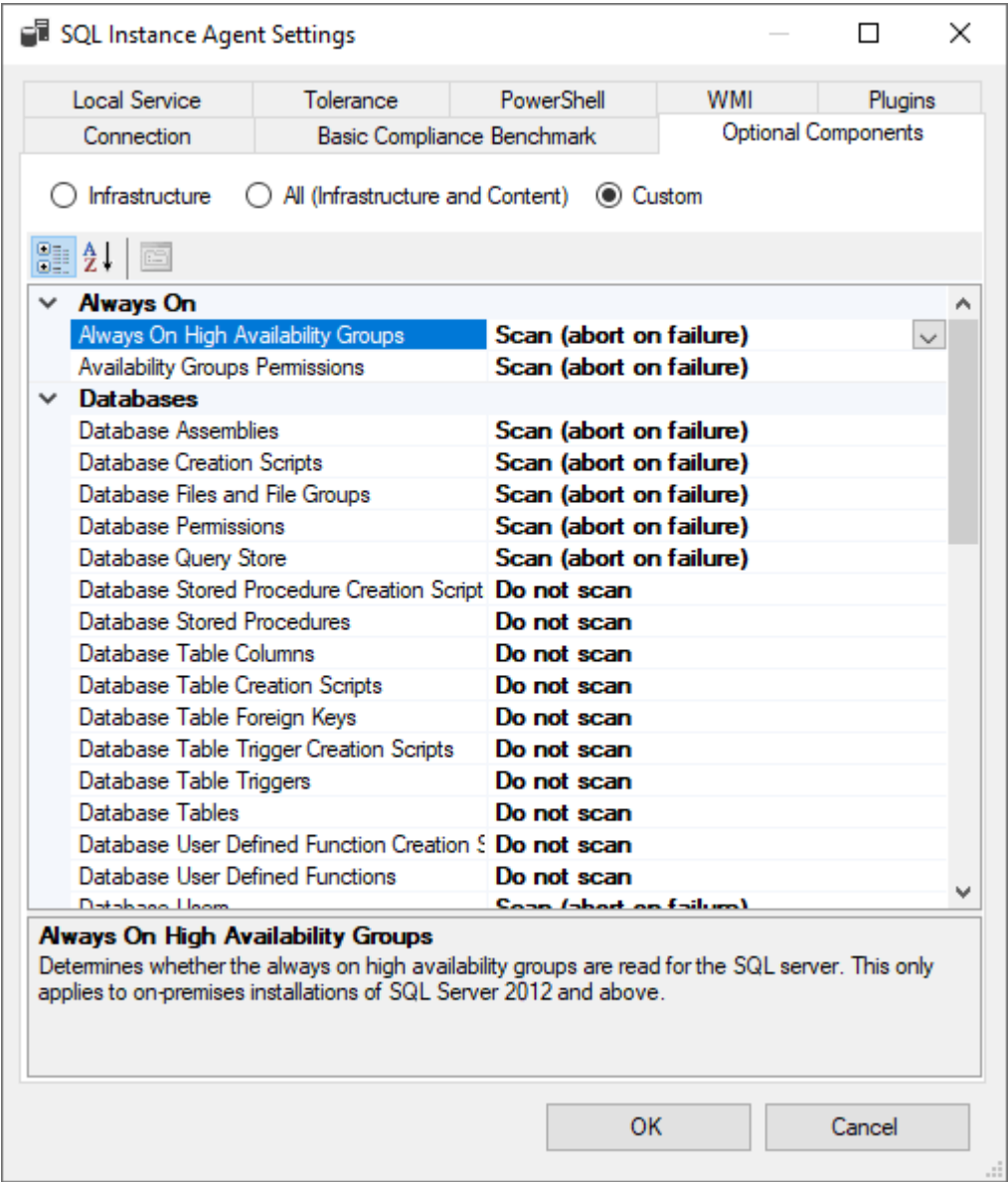
None: None.

Failure: Failed logins only.

Success: Successful logins only.

All: Both failed and successful logins.

Optional Components



Infrastructure

Configures the optional components to collect common infrastructure information but does not collect content including tables, stored procedures, user defined functions, or views.

All (Infrastructure and Content)

Configures the optional components to collect all information including tables, stored procedures, user defined functions, or views.

Custom

Configures the optional components to use custom settings.

Always On High Availability Groups

Determines whether the always on high availability groups are read for the SQL server. This only applies to on-premises installations of SQL Server 2012 and above.

Availability Groups Permissions

Determines whether the permissions for availability groups are read for the SQL server. This only applies to on-premises installations of SQL Server 2012 and above.

Database Assemblies

Determines whether assemblies are read for databases hosted by the SQL instance.

Database Creation Scripts

Determines whether the creation scripts are read for databases hosted by the SQL instance.

Database Files and File Groups

Determines whether the files and file groups are read for databases hosted by the SQL instance. This applies to on-premises SQL Server installations.

Database Permissions

Determines whether the permissions are read for databases hosted by the SQL instance.

Database Query Store

Determines whether the query store settings are read for databases hosted by the SQL instance. This applies to Azure and on-premises SQL Server 2016 and above.

Database Stored Procedure Creation Scripts

Determines whether the creation scripts for stored procedures are read for databases hosted by the SQL instance.

Database Stored Procedures

Determines whether the stored procedures are read for databases hosted by the SQL instance.

Database Table Columns

Determines whether the columns of tables are read for databases hosted by the SQL instance.

Database Table Creation Scripts

Determines whether the creation scripts are read for tables hosted by the SQL instance.

Database Table Foreign Keys

Determines whether the foreign keys of tables are read for databases hosted by the SQL instance.

Database Table Trigger Creation Scripts

Determines whether the creation scripts are read for triggers for databases hosted by the SQL instance.

Database Table Triggers

Determines whether the triggers of tables are read for databases hosted by the SQL instance.

Database Tables

Determines whether the tables are read for databases hosted by the SQL instance.

Database User Defined Function Creation Scripts

Determines whether the creation scripts for user defined functions are read for databases hosted by the SQL instance.

Database User Defined Functions

Determines whether the user defined functions are read for databases hosted by the SQL instance.

Database Users

Determines whether the users are read for databases hosted by the SQL instance.

Database Views

Determines whether the views are read for databases hosted by the SQL instance.

Databases

Determines whether the databases are read for the SQL instance.

Databases (Snapshots)

Determines whether database snapshots are read for the SQL instance.

Databases (System Databases)

Determines whether system databases are read for the SQL instance.

Host Information

Determines whether the host information is read for the SQL server. Host information is required to gather the serial number which is used as the secondary [item identifier](#) for non-clustered on-premises installations of SQL Server. Changing this setting can cause duplicate [items](#) to be created. This only applies to on-premises installations of SQL Server.

Host Information Scan Method

The method by which the agent will gather host information for the SQL server.

Hosts Information (Clusters)

Determines whether the host information is read for clustered SQL server instances. This only applies to on-premises installations of SQL Server.

Database Mail Configuration

Determines whether the database mail configuration should be read for the instance. This only applies to on-premises installations of SQL Server.

Maintenance Plans

Determines whether maintenance plans are read for the SQL server. This only applies to on-premises installations of SQL Server.

Resource Governor

Determines whether the resource governor configuration is read for the SQL server. This only applies to on-premises installations of SQL Server.

Credentials

Determines whether credentials are read for the SQL server. This only applies to on-premises installations of SQL Server.

Cryptographic Providers

Determines whether cryptographic providers are read for the SQL server. This only applies to on-premises installations of SQL Server.

Logins

Determines whether the logins are read for the SQL instance.

Server Permissions

Determines whether the server permissions are read for the SQL instance.

Server Roles

Determines whether the server roles are read for the SQL instance.

Backup Devices

Determines whether backup device information is read for the SQL server. This only applies to on-premises installations of SQL Server.

Endpoints

Determines whether endpoint information is read for the SQL server. This only applies to on-

premises installations of SQL Server.

Agent

Determines whether agent settings are read for the SQL server. This only applies to on-premises installations of SQL Server.

Alerts

Determines whether alerts are read for the SQL server. This only applies to on-premises installations of SQL Server.

Jobs

Determines whether the jobs are read for the SQL server. This only applies to on-premises installations of SQL Server.

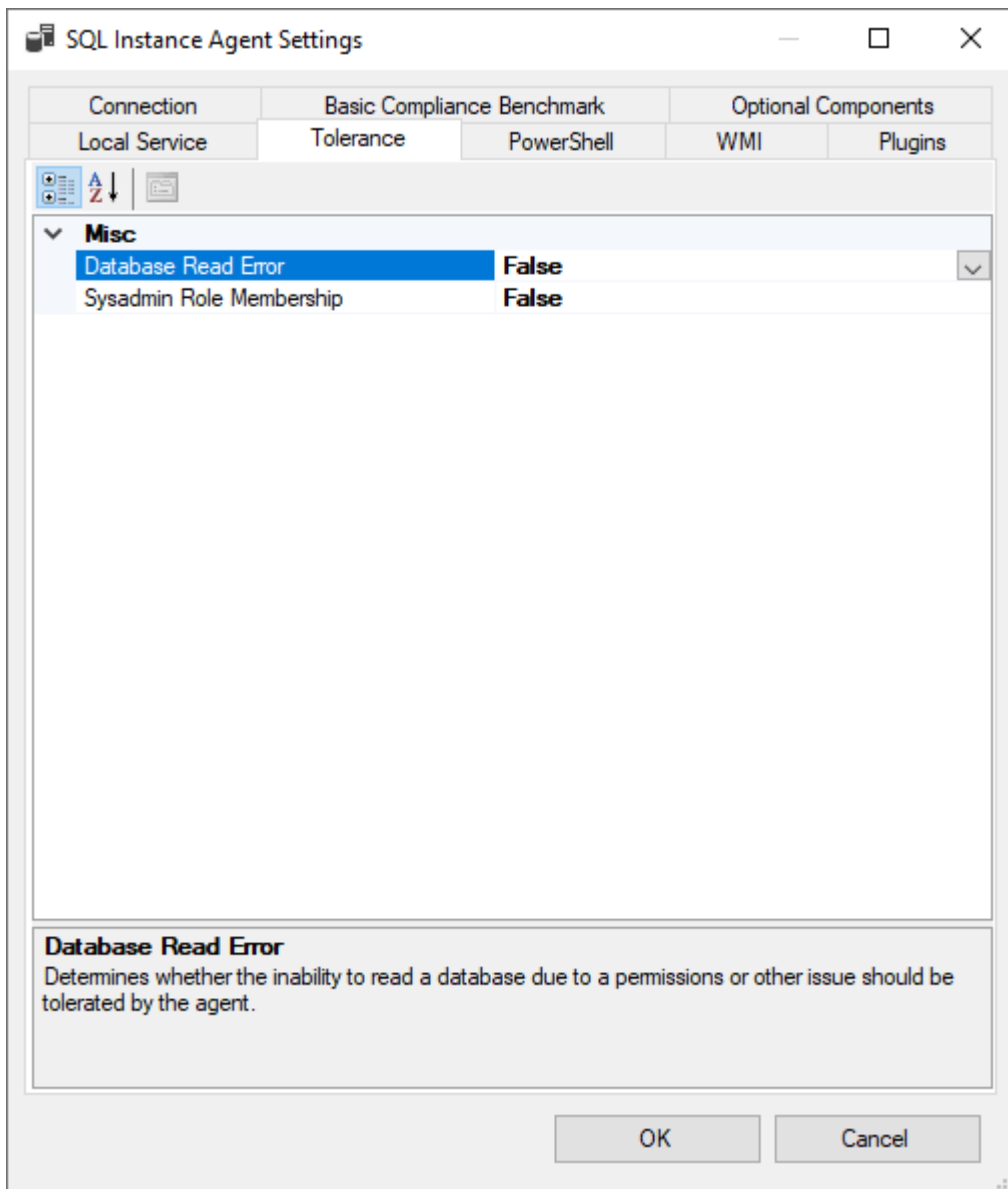
Operators

Determines whether the operators are read for the SQL server. This only applies to on-premises installations of SQL Server.

Proxy Accounts

Determines whether the proxy accounts are read for the SQL server. This only applies to on-premises installations of SQL Server.

Tolerance



Database Read Error

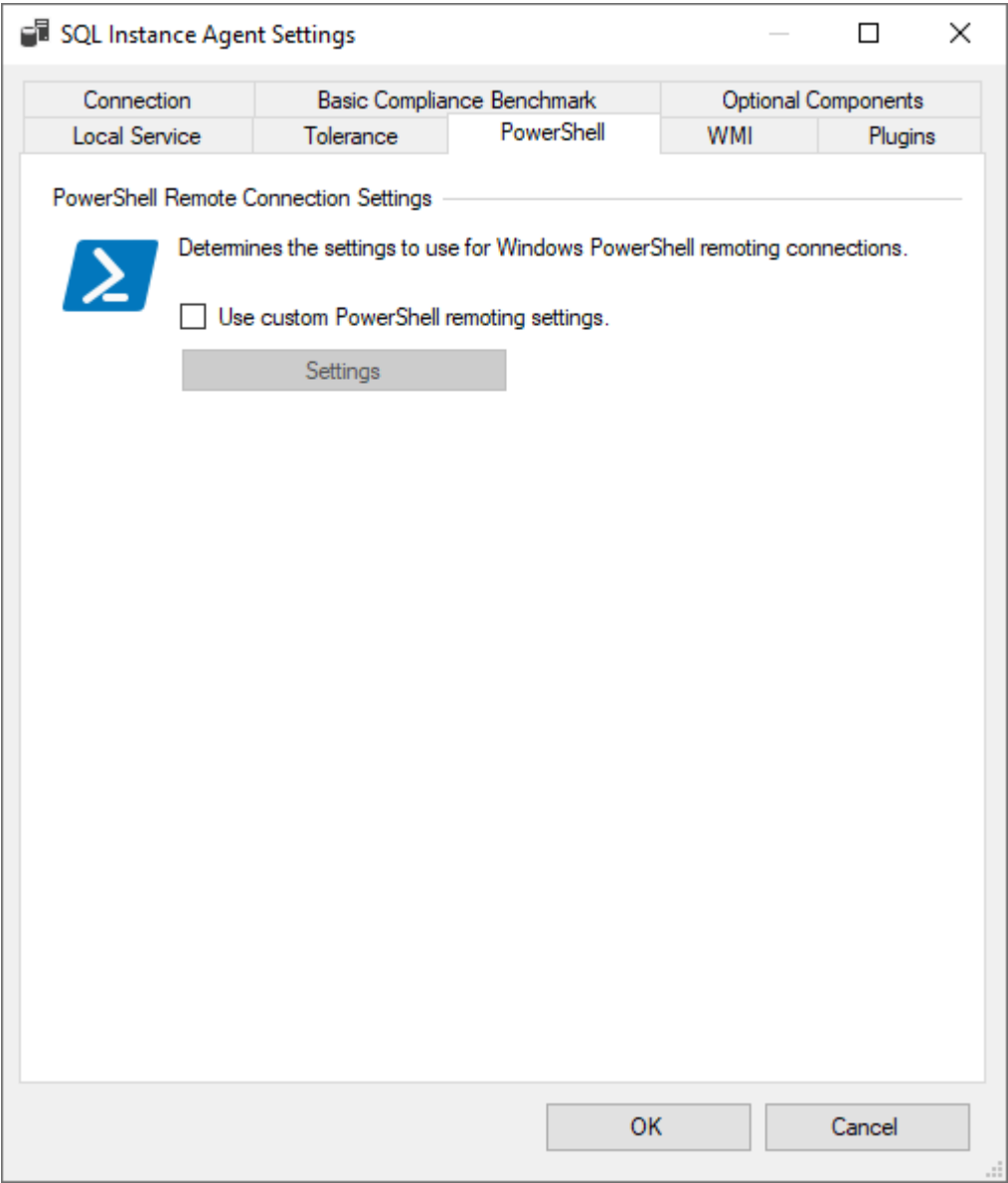
Determines whether the inability to read a database due to a permissions or other issue should be tolerated by the agent.

Sysadmin Role Membership

Determines whether the system should tolerate the user account performing the scan not having sysadmin role membership. Failure to have the required sysadmin rights may cause the SQL server instance to return limited information. This only applies to on-premises installations of SQL Server.

PowerShell

NOTE: PowerShell remoting is only used when reading [host information](#).



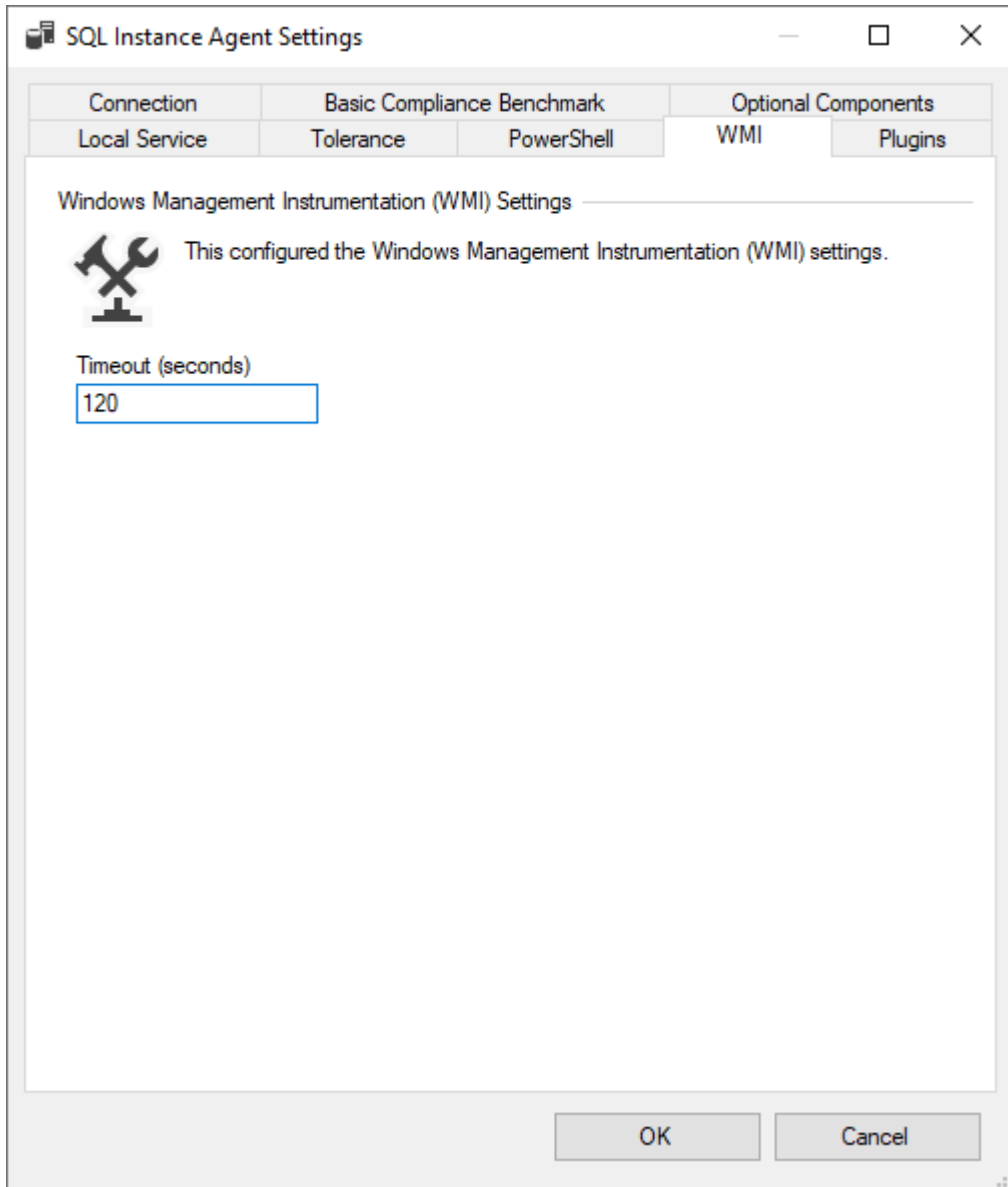
Use custom PowerShell remoting settings

Determines whether to use custom [PowerShell connection settings](#).

WMI

Determines the [Windows management instrumentation \(WMI\)](#) settings to use.

NOTE: [WMI](#) is only used when reading [host information](#) and [PowerShell remoting](#) is not available.



WMI Timeout

The timeout in seconds to use for WMI connections.

Item Identifiers

For more information about item identifiers see the [item identifiers](#) section.

Primary Identifier

The primary identifier is the SQL server or instance name for example CORPSQL or CORPSQL\Intranet depending on whether the instance is running as the default or named instance.

Secondary Identifier

For non-clustered on-premises installations of SQL Server the computer serial number is used, otherwise this identifier is not used. The host information [optional component](#) is required to gather the serial number, therefore changing host information setting can cause duplicate [items](#) to be created.

Tertiary Identifier

Not used.

Requirements

Supported Target Systems

The [SQL instance scan tasks](#) are supported on the following target systems:

- Microsoft Azure SQL Database
- SQL Server 2022
- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014
- SQL Server 2012
- SQL Server 2008 R2
- SQL Server 2008

Microsoft Azure SQL Database Access Settings

- Firewall access must allow access to the SQL port on the Microsoft Azure SQL Database by default 1433.
- The [service account](#) or [custom credentials](#) in use must have permissions to read the instance configuration and databases.
- When using either Azure Active Directory Password or Azure Active Directory Integrated [authentication](#) in the [settings](#), the [Microsoft Active Directory Authentication Library for Microsoft SQL Server](#) must be installed. This is automatically installed by [Microsoft SQL Server](#), and [Microsoft SQL Server Management Studio](#).

On-Premises Access Settings

The [SQL instance scan tasks](#) use the [SQL server management objects](#) to obtain information remotely from SQL instances, and either [WMI](#) or [PowerShell remoting](#) to obtain host information.

- Firewall access must allow access to the SQL port on the remote SQL instance - by default TCP/1433.
- To obtain [host information](#) such as manufacturer and serial number, firewall access must be permitted to the either [PowerShell remoting](#) or [WMI](#) ports on the remote machine.
- The [service account](#) or [custom credentials](#) must have administrator rights on the remote

machine to obtain [host information](#) using [WMI](#).

- The remote SQL instance must allow remote connections.
- The [service account](#) or [custom credentials](#) must have [sysadmin](#) access rights on the remote SQL Instance. This requirement can be overridden using the [tolerance settings](#).

Local Service

- ✓ The [SQL instance scan tasks](#) support the [local service](#).

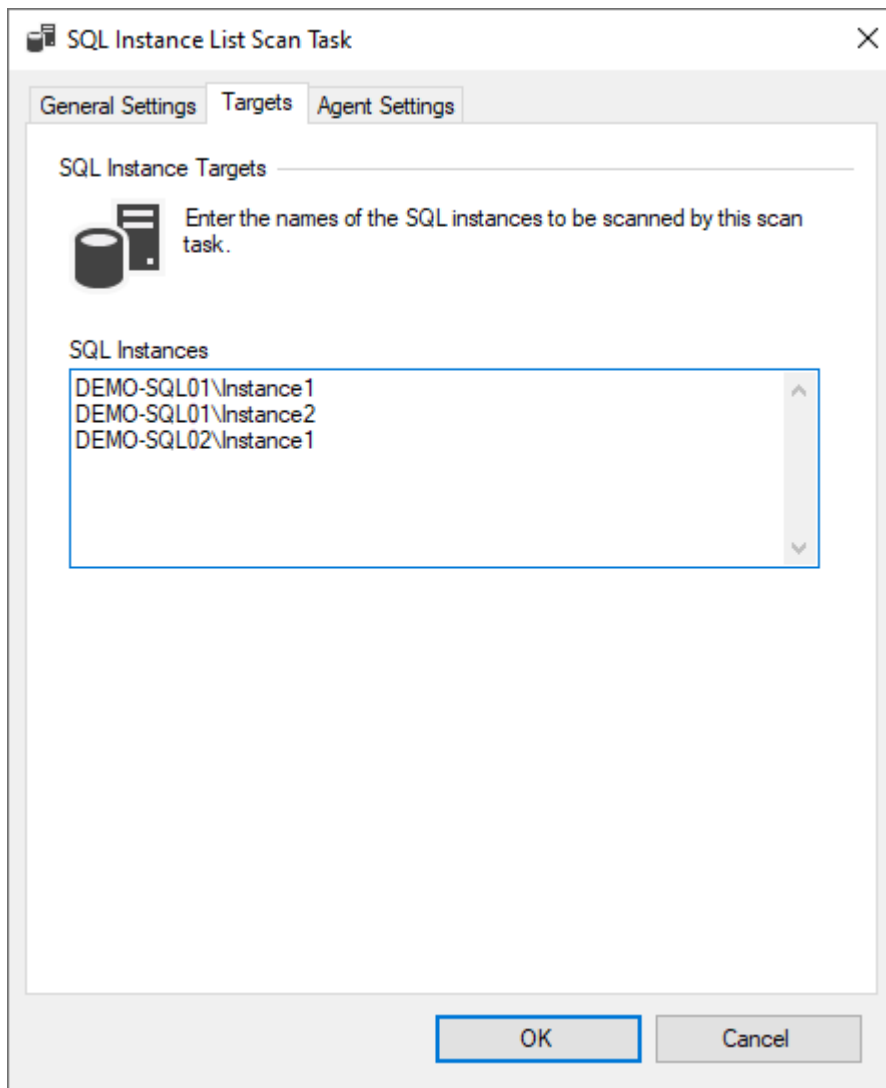
Automatic Detection

- ✓ SQL instances can be automatically detected and scanned by [Windows machine scan tasks](#).
- ✓ Clustered SQL instances can be automatically detected and scanned by [Microsoft failover cluster scan tasks](#).

SQL Instance List Scan Task

The SQL instance list task allows you to enter a list of [Microsoft SQL Server](#) on-premises installations and Microsoft Azure SQL databases to scan.

Targets



The screenshot shows a dialog box titled "SQL Instance List Scan Task" with a close button (X) in the top right corner. It has three tabs: "General Settings", "Targets", and "Agent Settings". The "Targets" tab is selected. Inside the tab, there is a section titled "SQL Instance Targets" with a sub-header "SQL Instance Targets" and a description: "Enter the names of the SQL instances to be scanned by this scan task." Below this is a list box labeled "SQL Instances" containing three entries: "DEMO-SQL01\Instance1", "DEMO-SQL01\Instance2", and "DEMO-SQL02\Instance1". At the bottom of the dialog are "OK" and "Cancel" buttons.

SQL Instance List Scan Task

General Settings Targets Agent Settings

SQL Instance Targets

Enter the names of the SQL instances to be scanned by this scan task.

SQL Instances

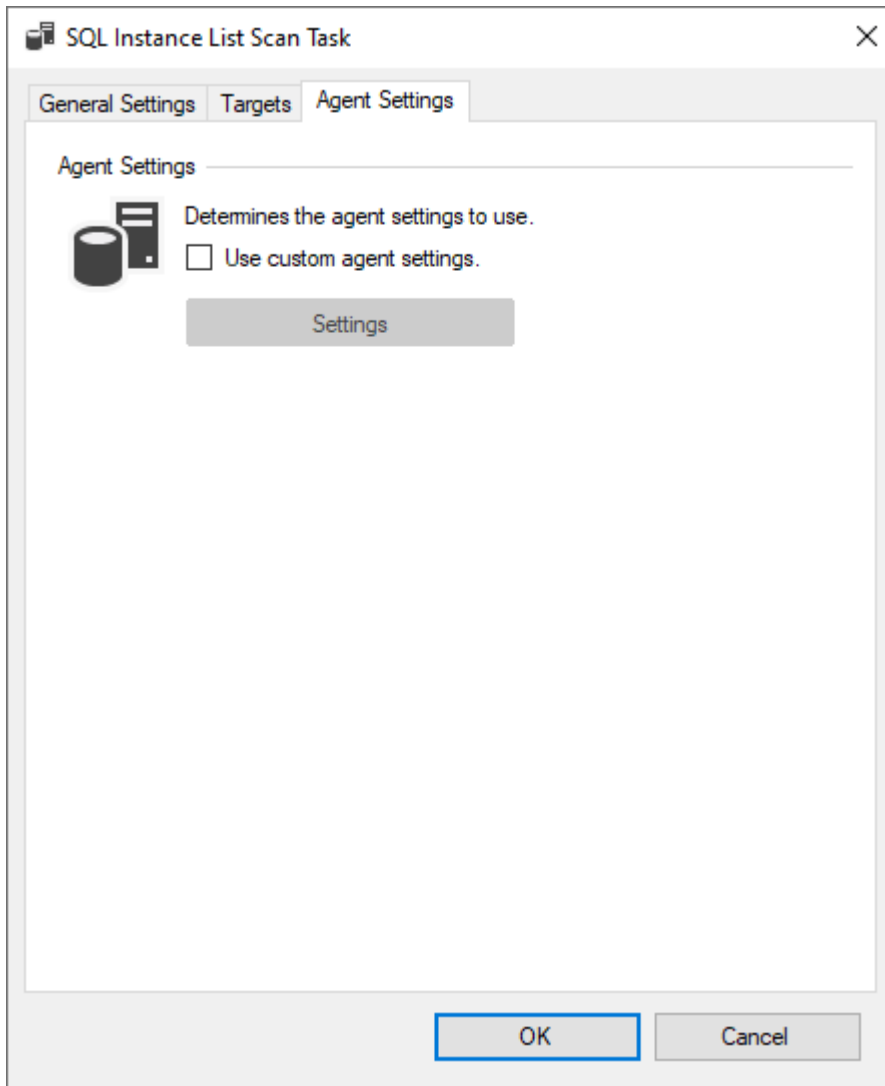
- DEMO-SQL01\Instance1
- DEMO-SQL01\Instance2
- DEMO-SQL02\Instance1

OK Cancel

SQL Instances

The names of the [SQL instances](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Could not connect to the SQL instance

Symptoms

When attempting to scan a remote [SQL Instance](#) you receive the following error.

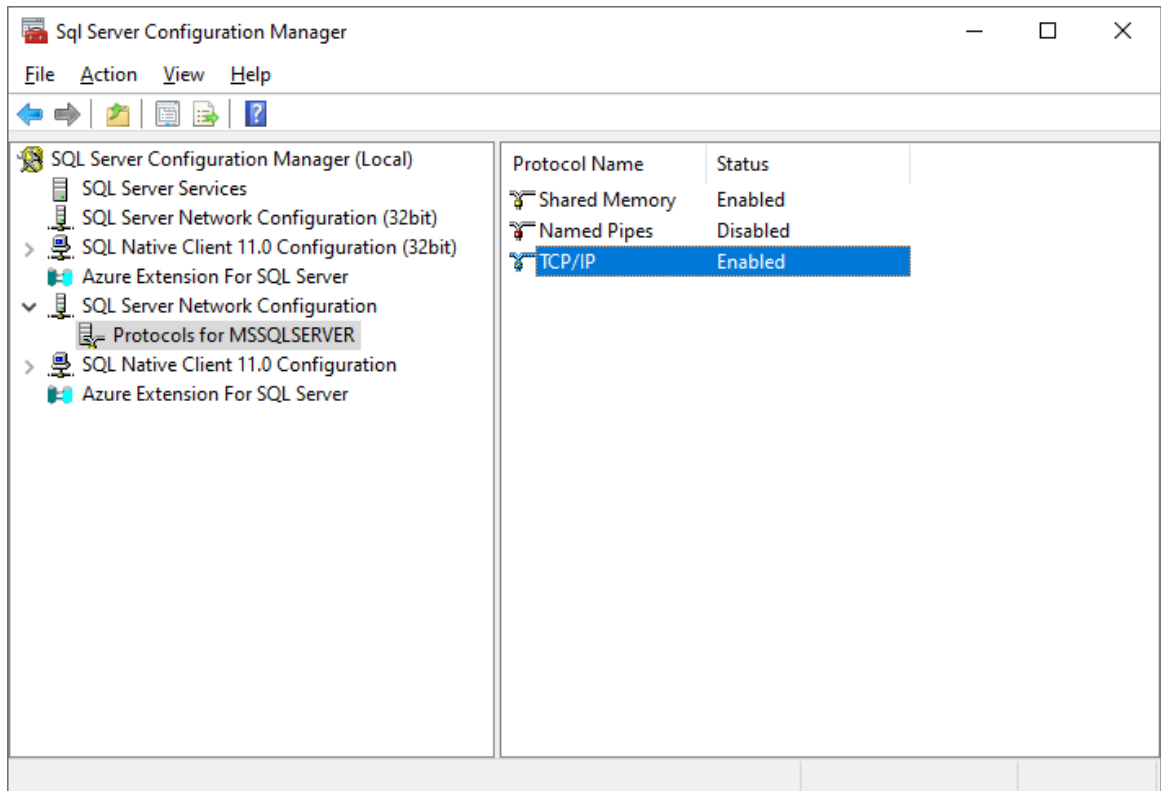
The SQL instance agent encountered an exception when 'Testing SMO access on instance "**Instance Name**". Could not connect to the SQL instance "**Instance Name**" via SQL XMO.

Cause

This error can be caused by several issues.

Resolution

- Ensure that the SQL instance is running
- Ensure that the name of the instance is correct - for example "CORP-SRV01" or "CORP-SRV01\SQLEXPRESS"
- Ensure that the SQL server is enabled for remote connections (see <http://support.microsoft.com/kb/914277> for more information).
 - On the SQL Server, open the [SQL Server Configuration Manager](#)
 - Select **SQL Server Network Configuration**
 - Select **Protocols for Instance Name**
 - *Ensure that the required protocols are enabled*



- Ensure that no firewalls are blocking the connection between the machine running the [XIA Configuration Client](#) and the SQL server.

Server doesn't support requested protocol

Symptoms

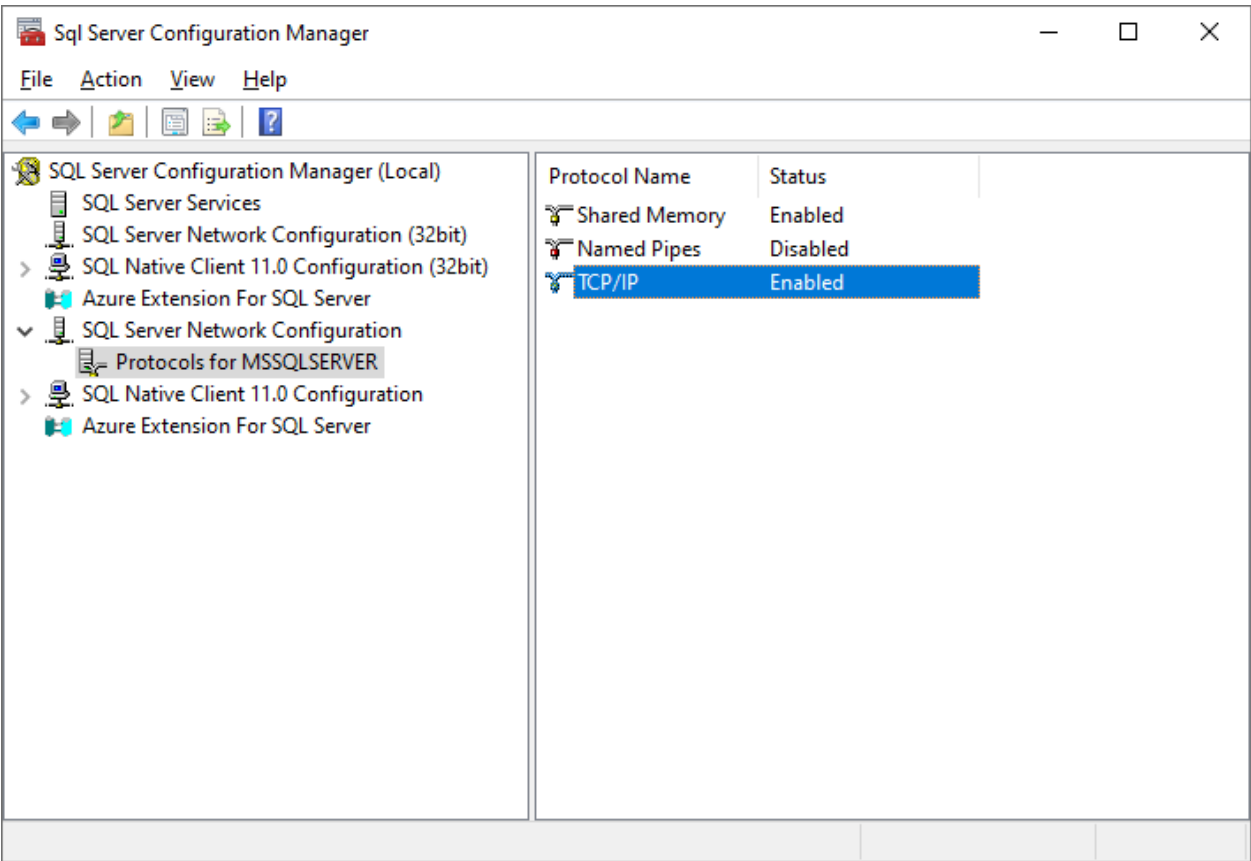
When attempting to scan a remote [SQL Instance](#) you receive the error "Server doesn't support requested protocol".

Cause

This error can be caused when the [SQL Instance](#) is not enabled for remote connections.

Resolution

- On the SQL Server, open the [SQL Server Configuration Manager](#)
- Select **SQL Server Network Configuration**
- Select **Protocols for *Instance Name***
- *Ensure that the required protocols are enabled*



Unable to load adalsql.dll

Symptoms

When attempting to scan a Microsoft Azure [SQL instance](#) you receive the following error.
Failed to connect to server *servername*. Unable to load adalsql.dll.

Cause

The [Microsoft Active Directory Authentication Library for Microsoft SQL Server](#) has not been installed.

Resolution

Download and install the [Microsoft Active Directory Authentication Library for Microsoft SQL Server](#).
For more information see the [requirements](#) section.

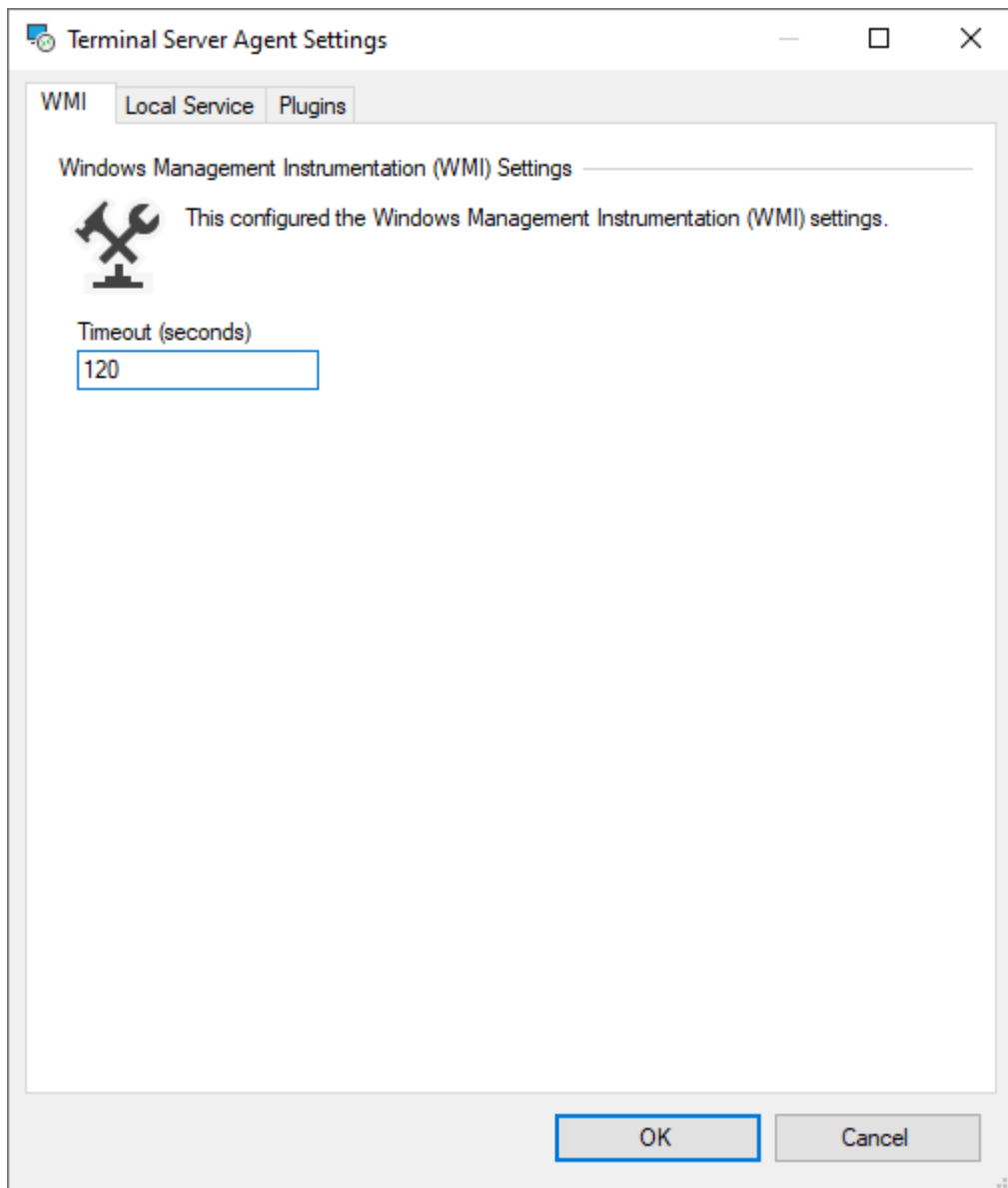
Terminal (RDP Session Host) Server

Terminal server scan tasks are able to document Microsoft Terminal Servers and Remote Desktop Session Hosts.

The data located by these tasks include the following information types:

- Connection (Session) Broker settings
- Connection settings including
- General Settings
- Logon Settings
- Client Settings
- Environment Settings
- Session Settings
- Remote Control Settings
- Client Settings
- Network Settings
- Security Permissions (Windows 2008 and above)
- RemoteApp application configuration

Agent Settings



WMI Timeout

The timeout in seconds to use for WMI connections.

Item Identifiers

For more information about item identifiers see the [item identifiers](#) section.

Primary Identifier

The primary identifier is the Terminal Server NetBIOS name - for example TERMSRV01.

Secondary Identifier

The secondary identifier is the serial number of the server.

Tertiary Identifier

Not used.

Requirements

Supported Target Systems

The Terminal Server scan tasks are supported on the following target systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

Access Settings

The Terminal Service scan tasks use a combination of WMI and the WinNT ADSI provider to obtain information remotely from Terminal Servers.

- Firewall access must allow access to the WMI ports on the remote machine
- Firewall access must allow access to the Server Service port on the remote terminal server.
- By default, the XIA Configuration client service account must have administrator rights on the remote machine (*this is a requirement for remote WMI access enforced by the operating system*)

Local Service

- ✓ These scan task(s) support and can be used with the XIA Local Service.

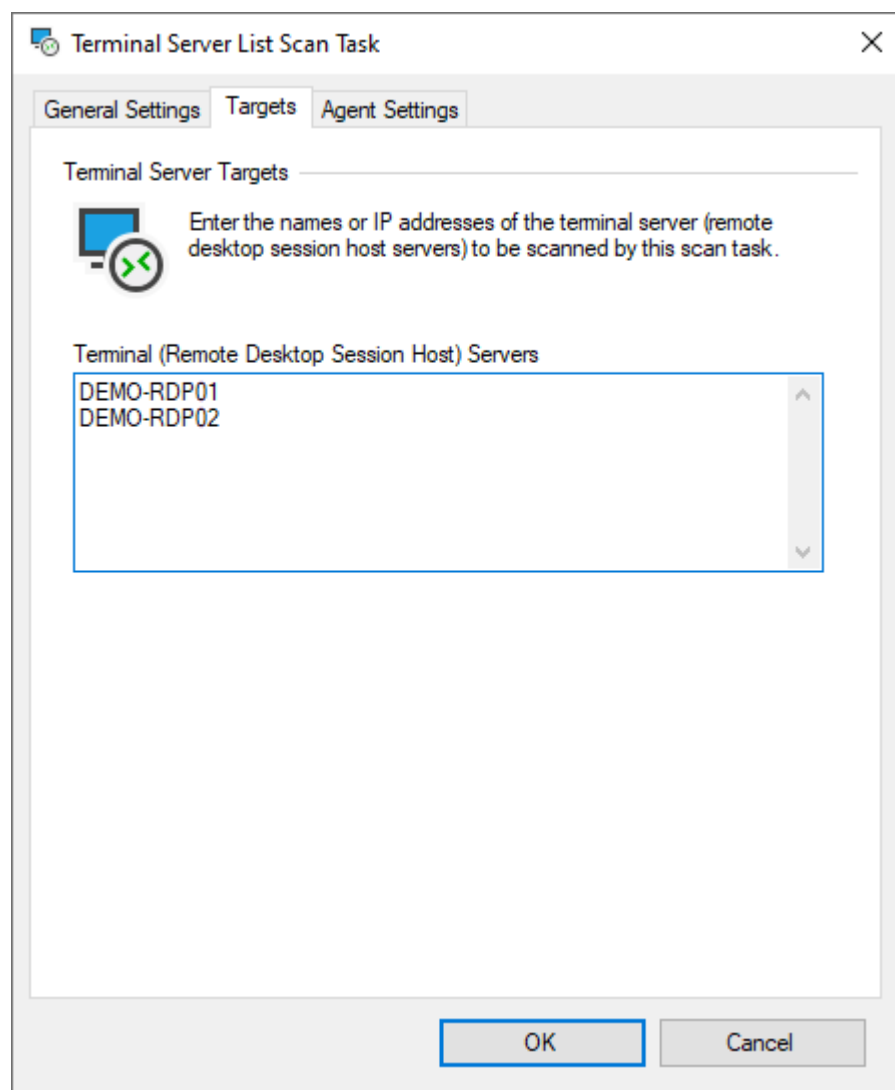
Automatic Detection

- ✓ Terminal Servers (Remote Desktop Session Hosts) are automatically detected and scanned by [Windows Machine Scan Tasks](#).

Terminal Server List Scan Task

The Terminal Server list task allows you to enter a list of Terminal Servers (Remote Desktop Session Hosts) that you wish to scan.

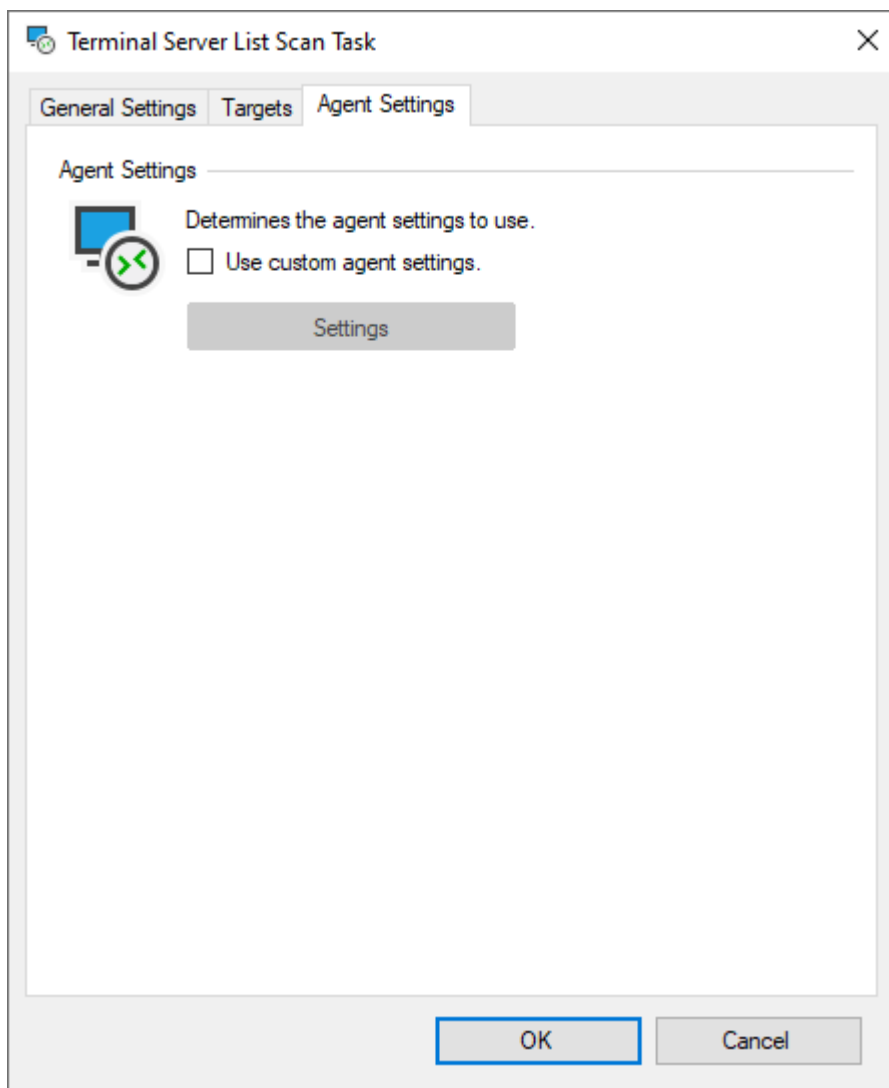
Targets



Terminal (Remote Desktop Session Host) Servers

The names of the [terminal \(remote desktop session host\) servers](#) to scan, one per line.

Agent Settings



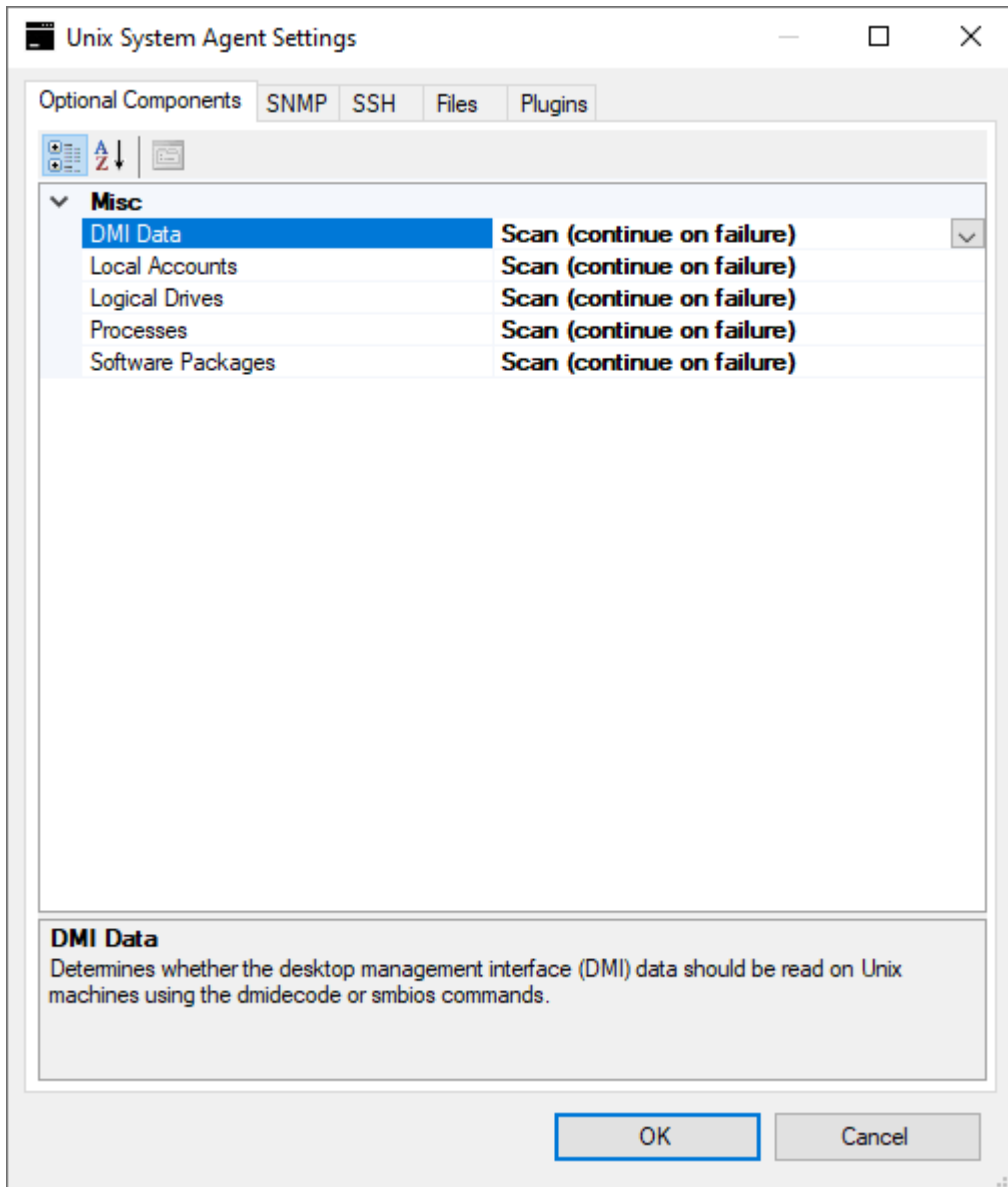
Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Unix System

Unix system scan tasks are able to document Unix and Linux platforms including [NetBSD](#), [Solaris](#), [Red Hat Enterprise Linux](#), [Ubuntu](#), [Fedora](#), and [Debian](#) using [SNMP](#) and [SSH](#).

Agent Settings



DMI Data

Determines whether the desktop management interface (DMI) data should be read on [Unix and Linux](#) based machines using the dmidecode or smbios commands. Desktop management interface (DMI) data includes manufacturer, model, serial number, asset tag, and motherboard information.

Local Accounts

Determines whether local user and group information should be read from the /etc/passwd file on [Unix and Linux](#) based systems. [SSH](#) must be enabled and configured for this information to be available.

Logical Drives

Determines whether logical drives should be read on [Unix and Linux](#) based machines.

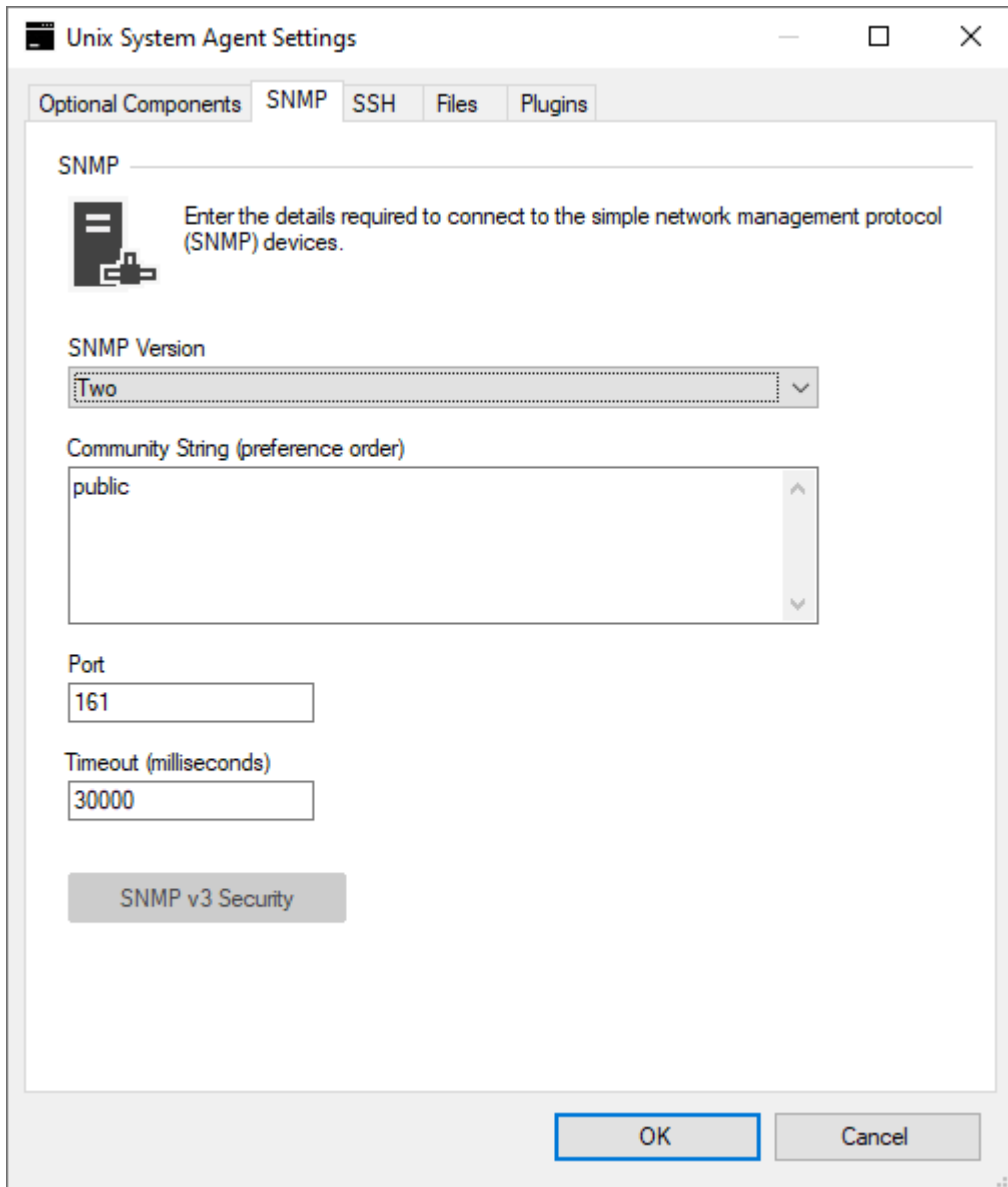
Processes

Determines whether running processes should be read from [Unix and Linux](#) based machines.

Software Packages

Determines whether software packages should be read from [Unix and Linux](#) based machines.

SNMP



The screenshot shows the 'Unix System Agent Settings' dialog box with the 'SNMP' tab selected. The dialog has a title bar with standard window controls. Below the title bar are tabs for 'Optional Components', 'SNMP', 'SSH', 'Files', and 'Plugins'. The 'SNMP' tab is active, displaying a section titled 'SNMP' with a sub-header 'Enter the details required to connect to the simple network management protocol (SNMP) devices.' and an icon of a server. The settings include a 'SNMP Version' dropdown menu set to 'Two', a 'Community String (preference order)' text field containing 'public', a 'Port' text field containing '161', and a 'Timeout (milliseconds)' text field containing '30000'. There is a button labeled 'SNMP v3 Security' and 'OK' and 'Cancel' buttons at the bottom right.

Unix System Agent Settings

Optional Components SNMP SSH Files Plugins

SNMP

Enter the details required to connect to the simple network management protocol (SNMP) devices.

SNMP Version

Two

Community String (preference order)

public

Port

161

Timeout (milliseconds)

30000

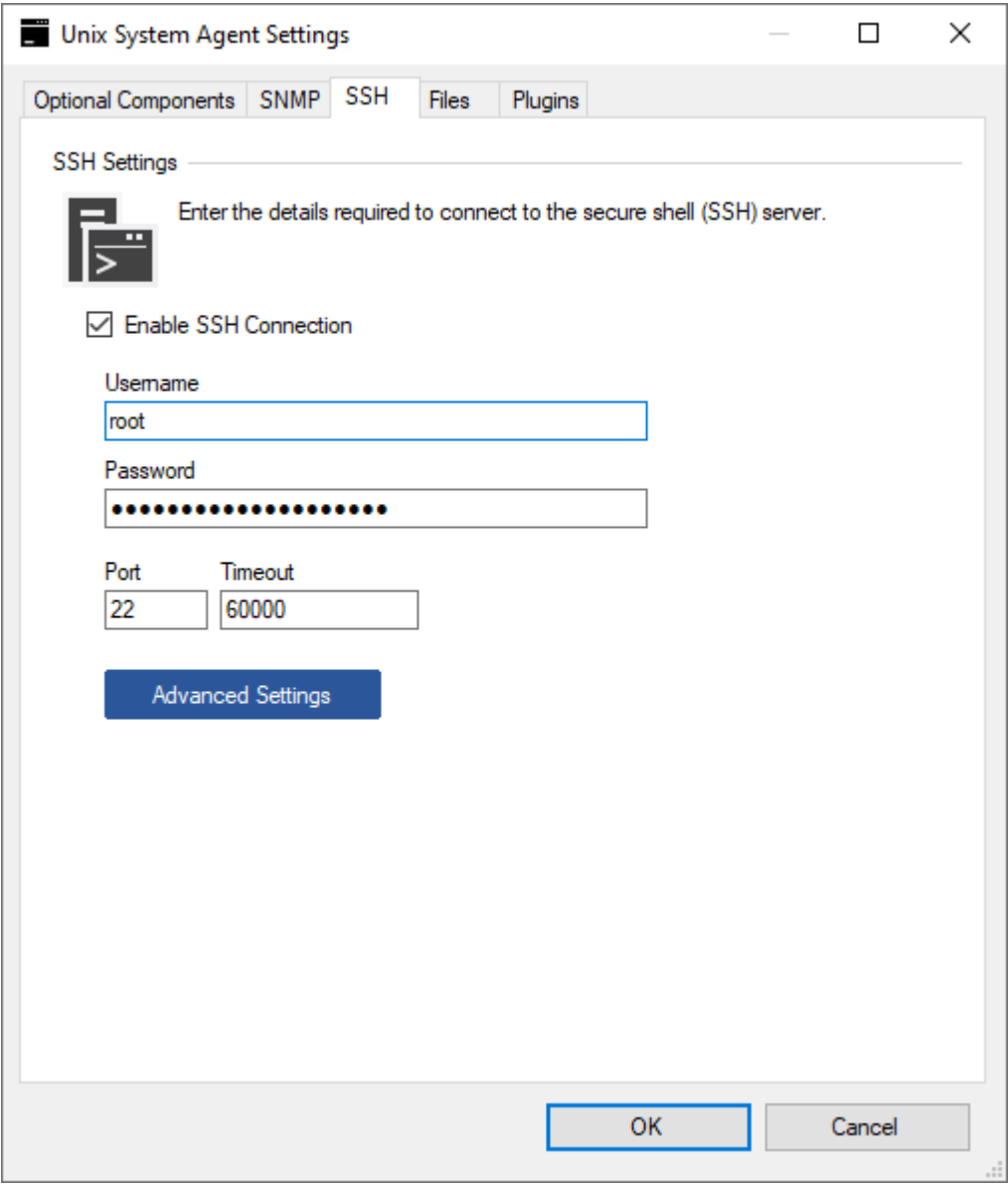
SNMP v3 Security

OK Cancel

SNMP

The [SNMP settings](#) for the [Unix system agent](#).

SSH

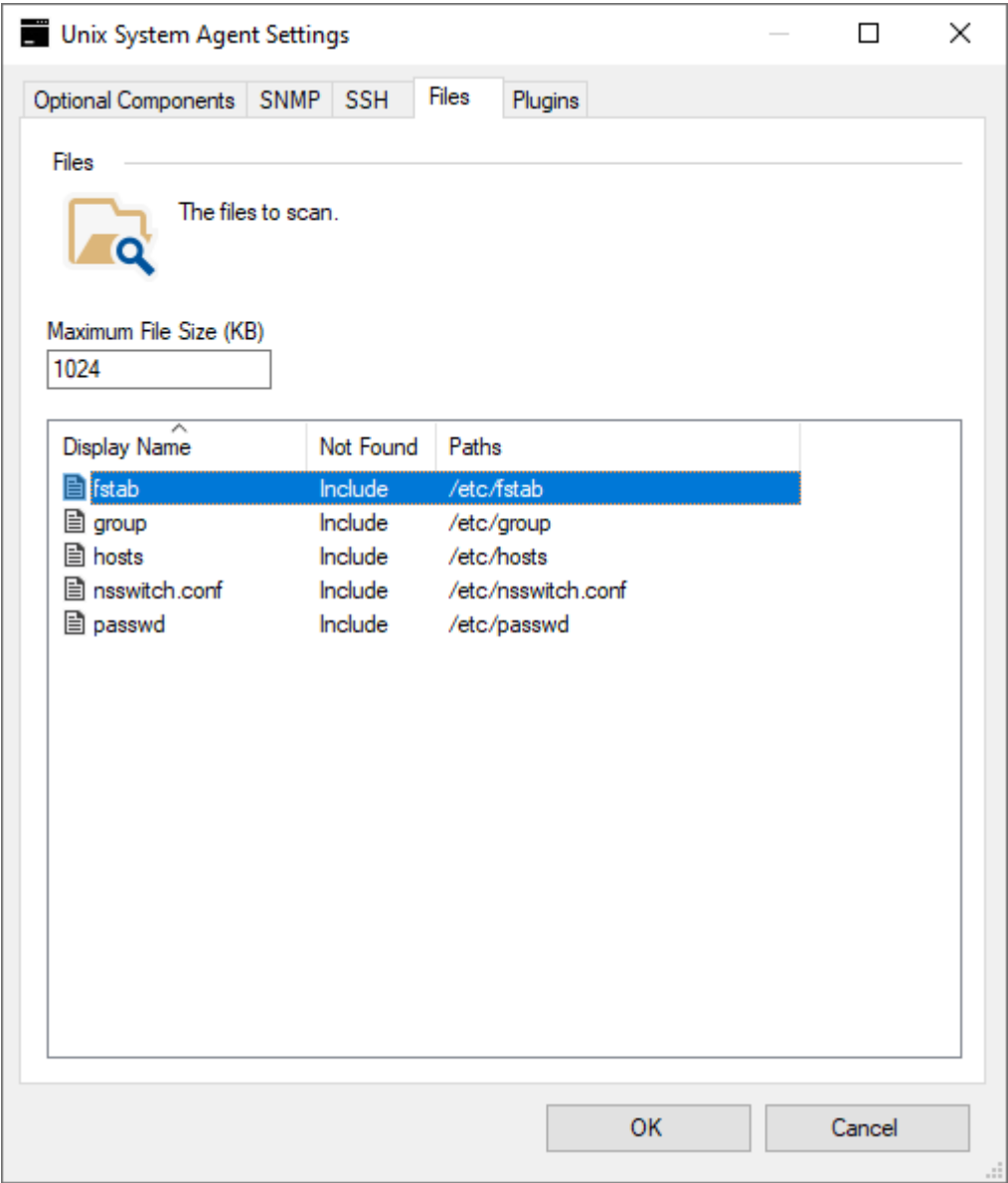


The SSH settings for the Unix System agent.

Files

Determines the files to scan on [Unix or Linux systems](#).

[SSH](#) must be enabled before files can be selected.



Maximum File Size (KB)

The maximum file size of files that can be scanned in kilobytes before an exception is thrown.

Display Name

The display name of the file

Not Found

The action to take if the file is not found.

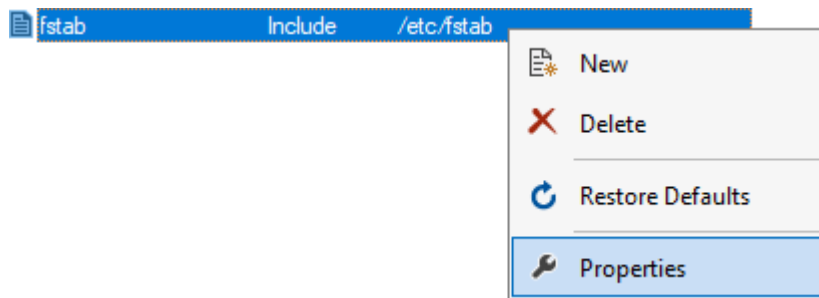
Paths

The possible paths of the file.

Right clicking the list of files displays the [context menu](#).

Context Menu

Right clicking a file in the [files](#) user interface displays the context menu.



New

Displays the [file settings](#) dialog to add a new [file](#) to scan.

Delete

Deletes the currently selected [file](#).

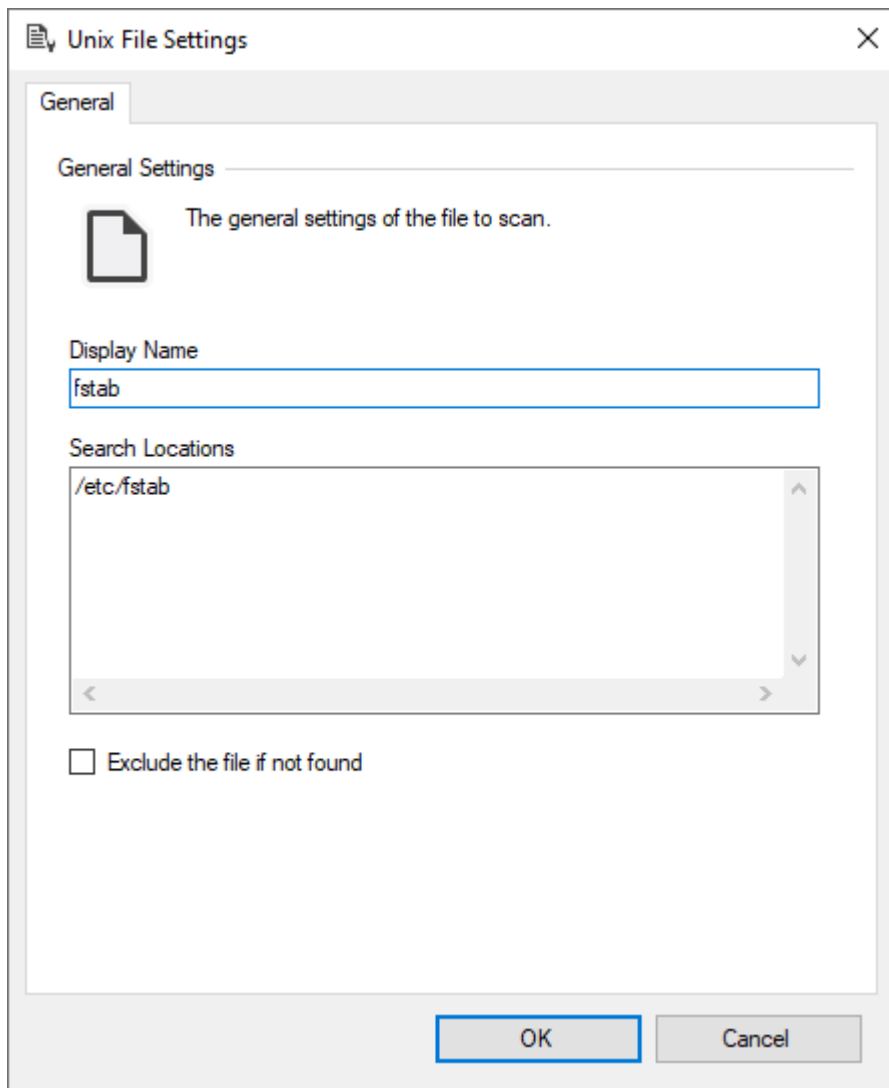
Restore Defaults

Restores the list of [files](#) to the defaults.

Properties

Displays the [file settings](#) dialog for the currently selected [file](#).

File Settings



The screenshot shows a window titled "Unix File Settings" with a close button (X) in the top right corner. The "General" tab is selected. Below the tab is a section titled "General Settings" with a document icon and the text "The general settings of the file to scan." Below this is a "Display Name" label followed by a text input field containing "fstab". Underneath is a "Search Locations" label followed by a list box containing "/etc/fstab". At the bottom left is an unchecked checkbox labeled "Exclude the file if not found". At the bottom right are "OK" and "Cancel" buttons.

Display Name

The display name for the file to scan - for example "Samba Configuration File" or "smb.conf".

Search Locations

The search locations for the file, one per line, in order of preference.

Exclude the file if not found

Determines whether the file should be excluded if it is not found in any of the specified search locations.

Item Identifiers

For more information about item identifiers see the [item identifiers](#) section.

Primary Identifier

The Unix system name.

Secondary Identifier

The MAC address of the primary network interface card, if available.

Tertiary Identifier

Not used.

Network Device Search Scan Task

For more information please see the [network device search scan task](#).

Requirements

Supported Target Systems

The [Unix systems](#) scan tasks are supported on both [Unix and Linux based systems](#).

Access Settings

The [Unix systems](#) scan tasks use a combination of [SNMP](#) and [SSH](#) to gather the information.

- [SNMP](#) must be installed and configured on the remote Unix machine.
- [SSH](#) must be installed and configured on the remote Unix machine for certain [optional components](#) such as local accounts to be collected.
- When using [SSH](#), appropriate credentials to access the required files on the remote Unix machine must be provided.
- To gather information such as manufacturer, model and serial number as well as BIOS and motherboard information [SSH](#) must be enabled, and dmidecode or smbios must be installed on the remote system.

NOTE: On Linux based systems (that use dmidecode) it is required that you use the root username and password or sudo can be used by following the instructions in

[Using a non-root account for dmidecode](#).

NOTE: Certain [Unix systems](#) may by default prevent the logging on as root which will be reported as "A supplied password or user name is incorrect." Please see the documentation for your [Unix system](#) for more information.

Firewall Access

- ✔ Firewalls should allow access to the [SNMP](#) port on the remote machine which is by default UDP/161.
- ✔ Firewalls can optionally allow access to the [SSH](#) port on the remote machine which is by default TCP/22.

Local Service

- ⬇ [Unix system](#) scan tasks cannot be used with the [local service](#).

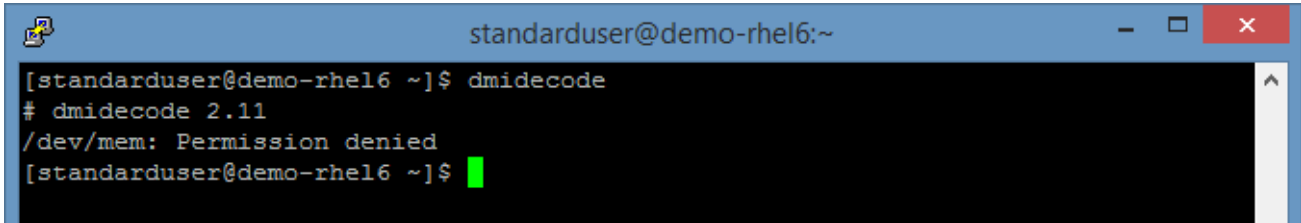
Automatic Detection

- ✔ Unix systems can be automatically detected and scanned by the [network device search scan task](#).

Using a non-root account for dmidecode

By default, the dmidecode command can only be run on [Unix systems](#) using the root user account.

Using a standard user account will display the following error
/dev/mem: Permission denied

A terminal window titled 'standarduser@demo-rhel6:~' showing the execution of the 'dmidecode' command. The output shows the version '# dmidecode 2.11' followed by the error message '/dev/mem: Permission denied'. The prompt returns to the user's shell.

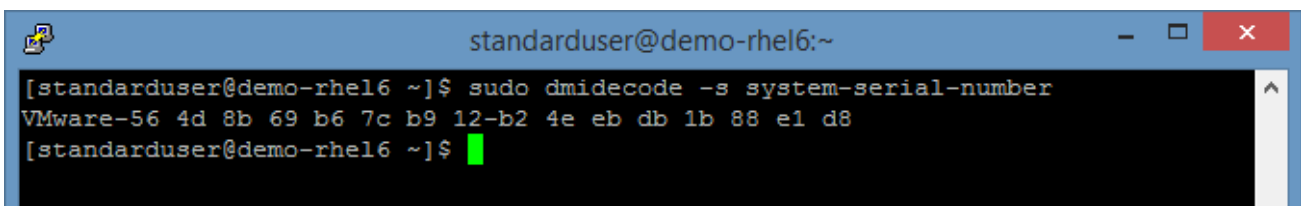
```
standarduser@demo-rhel6:~  
[standarduser@demo-rhel6 ~]$ dmidecode  
# dmidecode 2.11  
/dev/mem: Permission denied  
[standarduser@demo-rhel6 ~]$
```

To allow a non-root account to execute the dmidecode application the following steps must be completed.

- Select an existing account, or create a new dedicated user account on the [Unix systems](#).
- Open the *sudoers* configuration file - typically */etc/sudoers*.
- Add the following settings to the sudoers file

```
User_Alias XIACONFIGURATION = username  
Cmnd_Alias DMIDECODE = /usr/sbin/dmidecode  
XIACONFIGURATION ALL = NOPASSWD: DMIDECODE
```

The non-root user should now be able to execute the dmidecode command without being prompted for a password.

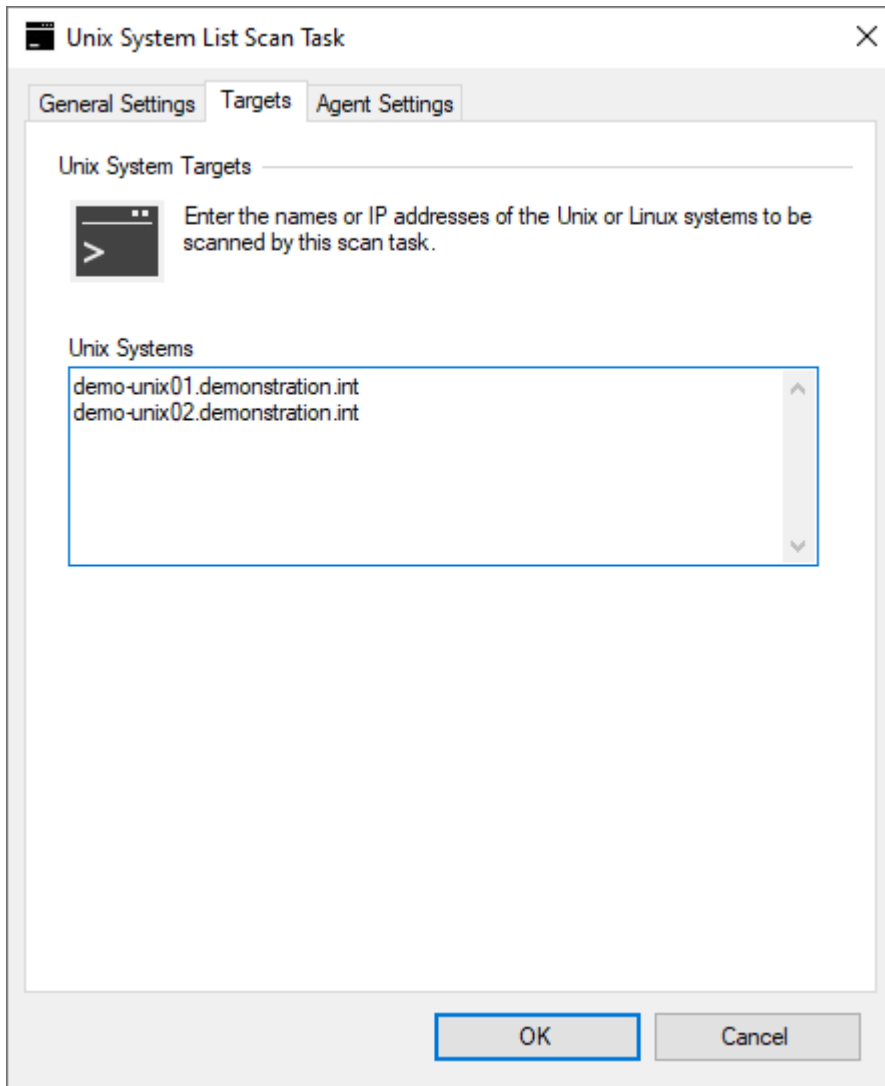
A terminal window titled 'standarduser@demo-rhel6:~' showing the execution of the command 'sudo dmidecode -s system-serial-number'. The output displays the system serial number in hexadecimal format: 'VMware-56 4d 8b 69 b6 7c b9 12-b2 4e eb db 1b 88 e1 d8'. The prompt returns to the user's shell.

```
standarduser@demo-rhel6:~  
[standarduser@demo-rhel6 ~]$ sudo dmidecode -s system-serial-number  
VMware-56 4d 8b 69 b6 7c b9 12-b2 4e eb db 1b 88 e1 d8  
[standarduser@demo-rhel6 ~]$
```

Unix System List Scan Task

The Unix system list task allows you to enter a list of [Unix or Linux systems](#) that you wish to scan by name or IP address.

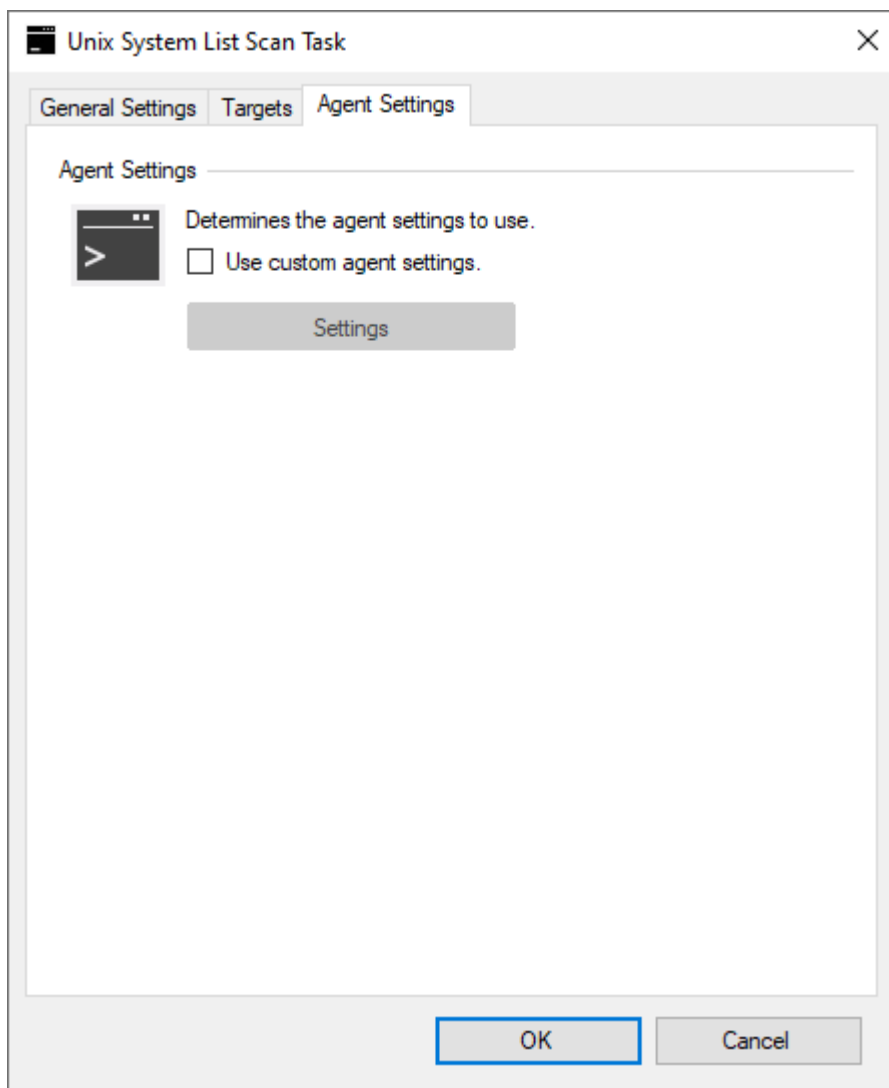
Targets



Unix Systems

The IP addresses or fully qualified domain names of the [Unix systems](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Troubleshooting

This section highlights the known issues for the [Unix system](#) agent and provides details of the solutions.

Error executing command 'dmidecode'

Symptoms

When you scan a [Unix system](#) and have [SSH](#) enabled, you may see the error Error executing command 'dmidecode -s system-manufacturer'. Executing the sudo command failed for user '*username*'. Please ensure that the user is configured for sudo.

Cause

This error can be seen when the Unix system has the dmidecode application installed and the [SSH](#) user account is not root, and has not been configured for sudo.

More Information

The dmidecode application requires root level permissions.

Resolution

The resolution is described in the [using a non-root account for dmidecode](#) section.

Information is missing or not available

Issue

When scanning a [Unix or Linux system](#) much of the information found is blank.

Cause

When [SNMP](#) is installed on certain distributions the default configuration file limits the data accessible to the system [SNMP](#) node (1.3.6.1.2.1) that contains basic information such as the system description and object identifier. Access to other SNMP information is prohibited.

A terminal window titled 'standarduser@demo-rhel6:~' with standard window controls. The terminal displays the following text:

```
group    notConfigGroup v2c          notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#      name          incl/excl      subtree      mask(optional)
view    systemview    included    .1.3.6.1.2.1
view    systemview    included    .1.3.6.1.2.1.25.1.1
```

The words 'systemview' in the last two lines are highlighted in yellow.

Resolution

Configure the [SNMP](#) configuration file which is typically */etc/snmp/snmpd.conf* with the appropriate security settings.

For more information please see the `snmpd` man pages for your specific distribution.

Software packages are not detected on Ubuntu

Issue

When scanning an [Ubuntu Linux](#) machine software packages are not detected.

Cause

This can be caused by the [SNMP](#) configuration being set such that the information is not available through [SNMP](#).

Resolution

Review and follow the instructions in the [information missing or not available](#) section.

VMware System

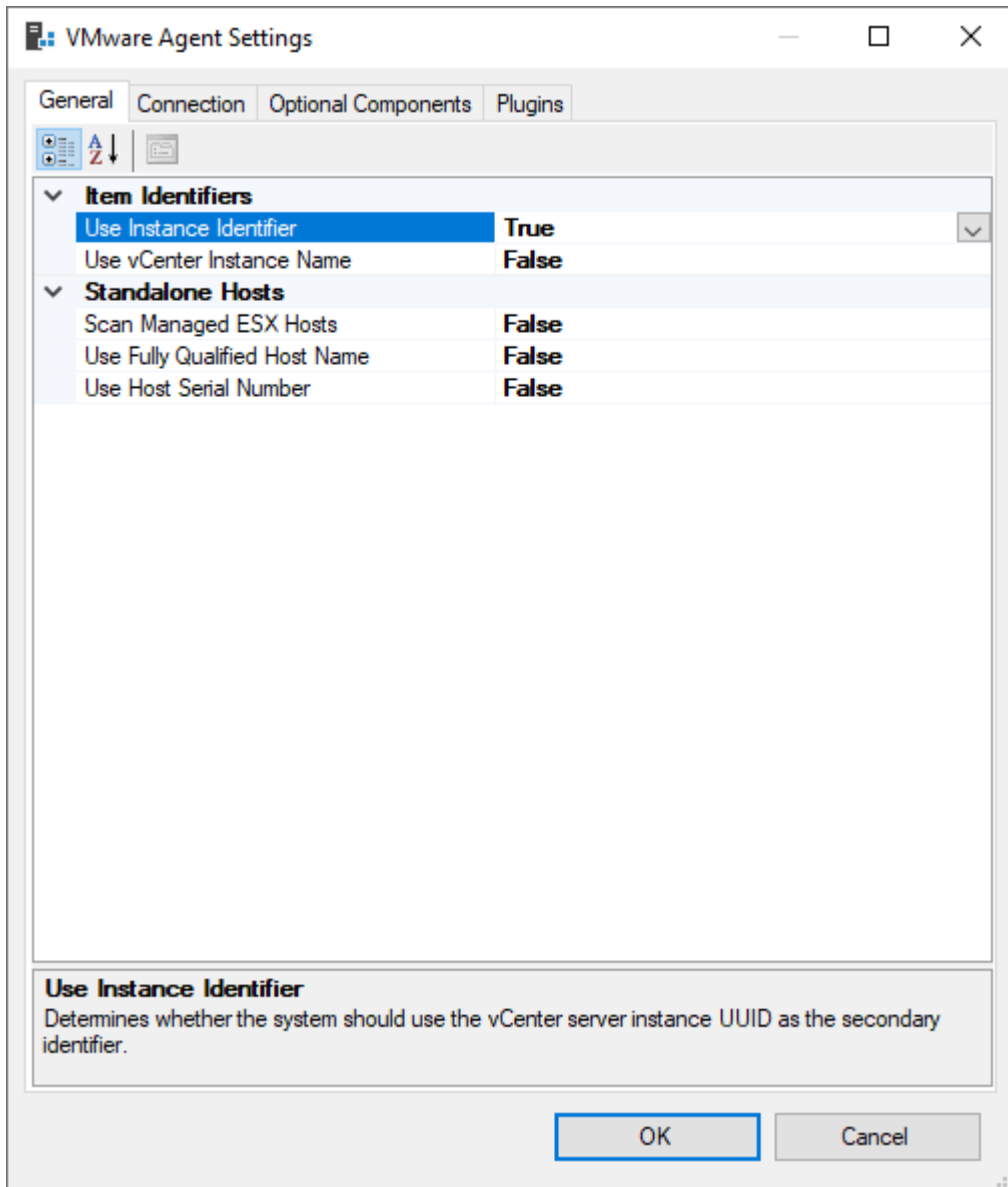
Overview

VMware scan tasks are able to document both VMware standalone hosts and entire [vCenter systems](#).

The data located by these tasks include the following information types:

- Clusters
- Datastores
- Datastore Clusters
- Distributed Switches
- Host Systems
- Virtual Machines
- Resource Pools
- vCenter Configuration
- Security Permissions

Agent Settings



Use Instance Identifier *

Determines whether the system should use the vCenter server instance UUID as the [secondary identifier](#). This allows multiple vCenter servers with the same name to be documented within [XIA Configuration Server](#).

This setting only applies when scanning vCenter servers.

Use vCenter Instance Name *

Determines whether the system should use the vCenter instance name as the item name and [primary identifier](#). This name format is then used for both the display name and the Primary Identifier when scanning vCenter servers.

Scan Managed ESX Hosts

Determines whether ESX hosts can be scanned directly even when they are managed by a vCenter server. It is recommended however to always document the vCenter server rather than individual managed ESX hosts.

Use Fully Qualified Host Name *

Determines whether the VMware system should be documented using its FQDN (if available) rather than hostname. This name format is then used for both the display name and the [primary identifier](#) when scanning ESX hosts directly.

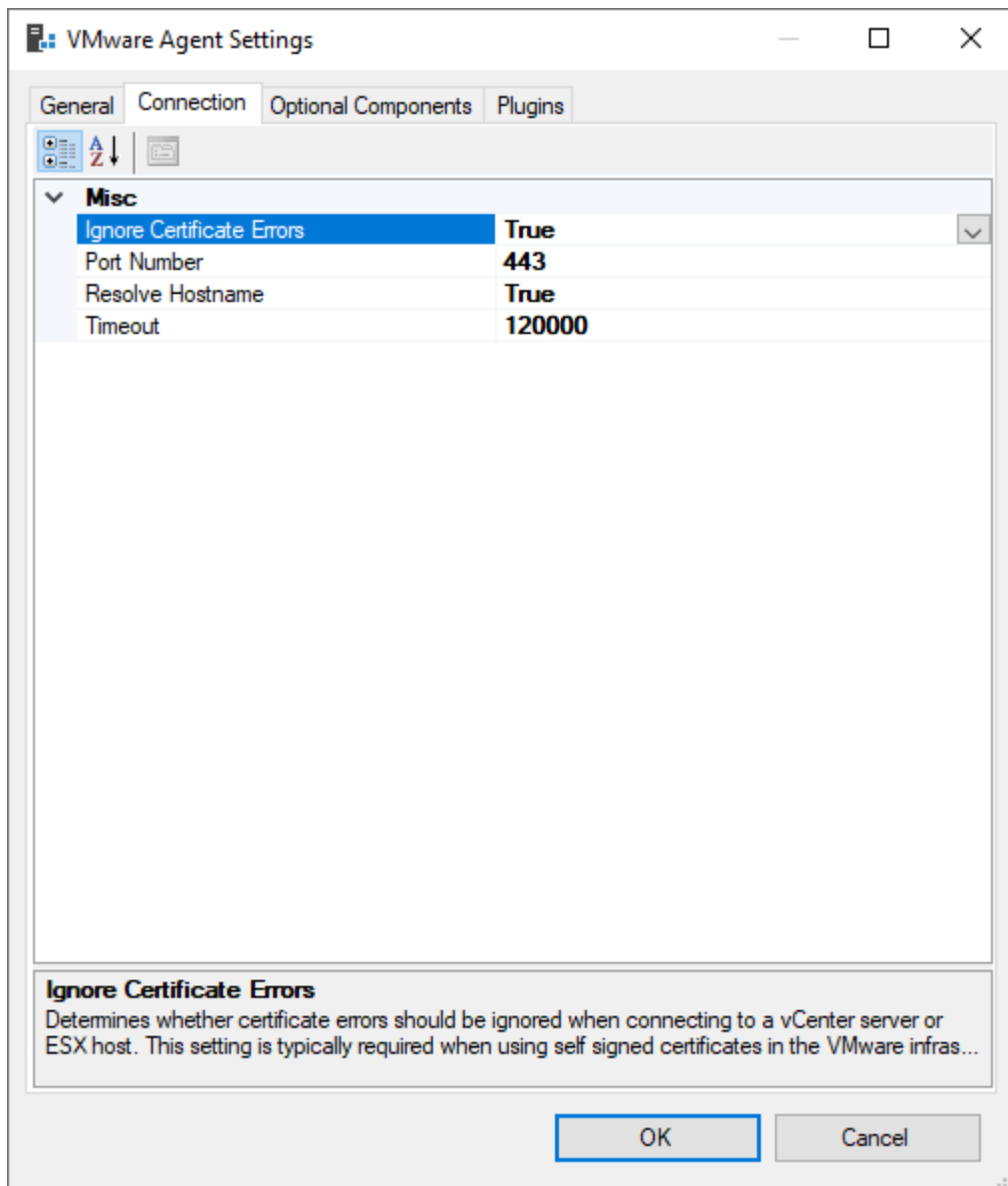
Use Host Serial Number *

Determines whether the system should use the host's serial number as the [secondary identifier](#). This allows multiple stand-alone ESX host servers with the same name to be documented within [XIA Configuration Server](#).

This setting only applies when scanning stand-alone ESX hosts directly.

* Changes to the item identifiers configuration for existing items will cause new items to be created.

Connection



Ignore Certificate Errors

Determines whether the system should ignore certificate errors when connecting to the remote system.

Port Number

The port number to use for the HTTPS connection, by default this is 443.

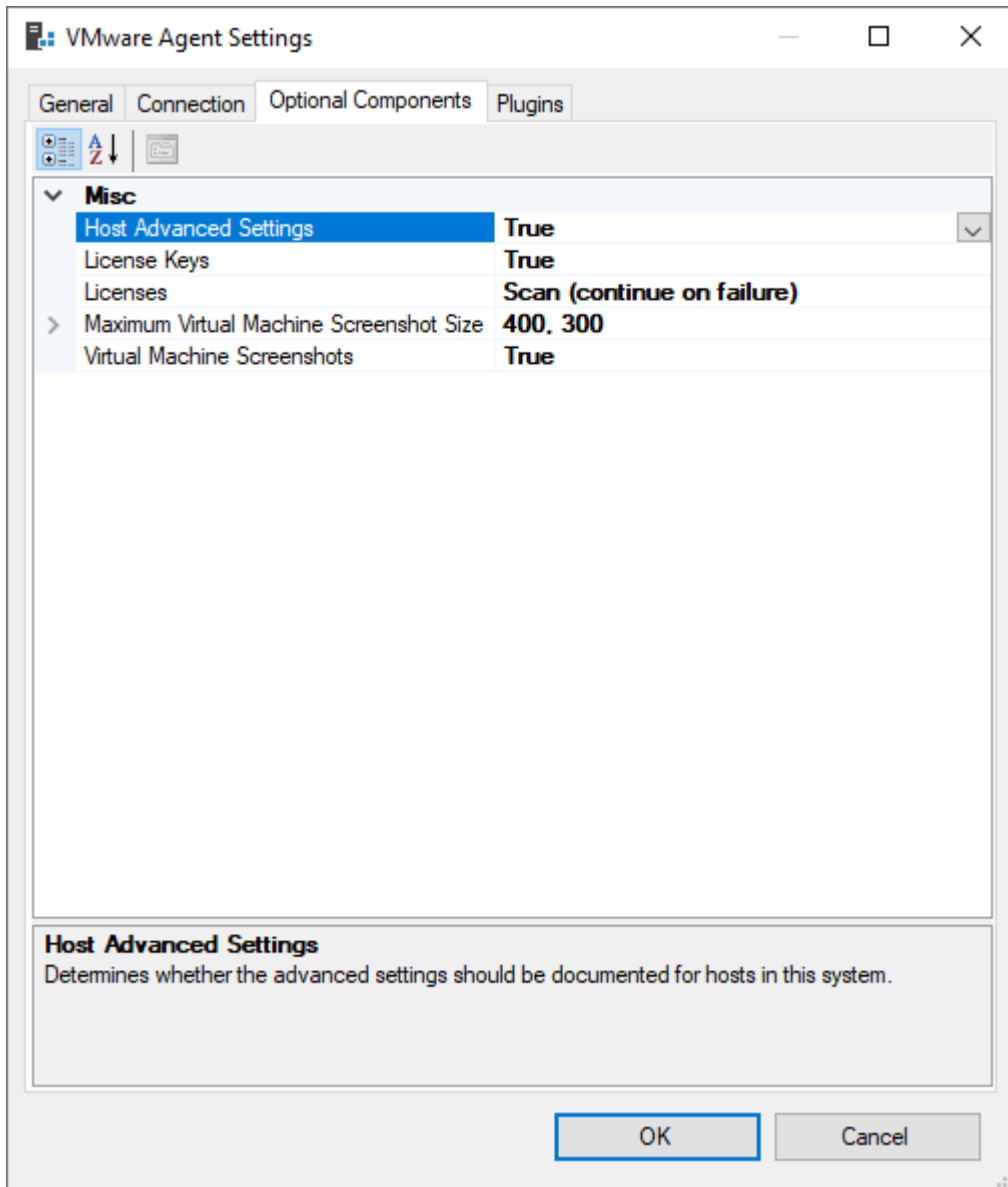
Resolve Hostname

Determines whether the specified hostname for the ESX or vCenter should be resolved. This setting should be enabled unless an IP address is entered that cannot be resolved.

Timeout

The timeout setting to use when communicating with the remote system in milliseconds.

Optional Components



Host Advanced Settings

Determines whether the advanced settings should be documented for hosts. By default, this is enabled however disabling this option can greatly reduce the size of the scan data created by the client.

License Keys

Determines whether individual license keys should be read from the system. This setting only applies to vCenter server when the **Licenses** option is enabled.

Licenses

Determines whether license information should be read from the system. This setting only applies to vCenter server.

Maximum Virtual Machine Screenshot Size

Determines the maximum screenshot size to capture from guest machines. This setting only applies

when **Virtual Machine Screenshots** is enabled.

Virtual Machine Screenshots

Determines whether screenshots should be captured from running virtual machines. This setting applies to vCenter server v5.1 and above only and when custom credentials are configured on the [credentials tab](#).

Item Identifiers

For more information about item identifiers please see the [item identifiers](#) section.

Primary Identifier

The VMware system name - for more information see the [agent settings](#).

Secondary Identifier

Not used by default

- The vCenter server instance identifier can be used when "Use Instance Identifier" is enabled in the [agent settings](#).
- The host serial number can be used when the "Use Host Serial Number" setting is enabled in the [agent settings](#).

Tertiary Identifier

Not used

In addition to the [VMware system](#) items that are created [VMware Physical ESX Host](#) items are also created from the same data. These items will use the following item identifiers.

Primary Identifier

The fully qualified domain name (FQDN) of the [VMware Physical ESX Host](#).

Secondary Identifier

The serial number of the [VMware Physical ESX Host](#).

Tertiary Identifier

Not used

Requirements

Supported Target Systems

The scan tasks are supported on the following target systems

- VMware vCenter and ESXi 8.0
- VMware vCenter and ESXi 7.0
- VMware vCenter and ESXi 6.7
- VMware vCenter and ESXi 6.5
- VMware vCenter and ESXi 6.0
- VMware vCenter and ESXi 5.5
- VMware vCenter and ESXi 5.1
- VMware vCenter and ESXi 5.0
- VMware vCenter and ESXi 4.0
- VMware vCenter 2.5 and ESXi 3

Access Settings

The VMware system scan tasks use the VMware VI SDK to communicate with both standalone ESX hosts and Virtual Center.

- Firewall access must allow access to the VI SDK on the remote ESX Host or Virtual Center. Typically, this is port 443 (HTTPS).
- Credentials must be provided for the remote system that have **read-only permissions** and the ability to read licenses.

Local Service

 These scan tasks are not supported for use with the XIA Local Service.

Automatic Detection

 vCenter servers hosted on [Windows machines](#) are automatically detected and scanned by [Windows machine scan tasks](#) unmanaged (standalone) ESX hosts are not automatically detected.

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Cannot complete login due to an incorrect user name or password

Issue

When scanning a [VMware system](#) a "Cannot complete login due to an incorrect user name or password" error is seen at the start of the scan.

Cause

This error can occur when

- **Default Credentials** are selected on the [credentials tab](#), and the computer running the [XIA Configuration Client](#) is a domain controller.
- **Default Credentials** are selected on the [credentials tab](#), but the Active Directory domain to which the user account belongs is not configured within the Single Sign On (SSO) configuration within vCenter server.
- The user name or password entered is incorrect.
- The account is locked out, or disabled.

Resolution

- When using **Default Credentials**, ensure that the [XIA Configuration Client](#) is installed on a computer that is **not** a domain controller, or switch to custom credentials.
- Review the Active Directory Identity Sources within the Single Sign On (SSO) configuration. More information can be found in the knowledge base article [2035510](#).
- Ensure that the username and password are entered correctly.
- Ensure that the account is enabled and not locked out in Active Directory.

Duplicate VMware system items are created

Issue

After scanning a [VMware system](#) a new item is created in the [XIA Configuration Server](#) interface, even though the VMware system already exists.

Cause

- The configuration of the [item identifiers](#) has been changed in the configuration.

Resolution

- Compare the [item identifiers](#) seen in the [client information](#) on both [VMware systems](#).
- View the VMware system [agent settings](#) and correct the configuration as needed.

More Information

Additional configuration options were added in [XIA Configuration Server](#) version 8.1 that allow for two vCenter servers or ESX hosts with the same name to be differentiated in the system.

Screenshots are not collected for guest machines

Issue

When scanning a [VMware system](#) the scan is completed successfully but no screenshots are collected for the guest virtual machines.

Cause

- **Default Credentials** are selected on the [credentials tab](#), guest screenshots are only available when custom credentials are used.
- The screenshots option is disabled in the [optional components tab](#).
- The virtual machine is not powered on.

Resolution

- Ensure that **custom credentials** are selected on the [credentials tab](#).
- Ensure that the screenshots option is enabled in the [optional components tab](#).
- Ensure that the virtual machine is powered on.

SSPI authentication error - The return code was '-2146893053'

Issue

When scanning a [VMware system](#) the following error is seen
Error initializing the security context. The return code was '-2146893053'.

Cause

This error can be seen when the "Use Default Credentials" setting is configured on the [credentials tab](#) and an IP address or other invalid name was used for the vCenter server.

Resolution

Use the fully qualified domain name of the vCenter server to be scanned

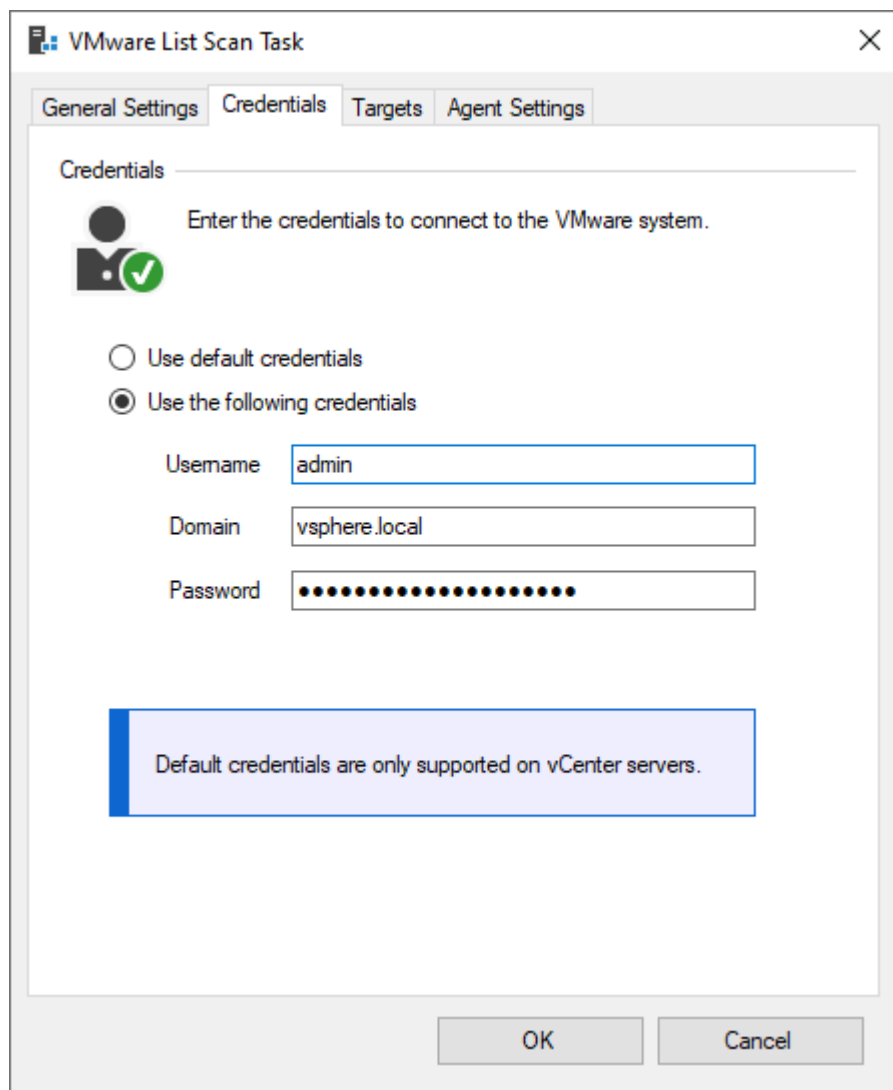
- or -

Manually enter valid credentials on the [credentials tab](#).

VMware System List Scan Task

The VMware List task allows you to enter a list of host names or IP addresses of the [VMware systems](#) (either standalone ESX hosts or vCenter servers) that you wish to scan.

Credentials



The screenshot shows the 'VMware List Scan Task' dialog box with the 'Credentials' tab selected. The dialog has four tabs: 'General Settings', 'Credentials', 'Targets', and 'Agent Settings'. The 'Credentials' tab contains a section titled 'Credentials' with a sub-header 'Enter the credentials to connect to the VMware system.' Below this is a radio button selection: 'Use default credentials' (unselected) and 'Use the following credentials' (selected). Under 'Use the following credentials', there are three input fields: 'Username' with the value 'admin', 'Domain' with the value 'vsphere.local', and 'Password' with a masked password represented by dots. At the bottom of the dialog are 'OK' and 'Cancel' buttons. A blue informational box at the bottom of the main content area states: 'Default credentials are only supported on vCenter servers.'

Use Default Credentials

The service account credentials (or custom credentials set on the [Credentials](#) tab of the scan profile) are used to connect to the vCenter server.

- Default credentials are only supported when connecting to vCenter server on Windows, or a vCenter server appliance.
- Default credentials are **not** supported when connecting to a stand-alone ESX host.
- Default credentials are **not** supported when the [XIA Configuration Client](#) is installed on a domain controller.

Use Specific Credentials

Determines the credentials to use when connecting to a vCenter server or standalone ESX host.

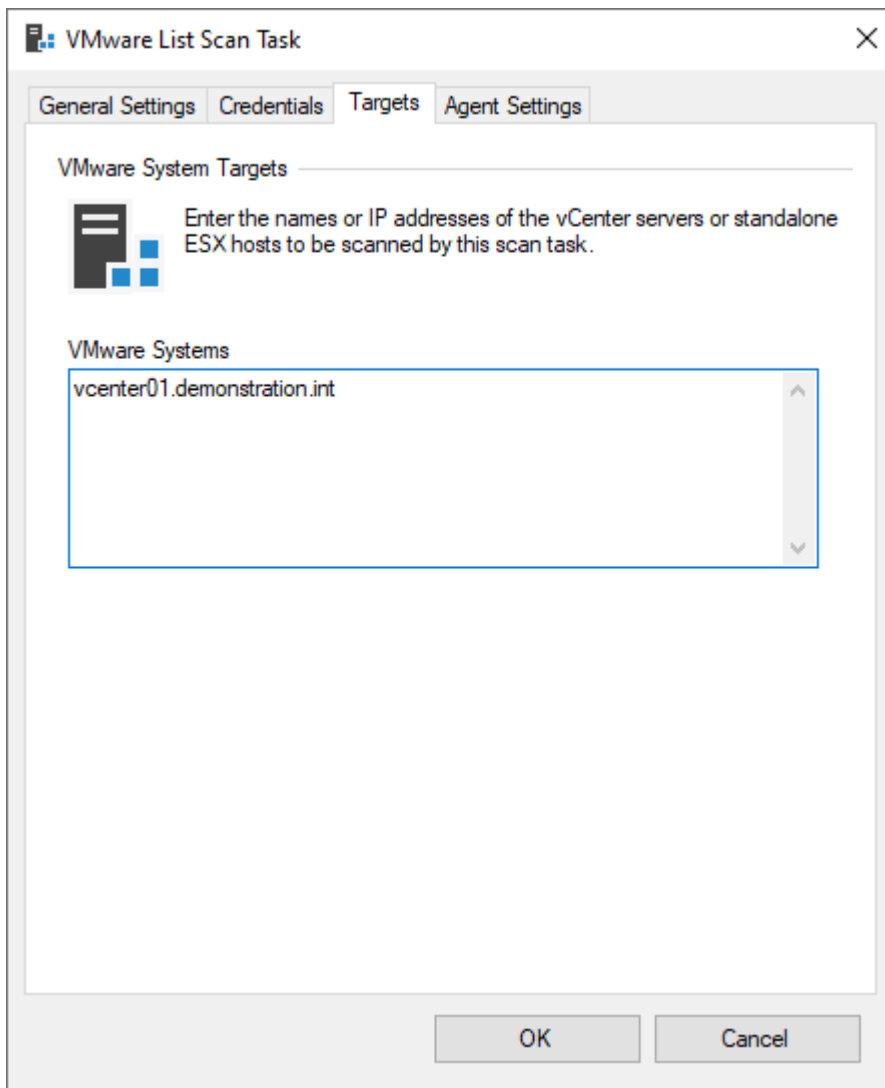
- For Windows credentials on a vCenter server **appliance** you must enter the username in the format *username@domainname* - for example "vcadmin@contoso.int", with the domain field

left blank.

- When entering local **vSphere** credentials, these can be entered in the **username** field for example "administrator@vsphere.local", with the domain field blank. ¹
- For Windows credentials on a vCenter server on a **workgroup** enter the username and password, the domain field should be left blank.
- For a standalone ESX host enter the username - for example "root" and password, the domain field should be left blank.
- For a vCenter server on an **Active Directory domain** enter the username, domain name and password. The domain name can be entered either in DNS or NetBIOS format.

¹ Alternatively, the username can be entered in the username field, and the domain field set to, for example, "vSphere.local".

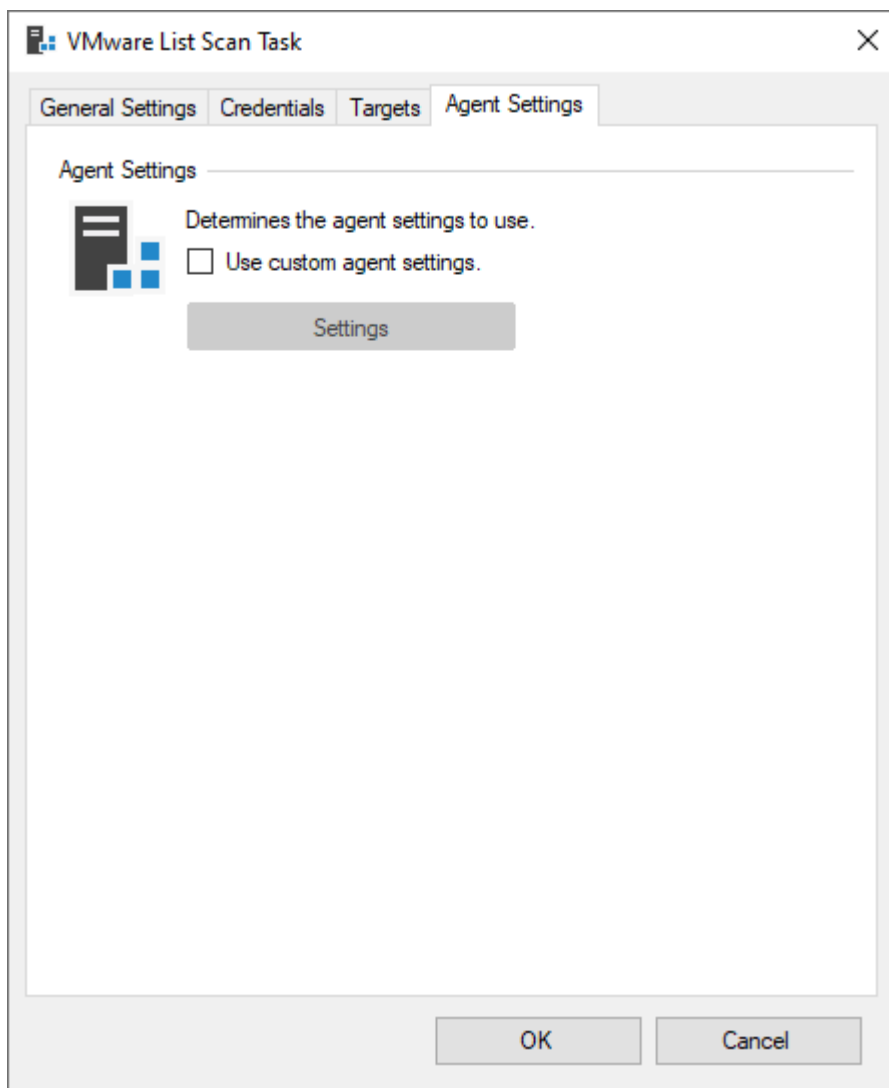
Targets



Unix Systems

The IP addresses or fully qualified domain names of the [VMware systems](#) to scan, one per line.

Agent Settings



Use custom agent settings

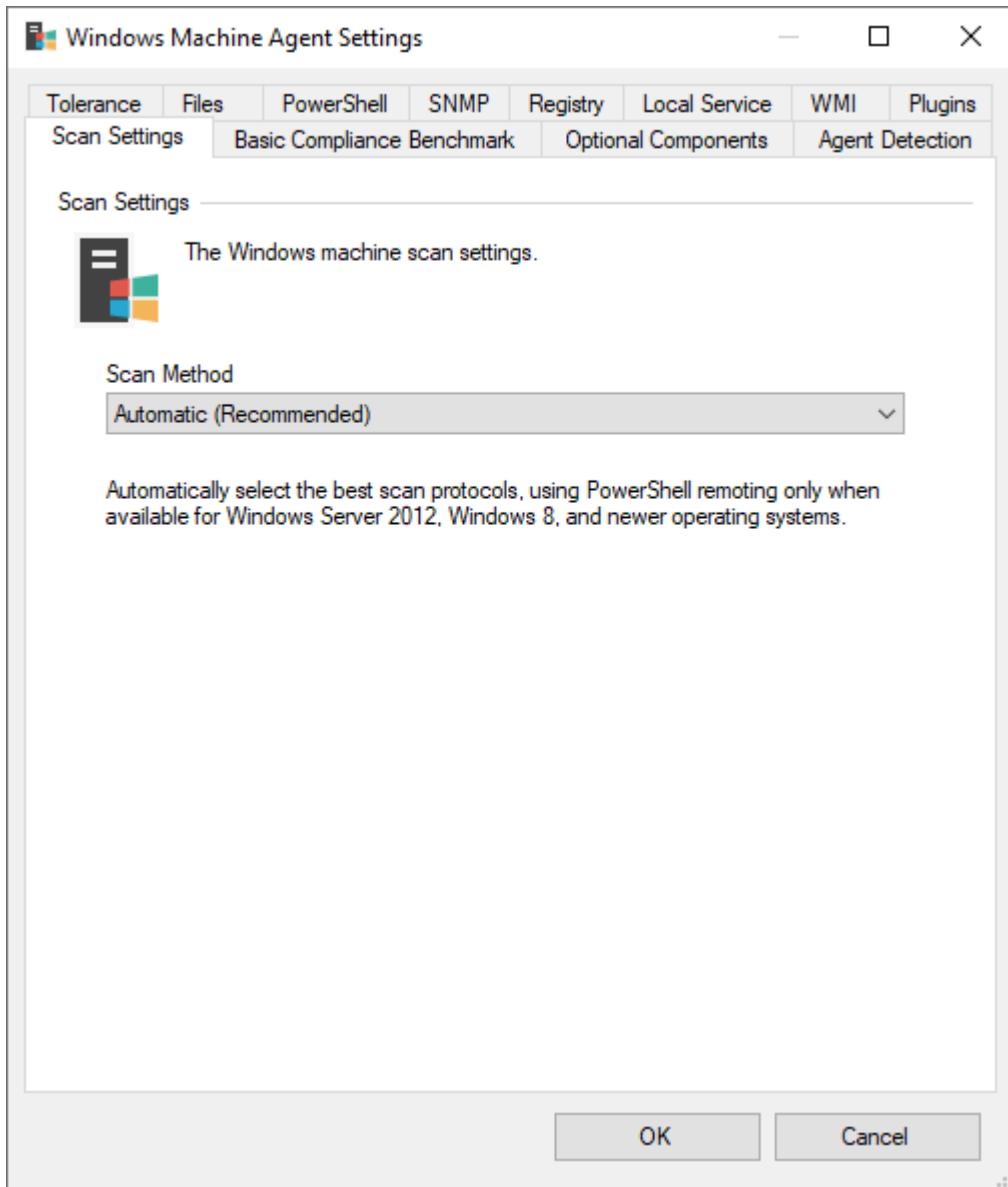
Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

Windows Machine

Windows machine scan tasks are able to document [Windows servers](#) and workstations.

The data located by these tasks include hardware, software, networking, and security information.

Agent Settings



This section determines the scan method to use.

Classic Only

Always use classic APIs, never connect [PowerShell remoting](#).

- Nano Server is not supported.
- Certain information such as advanced audit policies will not be available.

Automatic (Recommended)

Automatically select the best scan protocols, using [PowerShell remoting](#) only when available for Windows Server 2012, Windows 8, and newer operating systems.

Automatic (Strict)

Automatically select the best scan protocols, requiring [PowerShell remoting](#) for Windows Server 2012, Windows 8, and newer operating systems.

- Scans of Windows Server 2012, Windows 8, and above will fail if [PowerShell remoting](#) isn't enabled.

PowerShell Remoting Only

Always use [PowerShell remoting](#), never connect classic APIs.

- Operating systems prior to Windows Server 2012 and Windows 8 are not supported.

Basic Compliance Benchmark

The [Windows machine](#) basic [compliance benchmark](#) provides a simple overview of the security settings against simple security best practices and should be used for guidance only as this does not guarantee a secure system and customers should fully investigate the consequences of any security configuration changes prior to making them.

Name

Windows Basic Compliance Benchmark

Unique Identifier

144bbd41-e624-4f5f-a627-49c8aea00365

Provider

CENTREL Solutions Ltd

Requirements

Windows 8, Windows Server 2012 or above

More Information

Information used by this benchmark is provided by the following pages:

[Microsoft password policy guidelines](#)

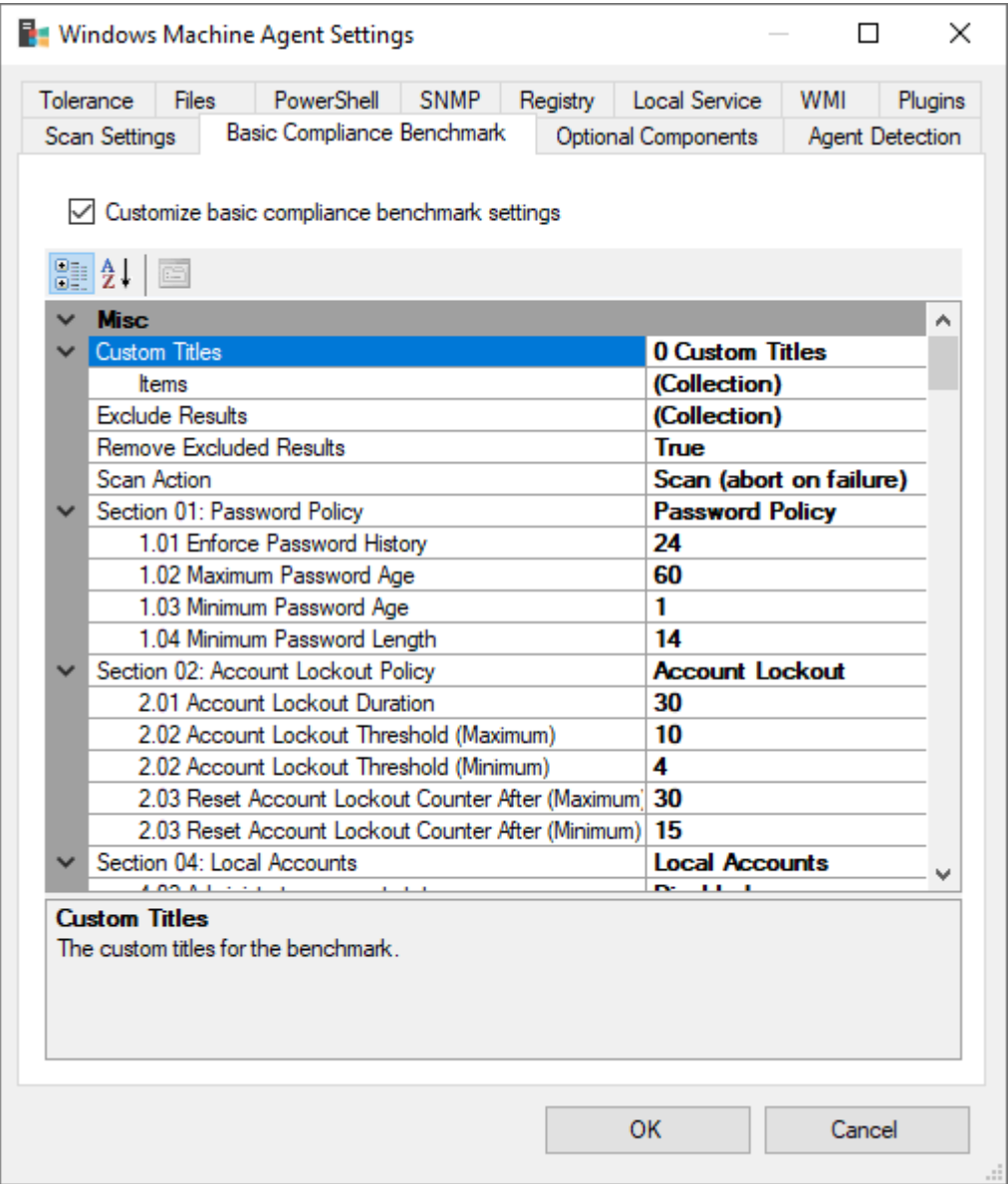
[Microsoft account lockout policy guidelines](#)

[Microsoft security options guidelines](#)

[Microsoft audit policy recommendations "Stronger Recommendation"](#)

Benchmark Settings

The [Windows Machine Basic Compliance Benchmark](#) has the following configurable options



Use Basic Compliance Benchmark Custom Settings

Determines whether the custom settings should be configured for the Windows machine [Basic Compliance Benchmark](#).

Custom Titles

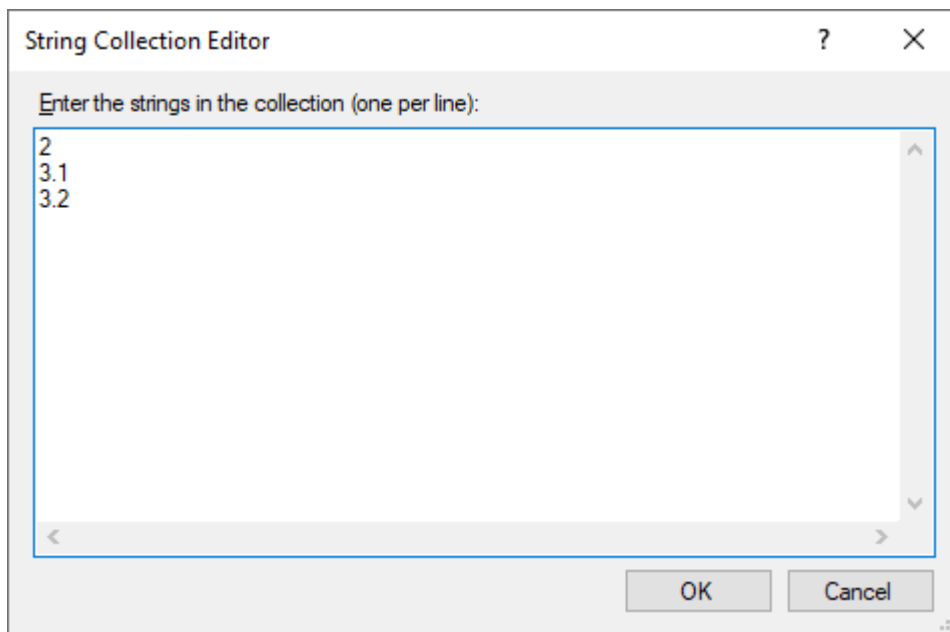
Determines the [custom text](#) to use for compliance benchmark titles.

Remove Excluded Results

Determines whether results that are excluded (for example by configuration or because the results do not apply to the target platform) should be removed from the result set.

Exclude Results

The results that should be excluded from the benchmark test - this can include the reference numbers of individual tests as well as the reference numbers of entire sections.



Scan Action *

The scan action that should be performed for the Basic Compliance Benchmark.

* **NOTE:** the option "Scan (abort on failure)" refers to the inability of the [XIA Configuration Client](#) to perform the benchmark test, rather than sections of the benchmark failing compliance.

Section 1: Password Policy

1.01 Enforce Password History

Determines the [enforce password history policy](#) desired value as the minimum number of unique new passwords that must be associated with a user account before an old password can be reused.

1.02 Maximum Password Age

Determines the [maximum password age policy](#) desired value as a period of time (in days) that a password can be used before the system requires the user to change it.

1.03 Minimum Password Age

Determines the [minimum password age policy](#) desired value as the period of time (in days) that a password can be used before the system allows the user to change it.

1.04 Minimum Password Length

Determines the [minimum password length policy](#) desired value as the minimum number of characters that can be used for a user account password.

Section 2: Account Lockout Policy

2.01 Account Lockout Duration

Determines the [account lockout duration](#) desired value as the number of minutes that a locked-out account remains locked out before automatically becoming unlocked. By default this is 30 minutes.

2.02 Account Lockout Threshold (Minimum)

Determines the [account lockout threshold](#) minimum desired value as the number of failed sign-in attempts that will cause a user account to be locked.

2.02 Account Lockout Threshold (Maximum)

Determines the [account lockout threshold](#) maximum desired value as the number of failed sign-in attempts that will cause a user account to be locked.

2.03 Reset Account Lockout Counter After (Minimum)

Determines the [reset account lockout counter after](#) minimum desired value as the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0.

2.03 Reset Account Lockout Counter After (Maximum)

Determines the [reset account lockout counter after](#) maximum desired value as the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0.

Section 4: Local Accounts

4.01 Rename the local Administrator account

The benchmark test "Rename the Administrator account to a less easily identifiable account name" tests the common localized values Microsoft provide for the administrator account and also tests whether any of the following are **included** in the administrator's account name - for example an account name of "Admin2" would fail this test.

Admin
Rendszergazda
Järjestelmänvalvoja
Администратор

For more information see:

[https://technet.microsoft.com/en-us/library/jj852273\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj852273(v=ws.11).aspx)

4.02 Administrator account state

Determines the desired value of the [account state of the administrator account](#).

Section 7: Audit Settings

Advanced Audit Policy

The [advanced audit policy](#) is based on the Microsoft [audit policy recommendations](#) "Stronger Recommendation"

- Certain settings are applicable to domain controllers only.
- Where the recommendation is for a single audit type only (for example "Success" or "Failure") and the system is configured for "Success and Failure" a warning will be issued.
- The [advanced audit policy optional component](#) must be enabled and complete for this section to complete, otherwise "Unknown" will be displayed.

The following settings can be configured to determine whether the advanced audit policy should be configured to audit success, failure, or both success and failure events.

7.04 Audit Credential Validation

Determines the desired value for the [Audit Credential Validation](#) advanced audit policy setting.

7.05 Audit Kerberos Authentication Service

Determines the desired value for the [Audit Kerberos Authentication Service](#) advanced audit policy setting.

7.06 Audit Kerberos Service Ticket Operations

Determines the desired value for the [Audit Kerberos Service Ticket Operations](#) advanced audit policy setting.

7.07 Audit Other Account Logon Events

The desired value for the [Audit Other Account Logon Events](#) advanced audit policy setting.

7.08 Audit Application Group Management

The desired value for the [Audit Application Group Management](#) advanced audit policy setting.

7.10 Audit Distribution Group Management

The desired value for the [Audit Distribution Group Management](#) advanced audit policy setting.

7.11 Audit Other Account Management Events

The desired value for the [Audit Other Account Management Events](#) advanced audit policy setting.

7.12 Audit Security Group Management

The desired value for the [Audit Security Group Management](#) advanced audit policy setting.

7.13 Audit User Account Management

The desired value for the [Audit User Account Management](#) advanced audit policy setting.

7.14 Audit DPAPI Activity

The desired value for the [Audit DPAPI Activity](#) advanced audit policy setting.

7.15 Audit PNP Activity

The desired value for the [Audit PNP Activity](#) advanced audit policy setting. This setting only applies to Windows 10, Windows Server 2016 and above.

7.16 Audit Process Creation

The desired value for the [Audit Process Creation](#) advanced audit policy setting.

7.17 Audit Process Termination

The desired value for the [Audit Process Termination](#) advanced audit policy setting.

7.18 Audit RPC Events

The desired value for the [Audit RPC Events](#) advanced audit policy setting.

7.19 Audit Detailed Directory Service Replication

The desired value for the [Audit Detailed Directory Service Replication](#) advanced audit policy setting. This only applies to domain controllers.

7.20 Audit Directory Service Access

The desired value for the [Audit Directory Service Access](#) advanced audit policy setting. This only applies to domain controllers.

7.21 Audit Directory Service Changes

The desired value for the [Audit Directory Service Changes](#) advanced audit policy setting. This only applies to domain controllers.

7.22 Audit Directory Service Replication

The desired value for the [Audit Directory Service Replication](#) advanced audit policy setting. This only applies to domain controllers.

7.23 Audit Account Lockout

The desired value for the [Audit Account Lockout](#) advanced audit policy setting.

7.24 Audit Group Membership

The desired value for the [Audit Group Membership](#) advanced audit policy setting. This setting only applies to Windows 10, Windows Server 2016 and above.

7.25 Audit IPsec Extended Mode

The desired value for the [Audit IPsec Extended Mode](#) advanced audit policy setting.

7.26 Audit IPsec Main Mode

The desired value for the [Audit IPsec Main Mode](#) advanced audit policy setting.

7.27 Audit IPsec Quick Mode

The desired value for the [Audit IPsec Quick Mode](#) advanced audit policy setting.

7.28 Audit Logoff

The desired value for the [Audit Logoff](#) advanced audit policy setting.

7.29 Audit Logon

The desired value for the [Audit Logon](#) advanced audit policy setting.

7.30 Audit Network Policy Server

The desired value for the [Audit Network Policy Server](#) advanced audit policy setting.

7.31 Audit Other Logon/Logoff Events

The desired value for the [Audit Other Logon/Logoff Events](#) advanced audit policy setting.

7.32 Audit Special Logon

The desired value for the [Audit Special Logon](#) advanced audit policy setting.

7.33 Audit User / Device Claims

The desired value for the [Audit User / Device Claims](#) advanced audit policy setting. This setting only applies to Windows 8, Windows Server 2012 and above.

7.34 Audit Application Generated

The desired value for the [Audit Application Generated](#) advanced audit policy setting.

7.35 Audit Central Access Policy Staging

The desired value for the [Audit Central Access Policy Staging](#) advanced audit policy setting. This setting only applies to Windows 8, Windows Server 2012 and above.

7.36 Audit Certification Services

The desired value for the [Audit Certification Services](#) advanced audit policy setting.

7.37 Audit Detailed File Share

The desired value for the [Audit Detailed File Share](#) advanced audit policy setting.

7.38 Audit File Share

The desired value for the [Audit File Share](#) advanced audit policy setting.

7.39 Audit File System

The desired value for the [Audit File System](#) advanced audit policy setting.

7.40 Audit Filtering Platform Connection

The desired value for the [Audit Filtering Platform Connection](#) advanced audit policy setting.

7.41 Audit Filtering Platform Packet Drop

The desired value for the [Audit Filtering Platform Packet Drop](#) advanced audit policy setting.

7.42 Audit Handle Manipulation

The desired value for the [Audit Handle Manipulation](#) advanced audit policy setting.

7.43 Audit Kernel Object

The desired value for the [Audit Kernel Object](#) advanced audit policy setting.

7.44 Audit Other Object Access Events

The desired value for the [Audit Other Object Access Events](#) advanced audit policy setting.

7.45 Audit Registry

The desired value for the [Audit Registry](#) advanced audit policy setting.

7.46 Audit Removable Storage

The desired value for the [Audit Removable Storage](#) advanced audit policy setting. This setting only applies to Windows 8, Windows Server 2012 and above.

7.47 Audit SAM

The desired value for the [Audit SAM](#) advanced audit policy setting.

7.48 Audit Audit Policy Change

The desired value for the [Audit Audit Policy Change](#) advanced audit policy setting.

7.49 Audit Authentication Policy Change

The desired value for the [Audit Authentication Policy Change](#) advanced audit policy setting.

7.50 Audit Authorization Policy Change

The desired value for the [Audit Authorization Policy Change](#) advanced audit policy setting.

7.51 Audit Filtering Platform Policy Change

The desired value for the [Audit Filtering Platform Policy Change](#) advanced audit policy setting.

7.52 Audit MPSSVC Rule-Level Policy Change

The desired value for the [Audit MPSSVC Rule-Level Policy Change](#) advanced audit policy setting.

7.53 Audit Other Policy Change Events

The desired value for the [Audit Other Policy Change Events](#) advanced audit policy setting.

7.54 Audit Non Sensitive Privilege Use

The desired value for the [Audit Non Sensitive Privilege Use](#) advanced audit policy setting.

7.55 Audit Other Privilege Use Events

The desired value for the [Audit Other Privilege Use Events](#) advanced audit policy setting.

7.56 Audit Sensitive Privilege Use

The desired value for the [Audit Sensitive Privilege Use](#) advanced audit policy setting.

7.57 Audit IPsec Driver

The desired value for the [Audit IPsec Driver](#) advanced audit policy setting.

7.58 Audit Other System Events

The desired value for the [Audit Other System Events](#) advanced audit policy setting.

7.59 Audit Security State Change

The desired value for the [Audit Security State Change](#) advanced audit policy setting.

7.60 Audit Security System Extension

The desired value for the [Audit Security System Extension](#) advanced audit policy setting.

7.61 Audit System Integrity

The desired value for the [Audit System Integrity](#) advanced audit policy setting.

Return Warning For Additional Auditing

Determines whether a warning [result](#) is returned if the [Windows machine](#) is configured to audit additional events over the desired value.

Section 12: Windows Event Log

12.01 Application Event Log Maximum Size (KB)

The desired value for the maximum size of the Application event log in KB. The value configured must match or exceed this value.

12.02 Security Event Log Maximum Size (KB)

The desired value for the maximum size of the Security event log in KB. The value configured must match or exceed this value.

12.03 Setup Event Log Maximum Size (KB)

The desired value for the maximum size of the Setup event log in KB. The value configured must match or exceed this value.

12.04 System Event Log Maximum Size (KB)

The desired value for the maximum size of the System event log in KB. The value configured must match or exceed this value.

12.05 Application Event Log Retention Policy

The desired retention policy value for the Application event log.

12.06 Security Event Log Retention Policy

The desired retention policy value for the Security event log.

12.07 Setup Event Log Retention Policy

The desired retention policy value for the Setup event log.

12.08 System Event Log Retention Policy

The desired retention policy value for the System event log.

Section 13: User Rights Assignment

The following settings can be configured to determine which user accounts should be assigned to each [user right assignment](#). The default values are based on the Microsoft [user right assignment](#) best practice guidelines.

13.01 Access Credential Manager as a trusted caller

The [desired value](#) for the [Access Credential Manager as a trusted caller](#) user right.

13.02 Access this computer from the network

The [desired value](#) for the [Access this computer from the network](#) user right.

13.03 Act as part of the operating system

The [desired value](#) for the [Act as part of the operating system](#) user right.

13.04 Add workstations to domain

The [desired value](#) for the [Add workstations to domain](#) user right. This setting only applies to domain controllers.

13.05 Adjust memory quotas for a process

The [desired value](#) for the [Adjust memory quotas for a process](#) user right.

13.06 Allow log on locally

The [desired value](#) for the [Allow log on locally](#) user right.

13.07 Allow log on through Remote Desktop Services

The [desired value](#) for the [Allow log on through Remote Desktop Services](#) user right.

13.08 Back up files and directories

The [desired value](#) for the [Back up files and directories](#) user right.

13.09 Bypass traverse checking

The [desired value](#) for the [Bypass traverse checking](#) user right.

13.10 Change the system time

The [desired value](#) for the [Change the system time](#) user right.

13.11 Change the time zone

The [desired value](#) for the [Change the time zone](#) user right.

13.12 Create a pagefile

The [desired value](#) for the [Create a pagefile](#) user right.

13.13 Create a token object

The [desired value](#) for the [Create a token object](#) user right.

13.14 Create global objects

The [desired value](#) for the [Create global objects](#) user right.

13.15 Create permanent shared objects

The [desired value](#) for the [Create permanent shared objects](#) user right.

13.16 Create symbolic links

The [desired value](#) for the [Create symbolic links](#) user right.

13.17 Debug programs

The [desired value](#) for the [Debug programs](#) user right.

13.18 Deny access to this computer from the network

The [desired value](#) for the [Deny access to this computer from the network](#) user right.

13.19 Deny log on as a batch job

The [desired value](#) for the [Deny log on as a batch job](#) user right.

13.20 Deny log on as a service

The [desired value](#) for the [Deny log on as a service](#) user right.

13.21 Deny log on locally

The [desired value](#) for the [Deny log on locally](#) user right.

13.22 Deny log on through Remote Desktop Services

The [desired value](#) for the [Deny log on through Remote Desktop Services](#) user right.

13.23 Enable computer and user accounts to be trusted for delegation

The [desired value](#) for the [Enable computer and user accounts to be trusted for delegation](#) user right.

13.24 Force shutdown from a remote system

The [desired value](#) for the [Force shutdown from a remote system](#) user right.

13.25 Generate security audits

The [desired value](#) for the [Generate security audits](#) user right.

13.26 Impersonate a client after authentication

The [desired value](#) for the [Impersonate a client after authentication](#) user right.

13.27 Increase a process working set

The [desired value](#) for the [Increase a process working set](#) user right.

13.28 Increase scheduling priority

The [desired value](#) for the [Increase scheduling priority](#) user right.

13.29 Load and unload device drivers

The [desired value](#) for the [Load and unload device drivers](#) user right.

13.30 Lock pages in memory

The [desired value](#) for the [Lock pages in memory](#) user right.

13.31 Log on as a batch job

The [desired value](#) for the [Log on as a batch job](#) user right.

13.32 Log on as a service

The [desired value](#) for the [Log on as a service](#) user right.

13.33 Manage auditing and security log

The [desired value](#) for the [Manage auditing and security log](#) user right.

13.34 Modify an object label

The [desired value](#) for the [Modify an object label](#) user right.

13.35 Modify firmware environment values

The [desired value](#) for the [Modify firmware environment values](#) user right.

13.36 Obtain an impersonation token for another user in the same session

The [desired value](#) for the Obtain an impersonation token for another user in the same session user right.

13.37 Perform volume maintenance tasks

The [desired value](#) for the [Perform volume maintenance tasks](#) user right.

13.38 Profile single process

The [desired value](#) for the [Profile single process](#) user right.

13.39 Profile system performance

The [desired value](#) for the [Profile system performance](#) user right.

13.40 Remove computer from docking station

The [desired value](#) for the [Remove computer from docking station](#) user right.

13.41 Replace a process level token

The [desired value](#) for the [Replace a process level token](#) user right.

13.42 Restore files and directories

The [desired value](#) for the [Restore files and directories](#) user right.

13.43 Shut down the system

The [desired value](#) for the [Shut down the system](#) user right.

13.44 Synchronize directory service data

The [desired value](#) for the [Synchronize directory service data](#) user right.

13.45 Take ownership of files or other objects

The [desired value](#) for the [Take ownership of files or other objects](#) user right.

User Rights Assignment Value

Each [user rights assignment](#) setting includes the following configuration options.

Domain Controllers

The settings to apply to [Active Directory](#) domain controllers.

Member Servers and Workstations

The settings to apply to [Active Directory](#) member servers and member workstations as well as stand-alone servers and workstations.

Account Names

The names of the accounts to match for the [user rights assignment](#).

- The account names can include any of the defined [variables](#).
- When the match type is set to "Include Only" the account names can include the % wildcard at the start, end, or both the start and end of the string.
- **NOTE:** When the match type is set to "Any" specifying account names has no effect.

Match Type

The match type for the [user rights assignment](#).

- When set to "Any" the user right may be assigned any account names, or no account names.
- When set to "Exact Match" the user right must be assigned to the specified account names exactly.
- When set to "Include Only" the user right may be assigned to any, or all, of the specified account names, but no account names that are not specified.
- When set to "Must Include" the user right must be assigned to all of the specified account names, and optionally, additional account names.

User Rights Assignment Variables

The following variables are available when defining the account names of a [user rights assignment value](#).

NOTE: All variables must be surrounded in square brackets and are case-insensitive.

[ACCOUNT_OPERATORS]

The localized account name of the built-in account operators group. This only applies to domain controllers.

[ADMINISTRATORS]

The localized account name of the built-in administrators group.

[AUTHENTICATED_USERS]

The localized account name of the authenticated users group.

[BACKUP_OPERATORS]

The localized account name of the built-in backup operators group.

[DEVICE_OWNERS]

The localized account name of the built-in device owners group. This only applies to Windows 10, Windows Server 2019 and above.

[GUESTS]

The localized account name of the built-in guests group.

[IIS_USRS]

The localized account name of the built-in IIS_USRS group.

[LOCAL_SERVICE]

The localized account name of the [local service account](#).

[MACHINENAME]

The NetBIOS name of the computer.

[NETWORK_SERVICE]

The localized account name of the [network service account](#).

[PERFORMANCE_LOG_USERS]

The localized account name of the built-in performance log users group.

[PRINT_OPERATORS]

The localized account name of the built-in print operators group. This only applies to servers.

[REMOTE_DESKTOP_USERS]

The localized account name of the built-in remote desktop users group.

[SERVER_OPERATORS]

The localized account name of the built-in print operators group. This only applies to domain controllers.

[SERVICE]

The localized group name of accounts authorized to log on as a service.

[SYSTEM]

The localized account name of the [local system account](#).

[S-1-5-32-547]

The localized account name of any valid security identifier including all [well known security identifiers](#).

[USERS]

The localized account name of the built-in users group.

Section 14: Windows Firewall Domain Profile

14.04 Display Notification

The desired value for 14.04 "Windows Firewall Domain Profile 'Display a notification' setting".

14.06 Log File Path

The desired value for 14.06 "Windows Firewall Domain Profile log file path".

14.07 Log File Size Limit

The desired value for 14.07 "Windows Firewall Domain Profile log file size limit".

14.09 Log Successful Connections

The desired value for 14.09 "Windows Firewall Domain Profile log successful connections setting".

Section 15: Windows Firewall Private Profile

15.04 Display Notification

The desired value for 15.04 "Windows Firewall Private Profile 'Display a notification' setting".

15.06 Log File Path

The desired value for 15.06 "Windows Firewall Private Profile log file path".

15.07 Log File Size Limit

The desired value for 15.07 "Windows Firewall Private Profile log file size limit".

15.09 Log Successful Connections

The desired value for 15.09 "Windows Firewall Private Profile log successful connections setting".

Section 16: Windows Firewall Public Profile

16.04 Display Notification

The desired value for 16.04 "Windows Firewall Public Profile 'Display a notification' setting".

16.06 Log File Path

The desired value for 16.06 "Windows Firewall Public Profile log file path".

16.07 Log File Size Limit

The desired value for 16.07 "Windows Firewall Public Profile log file size limit".

16.09 Log Successful Connections

The desired value for 16.09 "Windows Firewall Public Profile log successful connections setting".

Section 18: Security Options (Accounts)

18.01 Accounts: Block Microsoft Accounts

Determines the desired value for the [Accounts: Block Microsoft accounts](#) security option.

Section 21: Security Options (Credentials Delegation)

21.01 Credentials Delegation: Encryption Oracle Remediation

Determines the desired value for the [Credentials Delegation: Encryption Oracle Remediation](#) security option.

Section 25: Security Options (Domain Member)

25.05 Maximum Machine Account Password Age

Determines the desired value for the [Domain member: Maximum machine account password age](#) security option as the number of days before a domain member must submit a machine account password change.

Section 28: Security Options (Interactive Logon)

28.03 Machine Account Lockout Threshold (Maximum)

The maximum desired value for the [Interactive logon: Machine account lockout threshold](#) security option.

28.03 Machine Account Lockout Threshold (Minimum)

The minimum desired value for the [Interactive logon: Machine account lockout threshold](#) security option.

28.04 Machine Inactivity Limit

Determines the maximum desired value for the [Interactive logon: Machine inactivity limit](#) security option as the number of seconds of inactivity before a user's session locks by invoking the screen saver. This setting only applies to Windows 2012, Windows 8, and above.

28.05 Logon Message Text

The desired value for the [Interactive logon: Message text for users attempting to log on](#) security option. When empty, the benchmark ensures that a value is set and displays a [result type](#) of [manual validation required](#). When this value is set the value must match exactly.

28.06 Logon Message Title

The desired value for the [Interactive logon: Message title for users attempting to log on](#) security option. When empty, the benchmark ensures that a value is set and displays a [result type](#) of [manual validation required](#). When this value is set the value must match exactly.

28.07 Number Of Cached Logons (Workstations)

Determines the maximum desired value for the [Interactive logon: Number of previous logons to cache \(in case domain controller is not available\)](#) security option as the number of logons to cache to allow a user to log on to a Windows domain by using cached account information on workstation operating systems.

28.07 Number Of Cached Logons (Servers)

Determines the maximum desired value for the [Interactive logon: Number of previous logons to cache \(in case domain controller is not available\)](#) security option as the number of logons to cache to allow a user to log on to a Windows domain by using cached account information on server operating systems. This does not apply to domain controllers.

28.08 Prompt Password Change Before Expiration (Minimum)

Determines the minimum desired value for the [Interactive log on: Prompt the user to change passwords before expiration](#) security option as the number of days in advance users are warned that their passwords are about to expire.

28.08 Prompt Password Change Before Expiration (Maximum)

Determines the maximum desired value for the [Interactive log on: Prompt the user to change passwords before expiration](#) security option as the number of days in advance users are warned that their passwords are about to expire.

Section 38: Security Options (Network Access)

38.06 Anonymous Named Pipes

The desired values for the [Network access: Named Pipes that can be accessed anonymously](#) security option.

38.07 Remotely Accessible Registry Paths

The desired values for the [Network access: Remotely accessible registry paths](#) security option.

38.08 Remotely Accessible Registry Paths And Subpaths

The desired values for the [Network access: Remotely accessible registry paths and subpaths](#) security option.

38.10 Restrict Remote Calls To SAM

The desired value for the [Network access: Restrict clients allowed to make remote calls to SAM](#) security option as a security descriptor in SDDL format.

Section 40: Security Options (Network Provider)

40.01 Hardened UNC Paths

The desired values for the Network Provider: Hardened UNC Paths security option - for example

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
```

```
\\*\SYSVOL RequireMutualAuthentication=0, RequireIntegrity=1
```

Section 52: Security Options (System Settings)

52.01 Optional Subsystems

The desired values for the [System settings: Optional subsystems](#) security option.

Section 56: Security Options (Windows PowerShell)

56.01 Turn on PowerShell Script Block Logging

The desired value for the [Windows PowerShell: Turn on PowerShell Script Block Logging](#) security option.

56.02 Turn on PowerShell Transcription

The desired value for the [Windows PowerShell: Turn on PowerShell Transcription](#) security option.

SMB Version 1

The [Windows machine](#) basic [compliance benchmark](#) provides a simple way to check that the dated and vulnerable SMB version protocol has been disabled.

This setting can be evaluated in a number of ways.

Windows Server 2012 R2 and above

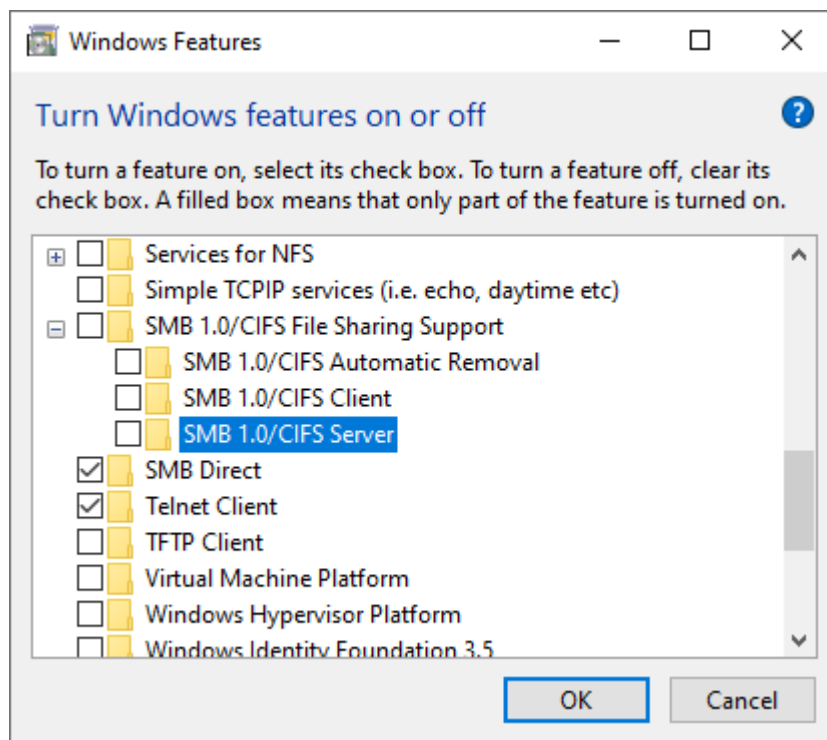
The "FS-SMB1" server feature is evaluated, if the feature is disabled the test passes.

If the server feature is enabled, or not available, the registry checks described below are performed.

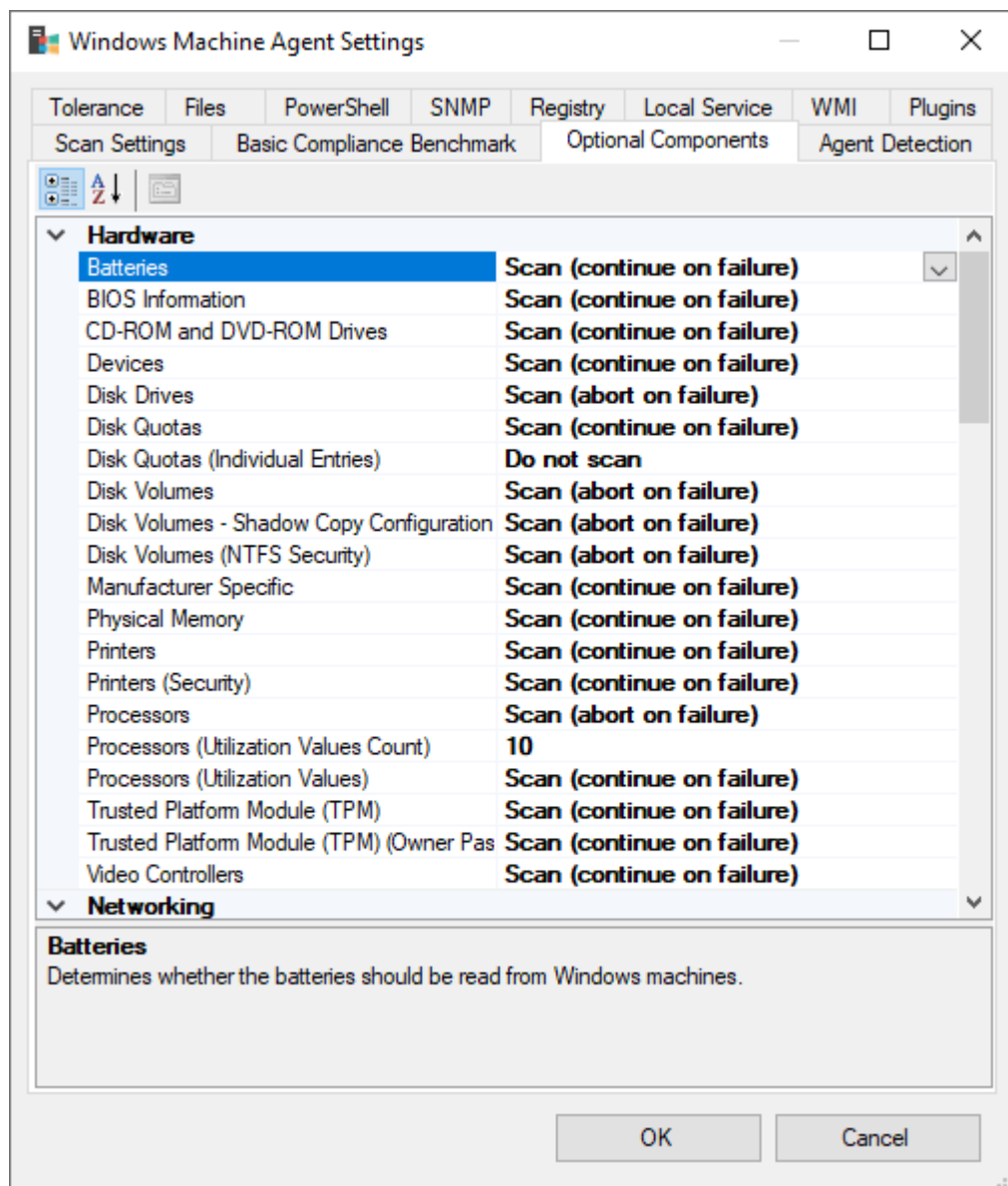
Windows 8.1 and above

The "SMB1Protocol-Server" is first evaluated if available, otherwise the "SMB1Protocol" feature is evaluated. If the optional feature is disabled the test passes.

If the optional feature is enabled, or not available, the registry checks are performed.



Optional Components



.NET Framework

Determines whether information about the optional features should be read. This only applies to desktop operating systems.

Advanced Audit Policy

Determines whether the [advanced audit policy](#) should be read. If this setting is set to abort on failure and [PowerShell remoting](#) cannot be connected, or the [scan mode](#) is set to classic only, the scan will fail.

Audit Policy

Determines whether the local [audit policy](#) should be read.

Antivirus Products

Determines whether the installed and supported antivirus products should be read. This currently only applies to [Microsoft Defender](#) on Windows Server 2016, Windows 10, and above.

Backup Products

Determines whether the installed and supported backup products should be read.

Batteries

Determines whether the batteries should be read from Windows machines.

BIOS Information

Determines whether BIOS information should be read from Windows machines.

Available Server Features

On Windows 2012 and above determines whether information should be read about Windows server roles and features that are available but not installed. By default, this is false.

CD-ROM and DVD-ROM Drives

Determines whether the CD-ROM and DVD-ROM drives should be read from Windows machines.

Devices

Determines whether [device and driver information](#) should be read from Windows machines.

Disk Drives

Determines whether the Windows agent should read [disk drives](#) from Windows machines.

Disk Quotas

Determines whether the Windows agent should read disk quota settings.

Disk Quotas (Individual Entries)

Determines whether the Windows agent should read individual user and group account disk quota entries, including disk space limits and usage.

Disk Volumes

Determines whether the Windows agent should read the disk volumes on a Windows machine. This applies to Windows Server 2003, and above.

Disk Volumes (NTFS Security)

Determines whether the NTFS security settings should be read for disk volumes.

Disk Volumes (Shadow Copy Configuration)

Determines whether the shadow copy configuration should be documented for the volumes on Windows machines. This only applies to server operating systems, and when the disk volumes option is enabled. This setting does not apply to Nano server.

Environment Variables

Determines whether this agent should read the environmental variables of the system.

Environment Variables (User)

Determines whether the agent should read the environmental variables assigned to individual users. This setting only applies when "Environment Variables" is enabled.

Event Logs

Determines whether event logs should be read for Windows machines.

Event Logs (Entries)

Determines whether event log entries should be read for Windows machines.

- Events for event log channels such as "Setup" and "Forwarded Events" can only be read on Windows Server 2012 and above when using [PowerShell remoting](#).
- When using [Windows Management Instrumentation \(WMI\)](#), only event log entries from the last 90 days are read.

Event Logs (Entries Maximum)

Determines the maximum number of the most recent event log entries that should be read for Windows machines. Valid values are from 1 to 200.

Event Logs (Internet Explorer Log)

Determines whether the Internet Explorer event log should be read for Windows machines when using [PowerShell remoting](#). This is disabled by default due to the security access control list preventing access.

Event Logs (Security)

Determines whether the security descriptor should be read for event logs. The default security descriptors can only be read on Windows Server 2012 and above when using [PowerShell remoting](#).

Failover Clustering

Determines whether basic failover clustering information should be collected for the Windows machine including whether failover clustering is enabled and the name of the cluster that the machine is a member of. For additional information, the failover cluster can be scanned using the [Microsoft failover cluster](#) agent.

Hosts File

Determines whether the agent should read the hosts file, including its contents, on a Windows machine.

Installed Programs

Determines whether the agent should read the [installed programs](#) on a Windows machine.

Internet Settings

Determines whether the agent should read the Internet settings on a Windows machine, this includes Internet Explorer version and system level proxy settings.

Local Account Policies

Determines whether the agent should read the local account and password policies of a Windows machine.

Local Accounts

Determines whether local user accounts (both users and groups) should be read from Windows machines. This setting does not apply to domain controllers.

Local Administrator Password Solution (LAPS) Settings

Determines whether the agent should read the [Local Administrator Password Solution \(LAPS\)](#)

settings on the Windows machine.

Machine Certificates

Determines whether the [machine level SSL certificates](#) including intermediate and trusted root certification authorities should be read from [Windows machines](#).

Manufacturer Specific

Determines whether the agent should read manufacturer specific information. This setting requires that the agent supports the specific hardware manufacturer, that SNMP is installed and that the manufacturer's SNMP support agents are installed.

Network Adapters

Determines whether the network adapter configuration should be read on Windows machines.

Network Load Balancing

Determines whether basic network load balancing information should be collected for the Windows machine including whether network load balancing is enabled and the names of the clusters that this machine is a member of. For additional information, the cluster can be scanned using the [Microsoft Network Load Balancing Cluster](#) agent.

ODBC Configuration

Determines whether the ODBC configuration should be read on Windows machines.

ODBC Passwords

Determines whether passwords from the ODBC configuration should be read on this machine. Passwords are stored in plain text. By default, this option is disabled.

Optional Features (Desktop Operating Systems)

Determines whether the agent should read information about the optional features for Windows machines. This only applies to desktop operating systems.

Operating System License

Determines whether operating system license information should be read for Windows machines running Windows Vista, Windows Server 2008, and above.

Page Files

Determines whether the page file configuration should be read for Windows machines.

Physical Memory

Determines whether the physical memory configuration should be read on Windows machines, including the total physical memory and installed physical memory devices.

PowerShell Configuration

Determines whether the agent should read the PowerShell configuration on Windows machines.

Printers

Determines whether printers should be read on Windows machines. The spooler service must be installed and running in order to perform the scan.

Printers (Security)

Determines whether printer security settings should be read on Windows machines. This setting only applies when the printers are read using [PowerShell remoting](#).

Processes

Determines whether the agent should read the running processes on Windows machines.

Processors

Determines whether the agent should read the processors on Windows machines.

Processors (Utilization Values)

Determines whether processor utilization values should be read from Windows machines.

Processors (Utilization Values Count)

The number of processor utilization values to read. The values are read one per second and can increase the overall scan time.

Process Descriptions (WMI)

Determines whether the agent should read the description from all running processes when using WMI. This requires that the agent connects to the remote machine using the administrative shares.

Remote Assistance

Determines whether the Remote Assistance settings should be read for Windows machines.

Remote Desktop

Determines whether the Remote Desktop settings should be read for Windows machines.

Routing Configuration

Determines whether the routing tables and persistent routes should be read on Windows machines.

Scheduled Tasks

Determines whether [scheduled tasks](#) should be read. Disabling the scanning of [scheduled tasks](#) will also affect the ability of the agent to determine the schedule of volume shadow copies.

Scheduled Tasks (Microsoft Built-In)

Determines whether built in tasks within the Microsoft folder in the [Scheduled Tasks](#) Library should be read. This applies to Windows Vista and 2008 and above only. This applies only when the Scheduled Tasks option is enabled. By default, this is false.

Security Identifiers

Determines whether the agent should read the security identifiers of on Windows machines.

Security Options

Determines whether the [security options](#) should be read from Windows machines.

Share Configuration

Determines the [share configuration options](#).

SNMP Configuration

Determines whether the SNMP Configuration including managers and community strings should be read from Windows machines.

Startup Commands

Determines whether the start-up commands should be read from Windows machines.

Trusted Platform Module (TPM)

Determines whether trusted platform module (TPM) information should be read for Windows machines running Windows 8, Windows Server 2012, and above.

Trusted Platform Module (TPM) (Owner Password)

Determines whether the trusted platform module (TPM) owner password should be read for Windows machines running Windows 8, Windows Server 2012, and above.

User Rights Assignment

Determines whether the agent should read the user rights assignments from Windows machines.

Video Controllers

Determines whether the video controllers should be read from Windows machines.

Windows Firewall

Determines whether the agent should read the [Windows Firewall](#) with Advanced Security configuration from Windows machines running Windows 2008 and above.

Windows Firewall Rules

Determines whether individual [Windows Firewall](#) rules should be read from Windows machines. This setting is ignored if all firewall profiles are disabled.

Windows Firewall Rules (Include Disabled Rules)

Determines whether disabled [Windows Firewall](#) rules that should be read from Windows machines.

Windows Firewall Rules (Maximum)

Determines the maximum number of [Windows Firewall](#) rules that should be read from Windows machines.

Windows Firewall Timeout (Classic)

The timeout in seconds when connecting to the Windows Firewall API. This cannot exceed 120 seconds. This setting does not apply when using [PowerShell Remoting](#).

Windows Patches

Determines whether the agent should read the installed [Windows patches](#) from Windows machines.

Windows Remote Management (WinRM)

Determines whether the agent should read the [Windows Remote Management \(WinRM\)](#) configuration from Windows machines.

Windows Update Configuration

Determines whether the agent should read the installed Windows Update configuration from Windows machines.

Windows Update History

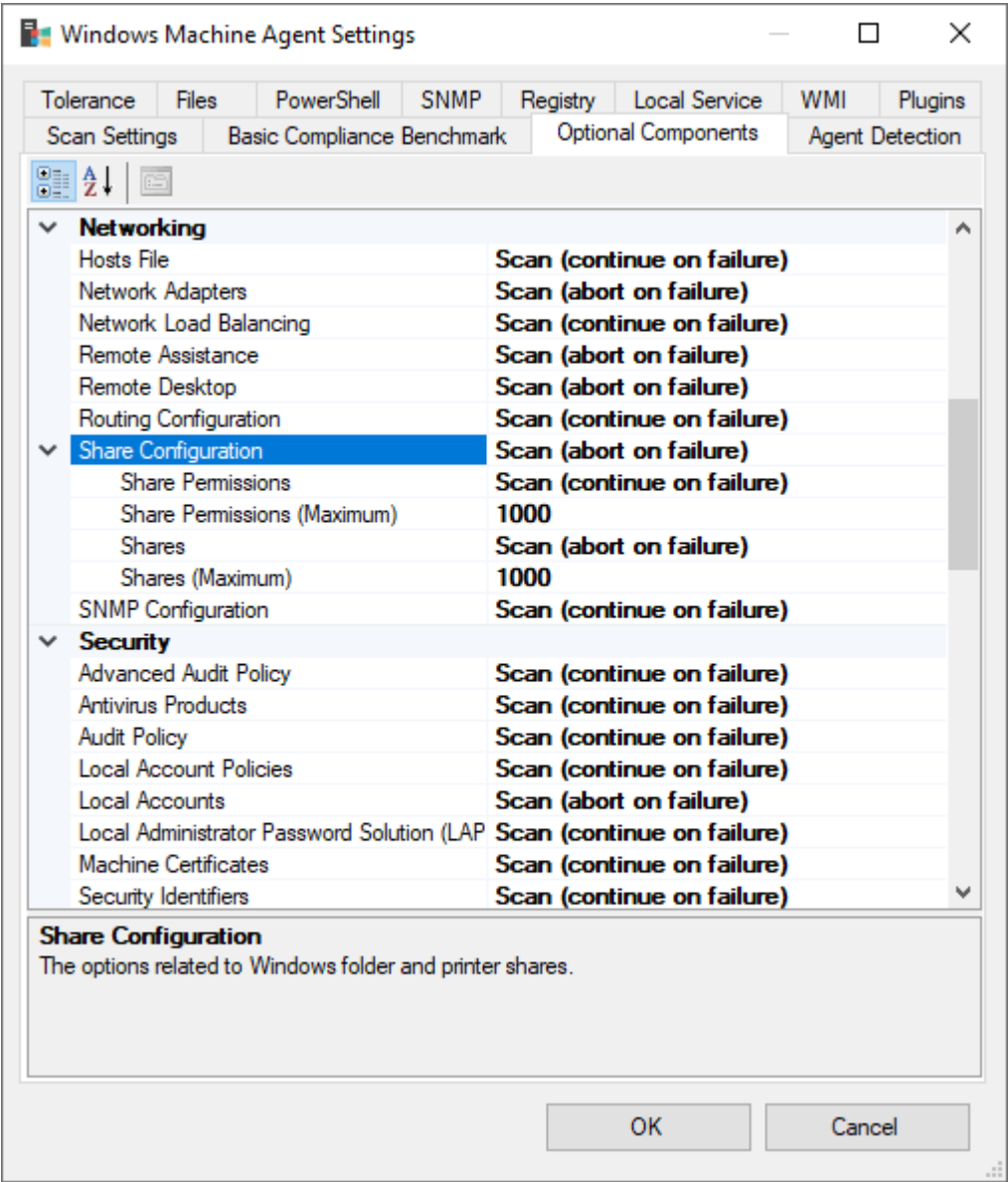
Determines whether the agent should read the installed Windows Update history from Windows

machines.

Windows Update Timeout

The timeout for reading Windows Update history and configuration in seconds. This setting does not apply when using PowerShell remoting. By default, this is 120 seconds.

Share Configuration Options



Shares

Determines whether the Windows agent should read the shares configured on [Windows machines](#) and whether to proceed on errors.

Shares (Maximum)

The maximum number of shares that can be configured on a [Windows machines](#) before the agent will bypass reading the share configuration.

Share Permissions

Determines whether the agent should read the share and NTFS permissions configured on Windows shared folders. This setting is disabled if the "Shares" setting is disabled.

Share Permissions (Maximum)

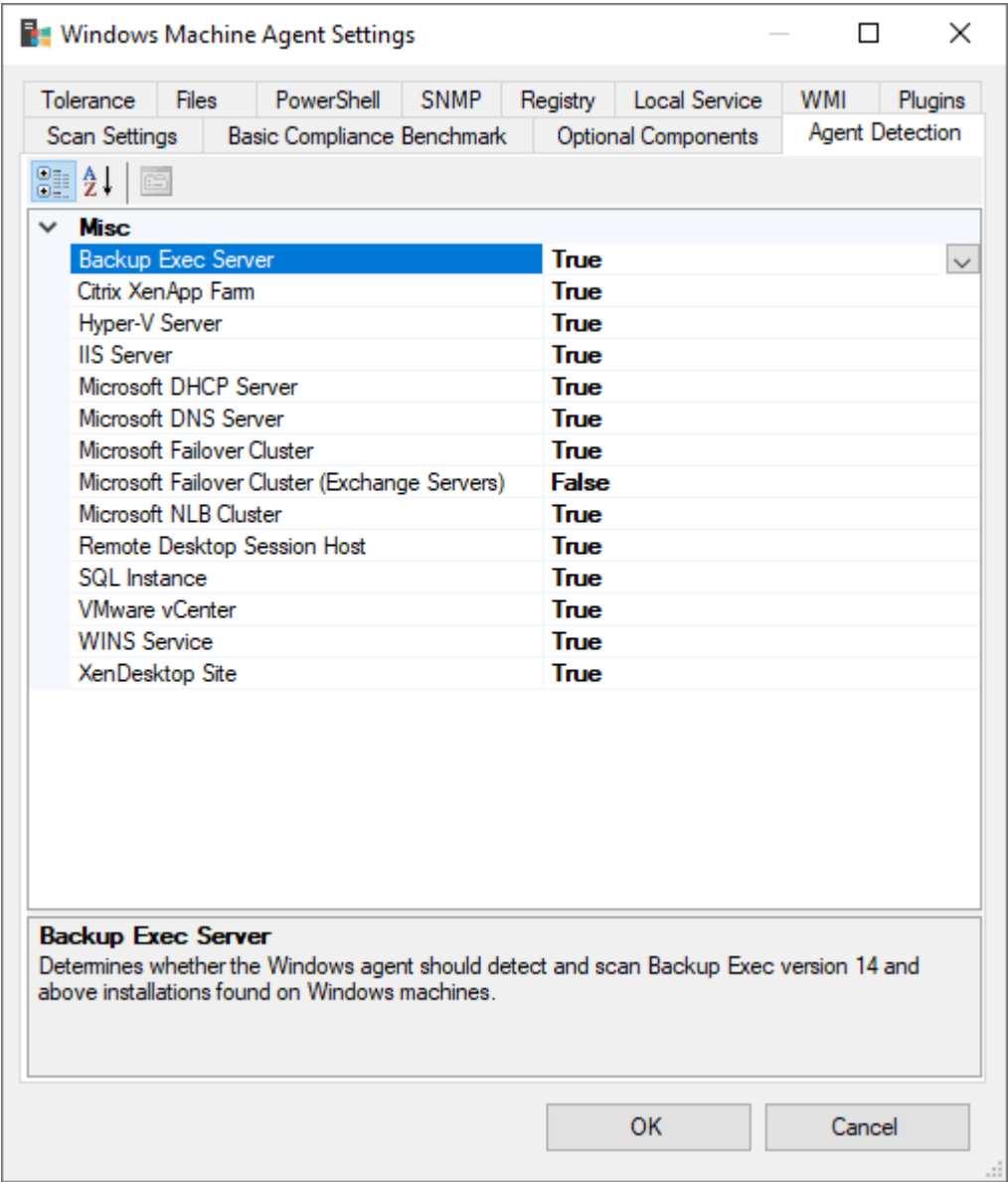
The maximum number of shares that can be configured on [Windows machines](#) before the agent will bypass reading the share and NTFS permissions.

Server Service State

The following behaviour applies when scanning the shares configured on [Windows machines](#)

- When the *Server service* is disabled and stopped the section is marked as *Disabled*.
- When the *Server service* is disabled but running the shares as scanned as normal.
- When the *Server service* is enabled but *not* running an error occurs, and the behaviour configured for the **Shares** setting applies.

Agent Detection

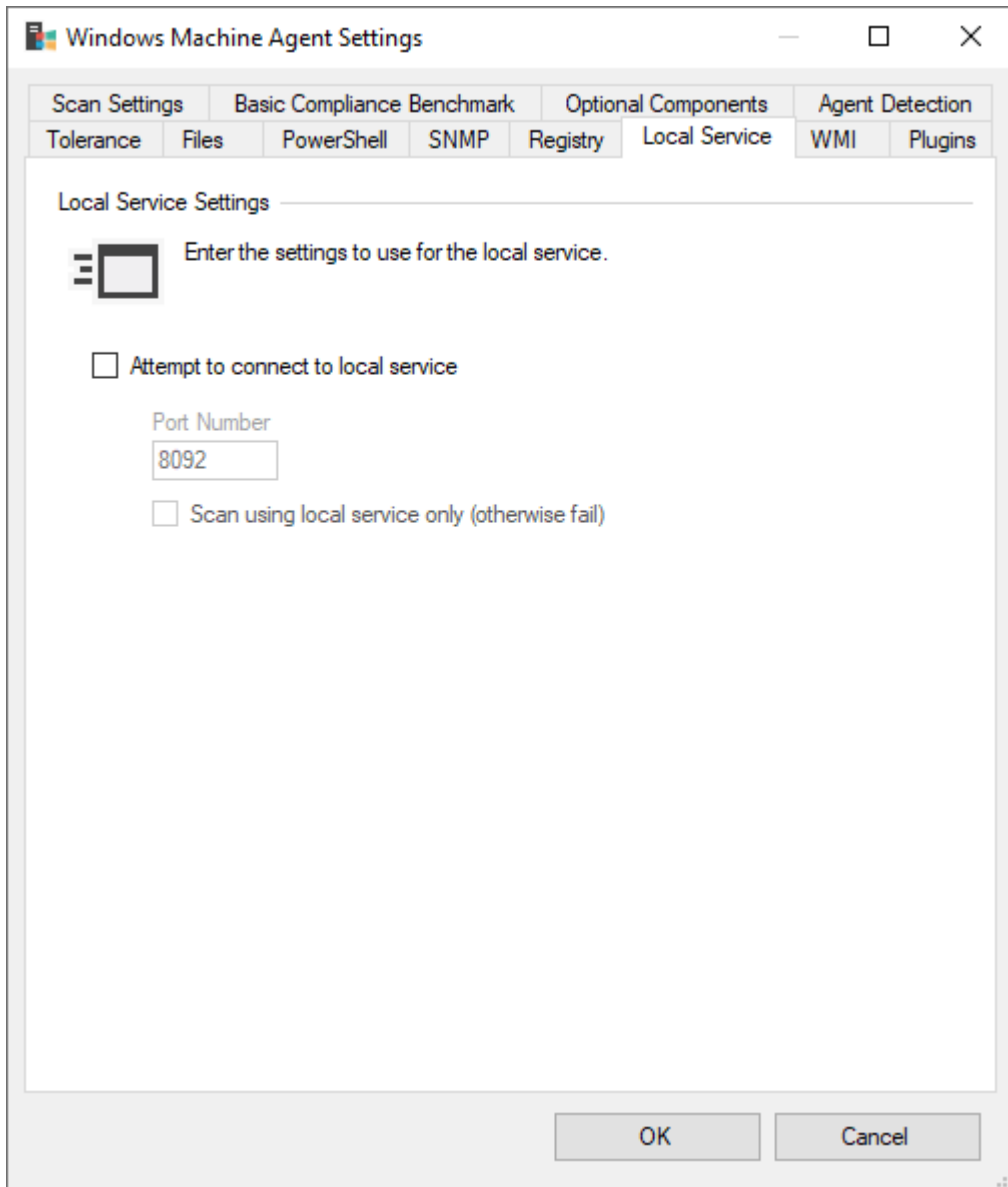


The detection tab determines whether other agents should automatically be used to scan the [Windows machine](#) when the machine is determined to be running that role or service.

Microsoft Failover Cluster (Exchange Servers)

By default [Microsoft Failover Clusters](#) are not detected when they are configured on a Microsoft Exchange Server as the configuration is handled by the [Microsoft Exchange organization](#) scan tasks.

Local Service



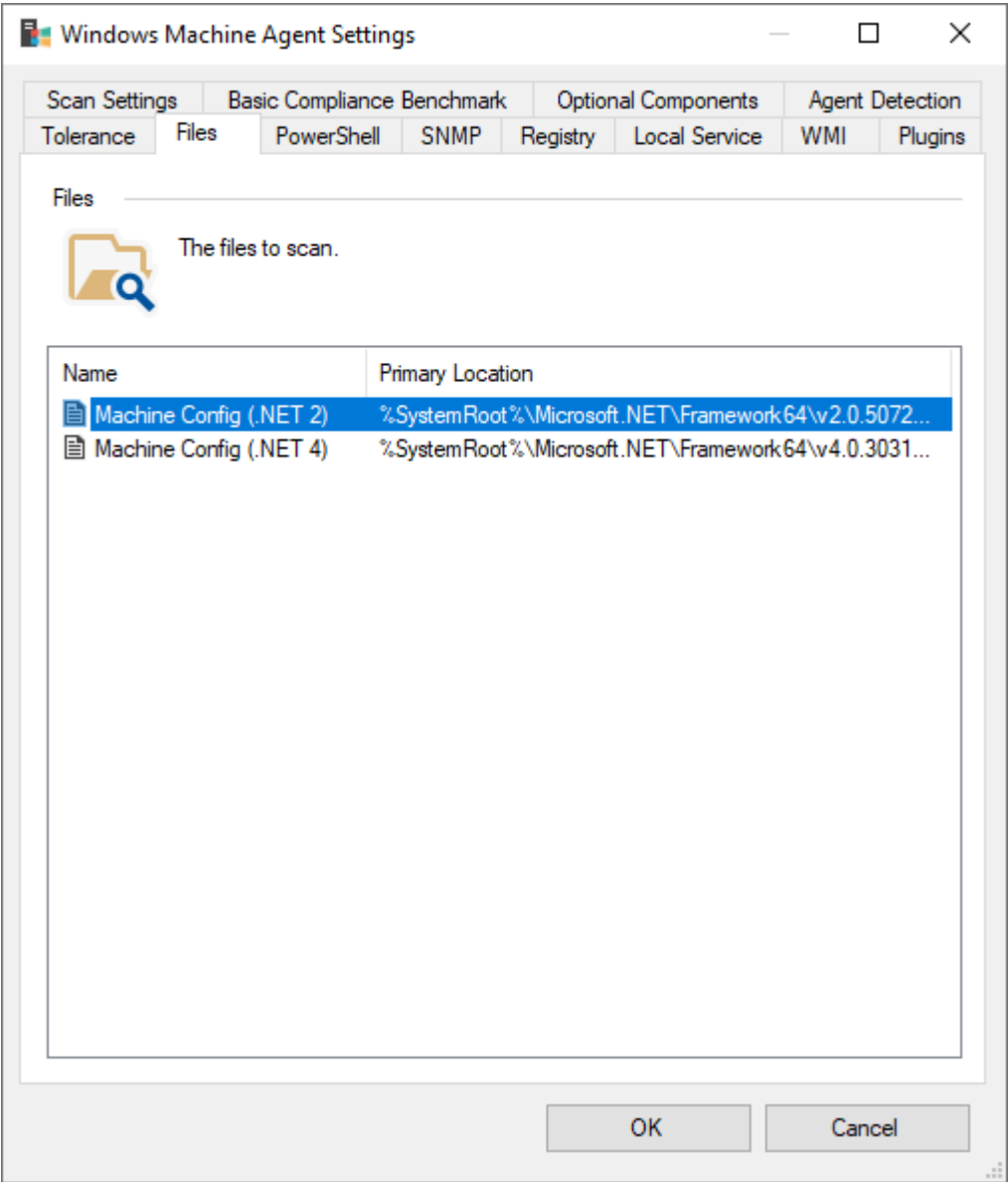
The screenshot shows the 'Windows Machine Agent Settings' dialog box with the 'Local Service' tab selected. The tab bar at the top includes 'Scan Settings', 'Basic Compliance Benchmark', 'Optional Components', 'Agent Detection', 'Tolerance', 'Files', 'PowerShell', 'SNMP', 'Registry', 'Local Service', 'WMI', and 'Plugins'. The 'Local Service Settings' section contains a text box with a list icon and the instruction 'Enter the settings to use for the local service.' Below this is an unchecked checkbox labeled 'Attempt to connect to local service'. Underneath the checkbox is a 'Port Number' label and a text box containing '8092'. At the bottom of the settings section is another unchecked checkbox labeled 'Scan using local service only (otherwise fail)'. The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

Determines the settings to use for the [local service](#).

NOTE: When scanning machines running Windows 8, Windows Server 2012, and newer it is recommended that the [scan mode](#) is configured to allow the [Windows machine](#) to be scanned using [PowerShell remoting](#) instead of using the local service.

Files

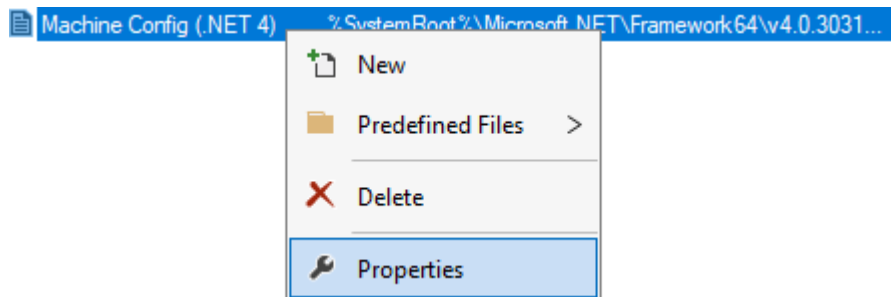
Determines the files to scan on [Windows servers](#) and [Windows workstations](#).



Right clicking the file list shows the [context menu](#).

Context Menu

Right clicking a file in the [files user](#) interface displays the context menu.



New

Displays the [file settings](#) dialog to add a new [file](#) to scan.

Predefined Files

Displays predefined files that can be added to the list of [files](#) to be scanned.

Delete

Deletes the currently selected [file](#).

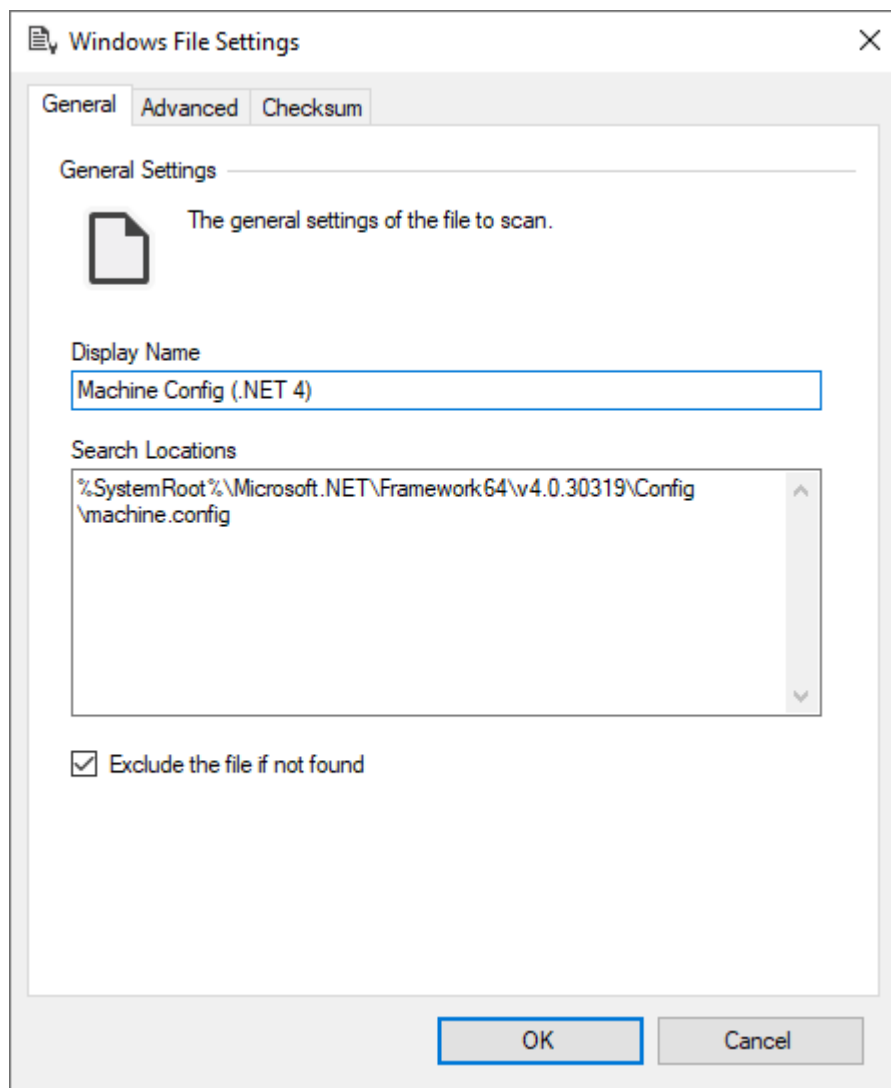
Restore Defaults

Restores the list of [files](#) to the defaults.

Properties

Displays the [file settings](#) dialog for the currently selected [file](#).

File Settings



Display Name

A descriptive, **unique** name of the file. This does not need to match the actual filename.

Search Locations

The list of locations in which the file may be located, in priority order. The location may include environment variables in the path.

When using [PowerShell remoting](#) any environment variable may be used, when WMI is used the following variables are available

%AllUsersProfile%

%CommonProgramFiles%

%ProgramFiles%

%ProgramFiles(x86)%

%SystemRoot%

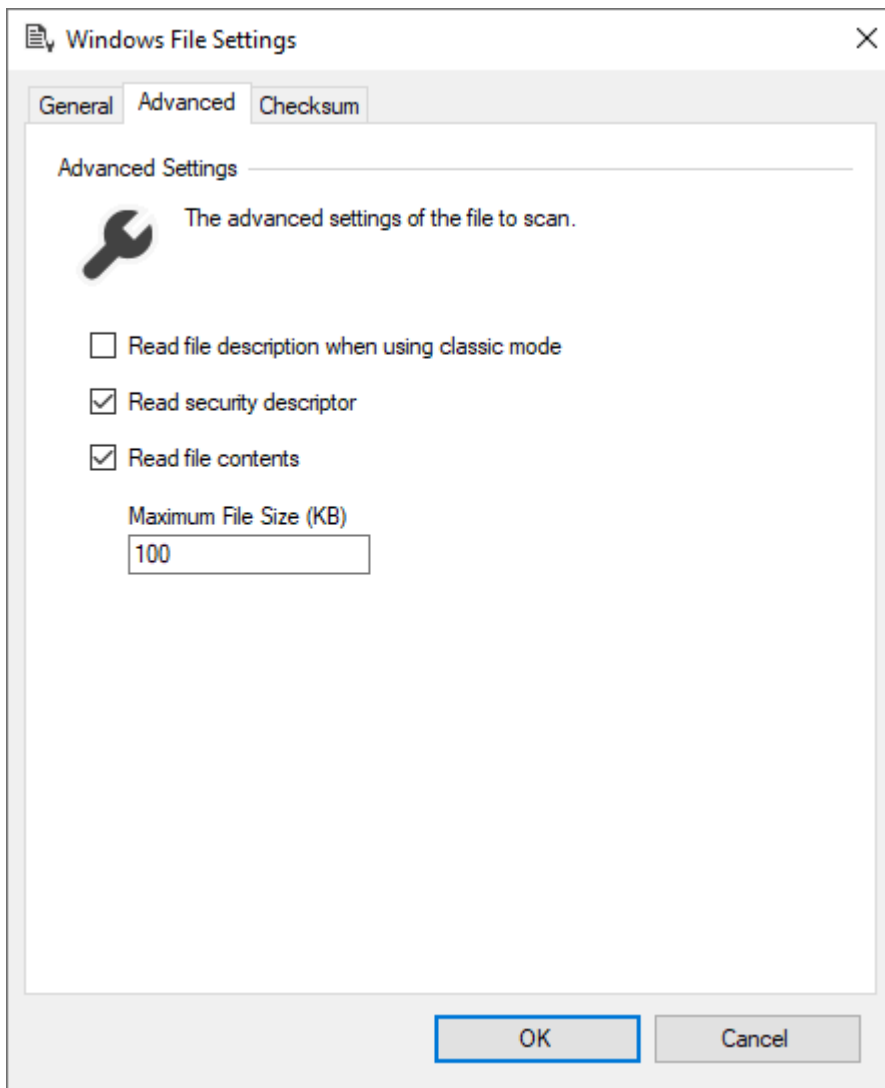
%SystemDrive%

Exclude the file if not found

Determines whether the file should be excluded if it is not found in any of the specified search

locations.

Advanced



Read file description when using classic mode

Determines whether the description of the file should be read when using classic mode. This requires that a network connection be made to the remote machine using a UNC path and the administrative shares. The description of the file is always read when using [PowerShell remoting](#).

Read security settings

Determines whether the NTFS security permissions should be read for the file.

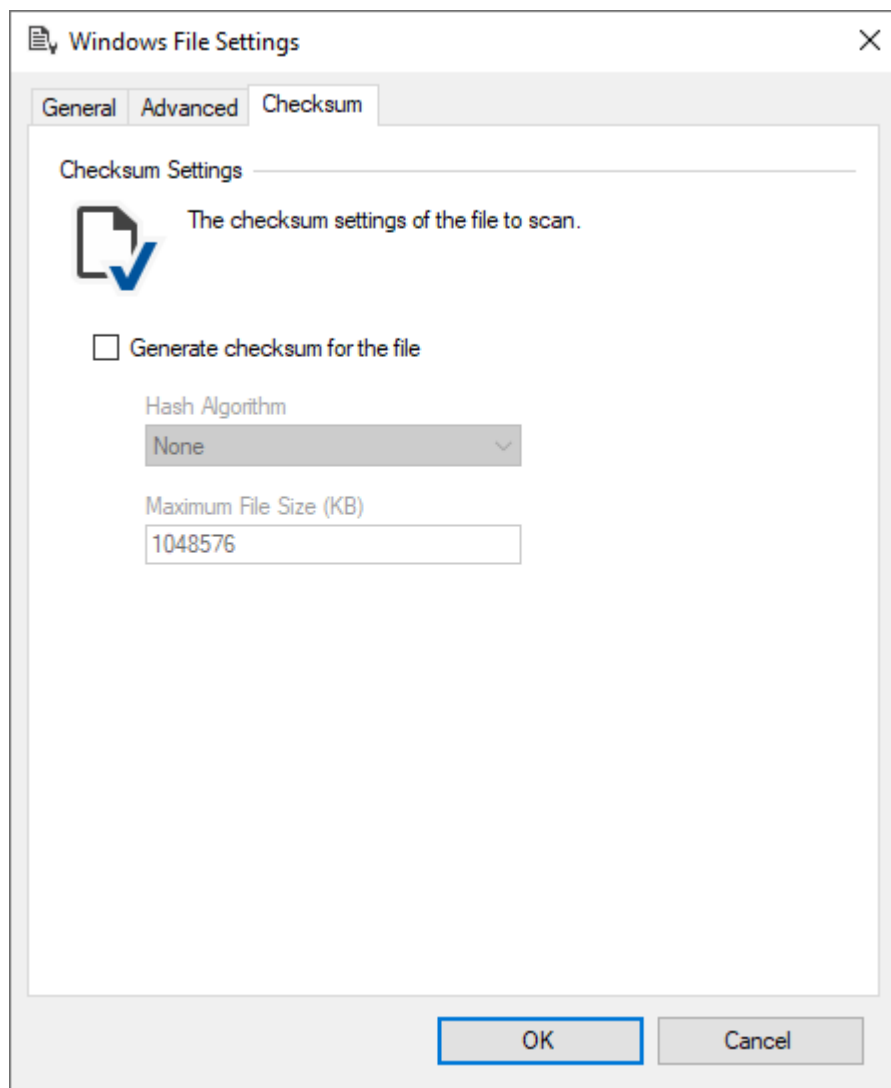
Read file contents

Determines whether to read the contents of the file. When using classic mode this requires that a network connection be made to the remote machine using a UNC path and the administrative shares, this is not a requirement when using [PowerShell remoting](#).

Maximum File Size (KB)

The maximum size of the file for which the contents should be read in kilobytes.

Checksum



Generate checksum for the file

Determines whether to generate a checksum of the file. When using classic mode this requires that a network connection be made to the remote machine using a UNC path and the administrative shares, this is not a requirement when using [PowerShell remoting](#). The checksum is used by the [item comparer](#) to detect when changes are made to the file.

Maximum File Size (KB)

The maximum size of the file for which the checksum should be read, in kilobytes.

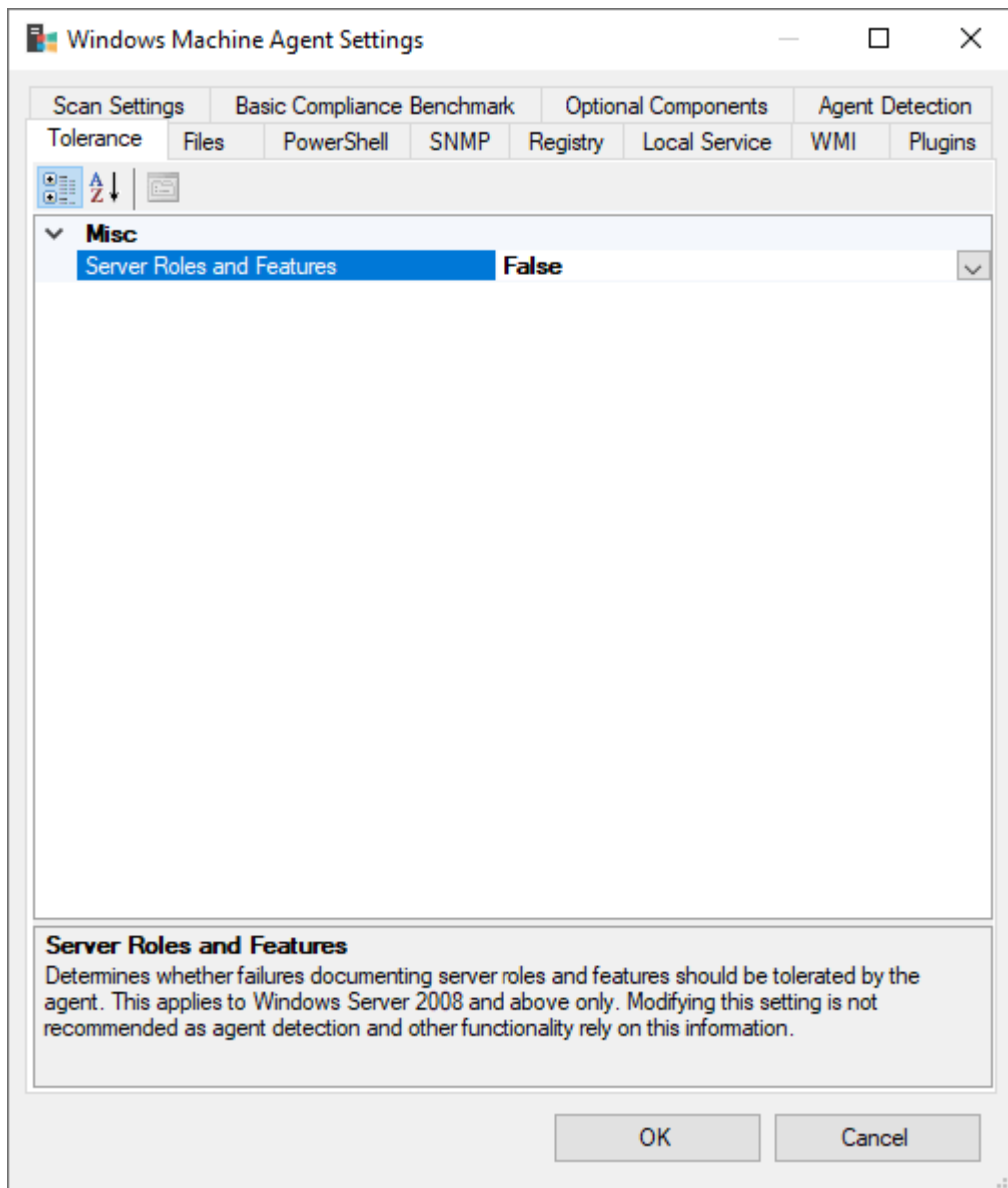
Hash Algorithm

The hash algorithm to use to generate the checksum.

- MD5
- SHA-256

- SHA-512

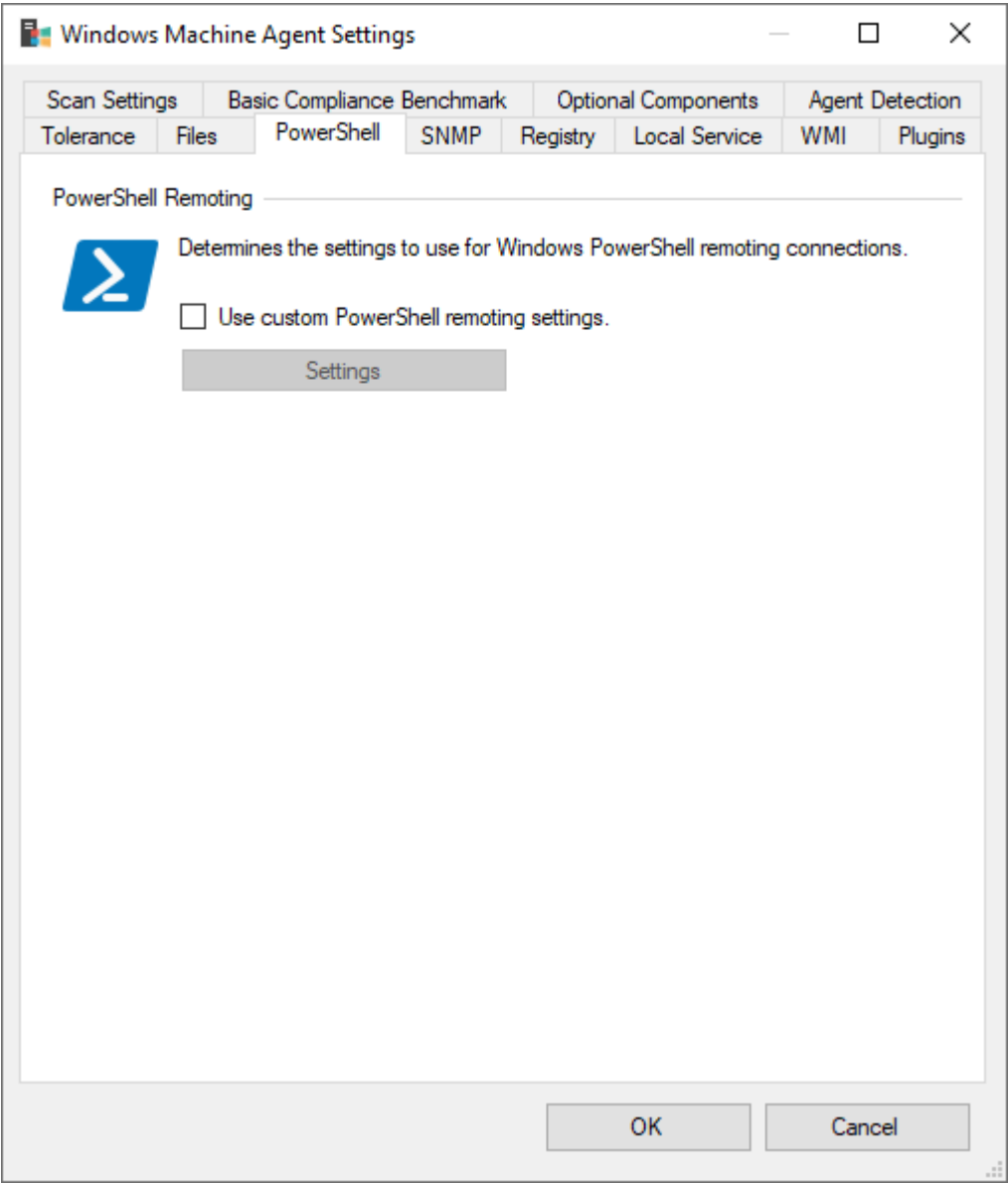
Tolerance



Server Roles and Features

Determines whether failures documenting server roles and features should be tolerated by the agent. This applies to Windows Server 2008 and above only. Modifying this setting is **not recommended** as agent detection and other functionality rely on this information.

PowerShell

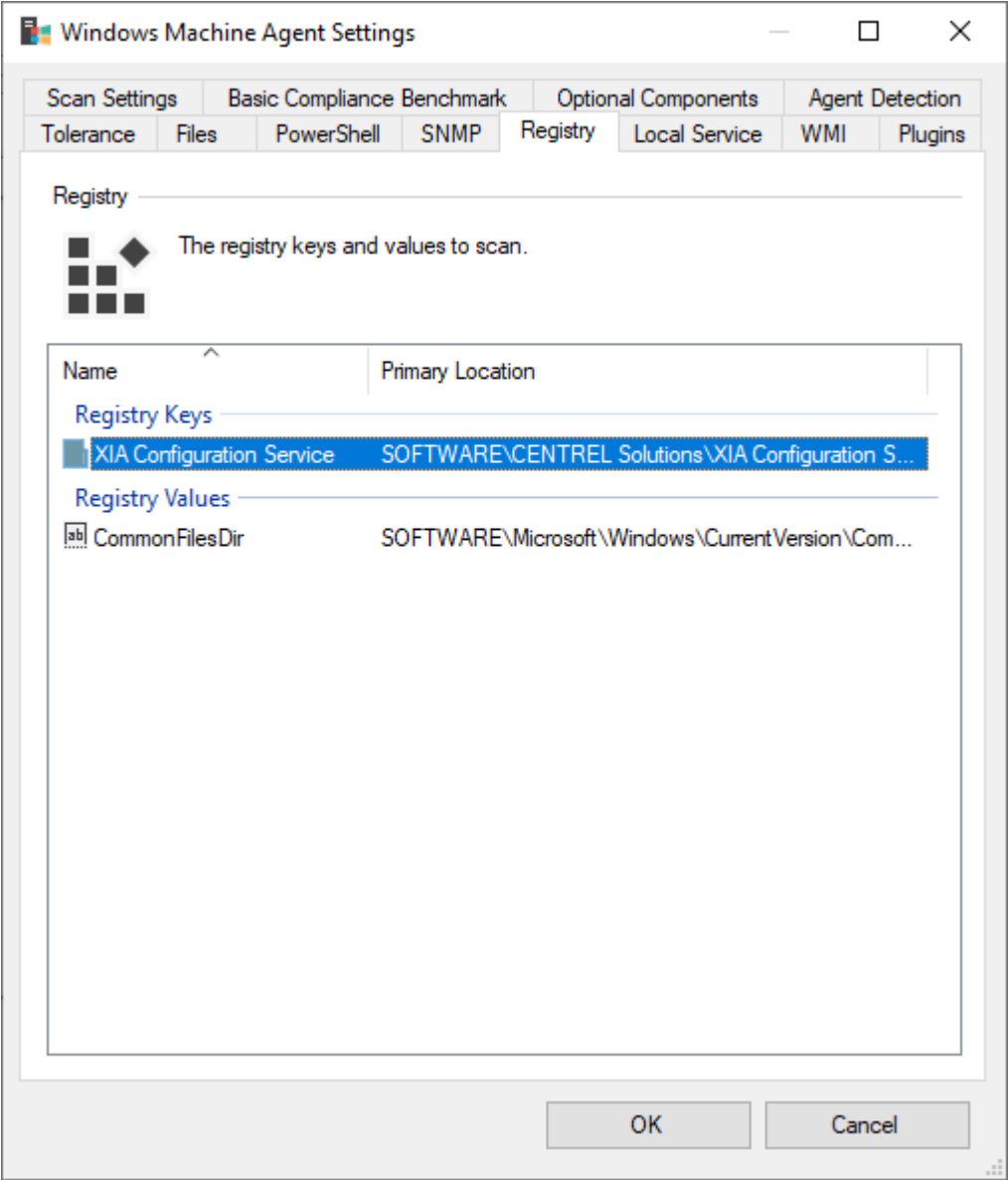


PowerShell Remote Connection Settings

The [PowerShell connection settings](#) to use to connect to the remote machine.

NOTE: This tab will be disabled when the [scan mode](#) is set to *Classic Only*.

Registry



This tab determines the [registry keys](#) and registry values to document for a [Windows machine](#).

Registry Key Properties

Windows Registry Key Settings

General Advanced

General Settings

The general settings of the registry key to scan.

Display Name

XIA Configuration Service

Registry Hive

HKEY_LOCAL_MACHINE

Search Locations

SOFTWARE\CENTREL Solutions\XIA Configuration Service

☒ Exclude the registry value if not found

OK Cancel

Display Name

The unique display name for the registry key.

Registry Hive

The registry hive in which the key is to be found.

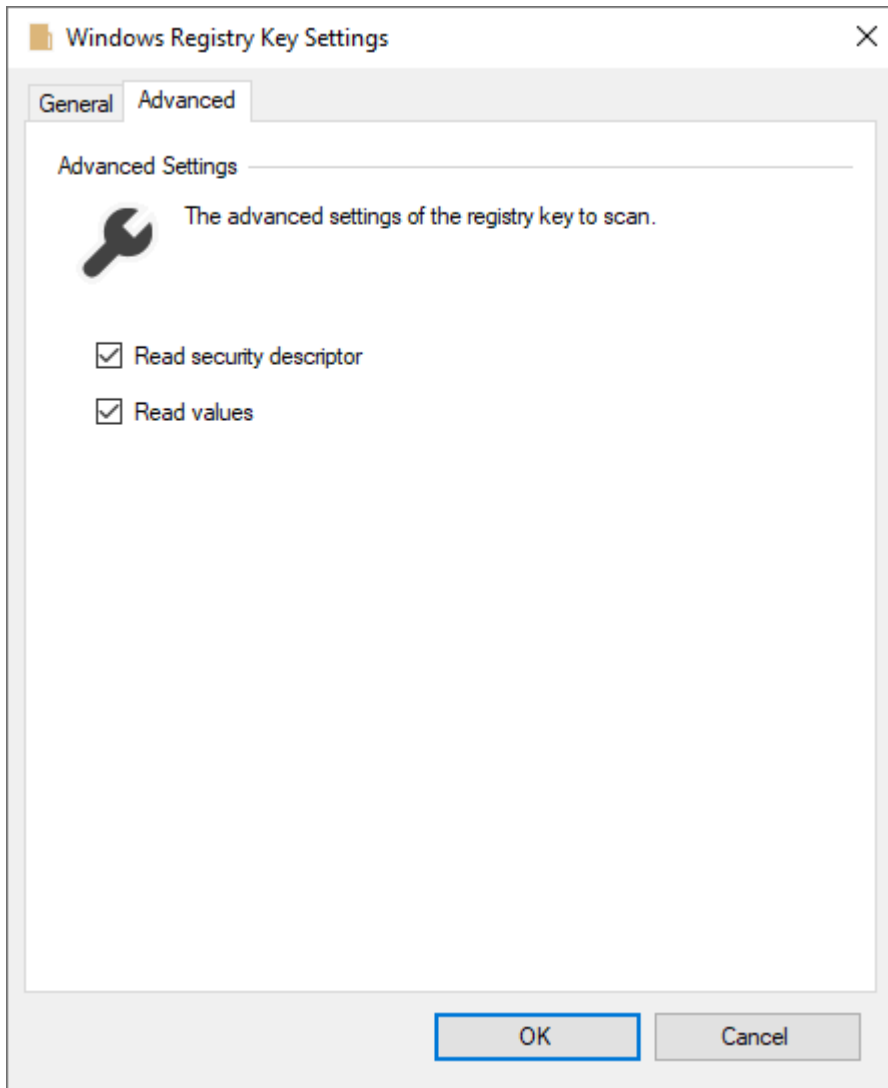
Search Locations

The possible locations of the registry key. If a hive name is entered, it will be automatically removed.

Exclude the registry key if not found

Determines whether the registry key should be excluded if it is not found in any of the specified search locations.

Advanced Properties



Read registry key values

Determines whether each of the values found immediately within the key should be documented.

Read security descriptor

Determines whether the security descriptor should be read for the registry key. Applies to Windows Server 2008 R2 and above.

Registry Value Properties

Windows Registry Value Settings

General

General Settings

The general settings of the registry value to scan.

Display Name

CommonFilesDir

Registry Hive

HKEY_LOCAL_MACHINE

Search Locations

SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir

☒ Exclude the registry value if not found

OK Cancel

Display Name

The unique display name for the registry value.

Registry Hive

The registry hive in which the value is to be found.

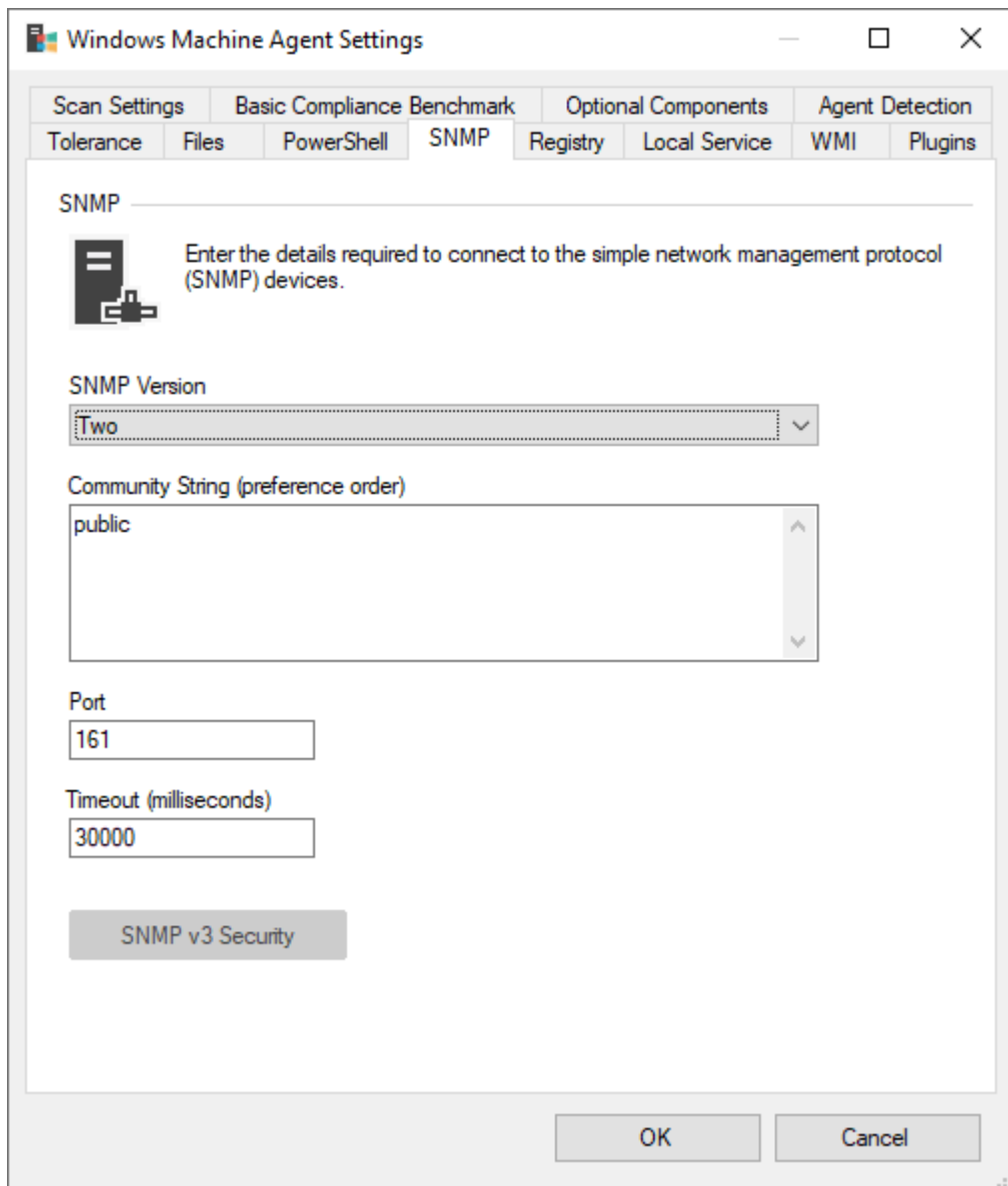
Search Locations

The possible locations of the registry value including the value name. If a hive name is entered, it will be automatically removed.

Exclude the registry value if not found

Determines whether the registry value should be excluded if it is not found in any of the specified search locations.

SNMP



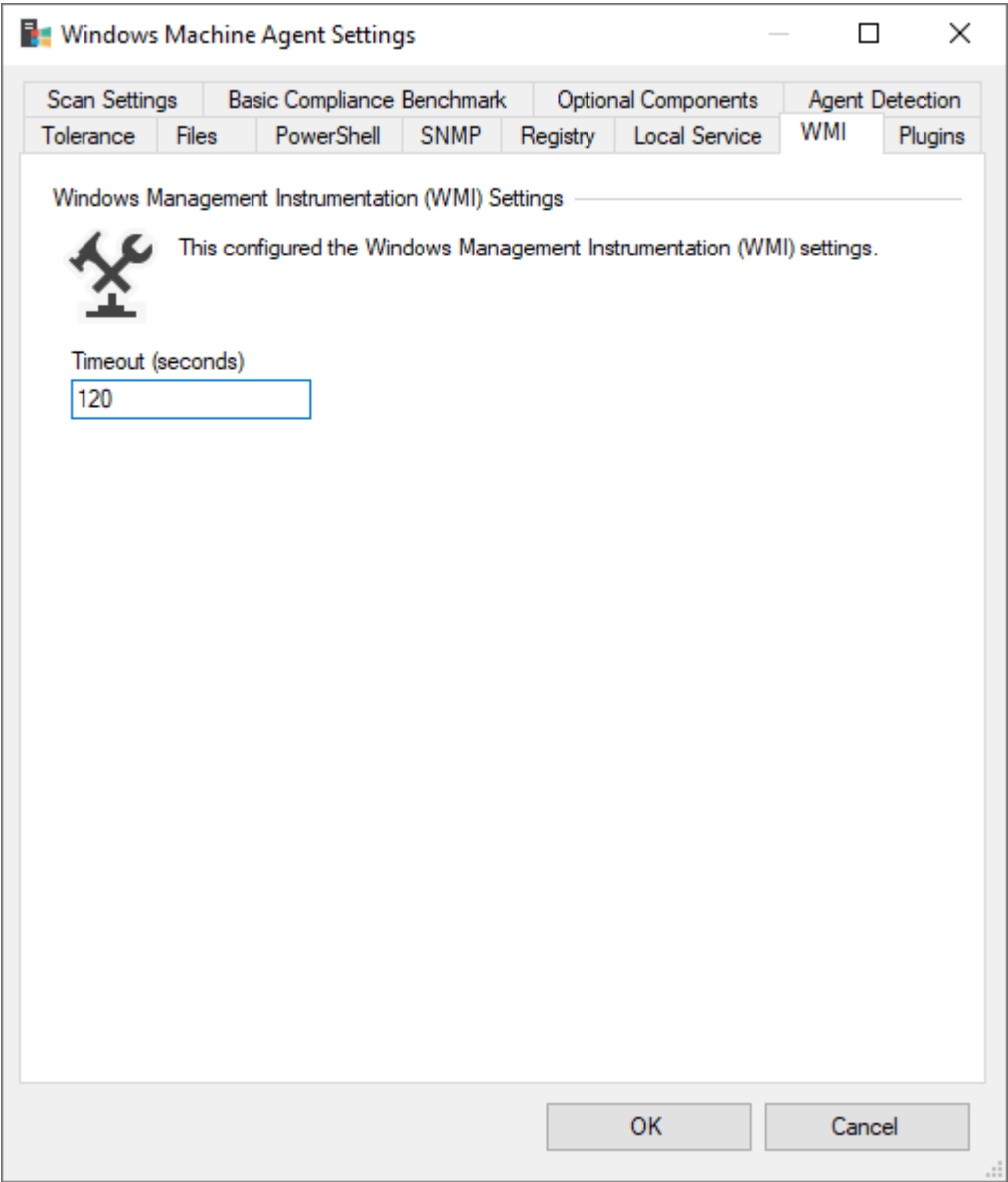
The screenshot shows the 'Windows Machine Agent Settings' dialog box with the 'SNMP' tab selected. The dialog has a title bar with standard Windows window controls. Below the title bar is a tabbed interface with the following tabs: 'Scan Settings', 'Basic Compliance Benchmark', 'Optional Components', 'Agent Detection', 'Tolerance', 'Files', 'PowerShell', 'SNMP' (selected), 'Registry', 'Local Service', 'WMI', and 'Plugins'. The 'SNMP' tab contains the following elements:

- A header 'SNMP' with a sub-header 'Enter the details required to connect to the simple network management protocol (SNMP) devices.' and an icon of a server rack.
- A 'SNMP Version' dropdown menu currently set to 'Two'.
- A 'Community String (preference order)' text box containing the value 'public'.
- A 'Port' text box containing the value '161'.
- A 'Timeout (milliseconds)' text box containing the value '30000'.
- A button labeled 'SNMP v3 Security'.
- 'OK' and 'Cancel' buttons at the bottom right.

Configures the [SNMP settings](#) used to access the remote machine to read manufacturer specific data.

NOTE: For [Windows machines](#) if the SNMP configuration [option](#) is enabled the agent will automatically use a valid community string that is detected.

NOTE: [Windows machines](#) do not support SNMP version 3.



WMI Timeout

The timeout for WMI connections in seconds.

NOTE: This tab will be disabled when the [scan mode](#) is set to *PowerShell Remoting Only*.

Item Identifiers

For more information about Item Identifiers please see the [item identifiers](#) section.

Primary Identifier

The computer name.

Secondary Identifier

The computer serial number.

Tertiary Identifier

Not used.

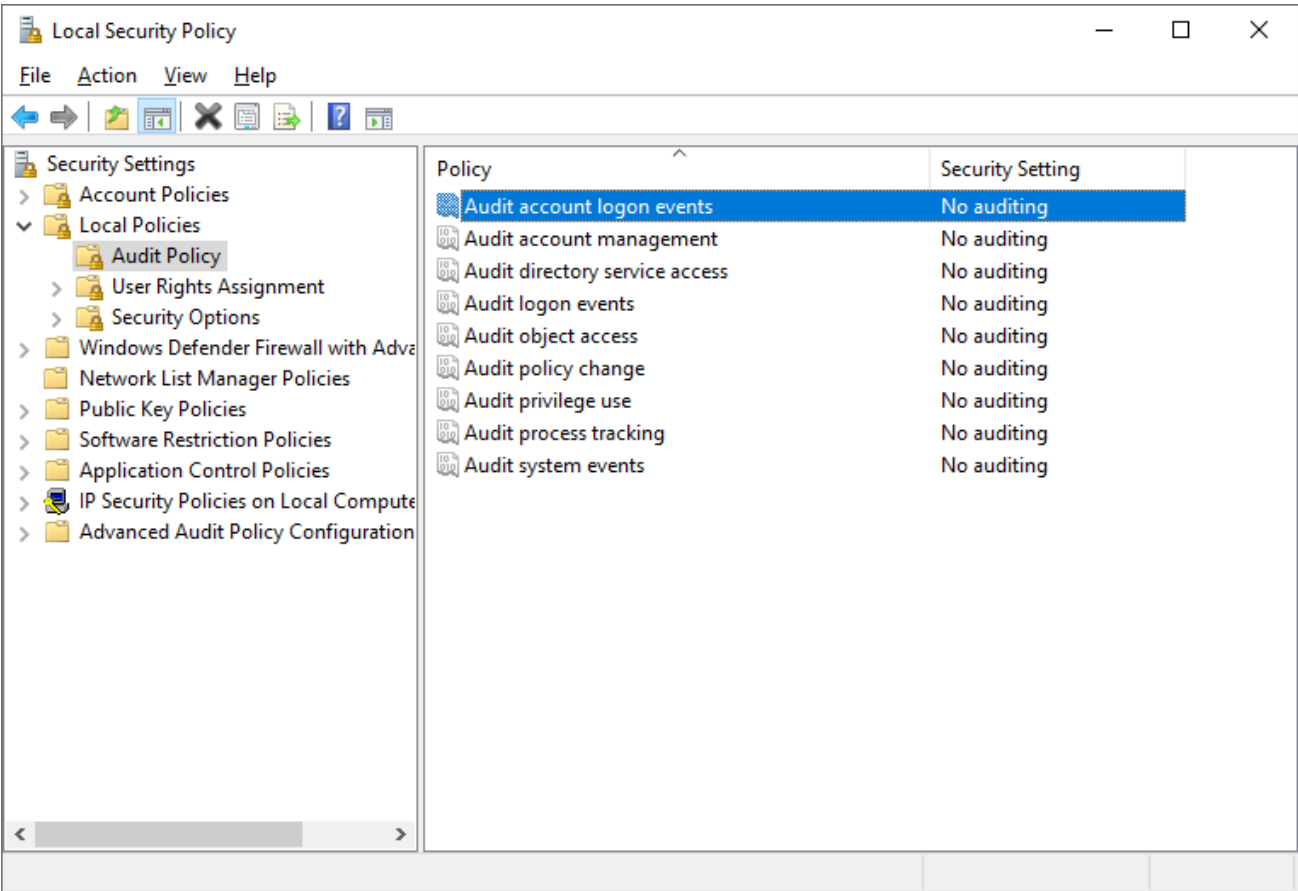
Optional Components

The follow section describes the [optional components](#) or capabilities of the [Windows machine agent](#).

These components may not be available on all Windows operating systems.

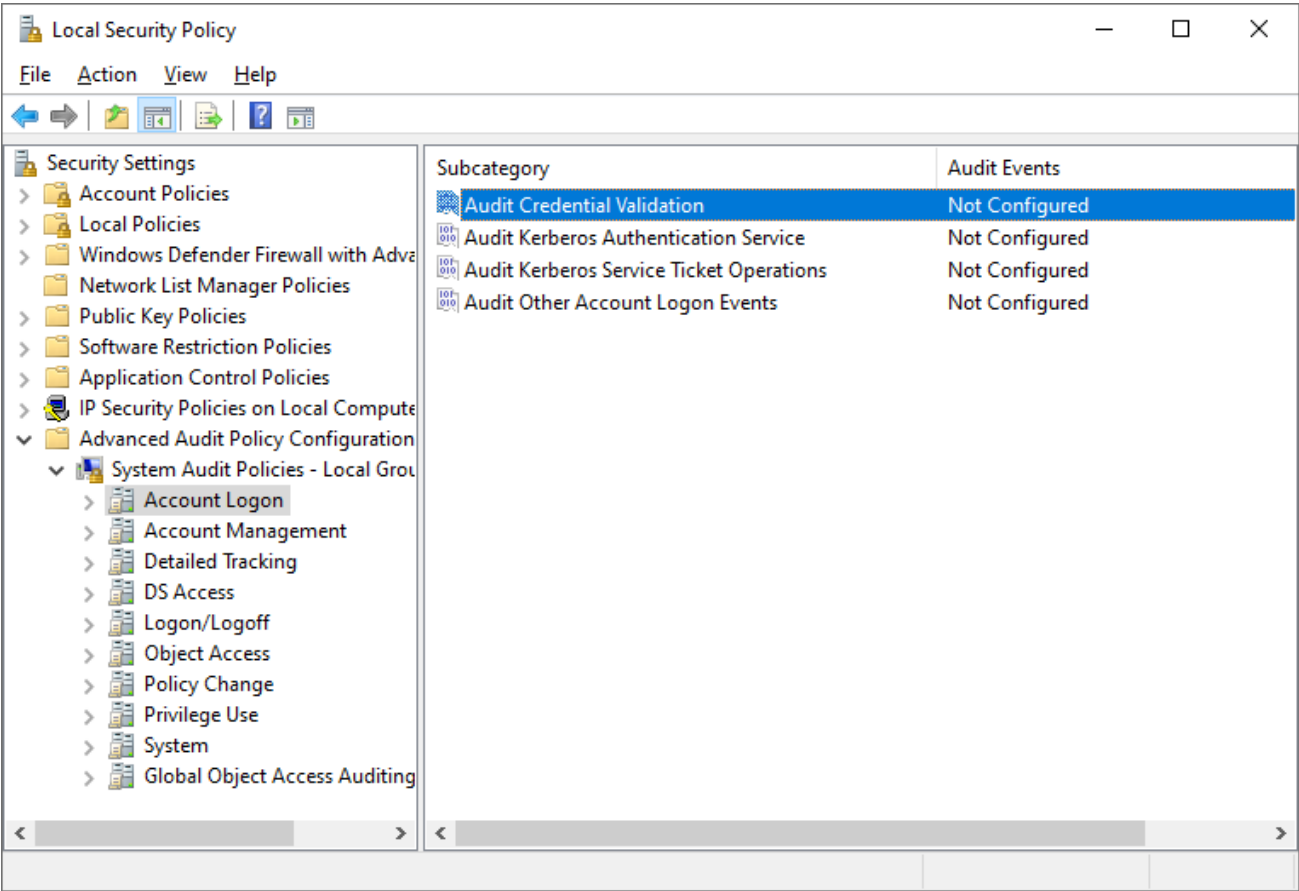
Audit Policy

The Audit Policy in Windows allows for the configuration of what actions should be audited. For more granular configuration of audit policies see [Advanced Audit Policy](#).



Advanced Audit Policy

The [advanced audit policy](#) in Windows allows more granular configuration of [audit policies](#).



XIA Configuration can collect this information on machines that are running Windows 2008 R2 or above that have [PowerShell remoting](#) enabled.

Device and Driver Information

The device drivers [optional component](#) determines whether the device and drivers installed on a [Windows machine](#) should be documented by the [Windows machine agent](#).

The information collected resembles that seen in Windows Device Manager.

NOTE: The device driver information is not available on operations systems prior to Windows Server 2003. No device information is collected for [Nano Server](#).

NOTE: The device class names may appear more accurately when the [Windows machine](#) is scanned using [PowerShell remoting](#) rather than [WMI](#). This is due to the class name being resolved on the machine being scanned, rather than the machine running the [XIA Configuration Client](#).

Disk Drives

The disk drives [optional component](#) determines whether the disk drives on a [Windows machine](#) should be documented by the [Windows machine agent](#).

The disk drives shown are the Windows operating system's concept of a disk device

The following information is only available when the [Windows machine](#) is running Windows Server 2012 or above, and is scanned using [PowerShell Remoting](#).

- Disk drives that are members of a storage pool.
- The GUID of GPT (GUID Partition Table) drives¹.
- The operational status of the drives.
- The drive location.
- Advanced bus types such as SATA or NVMe.

¹This information is not available for dynamic disks.

Installed Programs

The installed programs [optional component](#) determines whether the software installed on a [Windows machine](#) should be documented by the [Windows machine agent](#).

NOTE: Software installed on a per-user basis will not be detected by the [Windows machine agent](#).

NOTE: The display name of the installed program may differ slightly depending on whether the [Windows machine agent](#) collected the information using [WMI](#) or [PowerShell remoting](#). This is because the agent is able to resolve the localized names of the installed software when using [PowerShell remoting](#).

NOTE: The install date of the installed program will always be available when scanned using [PowerShell remoting](#), however may not always be available when using [WMI](#). This is because the agent is able to determine the install date for applications that don't register an "InstallDate" property when using [PowerShell remoting](#).

Local Administrator Password Solution (LAPS)

The [Local Administrator Password Solution \(LAPS\)](#) is a [Microsoft](#) installable solution that provides the ability to automatically update local administrator account passwords for domain joined computers.

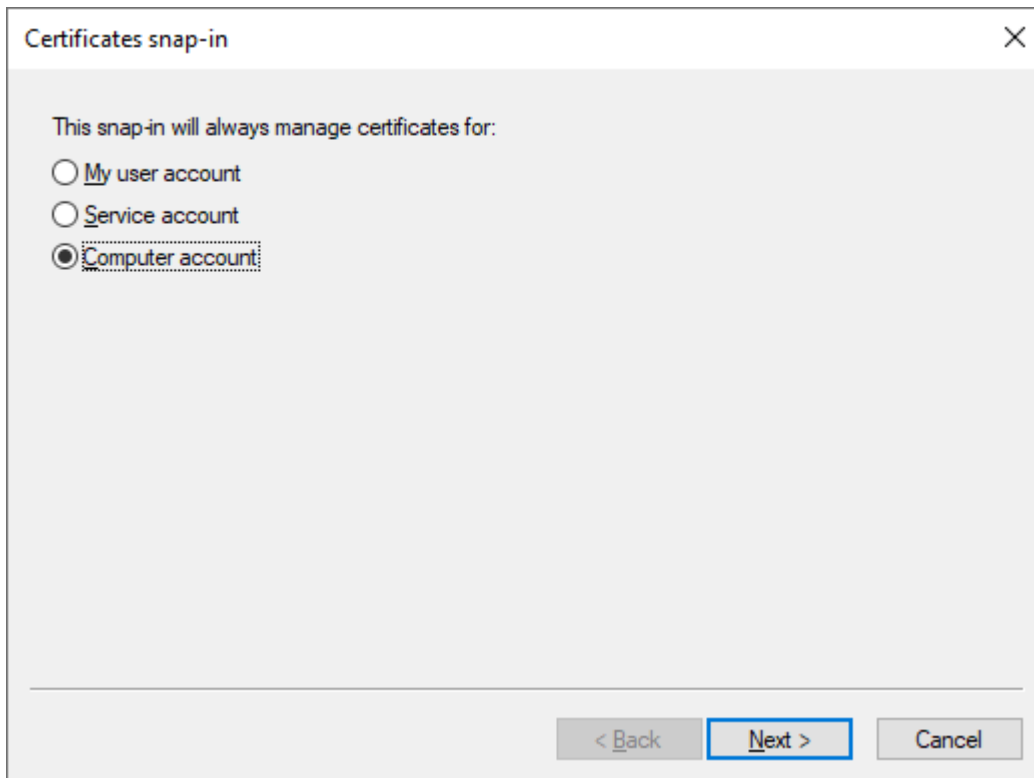
The [XIA Configuration Client](#) can collect this information on machines that are running Windows 2003 and Windows Vista or above that are domain joined and have the LAPS client installed.

NOTE: Information is not applicable to domain controllers and therefore not displayed.

Machine Certificates

The machines certificates section displays information about the X.509 certificates (commonly known as SSL certificates) that are found in the machine certificates store.

This information mirrors what is seen in the certificates MMC snap-in when "Computer account" is selected.



NOTE: The *Valid From* and *Expiry Date* fields are displayed in [XIA Configuration Server](#) as Coordinated Universal Time (UTC).

Management Controller

Management controllers (known as out of band management controllers) are hardware devices installed by some server manufacturers and allow the remote management and control of a server even when the machine is physically powered off.

To obtain this information the [XIA Configuration Client](#) must have access to the server using SNMP and the manufacturer and model of the server must be supported.

For more information about SNMP please see the [SNMP Settings](#) section.

Hewlett-Packard

Management controllers within Hewlett-Packard servers are known as iLO (Integrated Lights Out).

To document iLO devices the HP management agents must be installed on the server that support **cpq-sm2.mib**. Viewing the HP Systems Management Homepage on the remote server allows you to confirm that the information will be available to the [XIA Configuration Client](#).

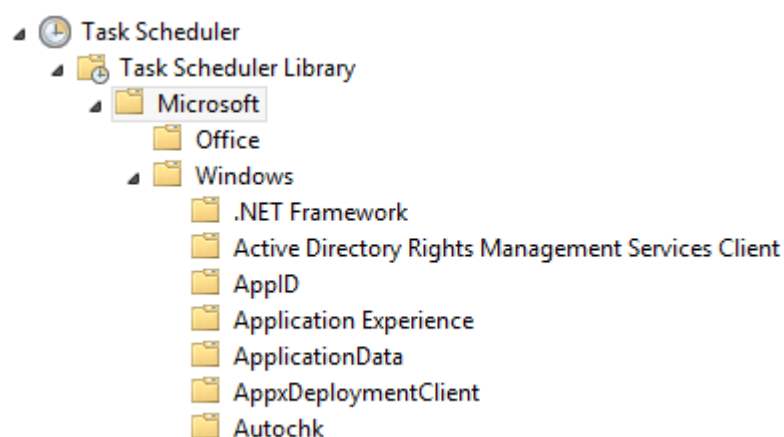
Scheduled Tasks

Scheduled Tasks are configured using the Task Scheduler MMC snap-in which helps you to schedule automated tasks that perform actions at a specific time or when a certain event occurs. For older operating system such as Windows XP, Windows Server 2003 and older please see the [scheduled tasks \(classic\)](#) section.

The [Windows machine agent](#) can scan scheduled tasks either using a combination of WMI and administrative shares, or on Windows Server 2012 and above, using [PowerShell remoting](#).

Microsoft Built-In

Within the Task Scheduler are an array of built-in Microsoft scheduled tasks. These are not scanned by the [Windows machine agent](#) by default, unless explicitly enabled in the [optional components](#) section.



Time Zones

Within the scheduled tasks the start (or "activate") and expiry of the task can be configured to synchronize across time zones. When synchronize across time zones is checked and the settings are read using WMI and administrative shares the time will be displayed based on the time zone of the server running the [XIA Configuration Client](#). When scanned using [PowerShell remoting](#) the time will be displayed as it is on the machine being scanned.

Group Policy Preferences

The [Windows machine agent](#) is able to document scheduled tasks created manually, or using Group Policy objects.

Scheduled Tasks (Classic)

Scheduled Tasks allow you to schedule automated tasks that perform actions at a specific time or when a certain event occurs.

For older operating systems including Windows XP, Windows Server 2003 and older, these are referred to as "Classic Scheduled Tasks".

Newer operating systems including Windows Server 2008, Windows Vista, and above use the newer Task Scheduler Library. For more information see the [scheduled tasks](#) section.

Security Options

Security options policy settings allow you to configure the behavior of the local computer.

For more information see the following page

<https://docs.microsoft.com/windows/device-security/security-policy-settings/security-options>

The following settings are only read by the [XIA Configuration Client](#) when they are configured in a group policy object. If they are configured locally they are not displayed, though information about the Administrator and Guest account can also be viewed in the "Local User Accounts" section.

- Accounts: Administrator account status
- Accounts: Guest account status
- Accounts: Rename administrator account
- Accounts: Rename guest account
- Network access: Allow anonymous SID/Name translation
- Network security: Force logoff when logon hours expire

Windows Firewall

The [Windows Machine](#) agent is capable of documenting the [Windows Firewall with Advanced Security](#) settings on Windows Server 2008 and above and Windows 7 and above.

The system can use either [PowerShell remoting](#) or the Windows Firewall API to collect the information. When scanning using [PowerShell remoting](#), firewall rules configured using Group Policy can be documented, however using the Firewall API they cannot.

- For the scan to be successful using the Windows Firewall API the computer running the [XIA Configuration Client](#) must be running Windows Server 2008 and above or Windows 7 and above.
- For the scan to be successful using [PowerShell Remoting](#), [PowerShell Remoting](#) must be enabled on the remote machine and the remote machine must be running Windows 8, Windows Server 2012 or above.

By default the [Windows machine agent](#) will attempt to document the [Windows Firewall with Advanced Security](#) configuration, however individual rules are not documented, to enable or disable these options see the [options tab](#) page.

Windows Patches

The Windows patches section displays information about the patches installed on a [Windows machine](#). This section can be configured using the [optional components](#) tab.

The information provided in this section is provided by the [Win32_QuickFixEngineering](#) WMI class, even when the machine is scanned using [PowerShell remoting](#).

Requirements

Windows machine scan tasks are supported on the following target **operating systems**. Some features may not be supported on all operating systems.

Supported target Windows **server** operating systems:

- Microsoft Azure Local (Microsoft Azure Stack HCI)
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 2008 Server R2
- Windows 2008 Server
- Windows 2003 Server R2
- Windows 2003 Server
- Windows 2000 Server SP2 and above
- Windows NT 4 Server SP6a

Supported target Windows **desktop** operating systems:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista

- Windows XP
- Windows 2000 Workstation SP2 and above
- Windows NT 4 Workstation SP6a

Windows Firewall Requirements

For more information see the [firewall requirements](#) section.

Access Settings

Depending on the [scan mode](#) the Windows machine agent can either scan

- Using [PowerShell remoting](#) only (Windows 8, Windows Server 2012 and above)
- or -
- Using a combination of WMI, access to administrative shares and other classic technologies.

The [service account](#) or [custom credentials](#) must have administrator rights on the remote machine. This is a requirement enforced by the operating system to access many of the security related settings on the machine.

Local Service

- ✔ The [Windows machine](#) scan tasks support the [local service](#).

This section is deprecated for the [Windows machine agent](#) when scanning machines running Windows 8, Windows Sever 2012, and newer. Instead it is recommended that the [scan mode](#) is configured to allow the [Windows machine](#) to be scanned using [PowerShell remoting](#).

Automatic Detection

- ✔ [Windows machines](#) can be automatically detected and scanned by [Active Directory Search](#) scan tasks.

Firewall Requirements

For Windows 8, Windows Server 2012 and above when [PowerShell remoting](#) is enabled only the following firewall port is required

Windows Remote Management (HTTP-In)

This port allows the PowerShell remoting connection on port TCP/5985.

For operating systems prior to Windows 8 and Windows Server 2012, or when then [scan method](#) is set to *Classic Only*, see the [firewall requirements \(classic\)](#) section.

Firewall Requirements (Classic)

When using [Windows Firewall with Advanced Security](#) the following rules should be enabled to allow the [XIA Configuration Client](#) to scan the remote machine.

NOTE: the rule names may differ depending on the version of Windows on the remote machine.

✔ **File and Printer Sharing (NB-Name-In) [UDP/137]**

This is required to resolve names if you are not using DNS.

✔ **File and Printer Sharing (Echo Request - ICMPv4-In) [ICMP]**

This is required to respond to ping requests. This is only necessary when trying to detect the [Windows machine](#) using the [Network Range Search \(WMI\)](#) with ICMP enabled.

✔ **Windows Management Instrumentation (DCOM-In)**

Allows [Windows Management Instrumentation](#) (WMI) queries to be executed.

✔ **Windows Management Instrumentation (WMI-In)**

Allows [Windows Management Instrumentation](#) (WMI) queries to be executed.

✔ **Remote Service Management (NP-In) [TCP/445]**

The scan will complete if this firewall port is blocked, however

- Descriptions of running processes cannot be read.
- Scheduled tasks (Windows 2008 and above) cannot be read.

✔ **Remote Service Management (RPC)**

Allows the dynamic ports required for WMI. The scan will **fail** if this firewall rule is blocked

✔ **RPC Dynamic Ports [Manual RPC Dynamic Ports Rule]**

This is a manually created rule, though predefined RPC rules exist they are bound to a specific application.

The scan will complete if this firewall rule is blocked, however

- Windows Update configuration cannot be read.
- Windows Firewall configuration cannot be read using the Firewall API, however PowerShell Remoting can also be used to read this information.

✔ **File and Printer Sharing (NB-Session-In) TCP/139**

The scan will complete if this port is blocked and the "Scan Local Accounts" is set to false, however

- User rights assignment cannot be read.
- Local account policies cannot be read.
- Local users and groups cannot be read.
- Members of the Remote Desktop Users group cannot be read.

Windows Remote Management (HTTP-In)

The scan will complete if this port is blocked however components that depend on [PowerShell Remoting](#) will fail - for example

- Windows [advanced audit policy](#) cannot be read.

Scanning Azure Virtual Machines

Windows machines running on [Microsoft Azure](#) can be scanned by the [Windows machine agent](#) in the same manner as other [Windows](#) based machines.

It is recommended that a copy of the [XIA Configuration Client](#) is [installed](#) in the [Microsoft Azure](#) environment to perform the scan.

To gather information on the [Microsoft Azure](#) virtual machine configuration see the [Azure tenant agent](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

Access is denied scanning WORKGROUP machines

Symptoms

When you scan a [Windows machine](#) that is a member of a WORKGROUP you may see the error Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))

Cause

This can be caused by [User Access Control](#) settings on the WORKGROUP machine.

More Information

When accessing the [Windows machine](#) using a local account that is not the Administrator user, the Administrator group privileges are removed by default.

Resolution

- Configure the scan to use the built-in Administrator account credentials on the [credentials tab](#) of the [scan profile](#).

- or -

- Change the following registry key on the machine being scanned

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
LocalAccountTokenFilterPolicy = 1

WARNING: This change affects the security level.

For more information see

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/user-account-control-and-remote-restriction>

Cannot validate argument on parameter 'InterfaceAlias'

Symptoms

When you scan a [Windows machine](#) you see the error

The Windows Machine Agent encountered an exception when 'Reading network adapters using PowerShell remoting'. The agent failed to read the section 'Network Adapters'. Error executing the command 'Get-NetAdapterDetails'. Cannot validate argument on parameter 'InterfaceAlias'. The argument is null. Provide a valid value for the argument, and then try running the command again.

Cause

This is caused when the network interface name has been removed from the registry.

Windows Server 2016 and above

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkSetup2\Interfaces\{*identifier*}\Kernel\IfAlias

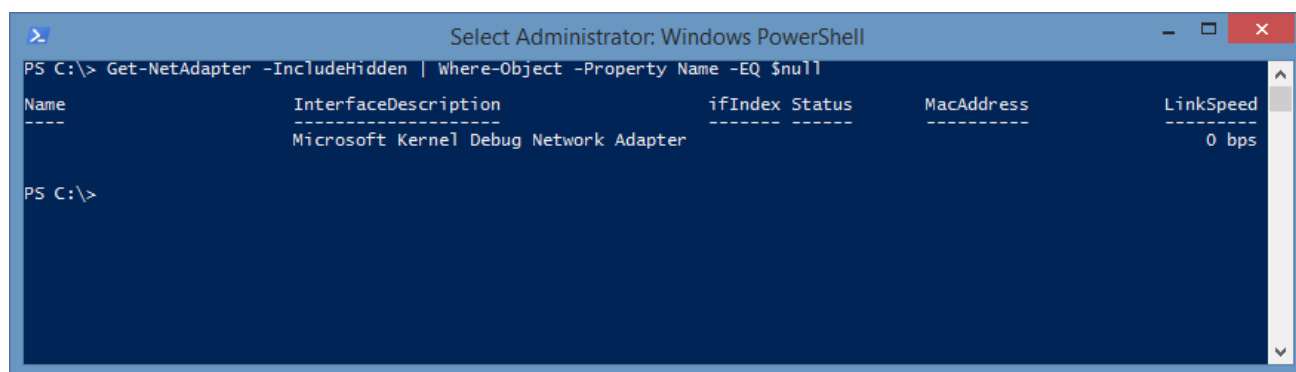
Windows Server 2012 R2 (binary value)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nsi\{*guid*}\index\value name

More Information

To find the adapter with the issue run the [Get-NetAdapter](#) cmdlet in PowerShell as an Administrator with the following parameters.

Get-NetAdapter -IncludeHidden | Where-Object -Property Name -EQ \$null



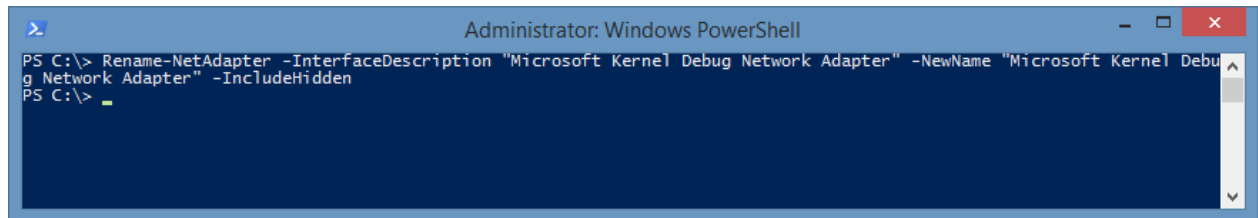
Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
	Microsoft Kernel Debug Network Adapter				0 bps

Resolution

WARNING: Ensure you have a full system backup before making any changes to the system.

- Using the interface description located in the command above execute the [Rename-NetAdapter](#) cmdlet in PowerShell as an Administrator with the following parameters.

```
Rename-NetAdapter -InterfaceDescription "Microsoft Kernel Debug Network Adapter" -  
NewName "New Name" -IncludeHidden
```



```
Administrator: Windows PowerShell
PS C:\> Rename-NetAdapter -InterfaceDescription "Microsoft Kernel Debug Network Adapter" -NewName "Microsoft Kernel Debug Network Adapter" -IncludeHidden
PS C:\>
```

- or -

- Remove the network adapter using Device Manager and re-add the adapter.

- or -

- Restore the system from a working backup.

- or -

- Set the Network Adapters [optional component](#) to "Do not scan" or "Scan (continue on failure)".

Error 0x80090350: An unknown security error occurred.

Symptoms

When you scan a [Windows machine](#) that is a member of a WORKGROUP from a domain member machine using [PowerShell remoting](#) you may see the error

Connecting to remote server *computername* failed with the following error message : WinRM cannot process the request. The following error with errorcode 0x80090350 occurred while using Negotiate authentication: An unknown security error occurred.

Cause

The error can occur when the following are true

- The computer running the [XIA Configuration Client](#) is a domain member and is running Windows Server 2008 R2.
- The [Windows machine](#) being scanned is a WORKGROUP member and is running Windows Server 2012 or above.
- [PowerShell remoting](#) is being used to scan the [Windows machine](#).

Resolution

- Upgrade the computer running the [XIA Configuration Client](#) to a newer operating system.
- or -
- Install a copy of the [XIA Configuration Client](#) to a machine running Windows Server 2008 R2 or above that is a member of the workgroup.

Error 80040154 reading Windows Update Configuration

Symptoms

When you scan a [Windows machine](#), the scan fails with the following error:

The agent failed to scan the section 'Windows Update Configuration'.

Retrieving the COM class factory for remote component with CLSID {91353063-774C-4F84-B05B-498FEC7FBE25} from machine demo-xcs02 failed due to the following error: 80040154.

Cause

This can be caused by the Windows update components not being installed on the machine.

Resolution

- Ensure that the Windows Update components are installed and configured on the target machine.

Workaround

- Within the [XIA Configuration Client](#), modify the Windows machine [agent settings](#) and on the [tolerance tab](#) enable the Windows Update tolerance option.

Error executing the command 'Get-ScheduledTaskDetails'

Symptoms

When you scan a [Windows machine](#) you see the error

Error executing the command 'Get-ScheduledTaskDetails'. The parameter is incorrect.

Cause

This is an internal issue with Windows.

More Information

Running PowerShell as Administrator on the [Windows machine](#) and executing the command [Get-ScheduledTask](#) also displays the error.

Resolution

Reboot the affected computer.

Error reading server features. Generic failure.

Symptoms

When you scan a [Windows machine](#) running a server operating system you may receive the error "Error reading server features. Generic failure."

Cause

This problem can be caused by a corrupt Windows files typically in the "C:\Windows\servicing\Packages" folder.

Running the **Server Manager** tool reports an error when viewing the Roles or Features on the server.

Resolution

- This is an operating system level problem and is out of the scope of this troubleshooting guide however more information may be obtained in the following article.
<http://support.microsoft.com/kb/947821/en-us>
- Configure the [XIA Configuration Client](#) to tolerate issues scanning the Windows Server Roles and Features on the [Tolerance](#) tab of the [Windows machine agent settings](#).

Error reading device driver information 'ThrowExceptionForHRInternal'

Issue

When scanning a [Windows machine](#) the agent fails when reading device driver information and the following error is seen

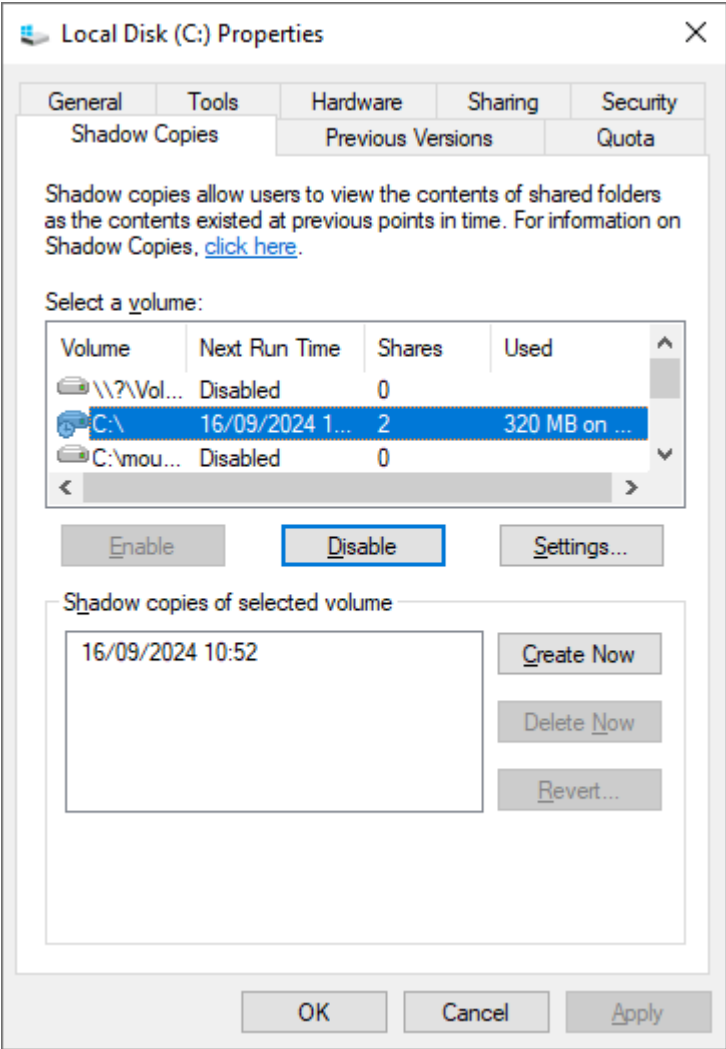
System.Runtime.InteropServices.COMException (0x800706BE) at
System.Runtime.InteropServices.Marshal.ThrowExceptionForHRInternal(Int32 errorCode, IntPtr
errorInfo)

Cause

This error can be caused when there are excessive volume shadow copies created for a drive.

Resolution

View the shadow copies configured for the drives on the [Windows machine](#) and remove as necessary.



More Information

The WMI query causing the issue can be tested directly by executing the following WQL using [wbemtest.exe](#).

```
SELECT * FROM Win32_PnpSignedDriver
```

Error reading security descriptor - unknown error (0x8004101d)

Issue

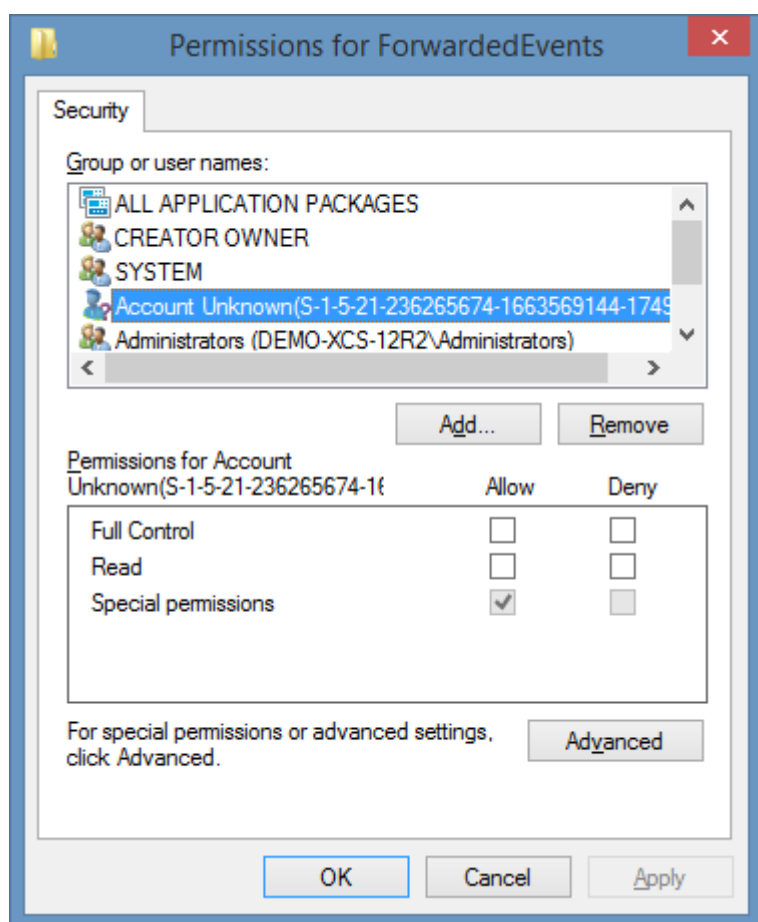
When scanning a [Windows machine](#) the agent fails when reading registry security descriptors and the following error is seen

Error reading the registry security descriptor for 'path'. Unknown error (0x8004101d).

Cause

This error can be caused when there is an unresolved account name in the security descriptor and the [Windows machine](#) is being scanned using [Windows Management Instrumentation \(WMI\)](#).

The security descriptor can be viewed in regedit by right clicking the affected key and selecting *security*.



Resolution

To resolve this issue either

- Correct the security descriptor.
- or -
- Scan the [Windows machine](#) using [PowerShell remoting](#).

More Information

The issue is caused by an underlying limitation of the [GetSecurityDescriptor](#) method of the [StdRegProv](#) class.

Error reading Windows Update history - 0x80240FFF.

Issue

When scanning a [Windows machine](#) the agent fails when reading Windows Update history and the following error is seen

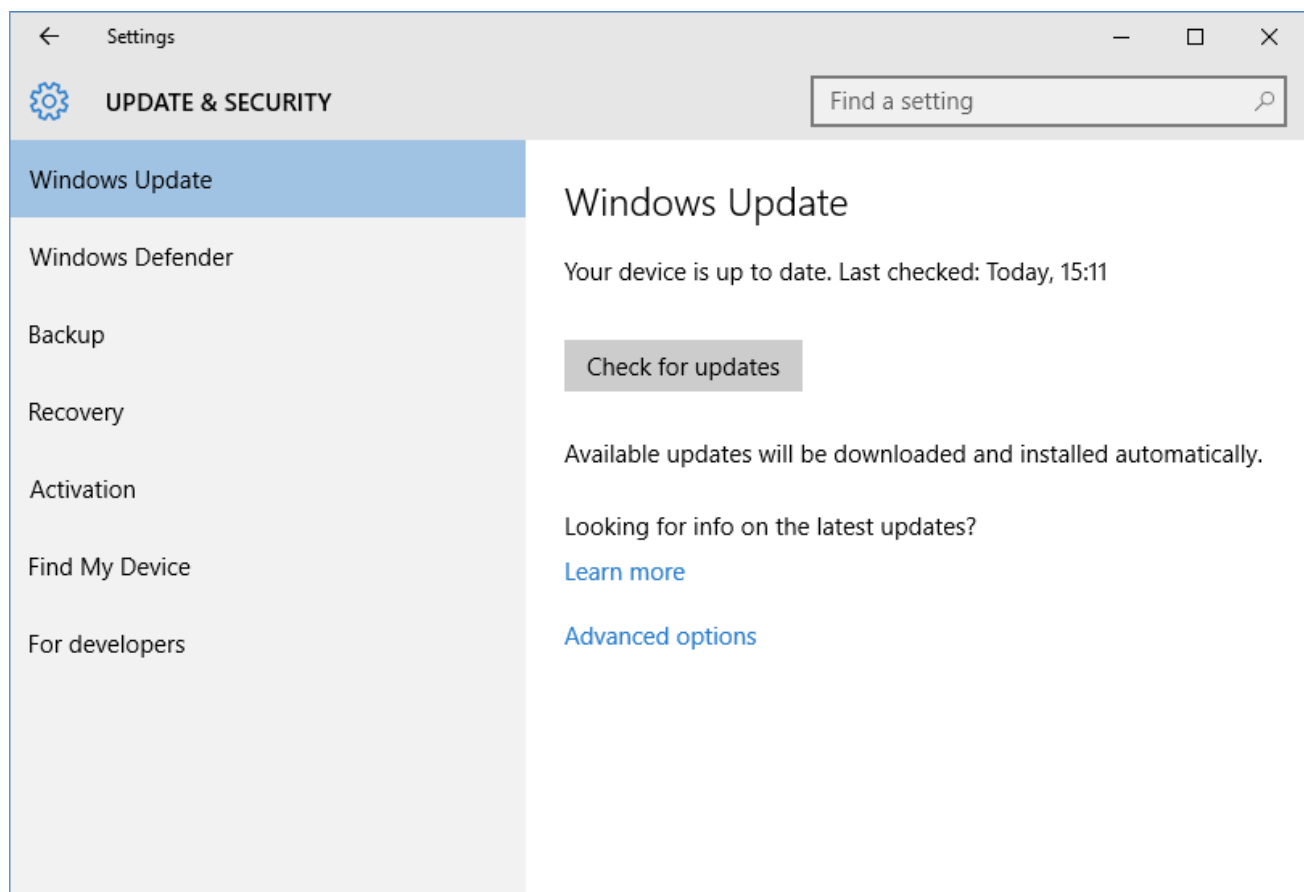
System.Runtime.InteropServices.COMException (0x80240FFF): Exception from HRESULT: 0x80240FFF

Cause

This error can be caused when there is an issue with the Windows Update configuration on the machine.

Resolution

Open the Windows Update configuration (see the operating system documentation for the affected operating system) on the machine and ensure that the machine can check for updates correctly. Resolve any issues as necessary and rescan the machine.



More Information

To test Windows Update history issues outside of the [XIA Configuration Client](#) see the [Testing Windows Update History](#) section.

Errors scanning Windows XP or Windows Server 2003 from up-level operating systems

Symptoms

When you scan a [Windows machine](#) that is running Windows XP, Windows Server 2003, or older you may see various scan errors including
The agent failed to scan the section 'Scheduled Tasks'. Could not contact the scheduled tasks system on '*machine name*'.

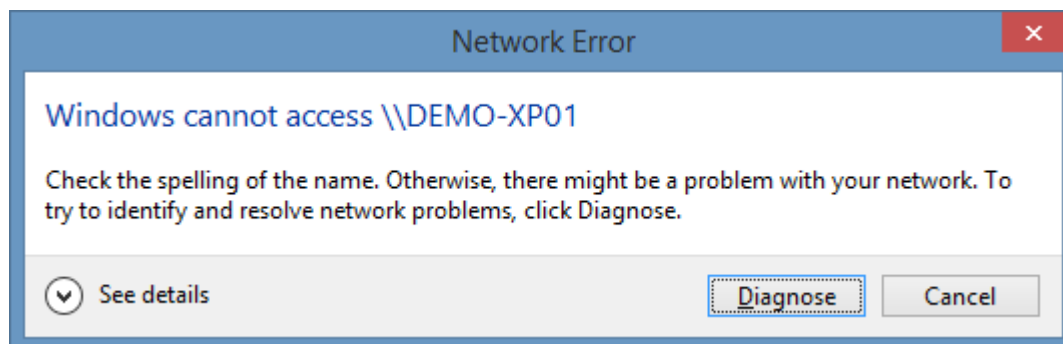
Cause

This issue can occur when using an up-level operating system such as Windows Server 2012 R2 or newer where SMB v1 has been disabled.

More Information

Windows XP, Windows Server 2003 and older operating systems only support SMB v1, an insecure version of the protocol. In newer Microsoft Windows operating systems this version of SMB is being disabled by default.

If you attempt to access the Windows XP, or Windows Server 2003 machine using a UNC path you may see the following error.



Resolution

Ensure that the SMB 1.0/CIFS File Sharing Support feature is installed.

WARNING: Enabling this feature reduces the security of the system and should only be performed if necessary.

Add Roles and Features Wizard

Select features

DESTINATION SERVER
DEMO-XCS-12R2

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

☐ Quality Windows Audio Video Experience

☐ RAS Connection Manager Administration Kit (CMA)

☐ Remote Assistance

☐ Remote Differential Compression

☐ Remote Server Administration Tools

☐ RPC over HTTP Proxy

☐ Simple TCP/IP Services

☒ SMB 1.0/CIFS File Sharing Support

☐ SMB Bandwidth Limit

☐ SMTP Server

☐ SNMP Service

☒ Telnet Client (Installed)

☐ Telnet Server

☐ TFTP Client

☒ User Interfaces and Infrastructure (Installed)

☐ Windows Biometric Framework

☐ Windows Feedback Forwarder

☐ Windows Identity Foundation 3.5

☐ Windows Internal Database

Description

Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.

< Previous

Next >

Install

Cancel

Page 1322 of 1553

XIA Configuration Administrator's Guide

Negotiate over HTTP error

Symptoms

When you scan a [Windows machine](#) you see the following error

Connecting to remote server failed with the following error message: The WinRM client cannot process the request. Default credentials with Negotiate over HTTP can be used only if the target machine is part of the TrustedHosts list or the Allow implicit credentials for Negotiate option is specified. For more information, see the about_Remote_Troubleshooting Help topic."

Cause

The [Windows machine agent](#) uses [Windows PowerShell remoting](#) to gather certain information from the remote machine. This error is seen when [custom credentials](#) are being used and the trusted hosts have not been configured for PowerShell.

Resolution

Follow the [Using Custom Credentials and PowerShell Remoting](#) instructions for the machine running the [XIA Configuration Client](#).

NTFS Permissions on 8.3 Paths

Issue

When you scan a [Windows machine](#) that has a shared folder that is shared against the 8.3 filename - for example "c:\mydocu~1" the NTFS permissions are not collected by the [XIA Configuration Client](#).

Cause

This is due to the [WMI](#) calls that [XIA Configuration Client](#) makes requiring the full path - for example "C:\My Documents".

Resolution

As 8.3 DOS style names are now deprecated it is recommended that you configure your shares to use the full Windows path names.

Reading shadow copy configuration: Provider failure.

Symptoms

When you scan a [Windows machine](#) running a server operating system you may receive the error "Reading shadow copy configuration for volume *Volume name*. Provider failure."

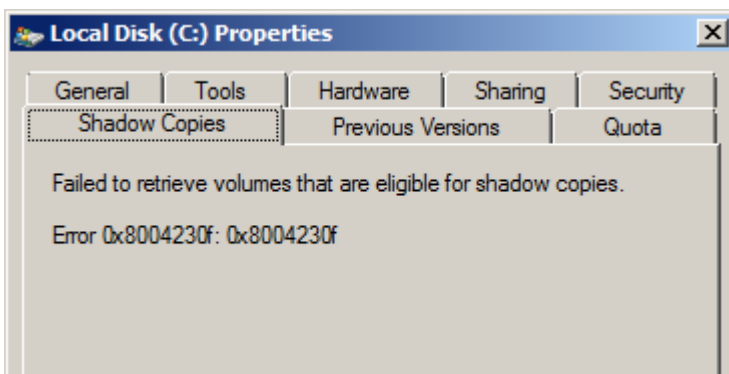
Cause

This problem can be caused by

- Misconfiguration of the Shadow Copy configuration on the server.
- Installation of the App-V version 4.x client

More Information

On the server open the properties of one of the volumes and ensure that the Shadow Copies tab reports the information correctly.



For more information about possible issues caused by the App-V client see the following page.
<https://support.microsoft.com/en-us/kb/2738812>

Resolution

- Review the event logs on the affected machine and resolve any Shadow Copy related configuration issues. Troubleshooting operating system issues is out of the scope of this document.
- Configure the [XIA Configuration Client](#) to tolerate issues scanning the Shadow Copy configuration on the [Options](#) tab of the [Windows machine agent settings](#).

Scanning Windows Firewall on Remote Desktop session hosts is exceptionally slow

Symptoms

When you scan a [Windows machine](#) that is a [Remote Desktop session host](#) you may find that scanning the [Windows Firewall](#) rules is exceptionally slow.

Cause

This can occur when the [Remote Desktop session host](#) is dynamically creating [Windows Firewall](#) rules for each logon and those rules are not subsequently deleted after logoff. The dynamically created rules can number in the tens of thousands.

Inbound Rules		
Name	Group	Application Package
 Cortana	Cortana	microsoft.windows.cortana_cw5n1h2bxewy
 Cortana	Cortana	microsoft.windows.cortana_cw5n1h2bxewy
 Cortana	Cortana	microsoft.windows.cortana_cw5n1h2bxewy
 Delivery Optimization (TCP-In)	Delivery Optimization	Any
 Delivery Optimization (UDP-In)	Delivery Optimization	Any
 Desktop App Web Viewer	Desktop App Web Viewer	microsoft.win32webviewhost_cw5n1h2bxewy

Resolution

- An update KB4467684 has been provided by Microsoft to address this issue <https://support.microsoft.com/topic/november-27-2018-kb4467684-os-build-14393-2639-7eb61afe-e3de-b34d-0d30-a77670f355fe>

Addresses an issue that slows server performance or causes the server to stop responding because of numerous Windows firewall rules.

To enable the changes, add a new registry key "DeleteUserAppContainersOnLogoff" (DWORD) on "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy" using Regedit, and set it to 1.

- or -

- Exclude the [Windows Firewall](#) rules [optional component](#) for the affected [machines](#).

Testing Windows Update History

Issue

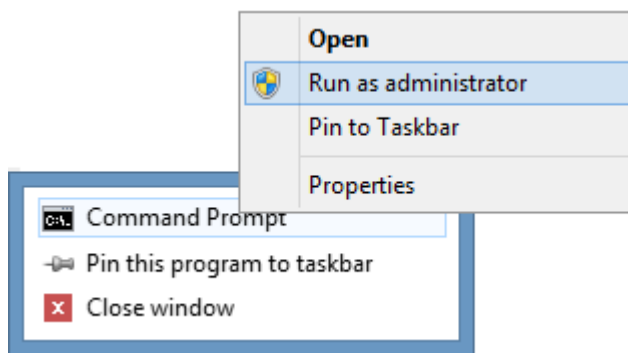
When scanning a [Windows machine](#) if the agent experiences an issue reading the Windows Update history you can test the access simply using VBscript.

Method

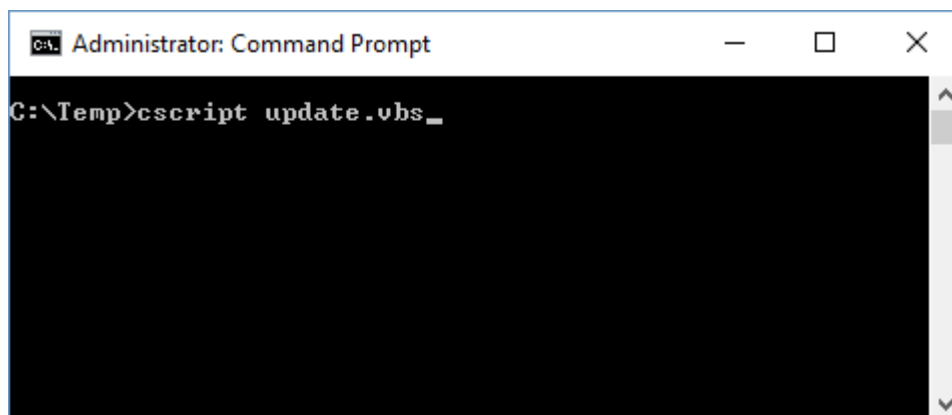
- Enter the following code into a text file, replacing the computer name with the name of the machine with the issue.
- Save the file with a .vbs extension

```
Set session = CreateObject("Microsoft.Update.Session", "ComputerName")
Set updateSearcher = session.CreateUpdateSearcher
intHistoryCount = updateSearcher.GetTotalHistoryCount
Set historyEntries = updateSearcher.QueryHistory(1, intHistoryCount)
For Each historyEntry in historyEntries
    Wscript.Echo historyEntry.Title
Next
```

- Run a command prompt as an administrator



- Start the script by running and note any errors shown
`cscript filename.vbs`



The client hangs when "Reading Windows Update Configuration"

Symptoms

When you scan a [Windows machine](#) you find that the client hangs when "Reading Windows Update Configuration".

Cause

This problem can be caused by a COM deadlock between WMI and other COM controls.

More Information

To replicate the issue outside of the [XIA Configuration Client](#) the following can be executed in PowerShell with **elevated** administrator privilege.

```
Write-Host "Getting WMI"
```

```
Get-WmiObject Win32_OperatingSystem -computer "computername"
```

```
Write-Host "Getting Windows Update"
```

```
$ObjWUA=$null
```

```
$ObjType = [type]::GetTypeFromProgID("Microsoft.Update.ServiceManager", "computername",  
$True)
```

```
$ObjWUA = [Activator]::CreateInstance($ObjType)
```

```
$ObjWUA.Services
```

Resolution

- Confirm the issue is not related to the [XIA Configuration Client](#) by executing the test PowerShell script listed above.
- Ensure there are no firewall or networking issues preventing the system from working correctly.

The Microsoft Storage Spaces SMP service is disabled

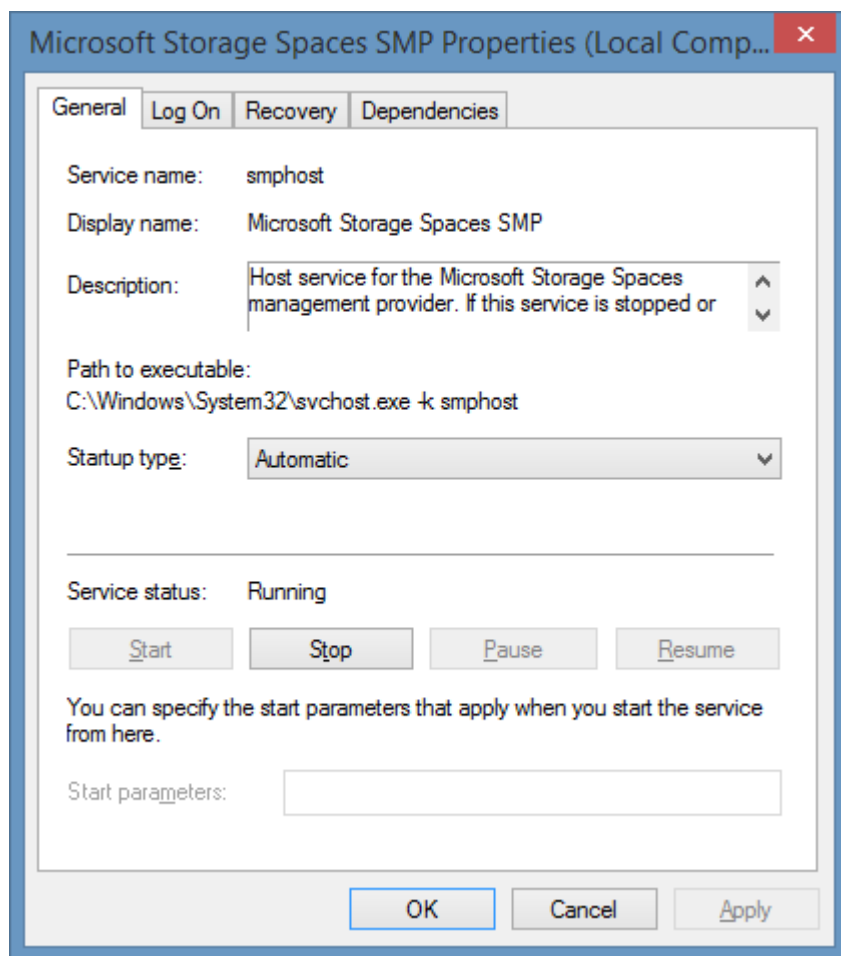
Symptoms

When you scan a [Windows machine](#) you encounter the error when scanning the disk volumes on the machine.

The Microsoft Storage Spaces SMP service is disabled. This service is required to read disk volumes on Windows 10, Windows Server 2016 and newer operating systems.

Cause

The Microsoft Storage Spaces SMP service is required to access information about disk volumes on Windows 10, Windows Server 2016 and newer operating systems when using [PowerShell remoting](#).



More Information

The [Windows machine agent](#) uses the [Get-Volume cmdlet](#) to access this information. This cmdlet itself has the dependency on the Microsoft Storage Spaces SMP service. Microsoft Server Manager will also be affected if this service is disabled.

Resolution

- Ensure that the Microsoft Storage Spaces SMP service is set to Manual or Automatic start-up.

- or -

- Configure the [agent settings](#) to use a classic connection. This is not recommended.

The network path was not found

Symptoms

When you scan a [Windows machine](#) you find that the client fails with a "The network path was not found" error when reading local user accounts.

Cause

This can be caused by a firewall blocking the [CIFS](#) port TCP/445.

More Information

The [Windows machine agent](#) uses the WinNT provider to read local user account information.

Resolution

- Ensure that port TCP/445 is open between the computer running the [XIA Configuration Client](#) and the [Windows machine](#) being scanned.

- or -

- If the [Windows machine](#) being scanned is on a separate, remote network consider [installing](#) a copy of the [XIA Configuration Client](#) in that network.

- or -

- Set the *Local Accounts* [optional component](#) to *Scan (Continue on Failure)*.

Timeout reading the driver file version on ODBC drivers

Symptoms

When scanning ODBC drivers file information is obtained for each ODBC driver.

Cause

It has been seen that servers experiencing issues with performance timeout when reading ODBC drivers.

Resolution

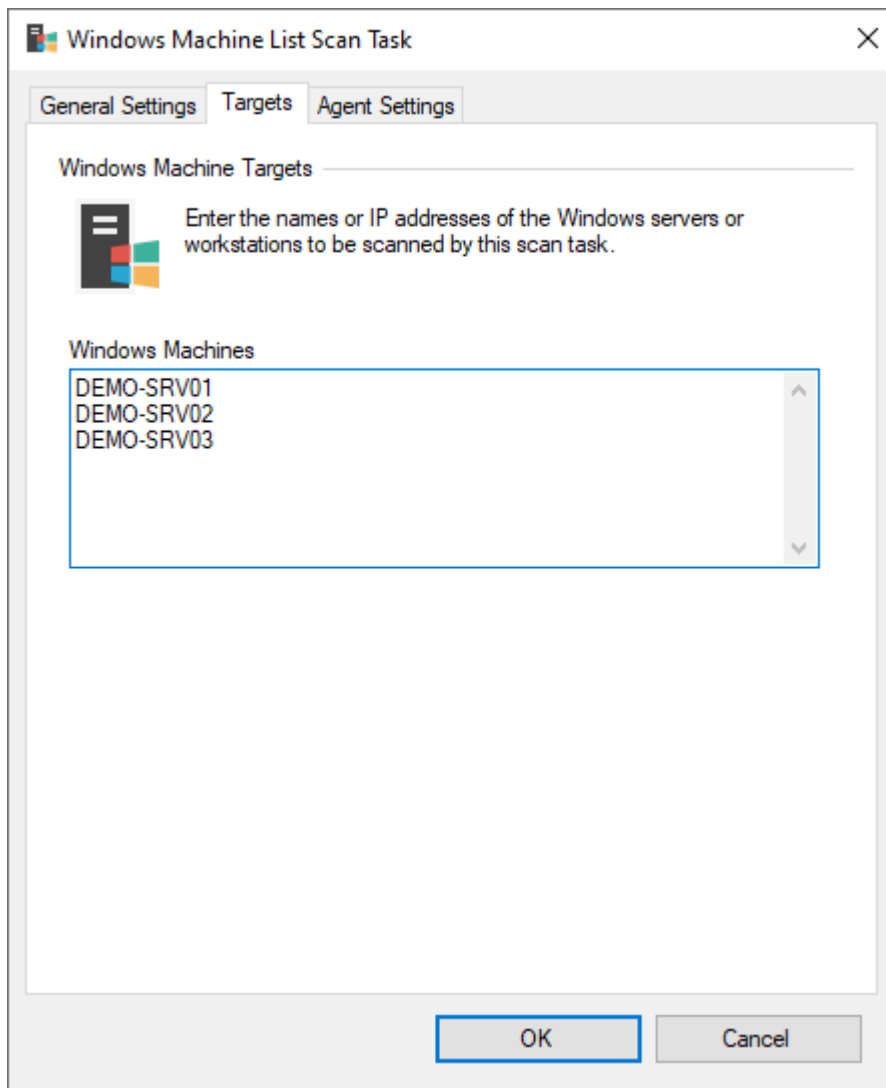
It has been seen that restarting the server has resolved this issue.

Windows Machine List Task

The Windows machine list task allows you to enter a list of machine names or IP addresses of the Windows machines that you wish to scan.

This task is useful for scanning a small number of specific machines, normally it is recommended that Windows machines are detected using the [Active Directory Search](#) scan task.

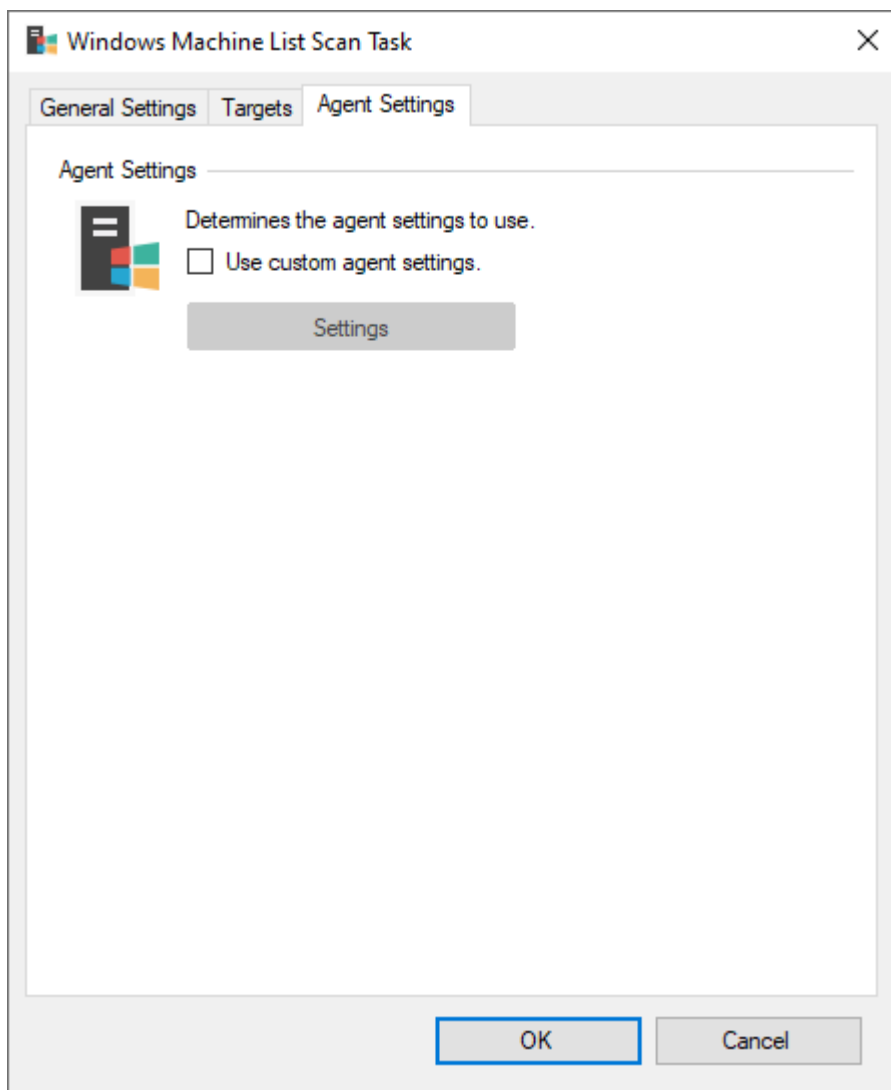
Targets



Windows Machines

The NetBIOS names, IP addresses, or fully qualified domain names of the [Windows machines](#) to scan, one per line.

Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

WINS Service

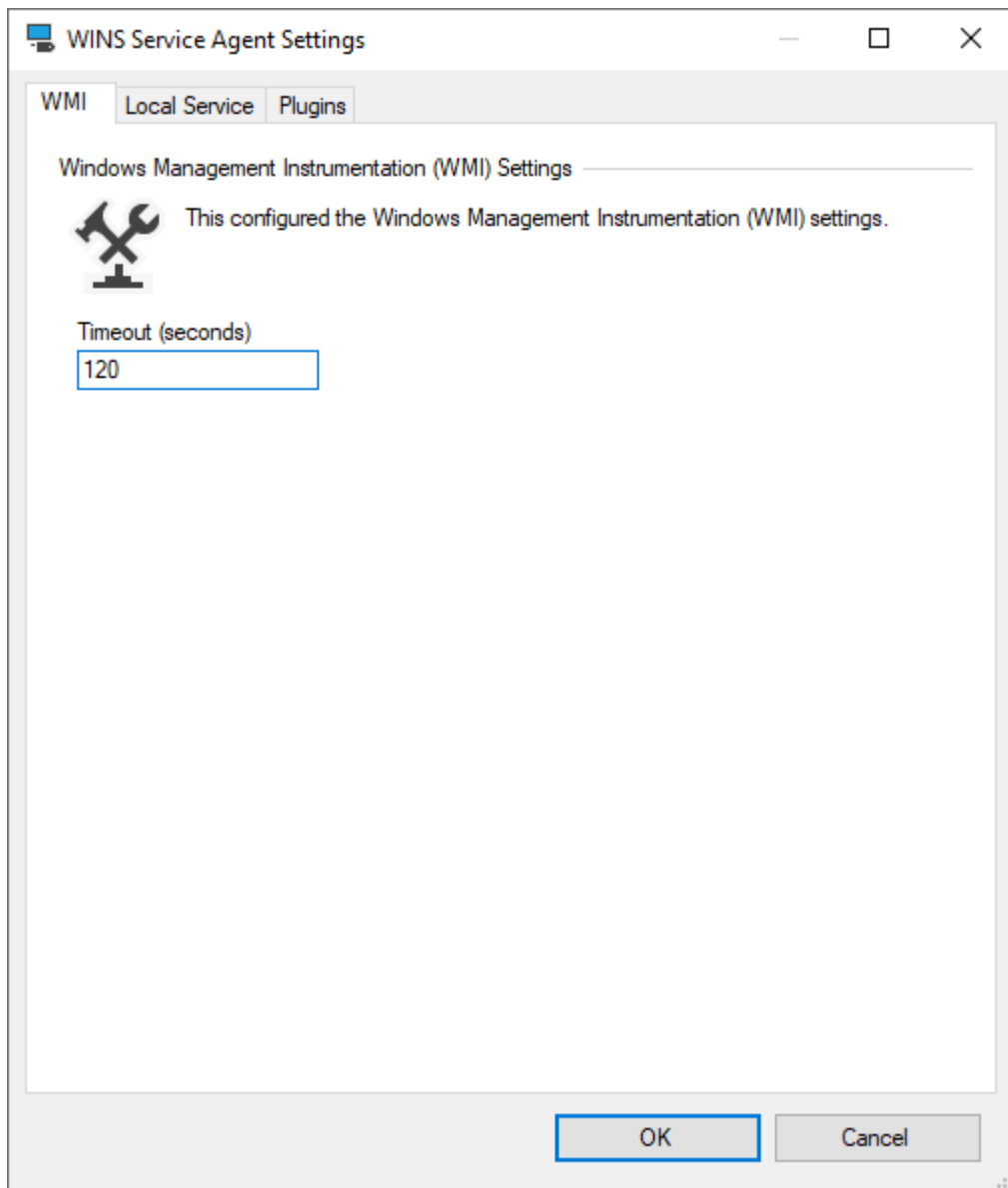
WINS Tasks are able to document WINS (Windows Internet Name Services) running on Windows Servers.

Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service. Running as a Windows Service, WINS provides a central mapping of NetBIOS computer names to IP addresses similar to the service provided by DNS.

The data located by these Tasks include the following information types:

- Database Settings
- Intervals
- Replication Settings
- Replication (Push and Pull) Partners

Agent Settings



WMI Timeout

The timeout in seconds to use for WMI connections.

Item Identifiers

For more information about Item Identifiers please see the [item identifiers](#) section.

Primary Identifier

The computer name.

Secondary Identifier

The computer serial number.

Tertiary Identifier

Not used.

Requirements

Supported Target Systems

The scan tasks are supported on the following target systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 Server SP2 and above
- Windows NT 4 Server SP6a

Access Settings

The Windows Machine agents use WMI to obtain WINS configuration settings from the registry of remote machines.

- Firewall access must allow access to the WMI ports on the remote machine
- The [service account](#) or [custom credentials](#) in use must have administrator rights on the remote machine (*this is a requirement for remote WMI access enforced by the operating system*).

Local Service

- ✓ These scan task are supported for use with the [local service](#).

Automatic Detection

- ✓ WINS services are automatically detected and scanned by [Windows machine scan tasks](#).

Troubleshooting

This section highlights the known issues for this specific agent and provides details of the solutions.

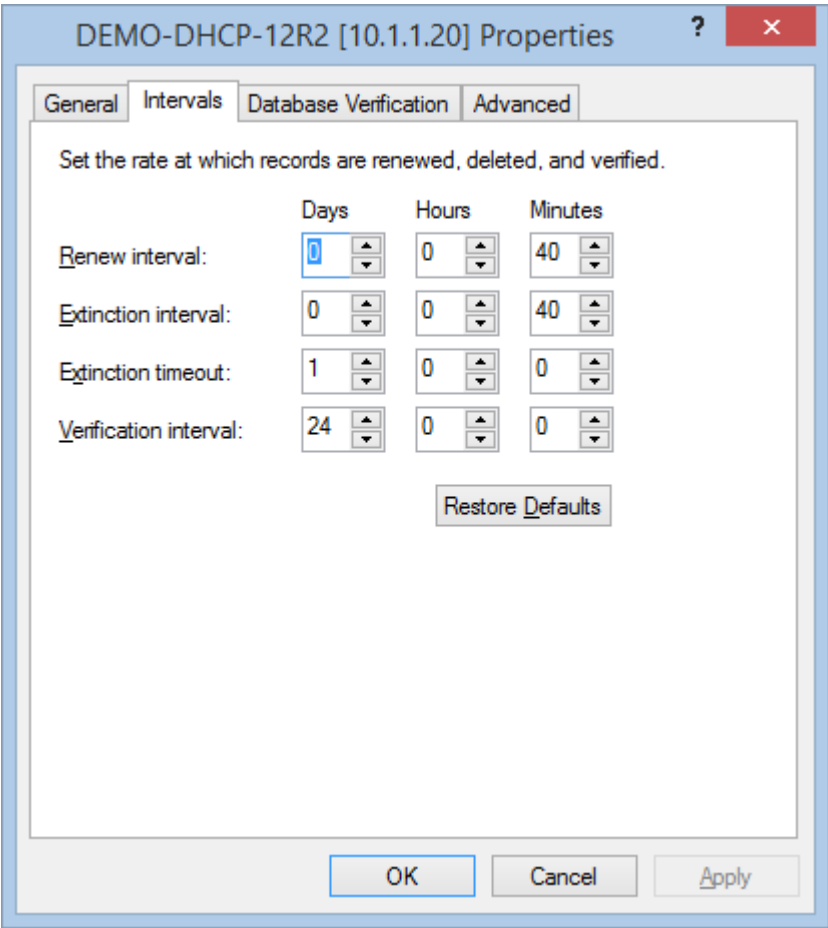
WINS service intervals show {Not Configured}

Symptoms

When you scan a **newly installed** WINS service that has yet to be configured several of the settings are displayed as {Not Configured}.

Intervals	
Renew Interval	{Not Configured}
Extinction Interval	{Not Configured}
Extinction Timeout	{Not Configured}
Verification Timeout	{Not Configured}

The settings are however displayed in the WINS MMC.



Cause

By default, when WINS is installed, the service does not set the registry entries for the service, what is displayed in the user interface are default settings.

Resolution

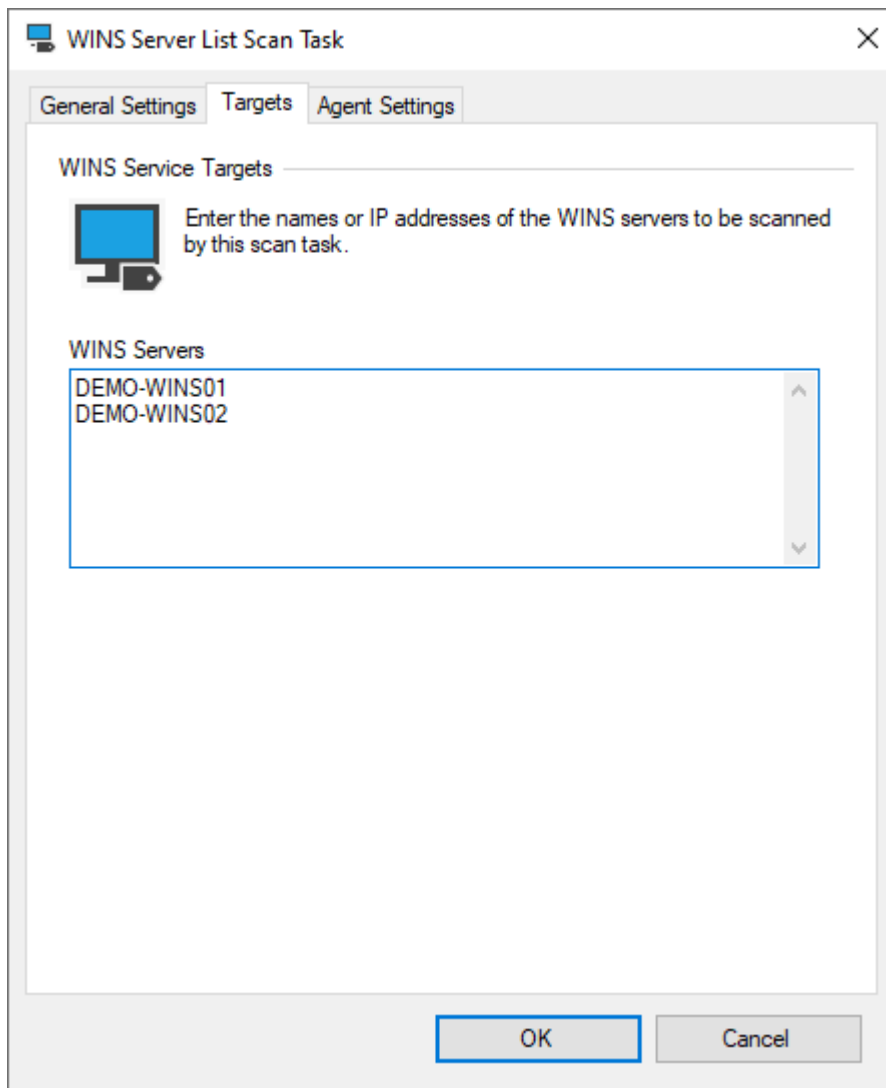
Open the server properties dialog for the WINS server and click OK. No changes to the configuration are required - all settings are then committed to the server.

WINS Service List Scan Task

The WINS service list scan task allows you to enter a list of [WINS services](#) you wish to scan.

NOTE: The [Windows machine](#) agent will by default automatically [detect](#) and scan [WINS services](#).

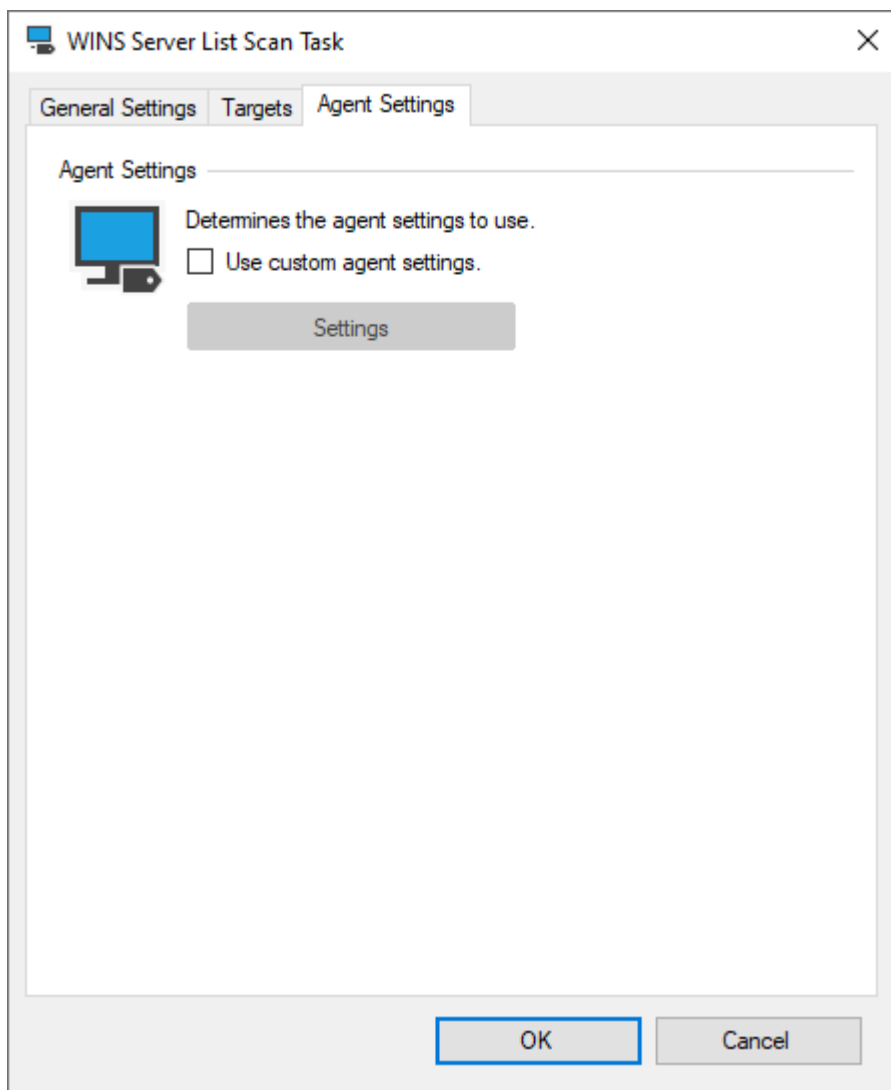
Targets



WINS Servers

The NetBIOS names, IP addresses, or fully qualified domain names of the [WINS servers](#) to scan, one per line.

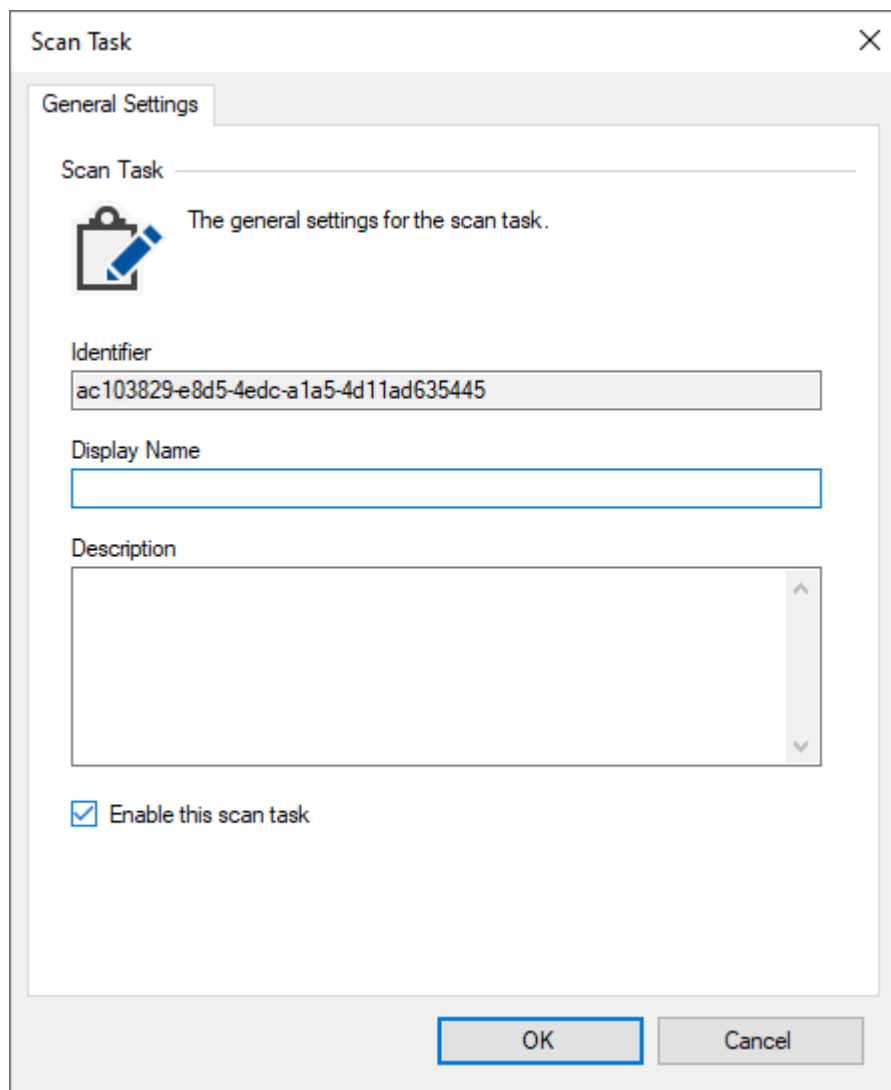
Agent Settings



Use custom agent settings

Determines whether to use custom [agent settings](#) rather than the [default agent settings](#) for the [scan profile](#).

General Settings



The screenshot shows a 'Scan Task' dialog box with a 'General Settings' tab. The dialog has a title bar with a close button. Inside, there's a section titled 'Scan Task' with a clipboard icon and the text 'The general settings for the scan task.' Below this are three input fields: 'Identifier' (containing 'ac103829-e8d5-4edc-a1a5-4d11ad635445'), 'Display Name' (empty), and 'Description' (empty text area). At the bottom, there's a checkbox labeled 'Enable this scan task' which is checked. The dialog ends with 'OK' and 'Cancel' buttons.

Scan Task

General Settings

Scan Task

The general settings for the scan task.

Identifier

ac103829-e8d5-4edc-a1a5-4d11ad635445

Display Name

Description

☒ Enable this scan task

OK Cancel

Identifier

The unique identifier of the scan task in [GUID](#) format.

Display Name

The display name of the [scan task](#).

Description

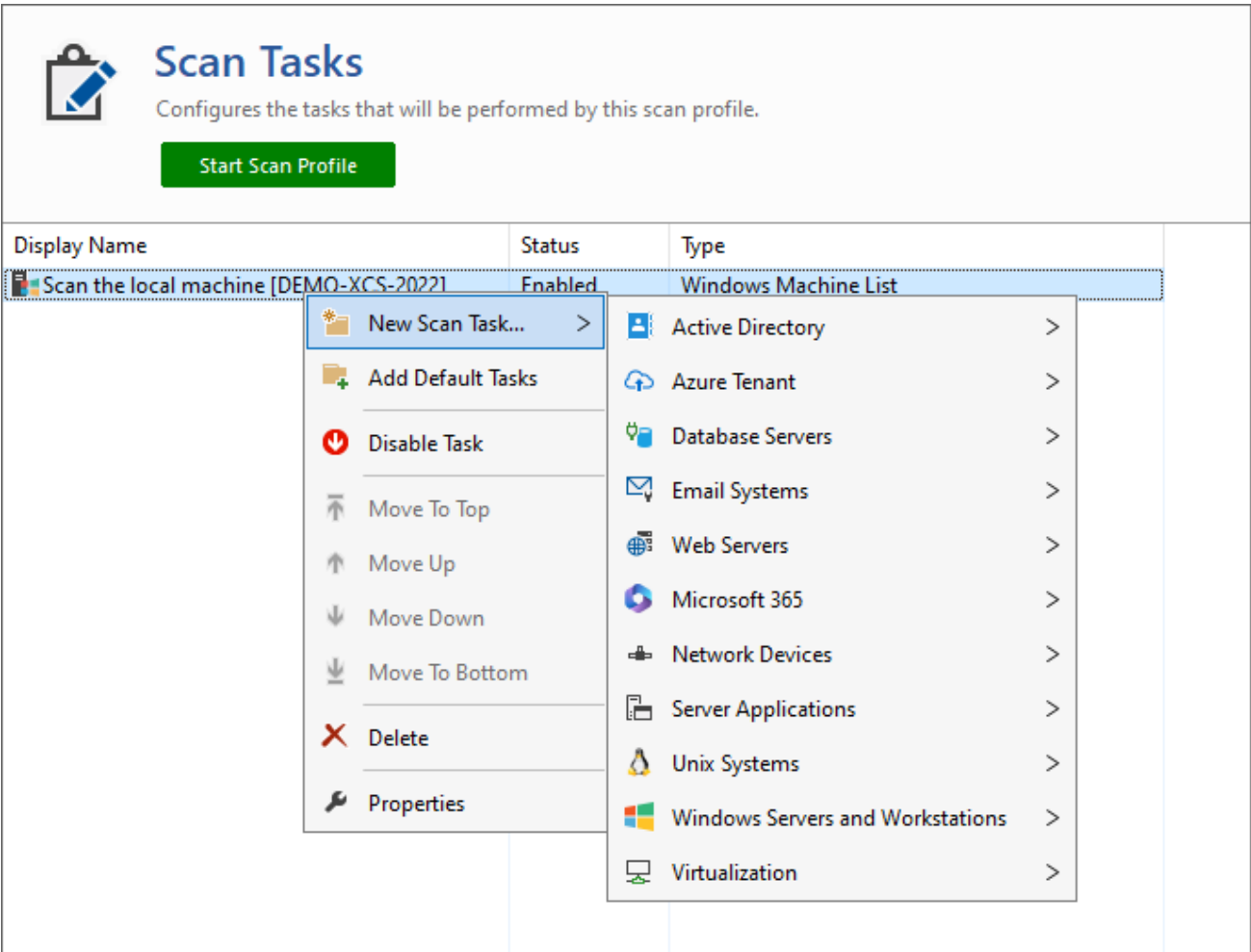
The description of the [scan task](#).

Enable this scan task

Determines whether the [scan task](#) is enabled.

Context Menu

Right clicking a [scan task](#) displays the context menu.



New Scan Task

Displays the possible [scan tasks](#) that can be created.

Add Default Tasks

Adds the default [scan tasks](#) that are normally created by [setup](#).

Enable / Disable Task

Enables or disables the [scan task](#) so that it is not run by the [scan profile](#).

Move To Top

Moves the [scan task](#) to the top of the list so that it is executed first.

Move Up

Moves the [scan task](#) up the list so that it is executed sooner.

Move Down

Moves the [scan task](#) down the list so that it is executed later.

Move To Bottom

Moves the [scan task](#) to the bottom of the list so that it is executed last.

Delete

Deletes the [scan task](#).

Properties

Displays the properties of the [scan task](#).

SDK

This section provides information related to [XIA Configuration Client](#) development.

For information related to [server development](#) please see the [server SDK](#) section.

Dynamic Agent Plugins

Dynamic agent plugins provide the ability to extend the capabilities of each agent using custom [C#.NET](#) code that is compiled and executed dynamically by the agent.

Dynamic agent plugins can be executed before or after the agent has completed the scan.



Dynamic Agent Plugins

Provides the configuration of the dynamic agent plugins available on this system.

New Agent Plugin

Display Name	Description
 Event Log Collection v1.0	Collects additional information from the Windows event log.

Display Name

The display name of the plug.

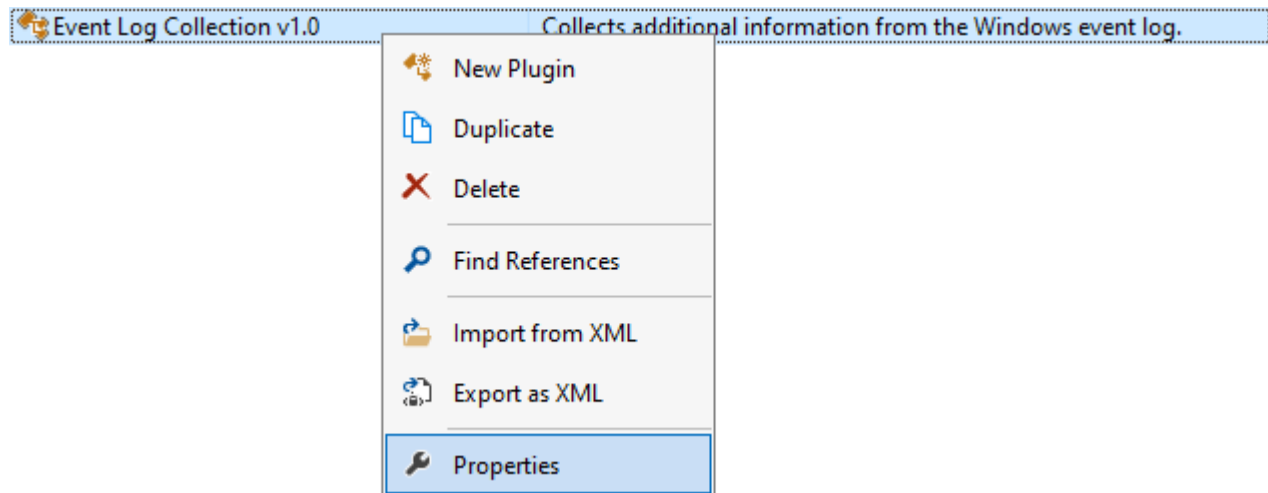
Description

The description of the plugin.

Right clicking a dynamic agent plugin shows the [context menu](#).

Context Menu

Right clicking a [dynamic agent plugin](#) displays the context menu.



New Plugin

Displays the [settings dialog](#) to add a new [plugin](#).

Duplicate

Creates a duplicate of the selected [plugin](#), with a new unique identifier.

Delete

Deletes the selected [plugin](#).

Find References

Finds any references where this [plugin](#) is used.

Import from XML

Imports a [plugin](#) from a saved XML file.

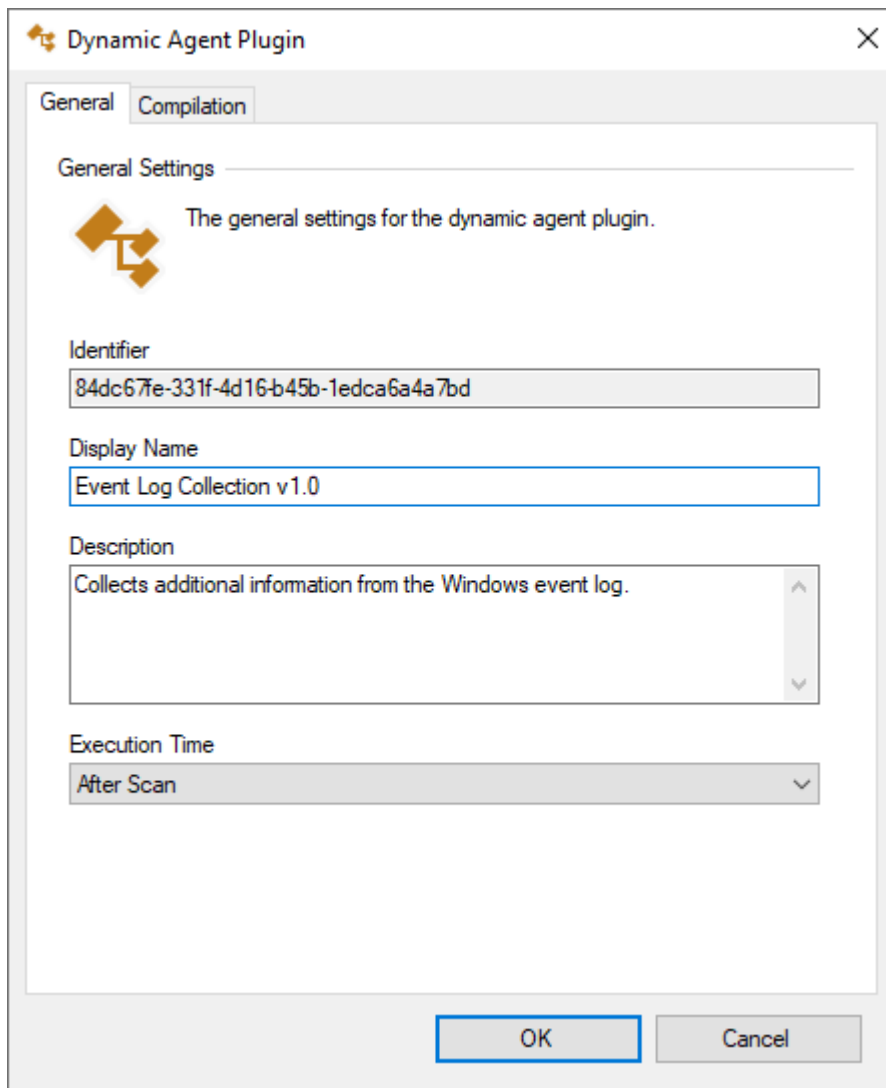
Save as XML

Saves the currently selected [plugin](#) to XML.

Properties

Displays the settings of the [plugin](#) in the [settings dialog](#).

Dynamic Agent Plugin Settings



The image shows a Windows-style dialog box titled "Dynamic Agent Plugin". It has two tabs: "General" (selected) and "Compilation". The "General Settings" section contains a description: "The general settings for the dynamic agent plugin." Below this are four fields: "Identifier" with the value "84dc67fe-331f-4d16-b45b-1edca6a4a7bd", "Display Name" with the value "Event Log Collection v1.0", "Description" with the value "Collects additional information from the Windows event log.", and "Execution Time" with a dropdown menu set to "After Scan". At the bottom are "OK" and "Cancel" buttons.

Dynamic Agent Plugin

General Compilation

General Settings

The general settings for the dynamic agent plugin.

Identifier

84dc67fe-331f-4d16-b45b-1edca6a4a7bd

Display Name

Event Log Collection v1.0

Description

Collects additional information from the Windows event log.

Execution Time

After Scan

OK Cancel

Identifier

The unique identifier for the [plugin](#) in [GUID](#) format.

Plugin Name

The display name of the [plugin](#).

Description

A description of the [plugin](#).

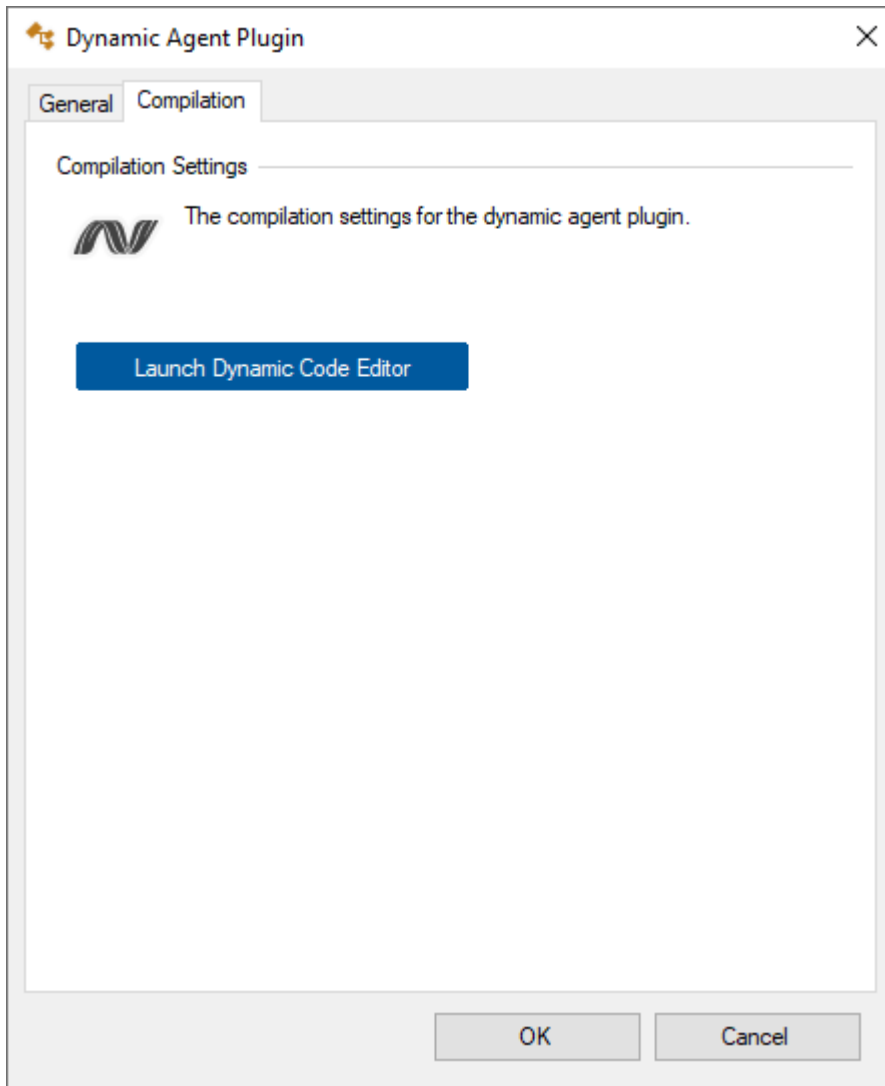
Before agent scan

The [plugin](#) will be executed before the agent has completed the scan.

After agent scan

The [plugin](#) will be executed after the agent has completed the scan.

Dynamic Agent Plugin Compilation

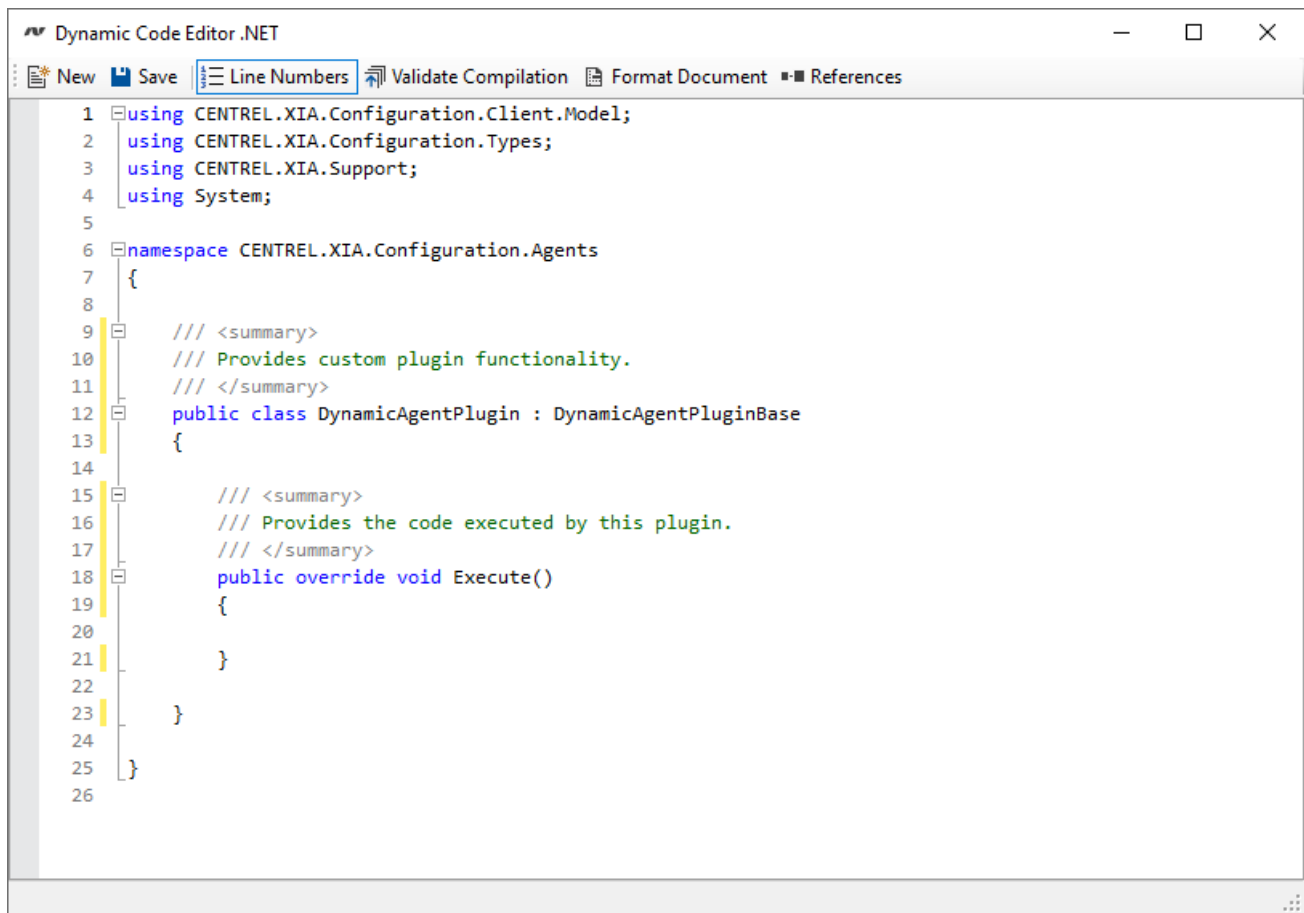


Launch Dynamic Code Editor

Opens the [dynamic code editor](#), allowing the modification of the custom code to be executed by the [plugin](#).

Dynamic Code Editor

The dynamic code editor allows the direct editing of the [C#.NET](#) code that is to be executed by the [plugin](#).



New

Clears the code and loads the default code.

Save

Saves the current code.

Line Numbers

Determines whether line numbers should be displayed in the editor.

Validate Compilation

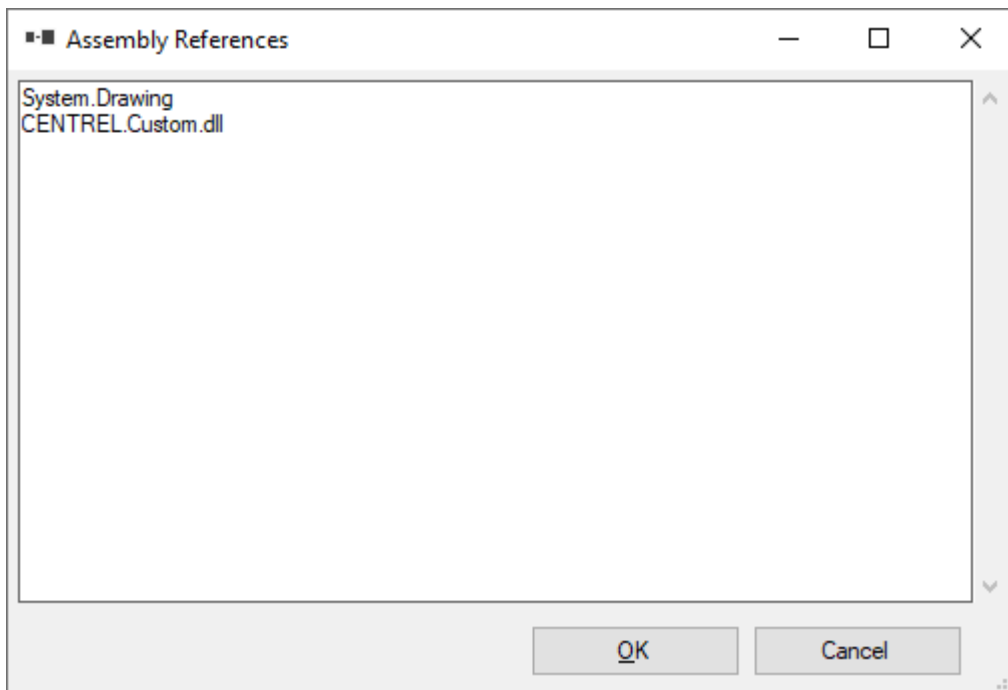
Compiles the source code and displays any compilations errors.

References

Allows the selection of the [assembly references](#).

Assembly References

Both assemblies inducing in the [.NET framework](#) and 3rd party assemblies may be referenced using assembly references.



- Enter the full name of the external assembly references including the ".dll" file extension.
- For built in .NET assemblies enter the assembly name **without** the extension.

The [dynamic code editor](#) automatically loads the assembly and provides [IntelliSense](#) style support.

```
System.Drawing.Image.FromFile(
```

▲ 1 of 2 ▼  **Image Image.FromFile(string filename)**
Creates an System.Drawing.Image from the specified file.
filename: A string that contains the name of the file from which to create the System.Drawing.Image.

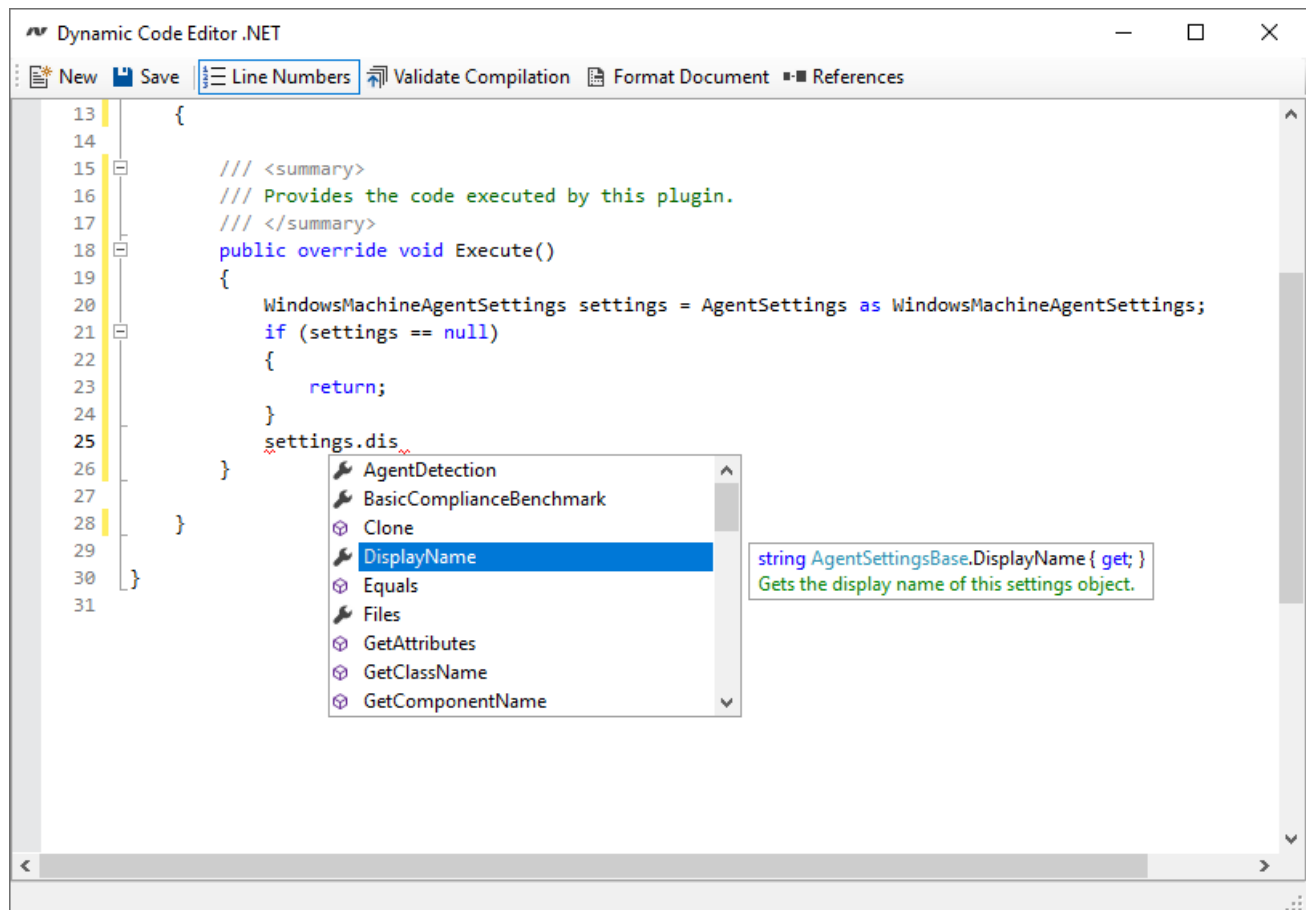
NOTE: The following assemblies are referenced automatically and do not need to be specified

- mscorlib.dll
- System.Core.dll
- System.dll
- System.Management.Automation.dll
- CENTREL.XIA.Configuration.Agents.DynamicAgentPluginBase.dll
- CENTREL.XIA.Configuration.Agents.BaseAgent.dll
- CENTREL.XIA.Configuration.Client.Model.dll
- CENTREL.XIA.Configuration.Types.dll
- CENTREL.XIA.Support.dll

Agent Settings

The settings used to execute the agent can be accessed using the *AgentSettings* property.

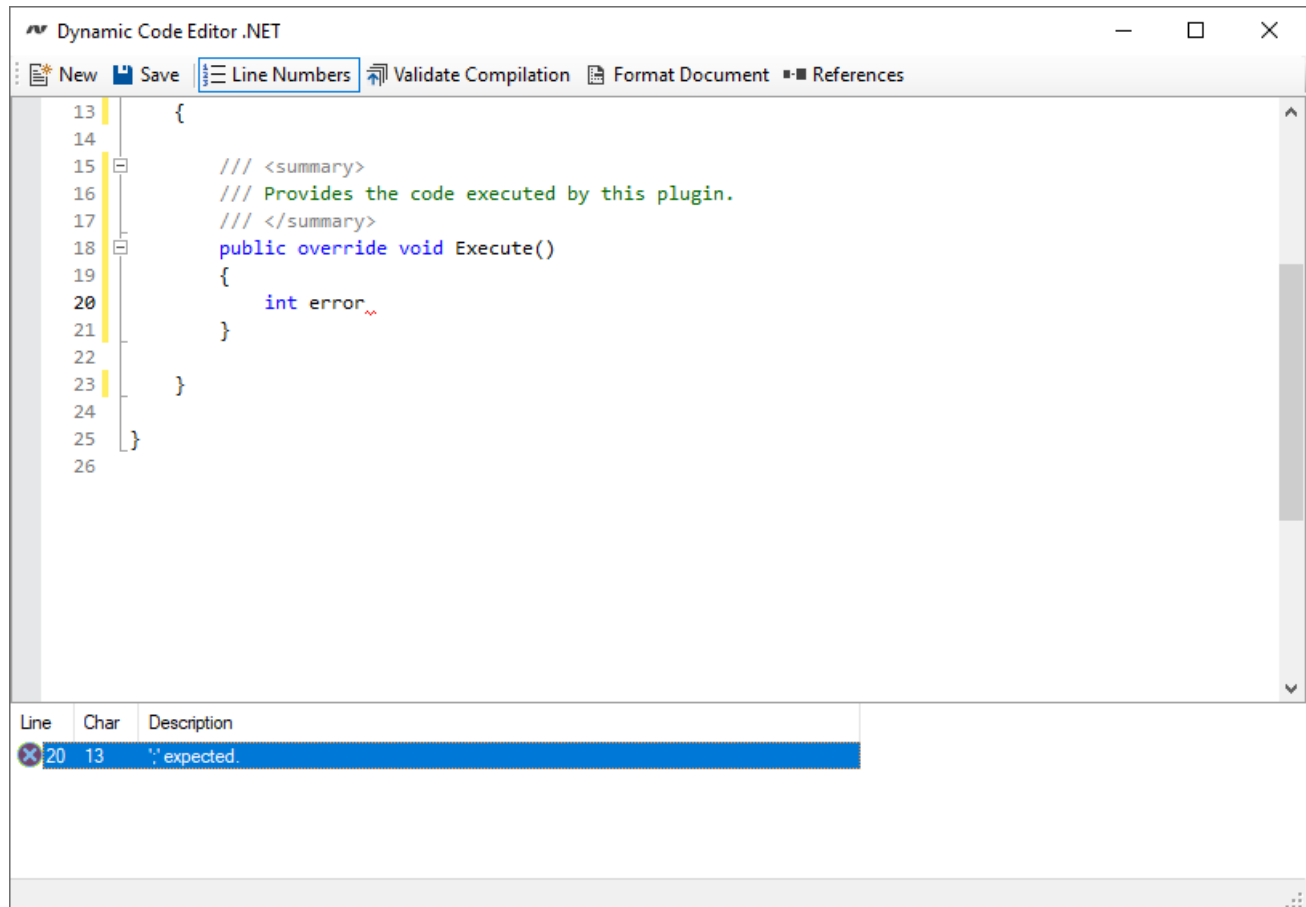
When the [plugin's properties](#) are configured to run *before agent scan*, changes made to the agent settings are then applied and used by the agent, if the plugin is configured to run *after agent scan*, changes to the agent settings have no effect.



Error List

The [dynamic code editor](#) automatically displays an syntax errors in the error list. The error list does not display compiler errors, to validate compilation click the validate compilation button in the toolbar.

Double clicking an error in the error lists moves the caret to the position of that error.



Line

The line in the code where the error was detected.

Char

The character in the line in the code where the error was detected.

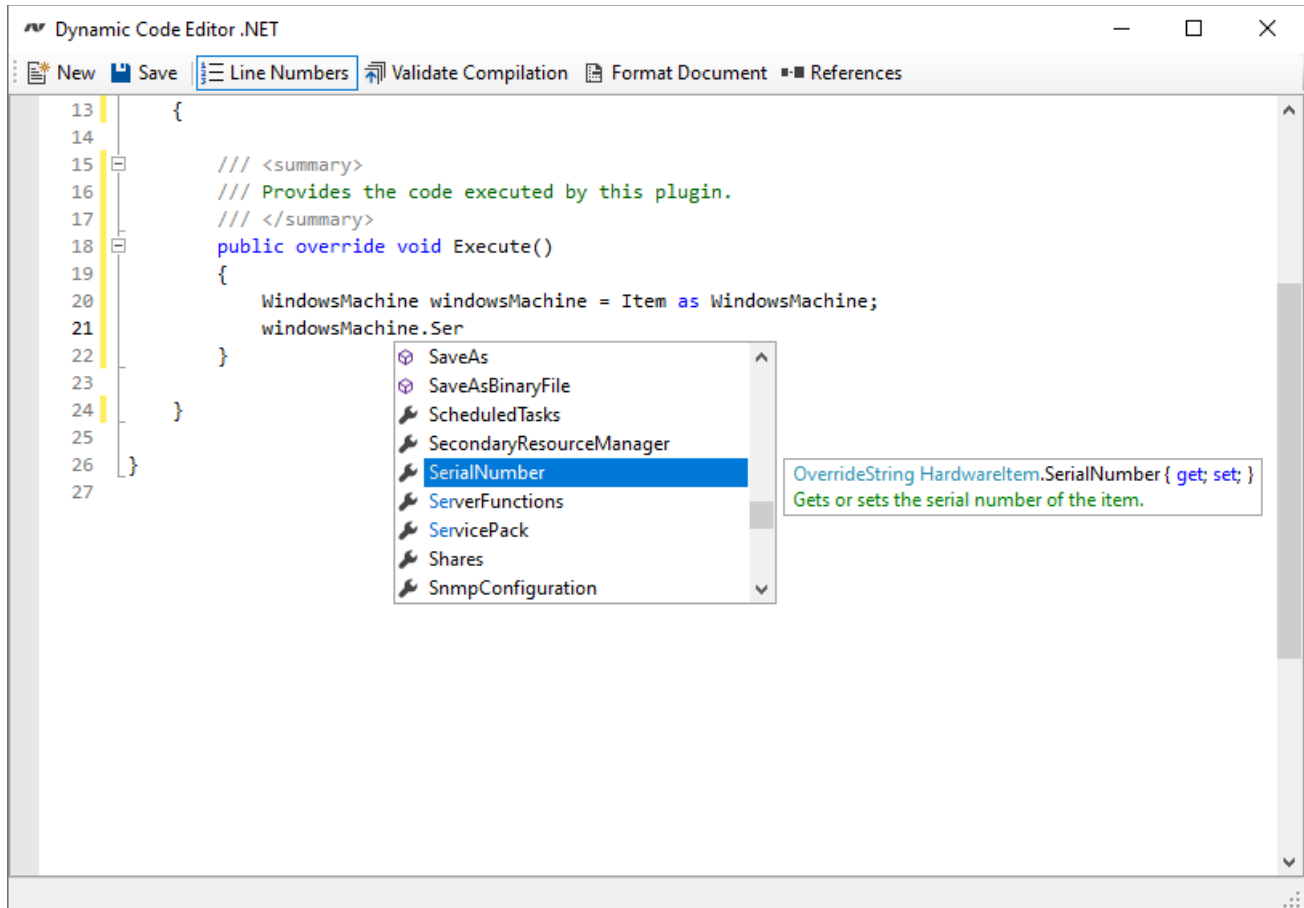
Description

A description of the error.

Item Property

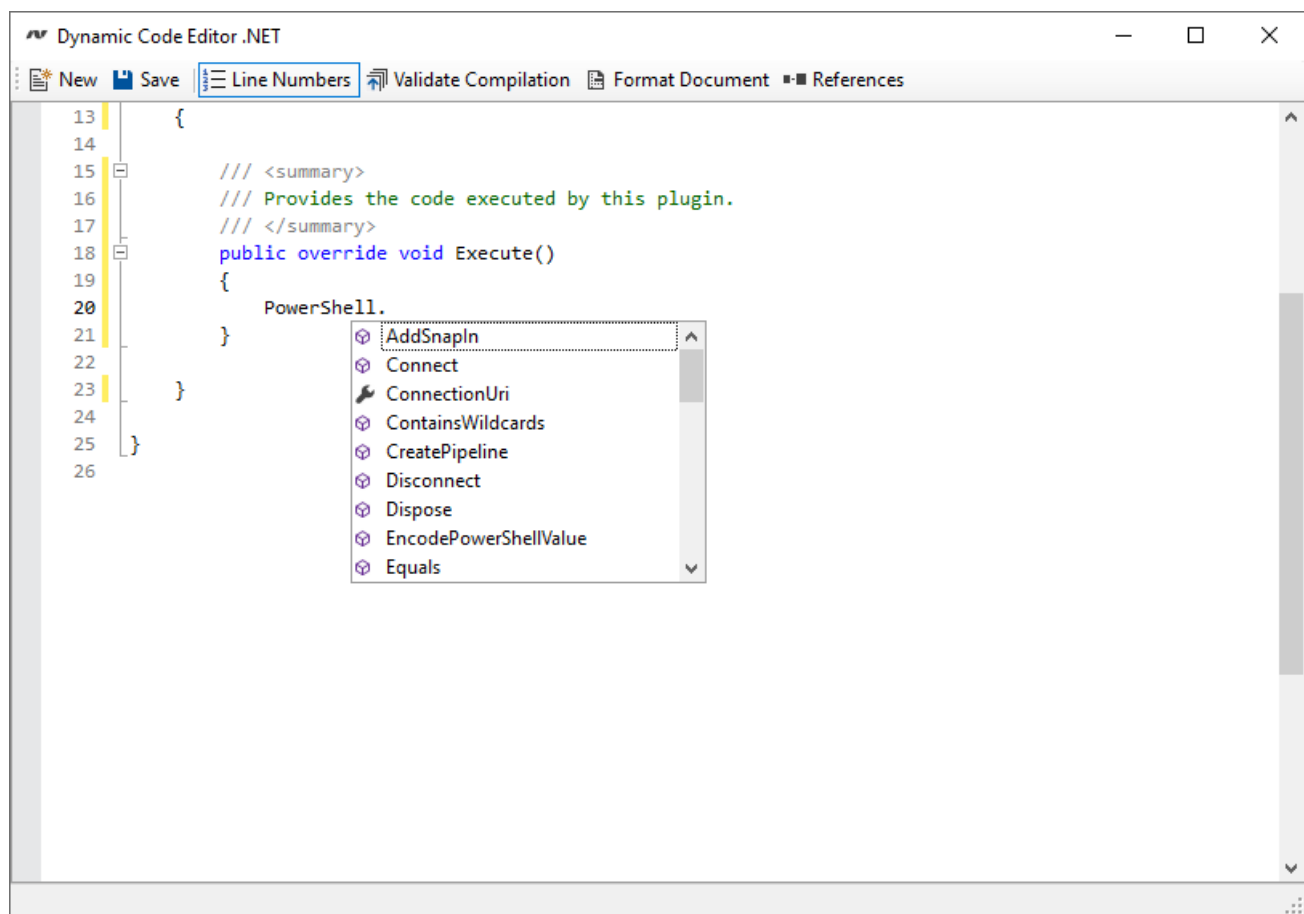
The **Item** property provides access to the item being documented by the agent as a `BaseConfigurationType`. This can be cast to the specific item type.

When the [plugin's properties](#) are configured to run **after agent scan**, the item is fully populated and any changes to the item are committed. When the plugin is configured to run **before agent scan** the item is not populated with information and any changes made may be overwritten by the agent.



PowerShell Support

[Agent plugins](#) are able to communicate with remote devices using [PowerShell remoting](#) with the built-in PowerShellSupport class, accessible through the PowerShell property.



IsConnected

Determines whether the [PowerShell remoting](#) system is connected and authenticated.

Connect

If the [PowerShell remoting](#) system is not already connected the Connect() method can be used.

Disconnect

Disconnects [PowerShell remoting](#) from the remote system.

FileSystem

Provides file system functions.

Registry

Provides registry related functionality on the connected machine.

Rsop

Provides resultant set of policy (RSOP) related functionality on the connected machine.

Security

Provides security related functionality on the connected machine.

System

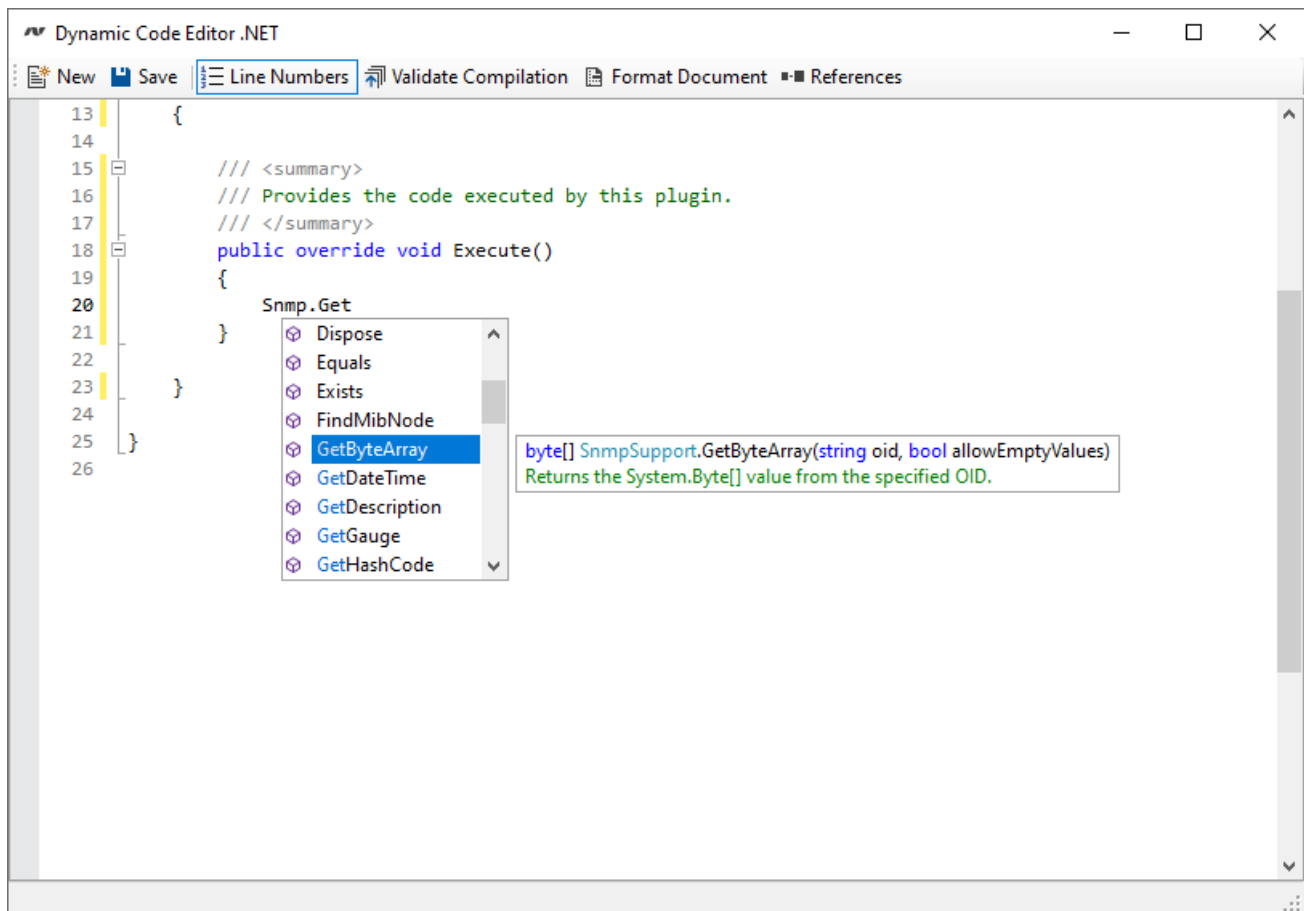
Provides system related functionality on the connected machine.

Wmi

Provides access to [Windows Management Instrumentation \(WMI\)](#) functionality through the [PowerShell remoting](#) connection.

SNMP Support

[Agent plugins](#) are able to communicate with remote devices using the Simple Network Management Protocol (SNMP) with the built-in `SnmpSupport` class, accessible through the `Snmp` property.



IsConnected

Determines whether the SNMP system is connected and authenticated.

Connect (SNMP v2)

It is recommended to use the existing connection, however if the SNMP system is not already connected the following method can be used to connect to the SNMP host. The community string will be stored in the code of the plugin in plain text.

```
SnmpSettings settings = new SnmpSettings();  
settings.CommunityStrings.Add("public");  
Snmp.Connect("devicename");
```

Connect (SNMP v3)

It is recommended to use the existing connection, however if the SNMP system is not already connected the following method can be used to connect to the SNMP host. The [SNMP v3 password](#) will be stored in the code of the plugin in plain text.

```
SnmpSettings settings = new SnmpSettings();  
settings.Version = SnmpSettingsVersion.Three;
```

```
settings.Security.AuthenticationPassword.SetPassword("SecurePassword");
settings.Security.AuthenticationProtocol = Snmpv3AuthenticationProtocol.Md5;
settings.Security.PrivacyPassword.SetPassword("SecurePassword");
settings.Security.PrivacyProtocol = Snmpv3PrivacyProtocol.Aes256;
settings.Security.Username = "Snmpv3Username";
Snmp.Connect("devicename");
```

CommunityString

The currently active community string. This setting is not used for [SNMP v3](#).

Contact

Gets the RFC1213 sysContact for the remote device.

Location

Gets the RFC1213 sysLocation for the remote device.

ObjectIdentifier

Gets the RFC1213 sysObjectID for the remote device.

ItemType

Gets the determined [item type](#) of the remote device.

GetByteArray

Gets the System.Byte[] value from the specified OID.

GetInteger

Gets the System.Int32 value from the specified OID.

GetDateTime

Gets the System.DateTime value from the specified OID.

GetGauge

Gets the System.Int64 value from the specified OID.

GetMacAddress

Gets the MAC address as a System.String value from the specified OID.

GetString

Gets the System.String value from the specified OID.

```
String sysName = Snmp.GetString("1.3.6.1.2.1.1.5.0");
```

GetTable

Gets the SNMP table from the specified OID.

```
SnmpTable table = snmp.GetTable("1.3.6.1.2.1.2.2");
foreach (SnmpTableRow row in table.Rows)
{
    String interfaceDescription = row.GetString("1.3.6.1.2.1.2.2.1.2");
}
```

GetTimeTicks

Gets the System.TimeSpan value from the specified OID.

Disconnect

Disconnects from the remote SNMP device. This is done automatically by the system when the scan completes.

Dispose

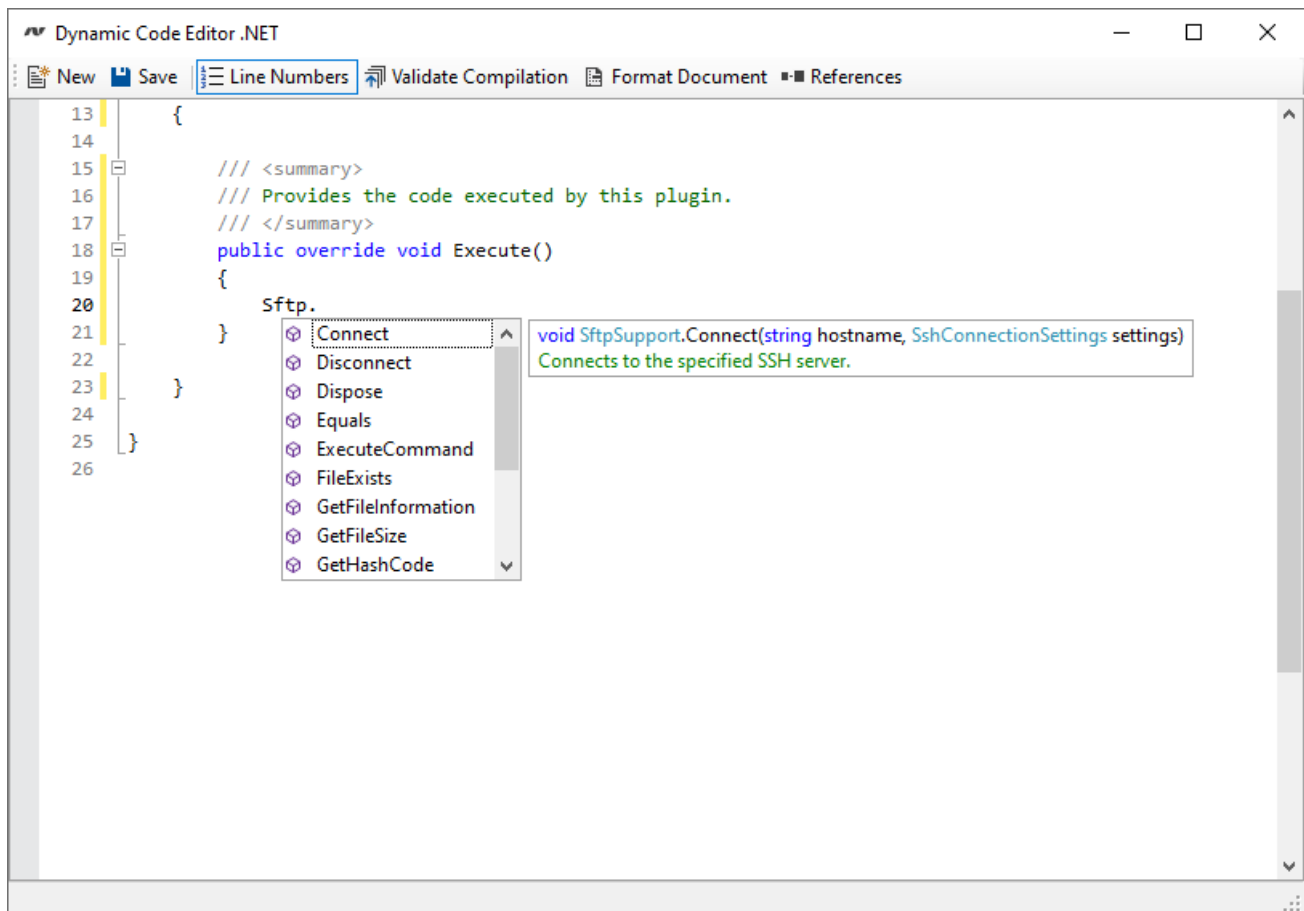
Disconnects from the remote SNMP device, and disposes of the connection. This is done automatically by the system when the scan completes.

Settings

The settings used to establish the SSH connection.

SFTP Support

Agent plugins are able to connect with remote devices using [secure shell \(SSH\)](#) version 2 and transfer files with the built-in SftpSupport class, accessible through the Sftp property.



IsConnected

Determines whether the SFTP system is connected and authenticated.

Connect

It is recommended to use the existing connection, however if the SFTP system is not already connected the following method can be used to connect to the SSH server.

The password will be stored in the code of the plugin in plain text.

```
SshConnectionSettings settings = new SshConnectionSettings();
settings.Enabled = true;
settings.Credentials.UseDefaultCredentials = false;
settings.Credentials.Username = "admin";
settings.Credentials.Password.SetPassword("password");
Sftp.Connect("demo-srv01", settings);
```

Disconnect

Disconnects from the remote SSH host. This is done automatically by the system when the scan completes.

Dispose

Disconnects from the remote SSH host, and disposes of the connection. This is done automatically by the system when the scan completes.

ExecuteCommand

Executes the specified command and returns the response.

FileExists

Determines whether a file at the specified path exists.

GetFileInformation

Returns the information about the file at the specified path such as creation date, last modified date, owner, and file size.

GetFileSize

Returns the size of the file at the specified path in bytes.

GetTextFileContents

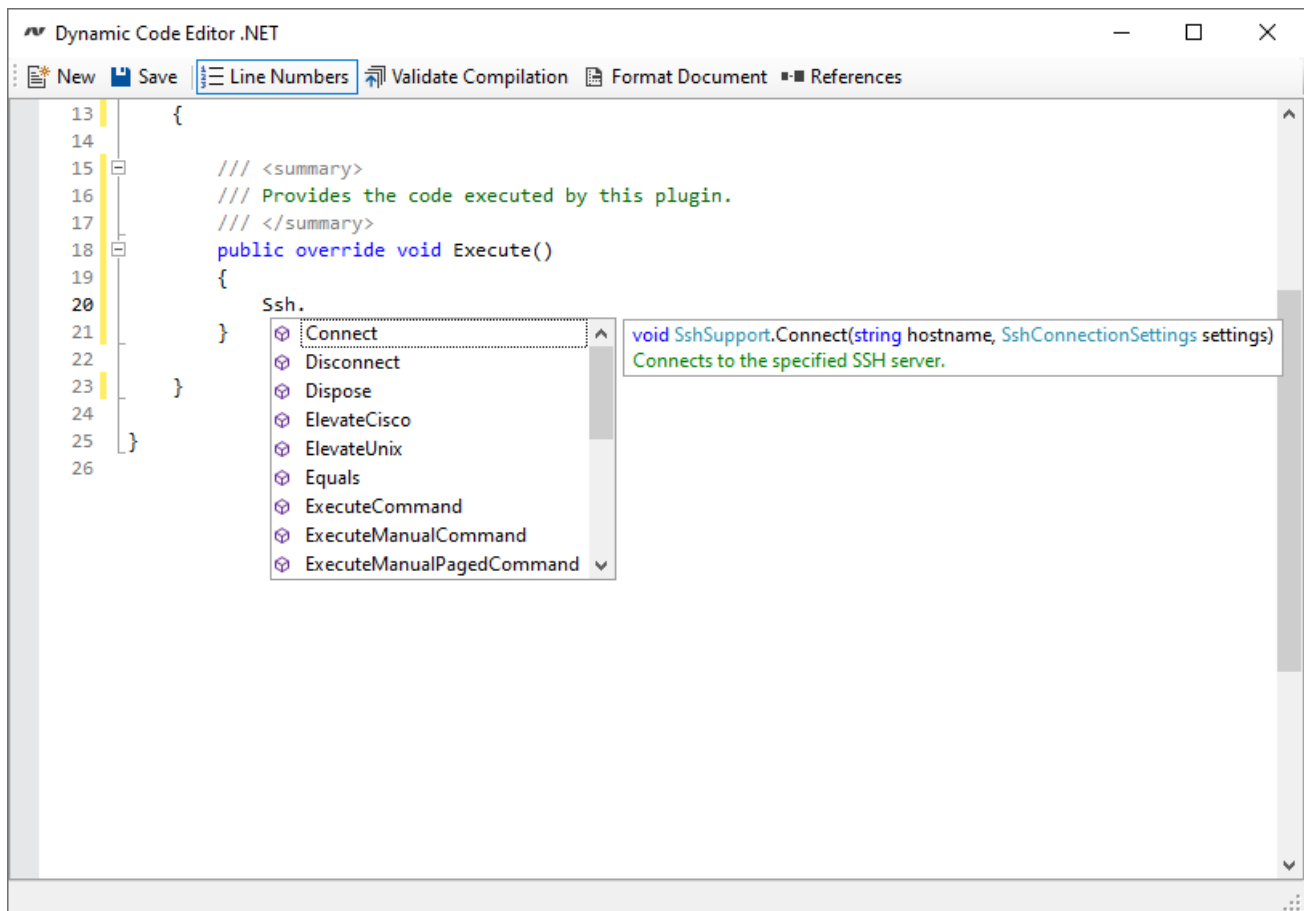
Returns the contents of the text file at the specified path.

Settings

The settings used to establish the SFTP connection over SSH.

SSH Support

Agent plugins are able to communicate with remote devices using [secure shell \(SSH\)](#) version 2 with the built-in SshSupport class, accessible through the Ssh property.



IsConnected

Determines whether the SSH system is connected and authenticated.

Connect

It is recommended to use the existing connection, however if the SSH system is not already connected the following method can be used to connect to the SSH server.

The password will be stored in the code of the plugin in plain text.

```
SshConnectionSettings settings = new SshConnectionSettings();
settings.Enabled = true;
settings.Credentials.UseDefaultCredentials = false;
settings.Credentials.Username = "admin";
settings.Credentials.Password.SetPassword("password");
Sftp.Connect("demo-srv01", settings);
```

```
SshConnectionSettings settings = new SshConnectionSettings();
settings.Enabled = true;
settings.Credentials.UseDefaultCredentials = false;
settings.Credentials.Username = "admin";
settings.Credentials.Password.SetPassword("password");
```

```
Sftp.Connect("demo-srv01", settings);
```

Disconnect

Disconnects from the remote SSH host. This is done automatically by the system when the scan completes.

Dispose

Disconnects from the remote SSH host, and disposes of the connection. This is done automatically by the system when the scan completes.

ExecuteCommand

Executes the specified command and returns the response.

ExecuteUnixCommand

Executes the specified command and returns the response on a Unix system. The exit code is checked and an exception thrown if the command did not execute successfully. The method takes the useSudo parameter to determine if sudo should be used to execute the command.

```
Ssh.ExecuteUnixCommand("cat /etc/hosts", true);
```

ExecuteManualCommand

Executes the specified command and returns the response on a remote system that does not respond using industry standard new line characters.

Prompt

The command prompt currently displayed on the SSH host.

Settings

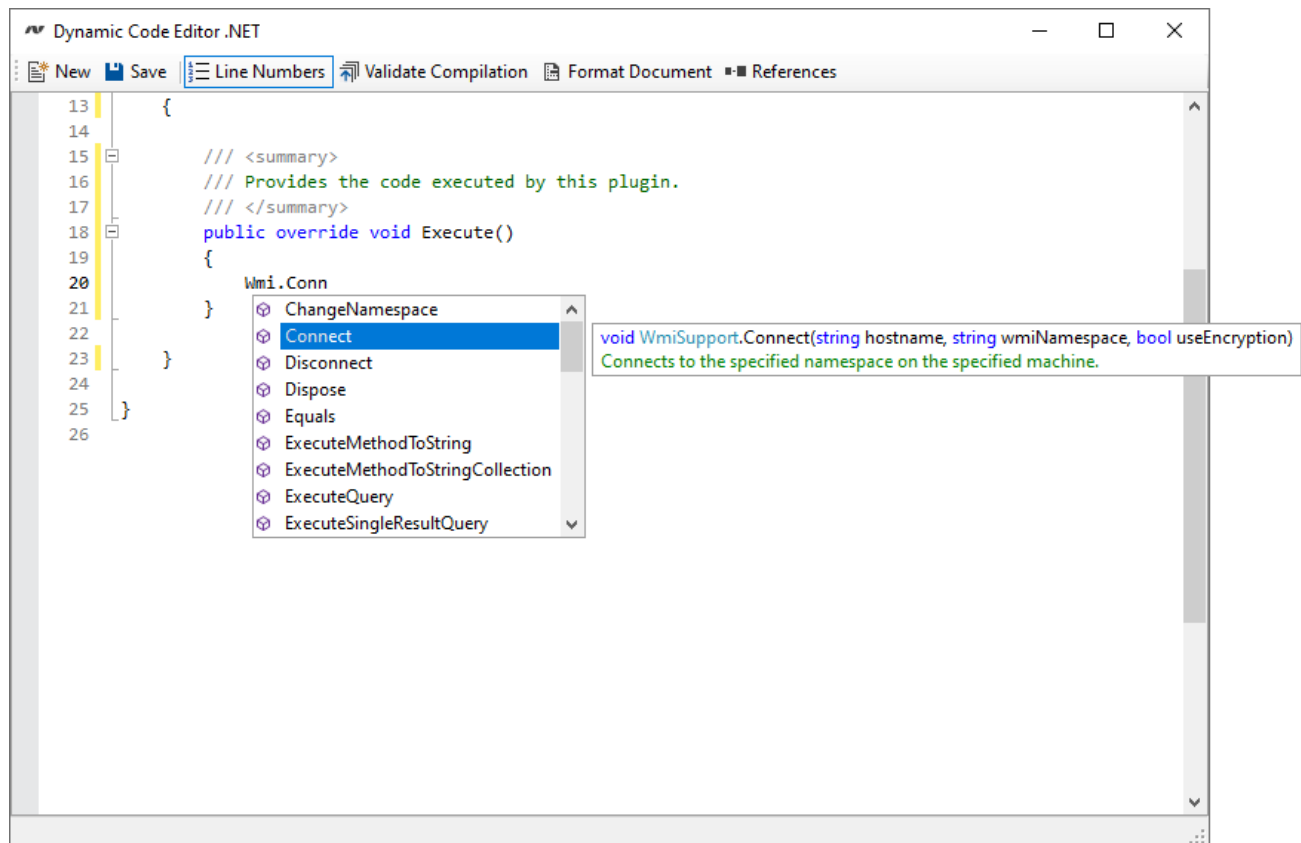
The settings used to establish the SSH connection.

WMI Support

Agent plugins are able to communicate with remote devices using direct [Windows Management Instrumentation \(WMI\)](#) connections with the built-in WmiSupport class, accessible through the Wmi property.

These methods encapsulate and simplify the [System.Management](#) functionality built into the .NET Framework.

For modern operating systems (Windows Server 2012 and above), the [PowerShell support functions](#) should be used where possible.



IsConnected

Determines whether the [WMI](#) system is connected and authenticated.

Connect

If the [WMI](#) system is not already connected the Connect() method can be used.

Disconnect

Disconnects [WMI](#) from the remote system.

ExecuteQuery

Executes the specified [WQL](#) query, and returns the results.

ExecuteSingleResultQuery

Executes the specified [WQL](#) query, and returns a single [System.Management.ManagementObject](#) result.

FileSystem

Provides file system functions.

ExecuteQuery

Executes the specified [WQL](#) query, and returns the results.

GetAssociators

Gets the [associators](#) of the specified [System.Management.ManagementObject](#) result.

Hostname

The name of the the remote system to which [WMI](#) is connected.

LocalSecurity

Provides security related functionality on the local machine.

LocalSystem

Provides system related functionality on the local machine.

Registry

Provides registry related functionality on the connected machine.

Rsop

Provides resultant set of policy (RSOP) related functionality on the connected machine.

Security

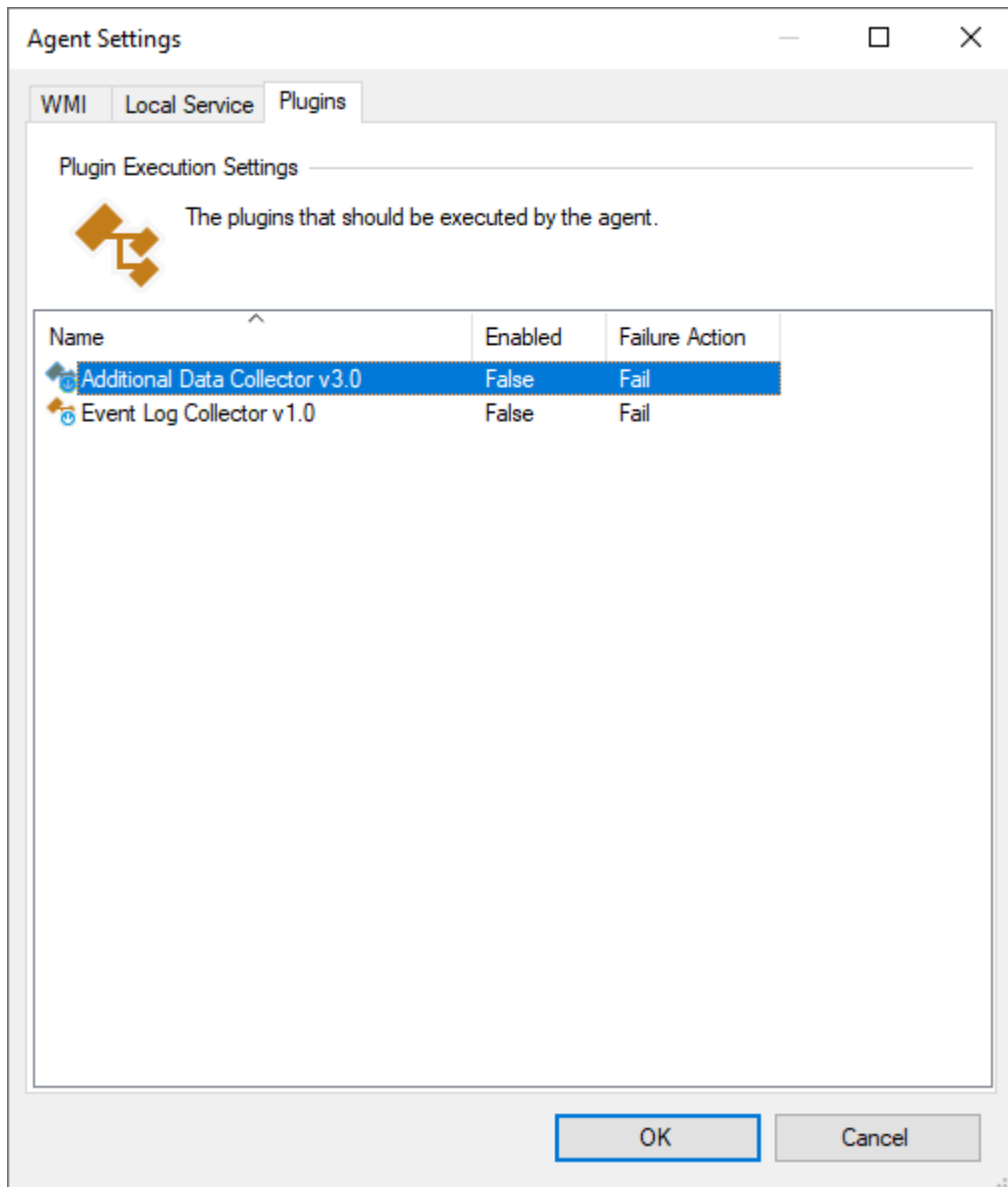
Provides security related functionality on the connected machine.

System

Provides system related functionality on the connected machine.

Dynamic Agent Plugins Execution Settings

When a [dynamic agent plugin](#) has been created it can be assigned to one or more item types using that items agent settings either assigned to a specific [scan task](#) or by assigning it to the default agent settings for a given [scan profile](#).



Name

The display name of the [dynamic agent plugin](#).

Enabled

Determines whether the [dynamic agent plugin](#) is enabled.

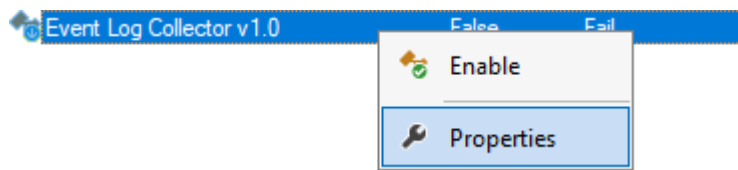
Failure Action

The failure action of the [dynamic agent plugin](#).

Right clicking the listview displays the [plugin execution settings context menu](#).

Context Menu

Right clicking the [dynamic agent plugins execution settings](#) user interface displays the context menu.



Enable

Enables the currently selected [agent plugin](#).

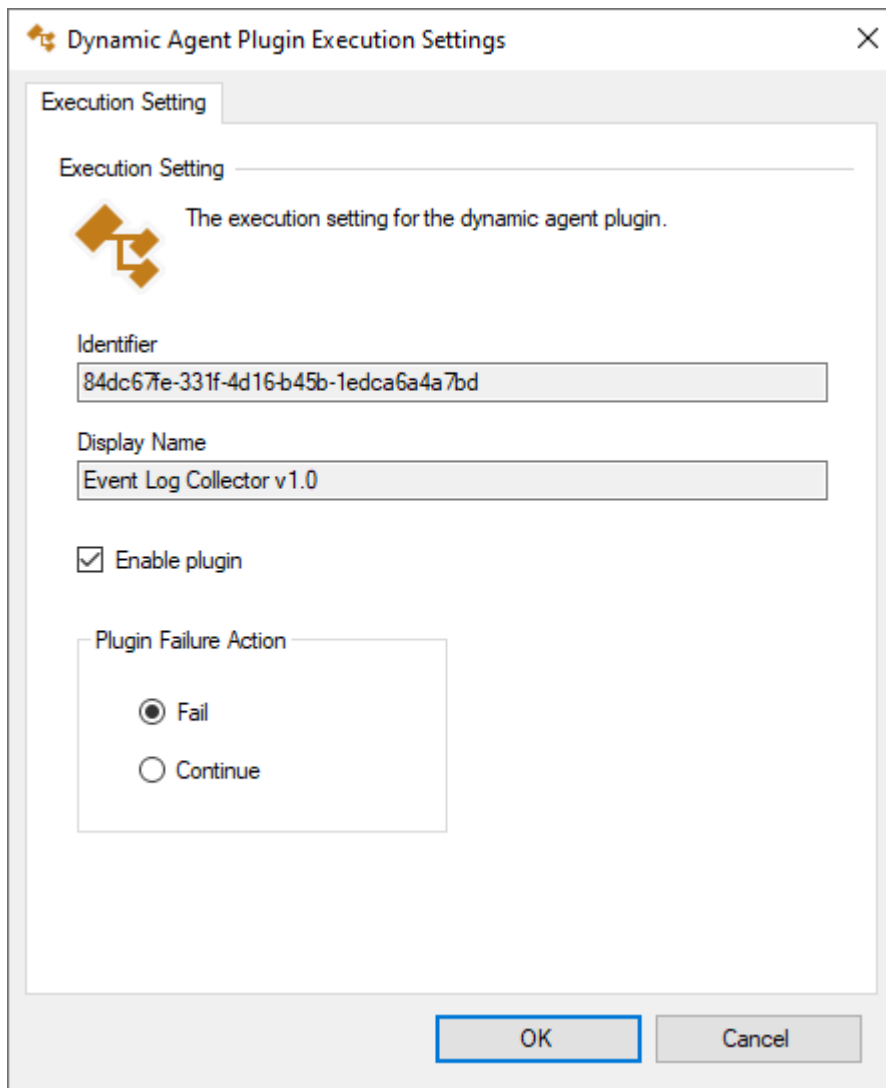
Disable

Disables the currently selected [agent plugin](#).

Properties

Displays the [plugin execution settings](#) for the selected [agent plugin](#).

Dynamic Agent Plugin Execution Settings



The image shows a Windows-style dialog box titled "Dynamic Agent Plugin Execution Settings". It has a close button (X) in the top right corner. The dialog contains several fields and options:

- Execution Setting**: A tabbed interface with one tab labeled "Execution Setting".
- Execution Setting**: A section header with a description: "The execution setting for the dynamic agent plugin." and an icon of three overlapping squares.
- Identifier**: A text field containing the GUID "84dc67fe-331f-4d16-b45b-1edca6a4a7bd".
- Display Name**: A text field containing "Event Log Collector v1.0".
- Enable plugin**: A checkbox that is checked.
- Plugin Failure Action**: A group box containing two radio buttons: "Fail" (selected) and "Continue".
- Buttons**: "OK" and "Cancel" buttons at the bottom right.

Identifier

The unique identifier of the [dynamic agent plugin](#) in [GUID](#) format.

Display Name

The display name of the [dynamic agent plugin](#).

Enable plugin

Determines whether the [dynamic agent plugin](#) is enabled for the agent.

Plugin Failure Action

Determines whether the agent scan should fail or continue should the execution of this [dynamic agent plugin](#) fail.

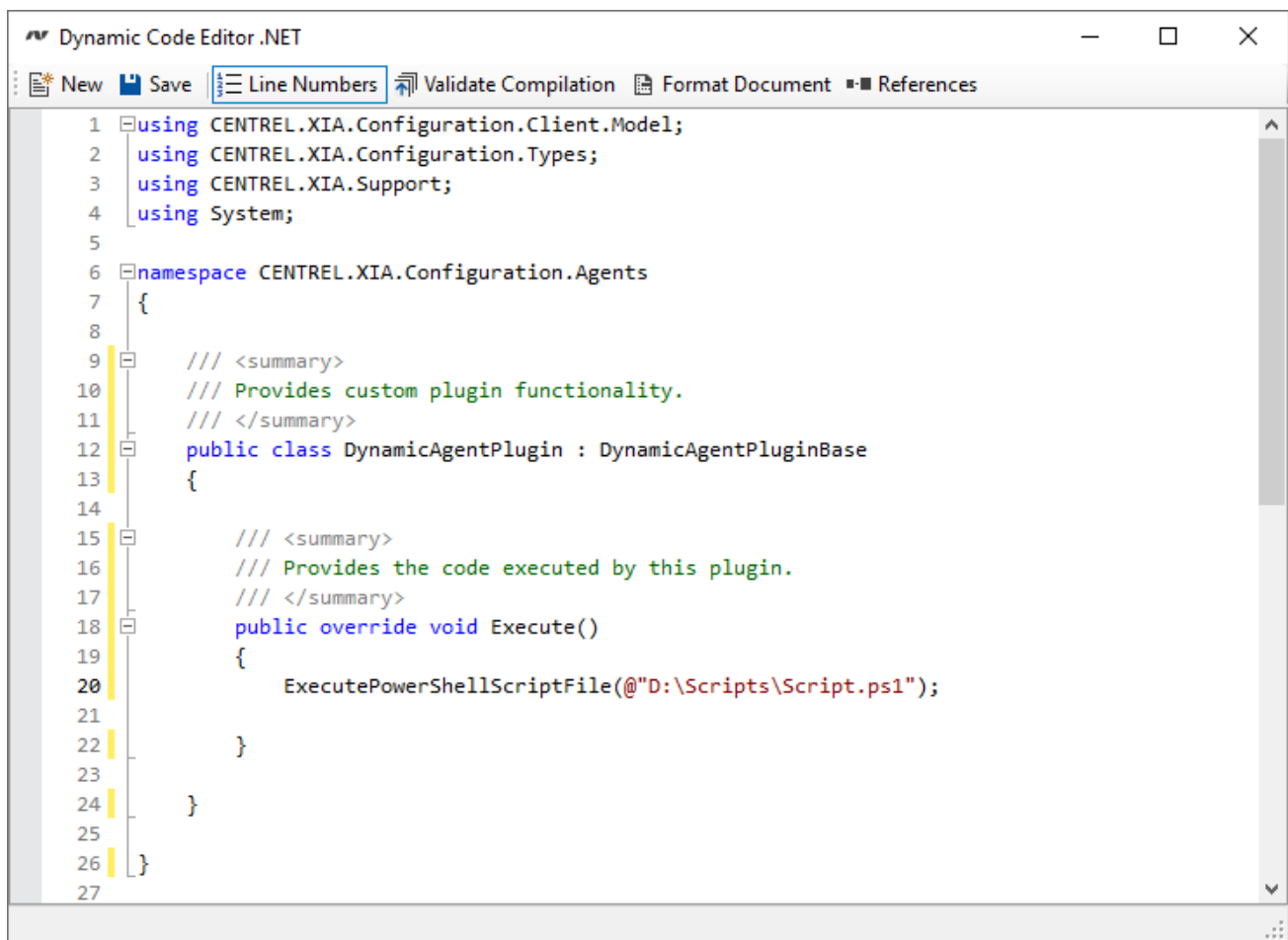
Executing PowerShell Scripts

The [Dynamic Code Editor](#) is designed to work with either C#.NET or VB.NET.

To work with [Windows PowerShell](#) scripts simply use the **ExecutePowerShellScriptFile** method, passing the absolute path of the PowerShell script file to execute.

NOTE: The script will be executed under the context of the [XIA Configuration Service Account](#) or the [Custom Credentials](#) in use therefore the script file must be secured and not able to be modified by unauthorised users.

NOTE: The script must be executed **After Agent Scan** on the [Plugin Properties](#) otherwise the item property will be null.



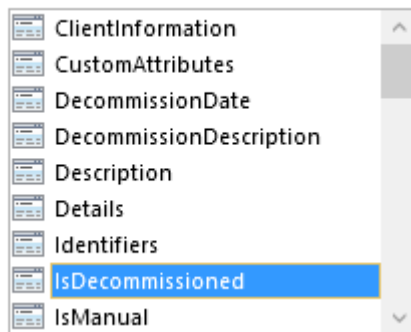
The PowerShell script file can then be modified with the [Windows PowerShell Integrated Scripting Environment](#) (ISE) or another editor.

The script should accept the parameter **\$item** which is the item being scanned by the [XIA Configuration Client](#).

```
param([CENTREL.XIA.Configuration.Types.BaseConfigurationType] $item)
Add-Type -Path "C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Support.dll"
Add-Type -Path "C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\CENTREL.XIA.Configuration.Types.dll"
```

The types should be added from the `CENTREL.XIA.Support.dll` and `CENTREL.XIA.Configuration.Types.dll` files, adjusting the paths as required. This allows the ISE to display the IntelliSense for these items.

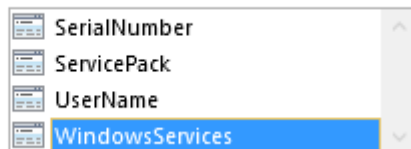
`$item.`



To obtain more detailed information the item can be cast as the specific item type for example, the following would cast the item as a Windows machine item type.

```
$windowsMachine = [CENTREL.XIA.Configuration.Types.WindowsMachine]$item
```

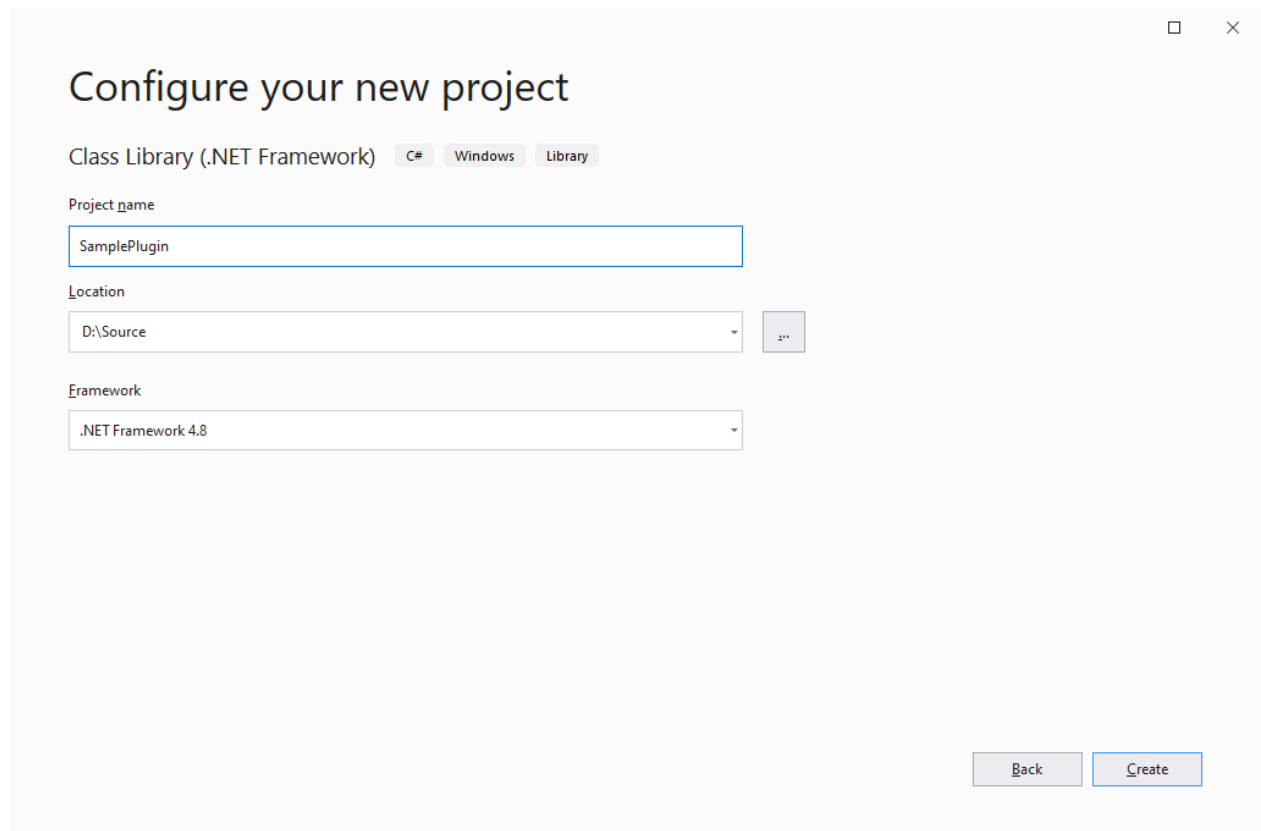
`$windowsMachine.`



Writing Agent Plugins in Visual Studio

Whilst it is recommended that [agent plugins](#) are created in the [dynamic code editor](#), it is also possible to create them using [Microsoft Visual Studio](#).

- Open Visual Studio and create a new *Class Library (.NET Framework)* project, ensuring that the [.NET Framework 4.8](#) is targeted.



- Open the installation directory on a machine where the [XIA Configuration Client](#) is installed, which is by default
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service

- Copy the following files to your development machine and add a reference to them in your project.

CENTREL.XIA.Configuration.Agents.DynamicAgentPluginBase.dll

CENTREL.XIA.Configuration.Agents.BaseAgent.dll

CENTREL.XIA.Configuration.Client.Model.dll

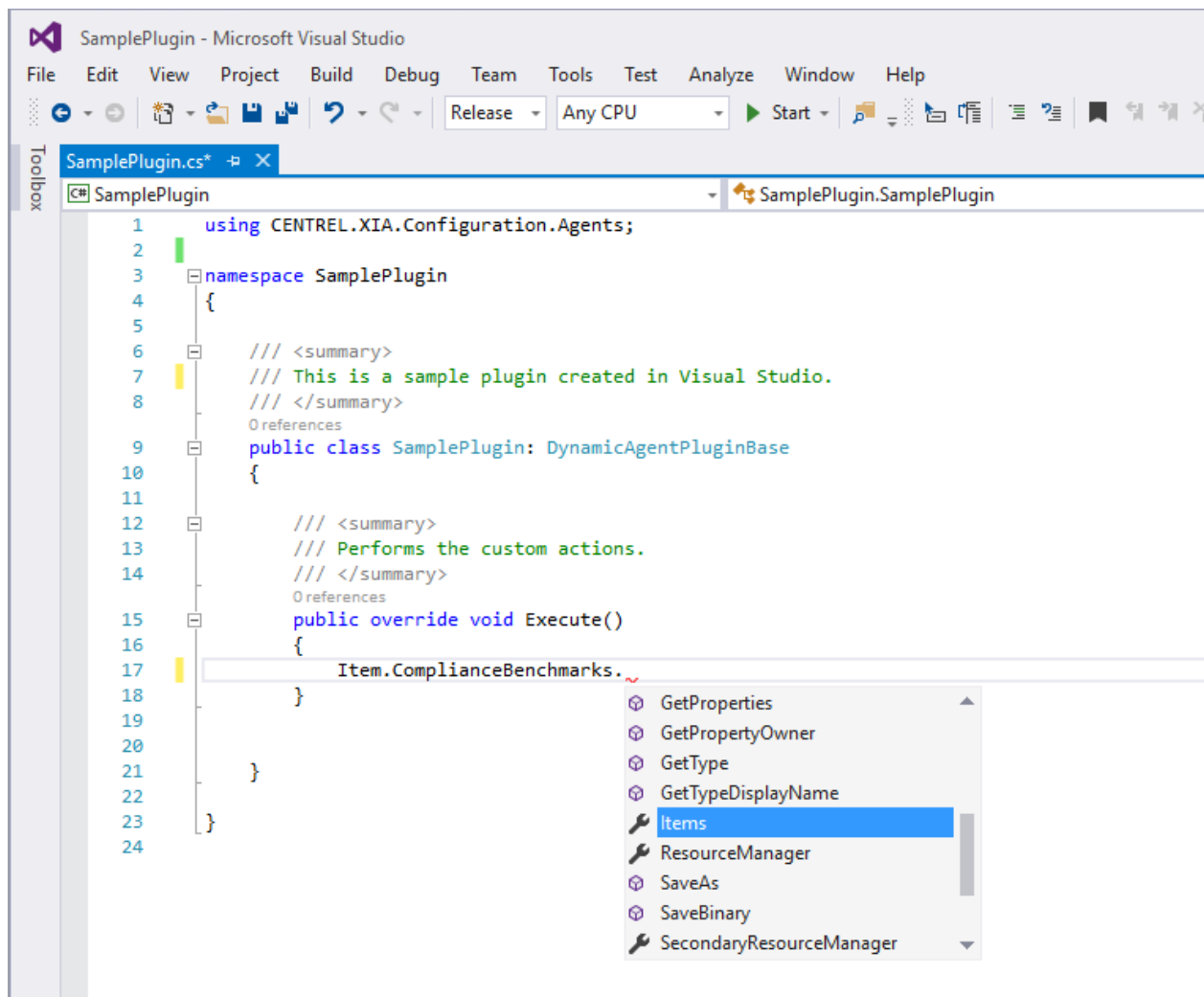
CENTREL.XIA.Configuration.Types.dll

CENTREL.XIA.Support.dll

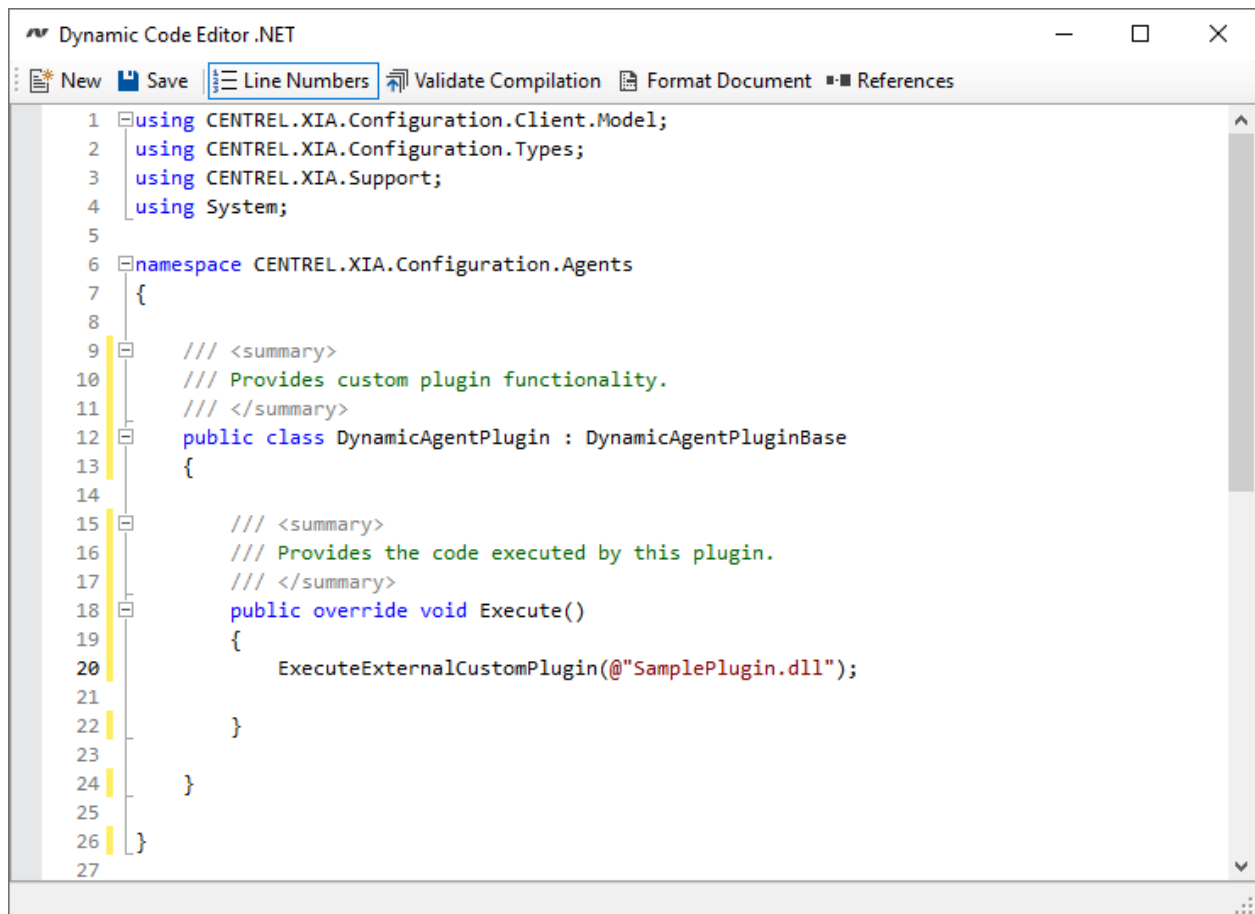
- Create a new class file, and within the class file create a new class which inherits from

DynamicAgentPluginBase.

- Override the Execute() method, and enter the custom code that is required. The [item property](#) and [agent settings](#) are accessible in the same way as within the [dynamic code editor](#).



- Compile the .dll file and deploy only the single .dll file, for example "SamplePlugin.dll" to the [XIA Configuration Client](#) service installation directory, which is by default C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service
- The external .dll file must be executed from the [dynamic code editor](#) from an [assigned plugin](#) with the **ExecuteExternalCustomPlugin** command, passing the filename of the plugin as the parameter.



The screenshot shows a code editor window titled "Dynamic Code Editor .NET". The menu bar includes "New", "Save", "Line Numbers", "Validate Compilation", "Format Document", and "References". The code is written in C# and defines a namespace and a class. Line numbers 1 through 27 are visible on the left margin. The code defines a namespace `CENTREL.XIA.Configuration.Agents` and a class `DynamicAgentPlugin` that inherits from `DynamicAgentPluginBase`. The class has a summary comment and an `Execute()` method that calls `ExecuteExternalCustomPlugin` with the path `@\"SamplePlugin.dll\"`.

```
1 using CENTREL.XIA.Configuration.Client.Model;
2 using CENTREL.XIA.Configuration.Types;
3 using CENTREL.XIA.Support;
4 using System;
5
6 namespace CENTREL.XIA.Configuration.Agents
7 {
8
9     /// <summary>
10     /// Provides custom plugin functionality.
11     /// </summary>
12     public class DynamicAgentPlugin : DynamicAgentPluginBase
13     {
14
15         /// <summary>
16         /// Provides the code executed by this plugin.
17         /// </summary>
18         public override void Execute()
19         {
20             ExecuteExternalCustomPlugin(@"SamplePlugin.dll");
21         }
22     }
23 }
24
25
26
27
```

- The code contained within the external plugin will be executed as part of the scan.

Agent Plugin Examples

The following section displays some example uses of [agent plugins](#).

Creating Compliance Benchmarks

Provides an example of how to write custom [compliance benchmarks](#).

Custom Attributes

Provides a complete walkthrough of writing [custom attributes](#) from an [agent plugin](#).

Network Switch Command Outputs

Provides an example of how to read additional [command outputs](#) for [network switches](#).

Customizing Windows Basic Compliance Benchmark

Provides an example of how to customize the [basic compliance benchmark](#) for [Windows machines](#).

Creating Compliance Benchmarks

Within the [dynamic code editor](#) it is possible to perform custom [compliance benchmarks](#) against supported items.

Firstly, create a new [agent plugin](#) and add a new using statement to the top of the as follows
`using CENTREL.XIA.Support;`

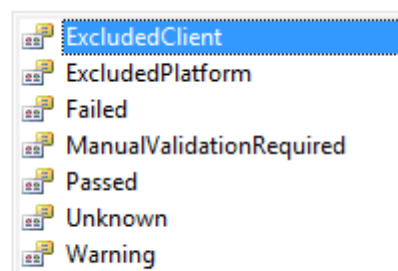
Then override the `Execute()` method

- Set the identifier to a unique GUID value
- Set the display name, version number and description
- Add the benchmark to the collection

```
/// <summary>
/// Provides the code executed by this plugin.
/// </summary>
public override void Execute()
{
    ComplianceBenchmark benchmark = new ComplianceBenchmark();
    benchmark.Identifier = new Guid("244bbd41-e714-4b5f-a627-49c8aea00365");
    benchmark.Name = "Sample benchmark";
    benchmark.Version.Major = 1;
    benchmark.Description = "Sample benchmark description";
    benchmark.Complete();
    Item.ComplianceBenchmarks.Items.Add(benchmark);
}
```

Once this has been completed you can add results to the benchmark.

- Each result must have a unique reference number in the form of a `SerializableReferenceNumber` - for example 1.0
- The currently configured value must be provided
- A boolean value can be passed, or a `ComplianceBenchmarkResultType`



```
e.AssetId.Value, ComplianceBenchmarkResultType.
```

Example 1: The AssetTag must be assigned to pass

```
WindowsMachine machine = Item as WindowsMachine;
benchmark.Results.Items.Add(new SerializableReferenceNumber(1,0),"Ensure the asset tag is assigned", machine.AssetId.Value, !String.IsNullOrEmpty(machine.AssetId.Value));
```

Example 2: The result does not apply so is marked as excluded on platform

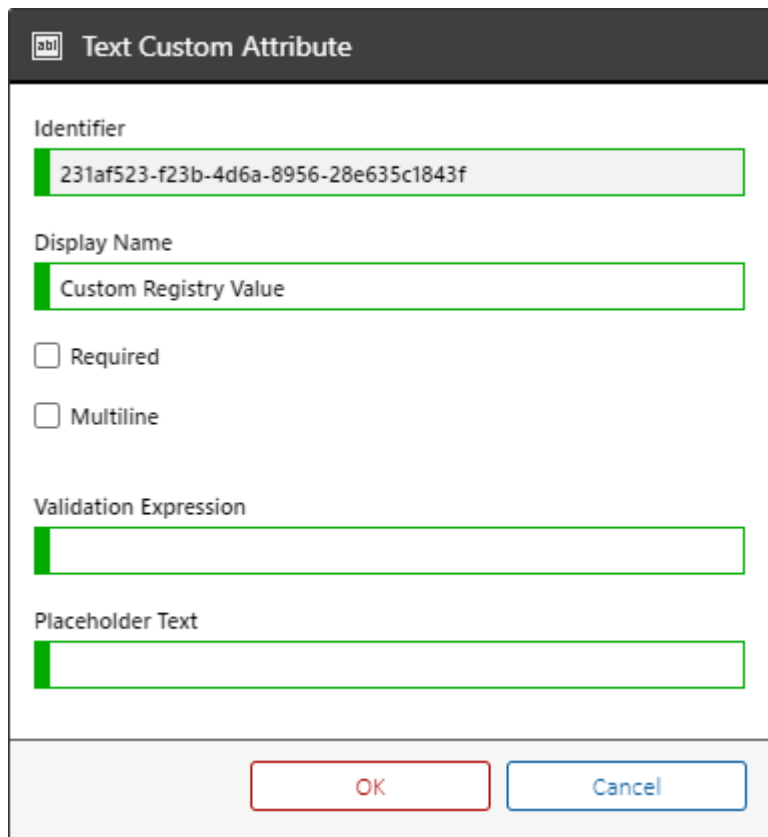
(For more information on result types see the [result types](#) section)

```
benchmark.Results.Items.Add(new SerializableReferenceNumber(1,0),"The 'Account Logon Events'  
setting must be enabled",  
machine.OperatingSystem.Security.AuditPolicy.AccountLogonEvents.AuditTypeString,  
ComplianceBenchmarkResultType.ExcludedPlatform);
```

Custom Attributes

The following walkthrough demonstrates how to create a [dynamic agent plugin](#) to read a registry entry from a [Windows machine](#) and store the information in a [custom attribute](#).

- Ensure that a [custom attribute](#) has been created and assigned to the appropriate [item types](#). Make a note of the identifier as this will be required later.



Text Custom Attribute

Identifier
231af523-f23b-4d6a-8956-28e635c1843f

Display Name
Custom Registry Value

☐ Required

☐ Multiline

Validation Expression

Placeholder Text

OK Cancel

- Within the [administration tools](#) go to the [dynamic agent plugins](#) section
- Right click the list and select new [dynamic agent plugin](#).



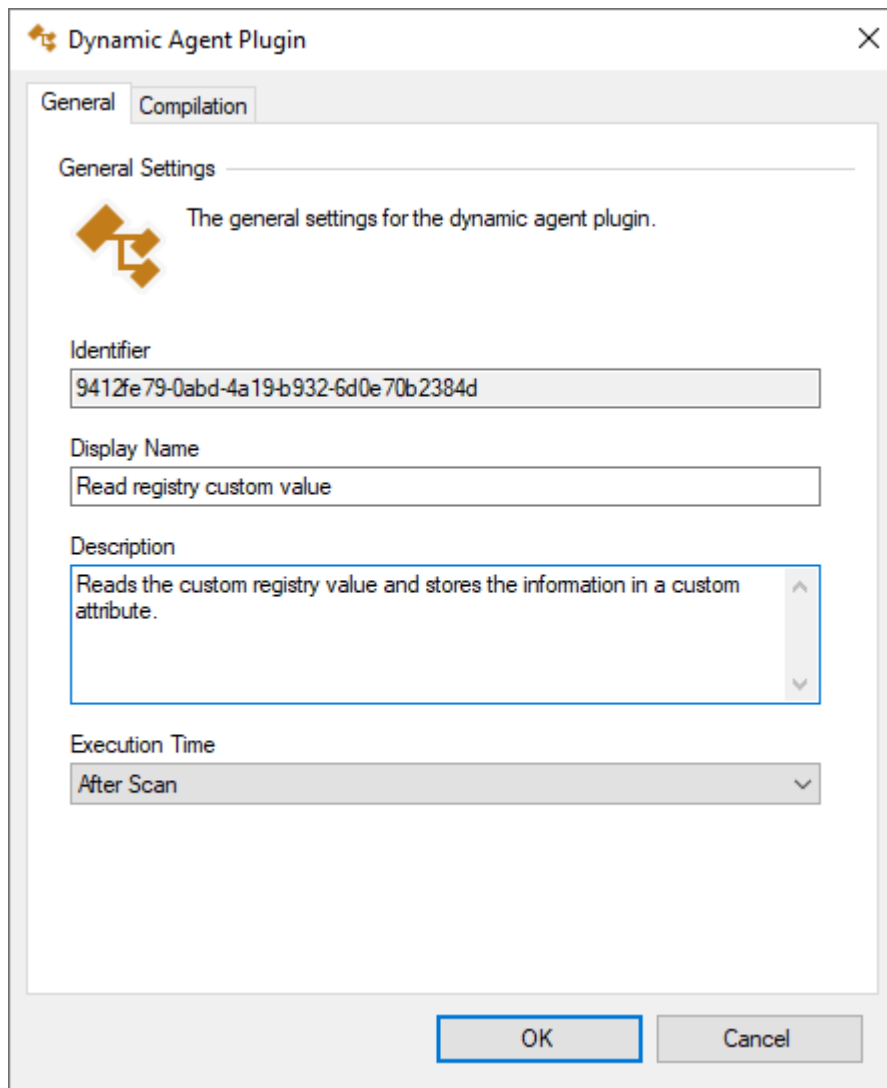
Dynamic Agent Plugins

Provides the configuration of the dynamic agent plugins available on this system.

New Agent Plugin

Display Name	Description
New Plugin Duplicate Delete Find References Import from XML Export as XML Properties	

- Enter the name and description of the [dynamic agent plugin](#).
- As the [dynamic agent plugin](#) will be modifying the data created by the agent, ensure that the execution time is set to after agent scan.



The image shows a dialog box titled "Dynamic Agent Plugin" with a close button (X) in the top right corner. It has two tabs: "General" and "Compilation". The "General" tab is selected. Under the "General Settings" section, there is a description: "The general settings for the dynamic agent plugin." Below this, there are four fields: "Identifier" with the value "9412fe79-0abd-4a19-b932-6d0e70b2384d", "Display Name" with the value "Read registry custom value", "Description" with the value "Reads the custom registry value and stores the information in a custom attribute.", and "Execution Time" with the value "After Scan". At the bottom right, there are "OK" and "Cancel" buttons.

Dynamic Agent Plugin

General Compilation

General Settings

The general settings for the dynamic agent plugin.

Identifier
9412fe79-0abd-4a19-b932-6d0e70b2384d

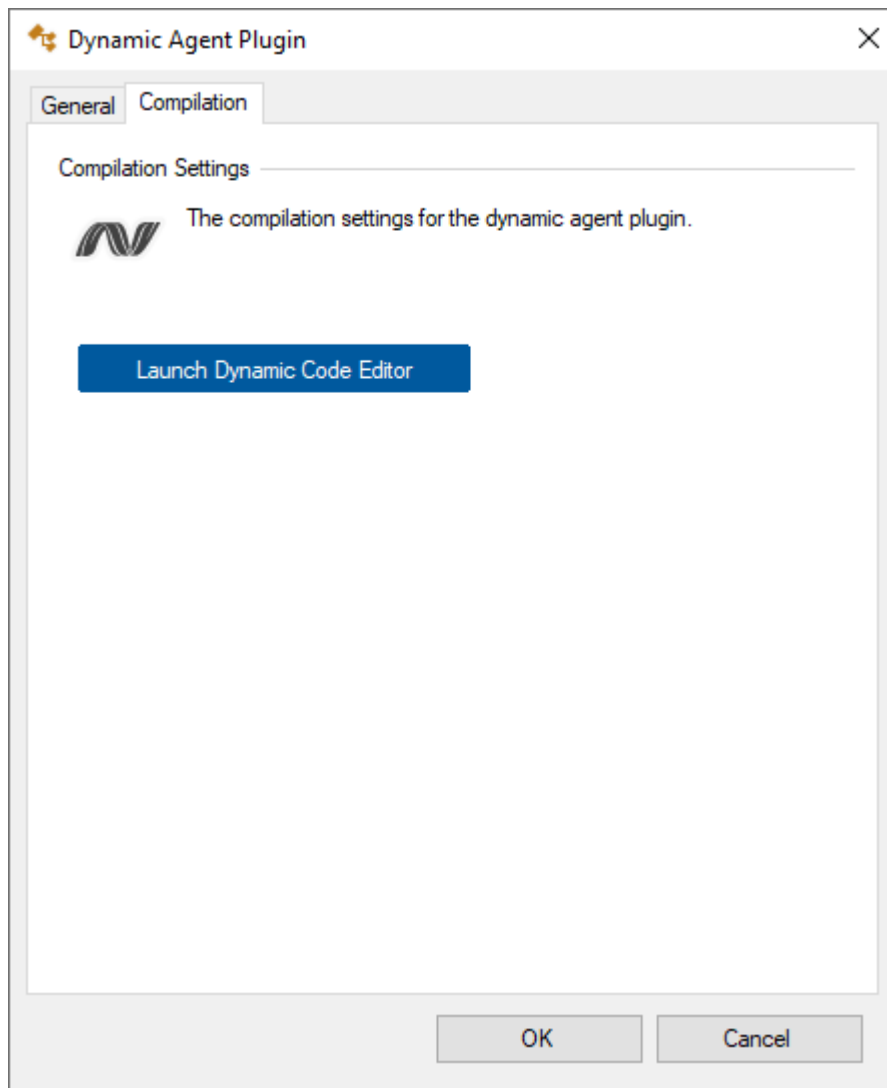
Display Name
Read registry custom value

Description
Reads the custom registry value and stores the information in a custom attribute.

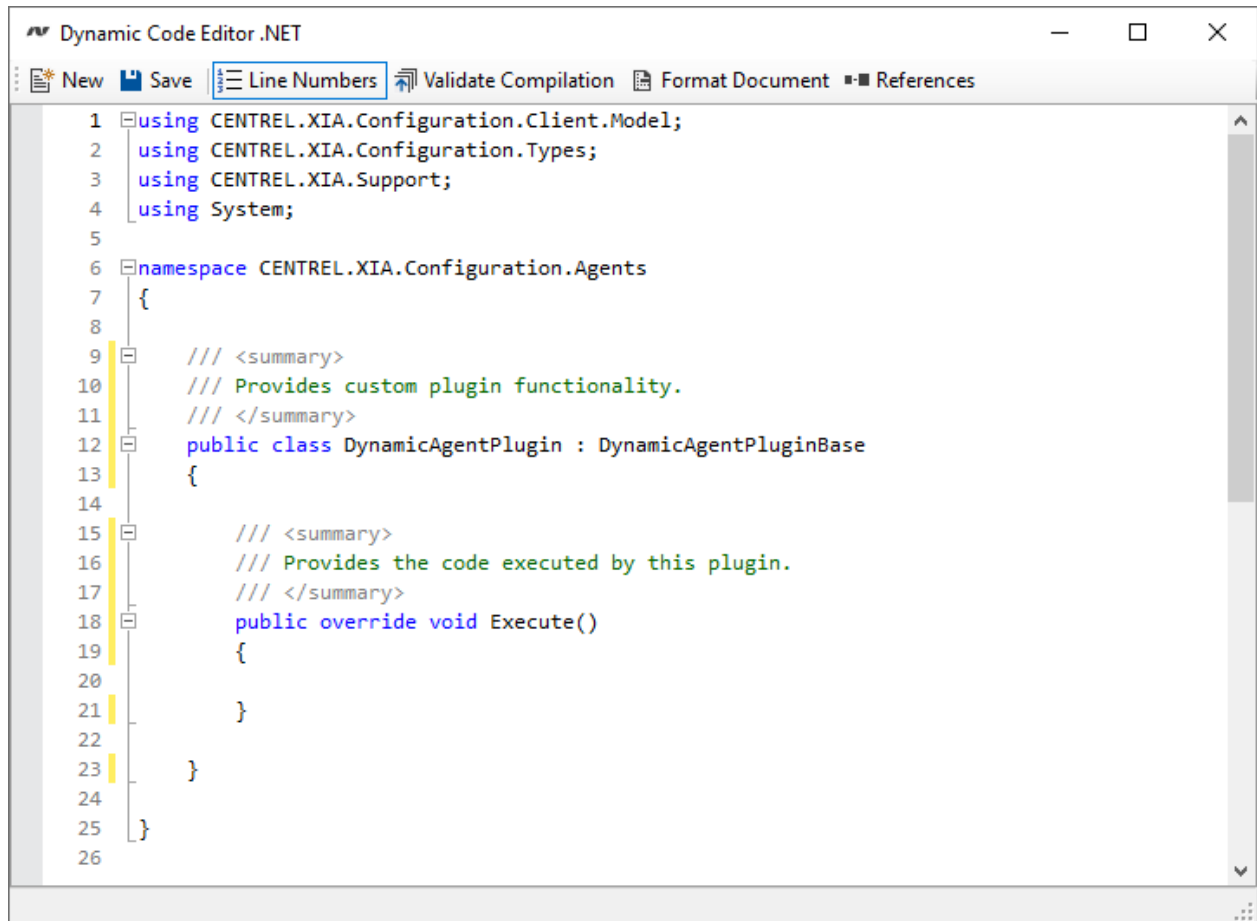
Execution Time
After Scan

OK Cancel

- On the *Compilation* tab, click the *launch dynamic code editor* button.



- This will display the [dynamic code editor](#).



- Enter the following code in the Execute() method.

```

/// <summary>
/// Provides the code executed by this plugin.
/// </summary>
public override void Execute()
{
    if (!PowerShell.IsConnected)
    {
        // Handle PowerShell not being connected.
    }
    String customValue = PowerShell.Registry.GetStringValue(@"SOFTWARE\CENTREL
Solutions\XIA Configuration Service", "InstallDirectory");
    Item.CustomAttributes.Items.Add(new Guid("231af523-f23b-4d6a-8956-28e635c1843f"),
String.Empty, customValue);
}

```

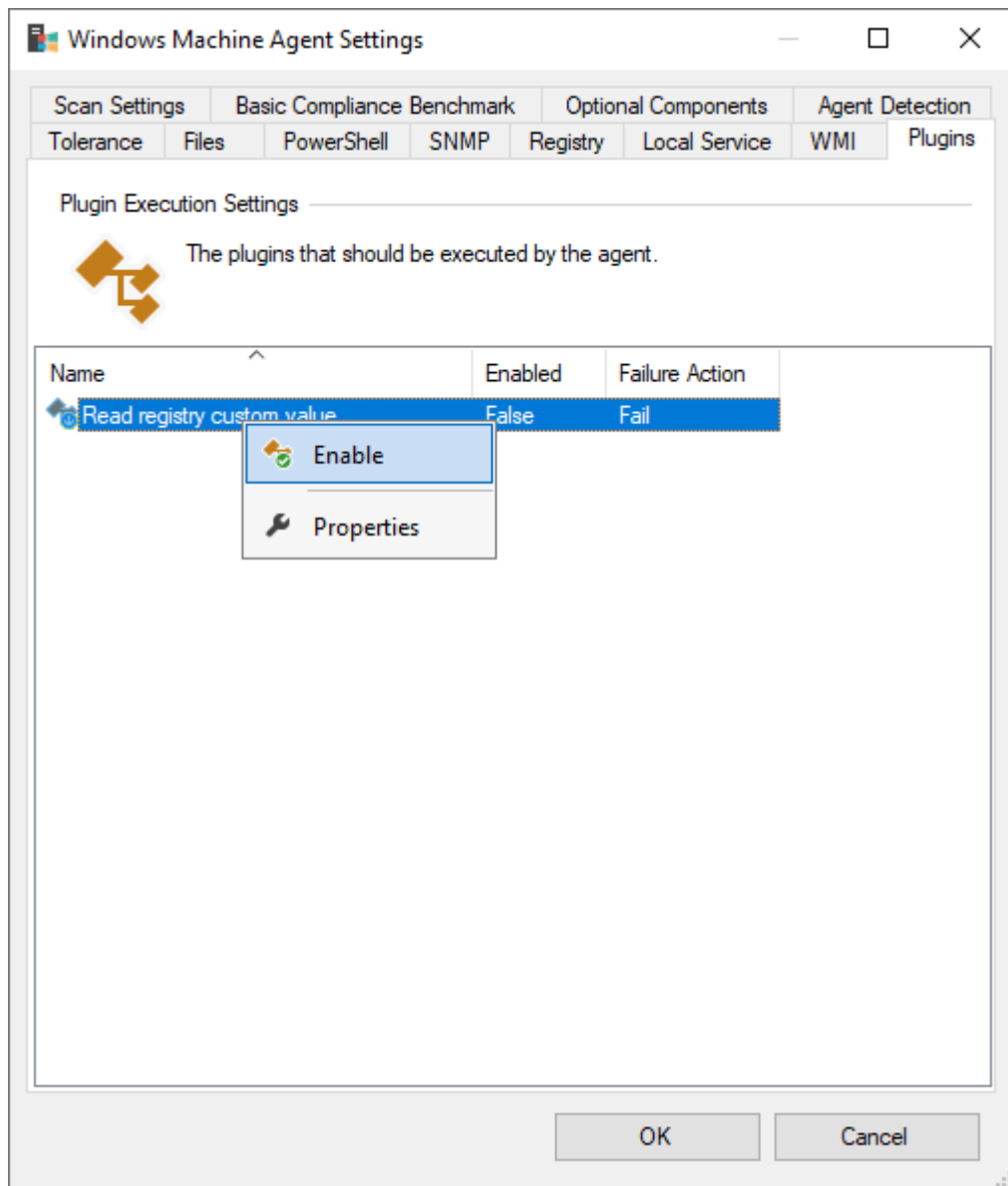
- The Registry property of the [PowerShell support](#) classes allows for direct access to the registry of the remote machine. In the example the "InstallDirectory" registry value of type [REG_SZ](#) is read.
- As the plugin is running after agent scan, the **Item** property provides access to the data generated by the agent, which can be modified. The custom attribute is added to the collection. The unique identifier of the custom attribute is the value that was noted at the start of this walkthrough.

```

Item.CustomAttributes.Items.Add(new Guid("231af523-f23b-4d6a-8956-28e635c1843f"),
String.Empty, customValue);

```

- Click the validate compilation button to ensure the code compiles correctly, and then click the save button.
- Close the [dynamic code editor](#) and click the OK button.
- Go to the [scan profile](#) that you are editing and go to the [default agent settings](#) and then the [Windows machine agent settings](#).
- On the [plugins](#) tab right click the newly created [dynamic agent plugin](#) and select enable.

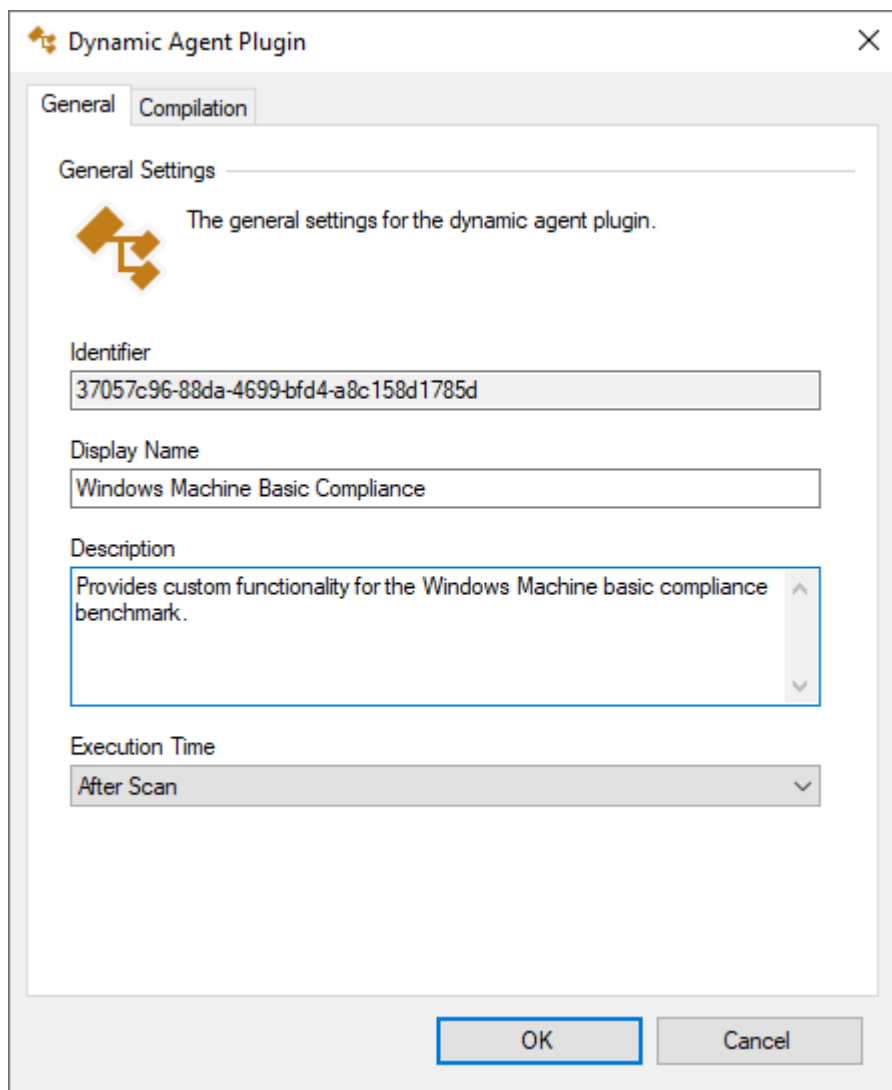


Customizing Windows Basic Compliance Benchmark

The [basic compliance benchmark](#) for [Windows machines](#) provides a simple overview of the security settings against security best practices.

Whilst it is possible to configure the [basic compliance benchmark](#) by using the [benchmark settings](#) additional flexibility can be gained by leveraging the [dynamic code editor](#).

- Create a new [dynamic agent plugin](#), ensuring that the [plugin](#) is configured to run **After Scan**.



The screenshot shows the 'Dynamic Agent Plugin' configuration window. It has two tabs: 'General' and 'Compilation'. The 'General' tab is active. Under 'General Settings', there is a description: 'The general settings for the dynamic agent plugin.' Below this are three fields: 'Identifier' with the value '37057c96-88da-4699-bfd4-a8c158d1785d', 'Display Name' with the value 'Windows Machine Basic Compliance', and 'Description' with the value 'Provides custom functionality for the Windows Machine basic compliance benchmark.' At the bottom, there is an 'Execution Time' dropdown menu set to 'After Scan'. The window has 'OK' and 'Cancel' buttons at the bottom right.

- Open the [dynamic code editor](#) and modify the code in the `Execute()` method.

```
/// <summary>
/// Provides the code executed by this plugin.
/// </summary>
public override void Execute()
{
    Guid identifier = ComplianceBenchmarkWellKnownIdentifiers.WindowsMachineBasic;
    ComplianceBenchmark benchmark =
```

```

Item.ComplianceBenchmarks.Items.FindByIdentifier(identifier);
    if (benchmark == null || !benchmark.IsComplete)
    {
        return;
    }
    ComplianceBenchmarkResult result = benchmark.Results.Items.FindByReferenceNumber(4, 1);
    if (String.Equals(result.ConfiguredDisplayValue, "root",
StringComparison.CurrentCultureIgnoreCase))
    {
        result.ResultType = ComplianceBenchmarkResultType.Failed;
    }
}

```

- Firstly the benchmark is obtained using the well known identifier.

```

Guid identifier = ComplianceBenchmarkWellKnownIdentifiers.WindowsBasic;
ComplianceBenchmark benchmark =
Item.ComplianceBenchmarks.Items.FindByIdentifier(identifier);

```

- In the example the benchmark result "4.1 Rename the local Administrator account to a less easily identifiable account name (does not apply to domain controllers)" is obtained.
- In the example the configured value has already been evaluated but is be further evaluated against the word "root". If the administrator account has been named "root" this will also cause the benchmark result to fail.

Network Switch Command Outputs

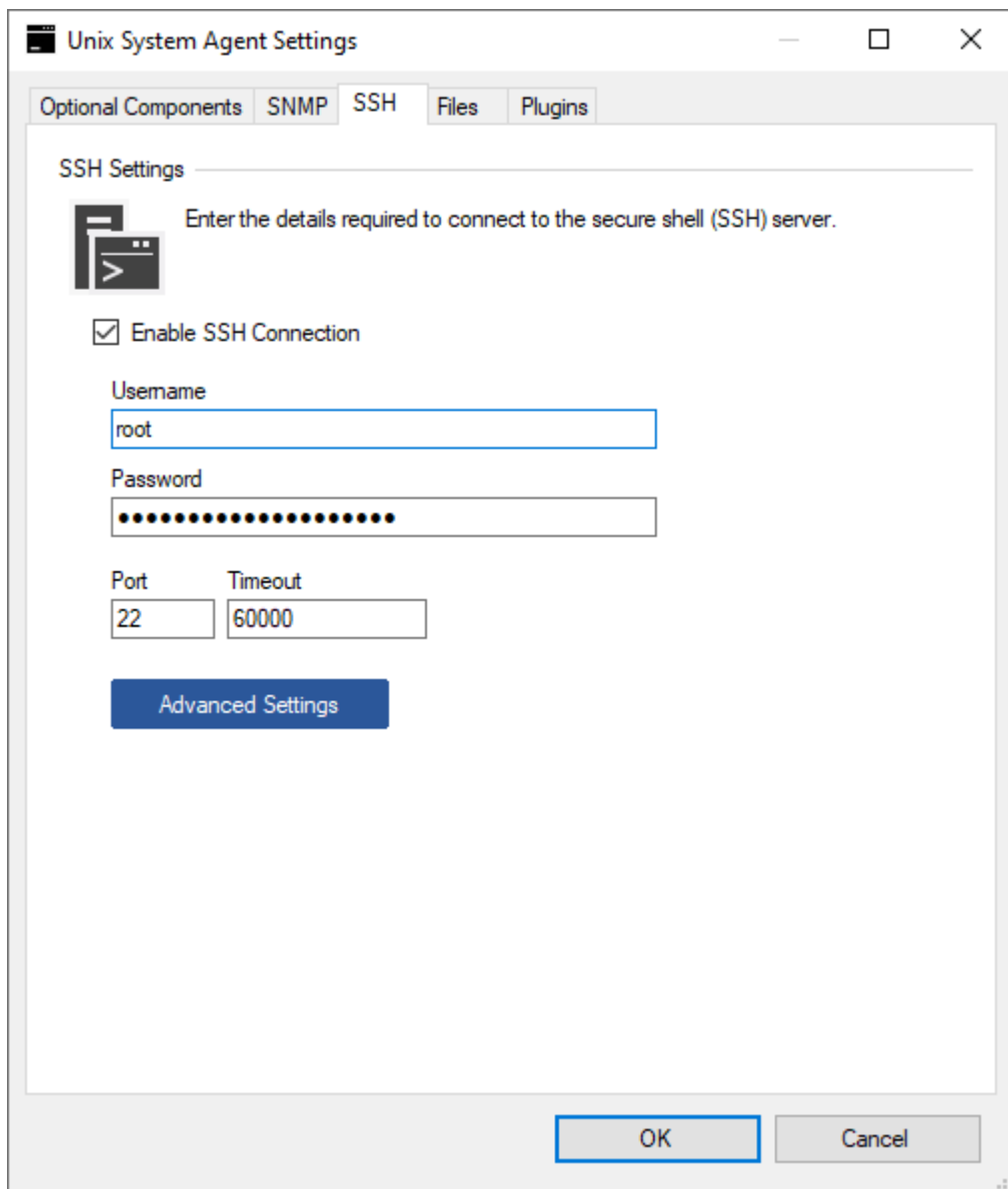
Within the [dynamic code editor](#) it is possible to read additional [command outputs](#) for supported [network switches](#) using the [SSH support](#) functions.

- Ensure that the [agent plugin](#) is configured to run after agent scan in the [plugin properties](#).
- Cast the [item](#) as a [network switch](#).
- Execute the required command and store the response as a `NetworkSwitchCommandOutput` object.
- Assign a new unique identifier in GUID format for the command output, this ensure consistency when [comparing items](#).

```
/// <summary>
/// Reads additional command outputs for network switches.
/// </summary>
public override void Execute()
{
    if (!Ssh.IsConnected){ return; }
    NetworkSwitch networkSwitch = (NetworkSwitch)Item;
    String response = Ssh.ExecuteManualCommand("show version");
    NetworkSwitchCommandOutput output = new NetworkSwitchCommandOutput();
    output.CommandText = "show version";
    output.DisplayName = "Switch Version Information";
    output.Identifier = new Guid("ec797b2c-5d39-415f-8294-98ab3410cb96");
    output.OutputText = response;
    networkSwitch.CommandOutputs.Items.Add(output);
}
```

SSH Settings

Secure Shell (SSH) allows for the execution of commands and the transfer of files on remote machines that support SSH-2 using a secure connection.



The screenshot shows the 'Unix System Agent Settings' dialog box with the 'SSH' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'Optional Components', 'SNMP', 'SSH', 'Files', and 'Plugins'. The 'SSH' tab is active, showing the 'SSH Settings' section. It includes a terminal icon and a description: 'Enter the details required to connect to the secure shell (SSH) server.' There is a checkbox for 'Enable SSH Connection' which is checked. Below this are input fields for 'Username' (containing 'root'), 'Password' (masked with dots), 'Port' (containing '22'), and 'Timeout' (containing '60000'). An 'Advanced Settings' button is located below the input fields. At the bottom right are 'OK' and 'Cancel' buttons.

Unix System Agent Settings

Optional Components SNMP **SSH** Files Plugins

SSH Settings

Enter the details required to connect to the secure shell (SSH) server.

☒ Enable SSH Connection

Username
root

Password
.....

Port Timeout
22 60000

Advanced Settings

OK Cancel

Enable SSH Connection

Determines whether the SSH connection should be enabled.

Username

The username to use for the connection.

Password

The password to use for the connection.

Port

The TCP port to use for the connection, by default this is port 22.

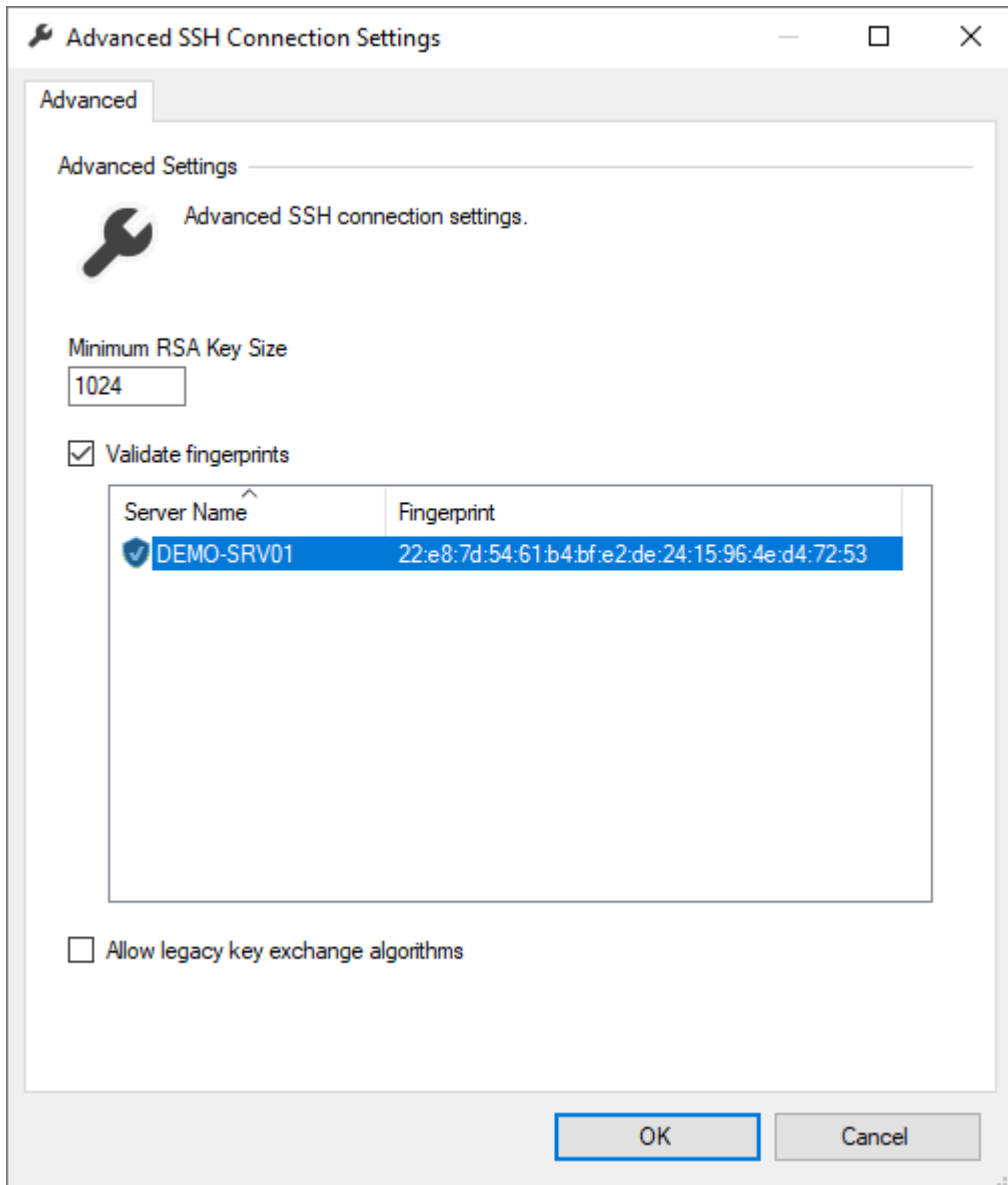
Timeout

The timeout to use for the connection in milliseconds.

Advanced Settings

The [advanced settings](#) to use for the connection.

Advanced Settings



The image shows a Windows-style dialog box titled "Advanced SSH Connection Settings". It has a tab labeled "Advanced" and a subtitle "Advanced Settings". Below the subtitle is a wrench icon and the text "Advanced SSH connection settings.".

There are three main settings:

- Minimum RSA Key Size:** A text box containing the value "1024".
- Validate fingerprints:** A checkbox that is checked.
- Allow legacy key exchange algorithms:** A checkbox that is unchecked.

Below the "Validate fingerprints" checkbox is a table with two columns: "Server Name" and "Fingerprint". The table contains one row with the following data:

Server Name	Fingerprint
DEMO-SRV01	22:e8:7d:54:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Minimum RSA Key Size

The minimum allowed size of the RSA key. The minimum value is 512 bits, with a default value of 1024 bits.

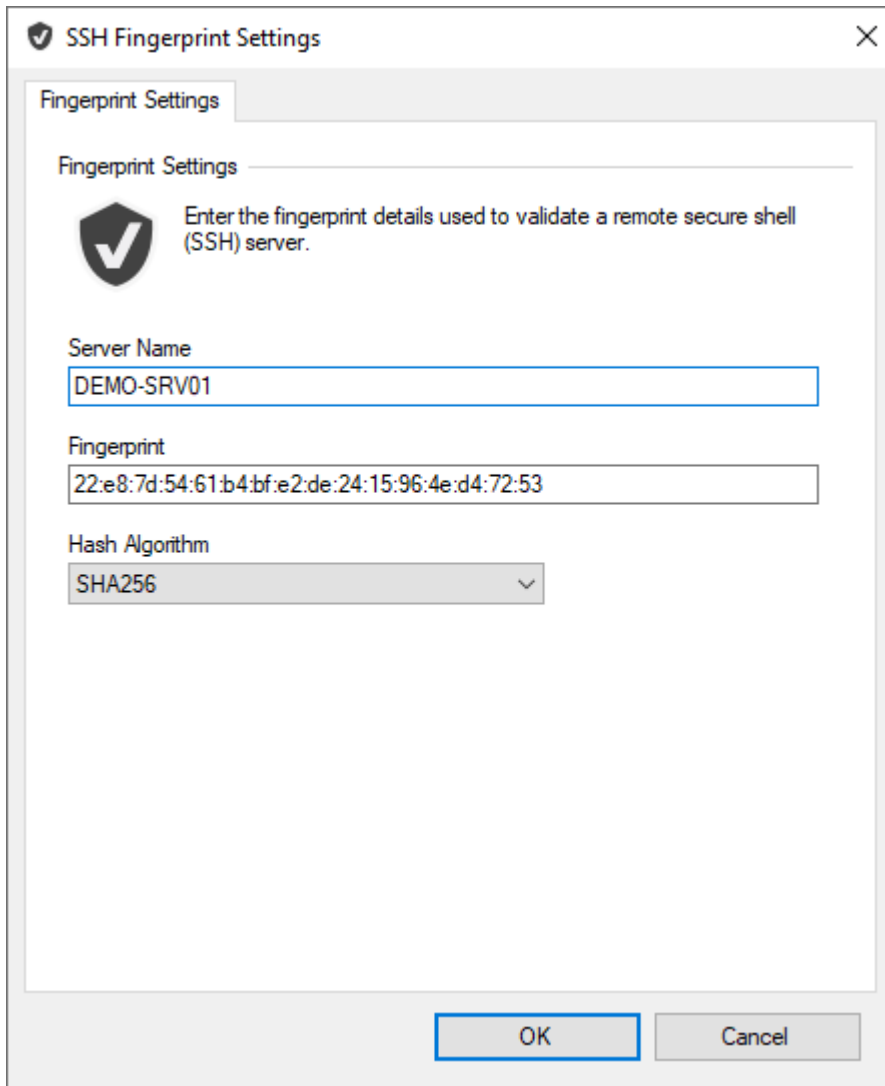
Validate fingerprints

Determines whether to validate the [fingerprints](#) of remote servers. This can increase security by verifying the identity of the servers being connected to before credentials are sent to the server. This can help to prevent a man in the middle attack.

Allow legacy key exchange algorithms

Determines whether the connection should allow for less secure legacy key exchange algorithms.

Fingerprint Settings



The image shows a dialog box titled "SSH Fingerprint Settings" with a close button (X) in the top right corner. Inside the dialog, there is a tab labeled "Fingerprint Settings". Below the tab, there is a section header "Fingerprint Settings" followed by a descriptive text: "Enter the fingerprint details used to validate a remote secure shell (SSH) server." To the left of this text is a shield icon with a checkmark. Below the text, there are three input fields: "Server Name" with the value "DEMO-SRV01", "Fingerprint" with the value "22:e8:7d:54:61:b4:bf:e2:de:24:15:96:4e:d4:72:53", and "Hash Algorithm" with a dropdown menu showing "SHA256". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

SSH Fingerprint Settings

Fingerprint Settings

Fingerprint Settings

Enter the fingerprint details used to validate a remote secure shell (SSH) server.

Server Name

DEMO-SRV01

Fingerprint

22:e8:7d:54:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

Hash Algorithm

SHA256

OK Cancel

Server name

The name or IP address of the server to which the connection is made.

Fingerprint

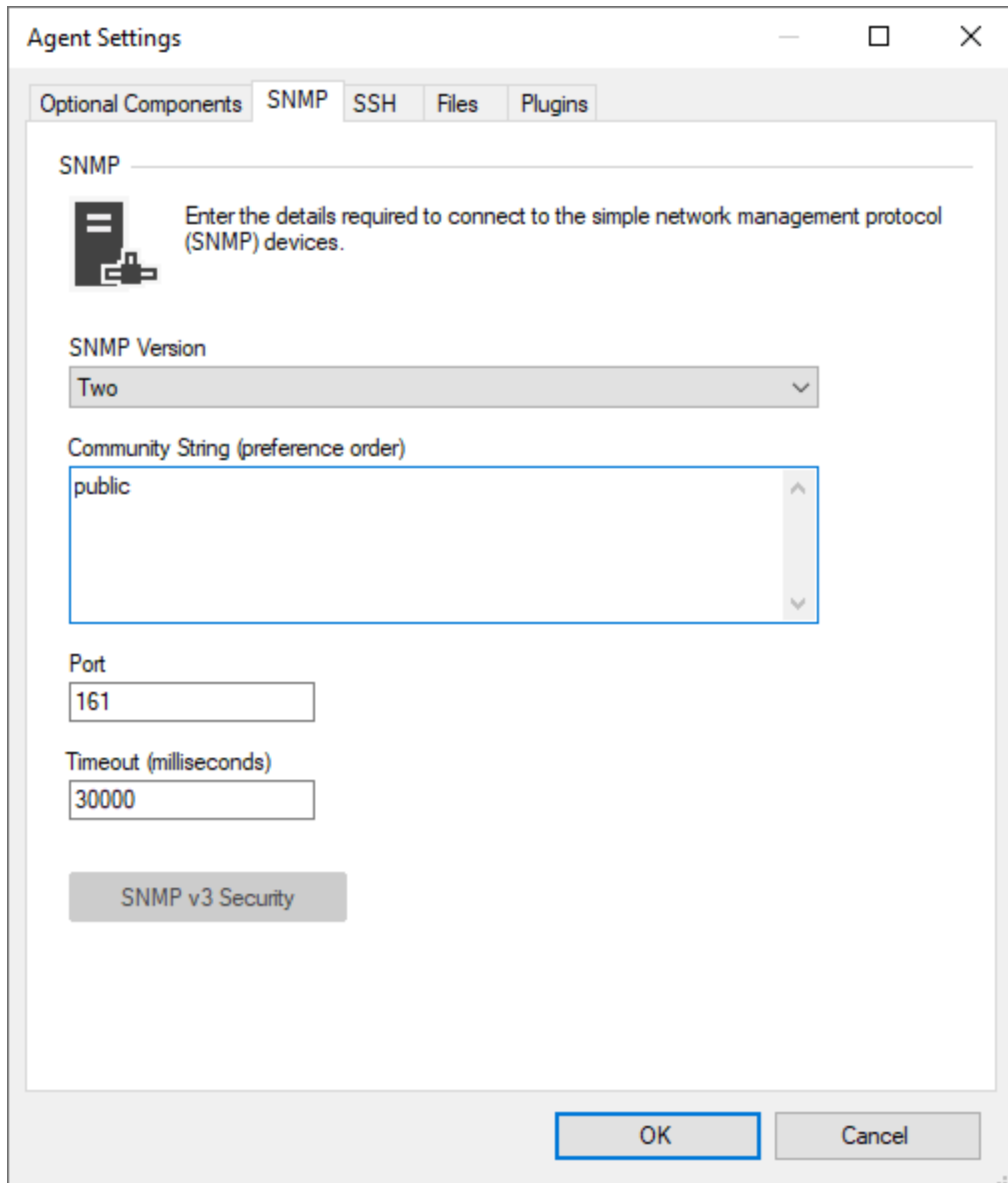
The fingerprint of the remote server in SHA256 format.

Hash Algorithm

The algorithm used to generate the fingerprint. This is always SHA256.

SNMP Settings

The simple network management protocol (SNMP) is used to communicate with network devices such as [network switches](#) and [network storage devices](#) as well as for obtaining additional information from other managed devices such as [Windows servers](#).



The image shows a Windows-style dialog box titled "Agent Settings". It has four tabs: "Optional Components", "SNMP", "SSH", "Files", and "Plugins". The "SNMP" tab is selected. Inside the dialog, there is a section for "SNMP" with a small icon of a server and a lock. Below this is a text box with the instruction: "Enter the details required to connect to the simple network management protocol (SNMP) devices." The settings include: "SNMP Version" set to "Two" in a dropdown menu; "Community String (preference order)" with a list box containing "public"; "Port" set to "161" in a text box; and "Timeout (milliseconds)" set to "30000" in a text box. There is a button labeled "SNMP v3 Security". At the bottom are "OK" and "Cancel" buttons.

SNMP Version

The version of SNMP to use for communication with the device.

Security

Configures the [SNMP version 3 security settings](#).

Community String

The community string to use in order of preference. When scanning [Windows machines](#) the [Windows machine agent](#) will detect the SNMP community string automatically.

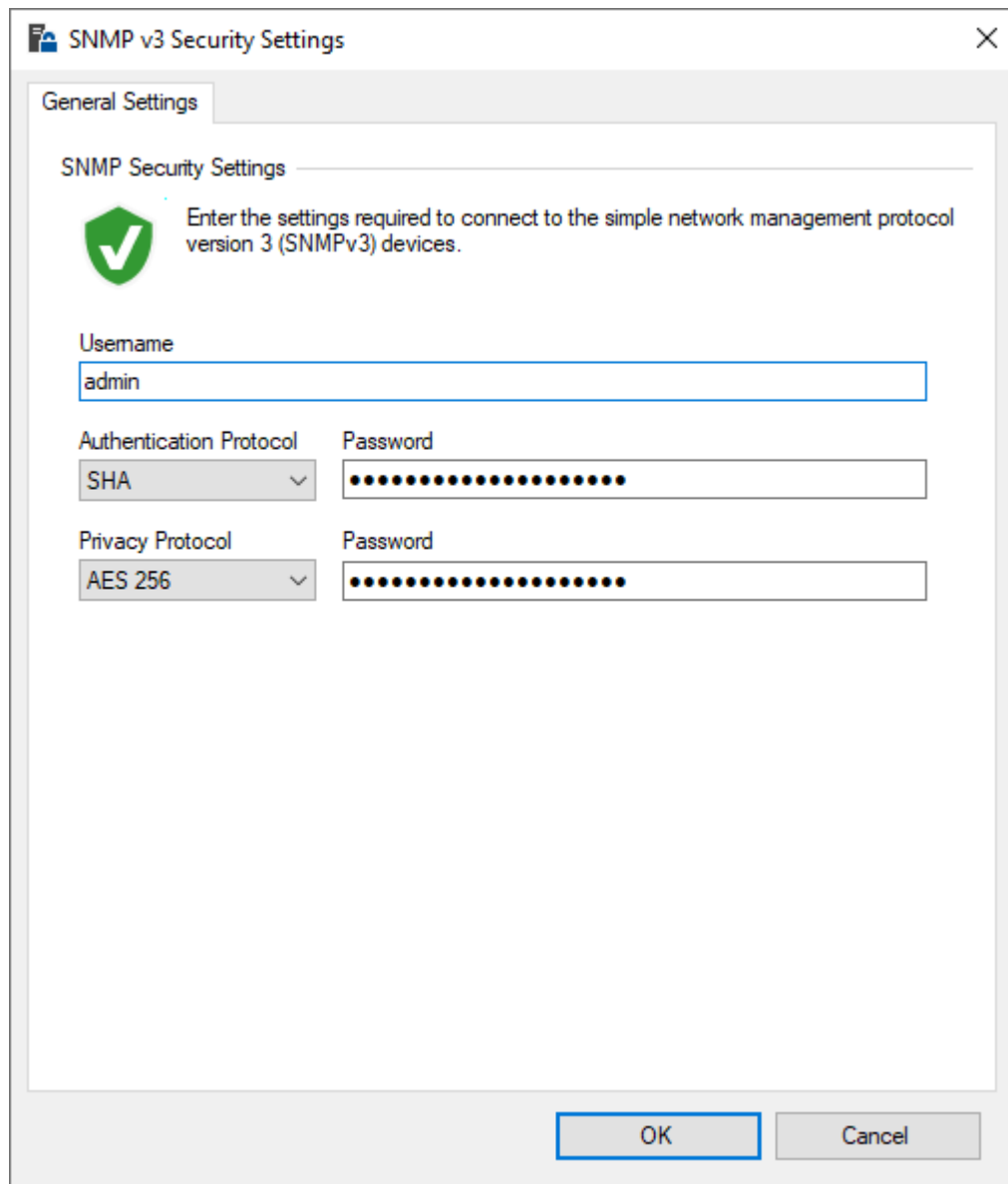
Port

The UDP port used to connect to SNMP on the remote device, by default this is 161.

Timeout

The timeout in milliseconds, by default this is 30,000ms.

SNMP v3 Security Settings



The image shows a Windows-style dialog box titled "SNMP v3 Security Settings". It has a "General Settings" tab selected. Inside the dialog, there is a green shield icon with a white checkmark. To the right of the icon, the text reads: "Enter the settings required to connect to the simple network management protocol version 3 (SNMPv3) devices." Below this, there are four input fields: "Username" with the value "admin", "Authentication Protocol" with a dropdown menu showing "SHA", "Password" (masked with dots), and "Privacy Protocol" with a dropdown menu showing "AES 256", followed by another "Password" field (also masked with dots). At the bottom right, there are "OK" and "Cancel" buttons.

SNMP v3 Security Settings

General Settings

SNMP Security Settings

Enter the settings required to connect to the simple network management protocol version 3 (SNMPv3) devices.

Username
admin

Authentication Protocol
SHA

Password
.....

Privacy Protocol
AES 256

Password
.....

OK Cancel

Username

The username to use for the connection.

Authentication Protocol

The protocol to use for authentication - None, MD5, or SHA.

Password

The password to use for authentication.

Privacy Protocol

The protocol to use for packet privacy - None, DES, Triple DES (3DES), AES 128, AES 192, or AES 256.

Password

The password to use for packet privacy.

Tools

The [XIA Configuration Client](#) includes the following additional tools.

Microsoft Online Agent UI

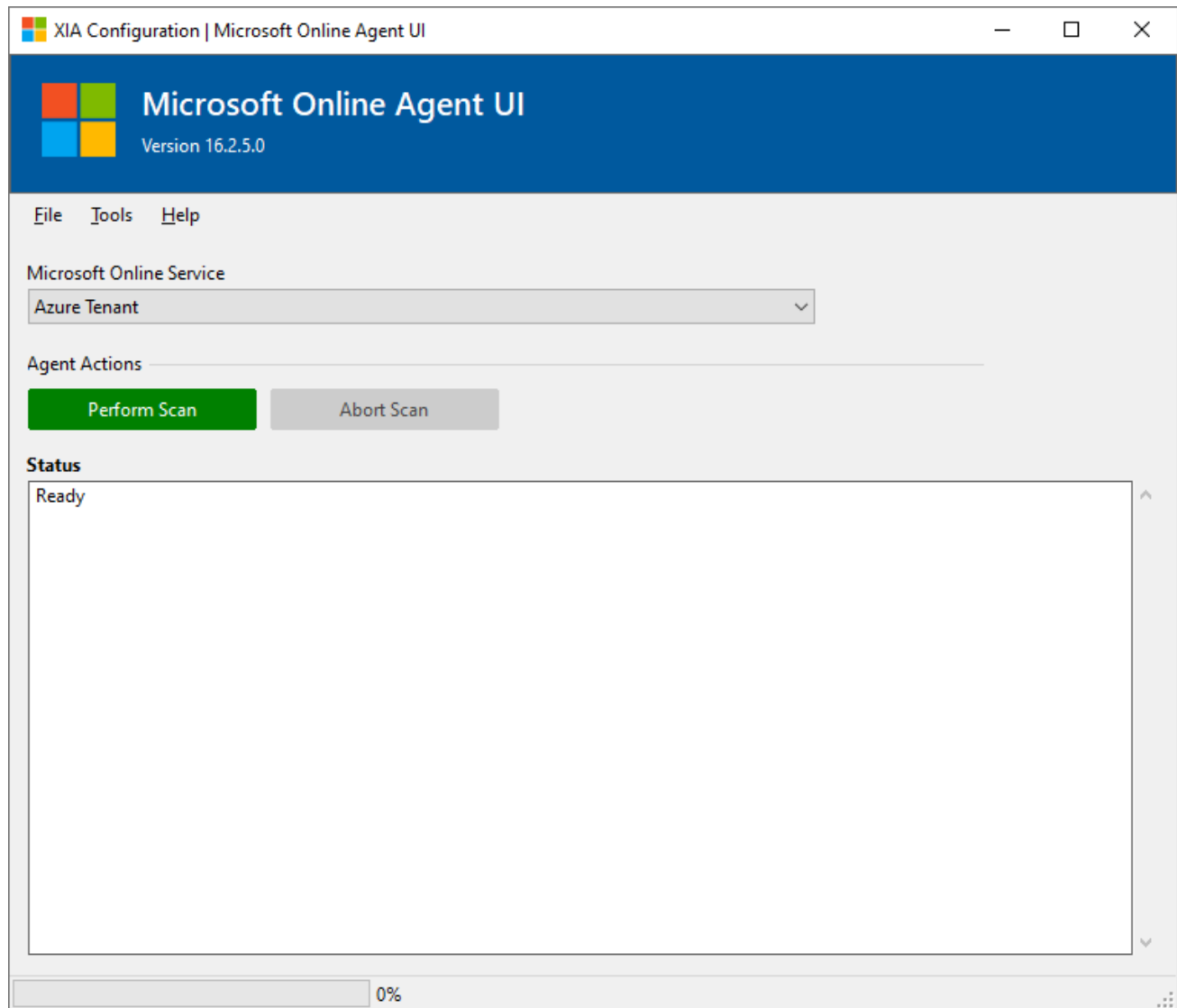
Displays the [Microsoft Online Agent UI](#) tool.

SNMP Data Collector

Displays the [SNMP data collector](#) tool.

Microsoft Online Agent UI

The Microsoft Online Agent UI is a stand-alone tool that allows the scanning of Microsoft Online services including [Azure Tenants](#), [Entra directories](#), and [Exchange Online](#) when interaction is required during the logon process - for example where two-factor authentication is required.



Microsoft Online Service

The type of service to scan

- [Azure Tenant](#)
- [Entra directory](#)
- [Exchange Online](#)

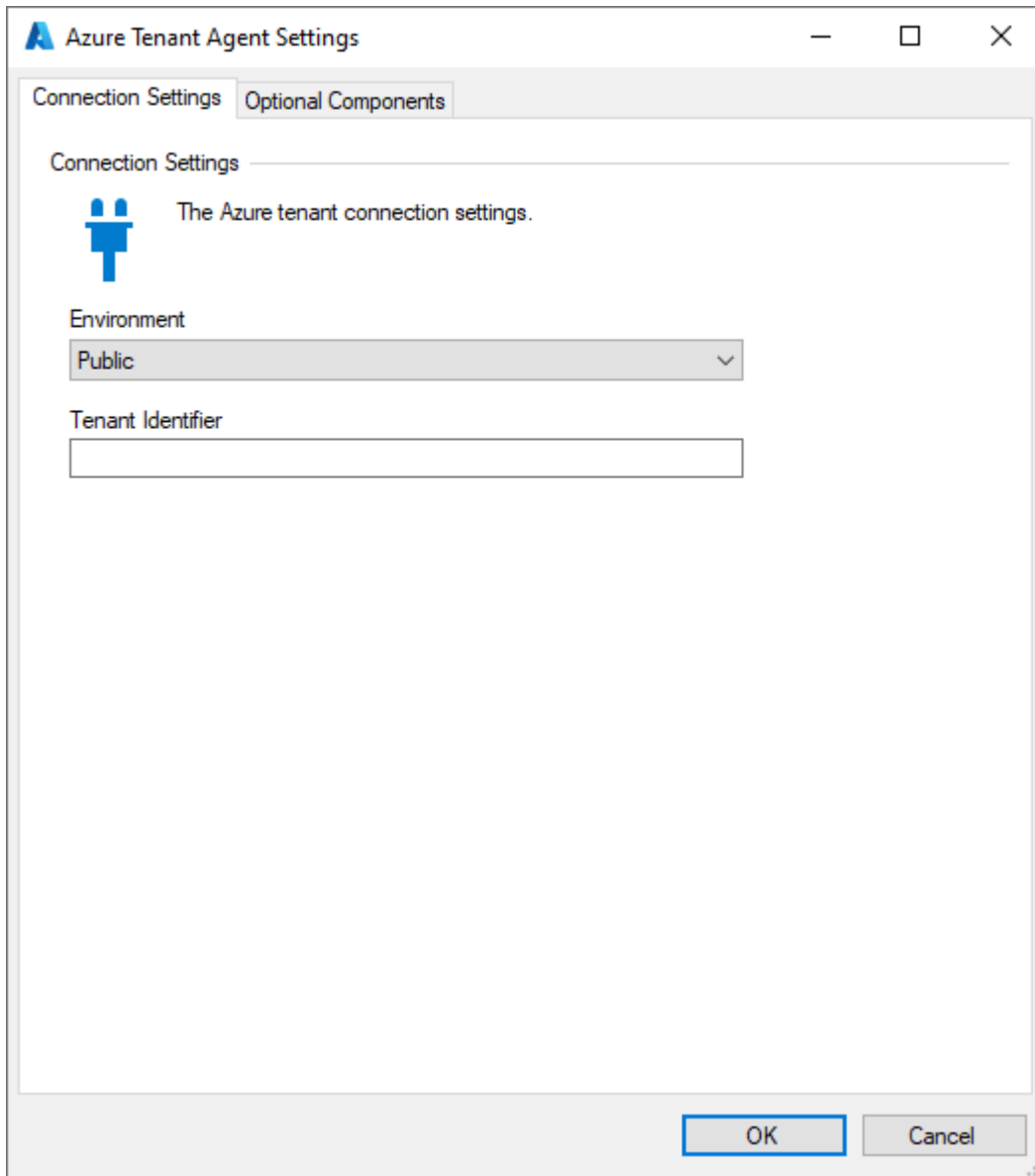
Perform Scan

Clicking the perform scan button starts the scan of the specified Microsoft Online service. For more information see the [performing a scan](#) section.

Abort Scan

Clicking the abort scan button aborts the scan.

Azure Tenant Agent Settings Dialog



Azure Tenant Agent Settings

Connection Settings | Optional Components

Connection Settings

 The Azure tenant connection settings.

Environment

Public

Tenant Identifier

OK Cancel

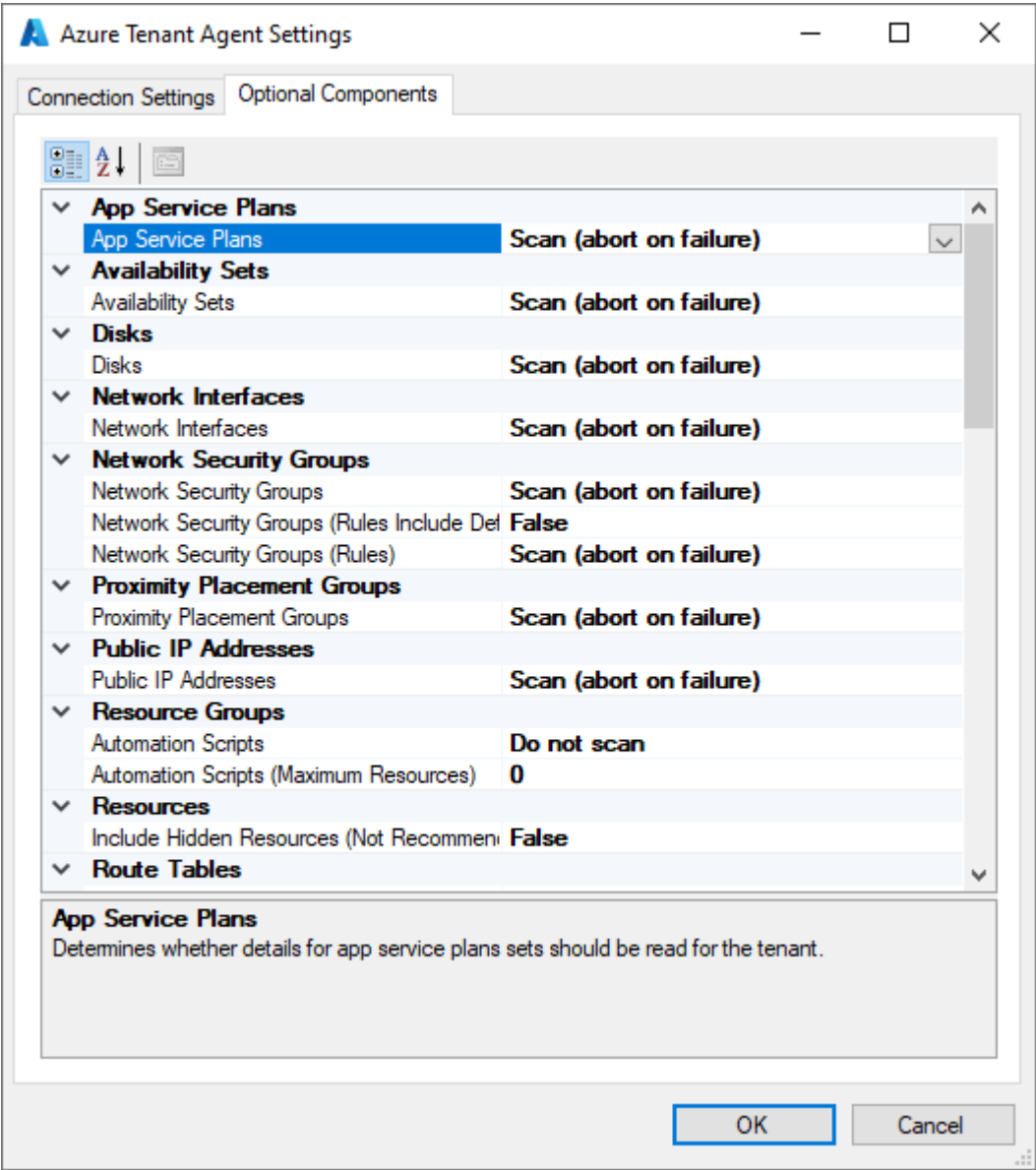
Environment

The Azure environment to connect to.

Tenant Identifier

The optional identifier of the Azure tenant in [GUID](#) format.

Optional Components

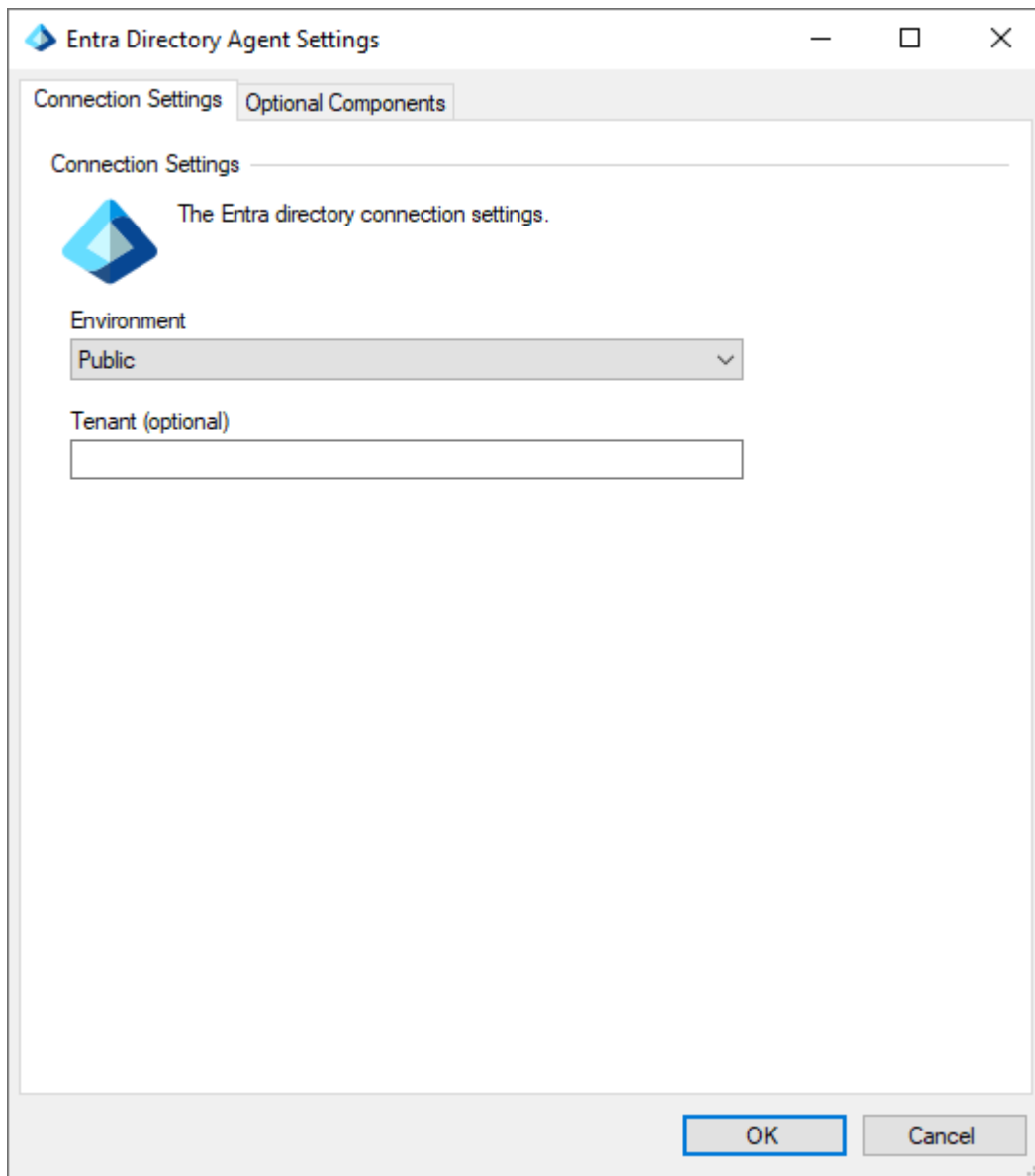


Optional Components

This determines the optional components of the scan.

For more information see the [optional components](#) section of the [Azure tenant agent](#).

Entra Directory Agent Settings Dialog



Entra Directory Agent Settings

Connection Settings Optional Components

Connection Settings

The Entra directory connection settings.

Environment

Public

Tenant (optional)

OK Cancel

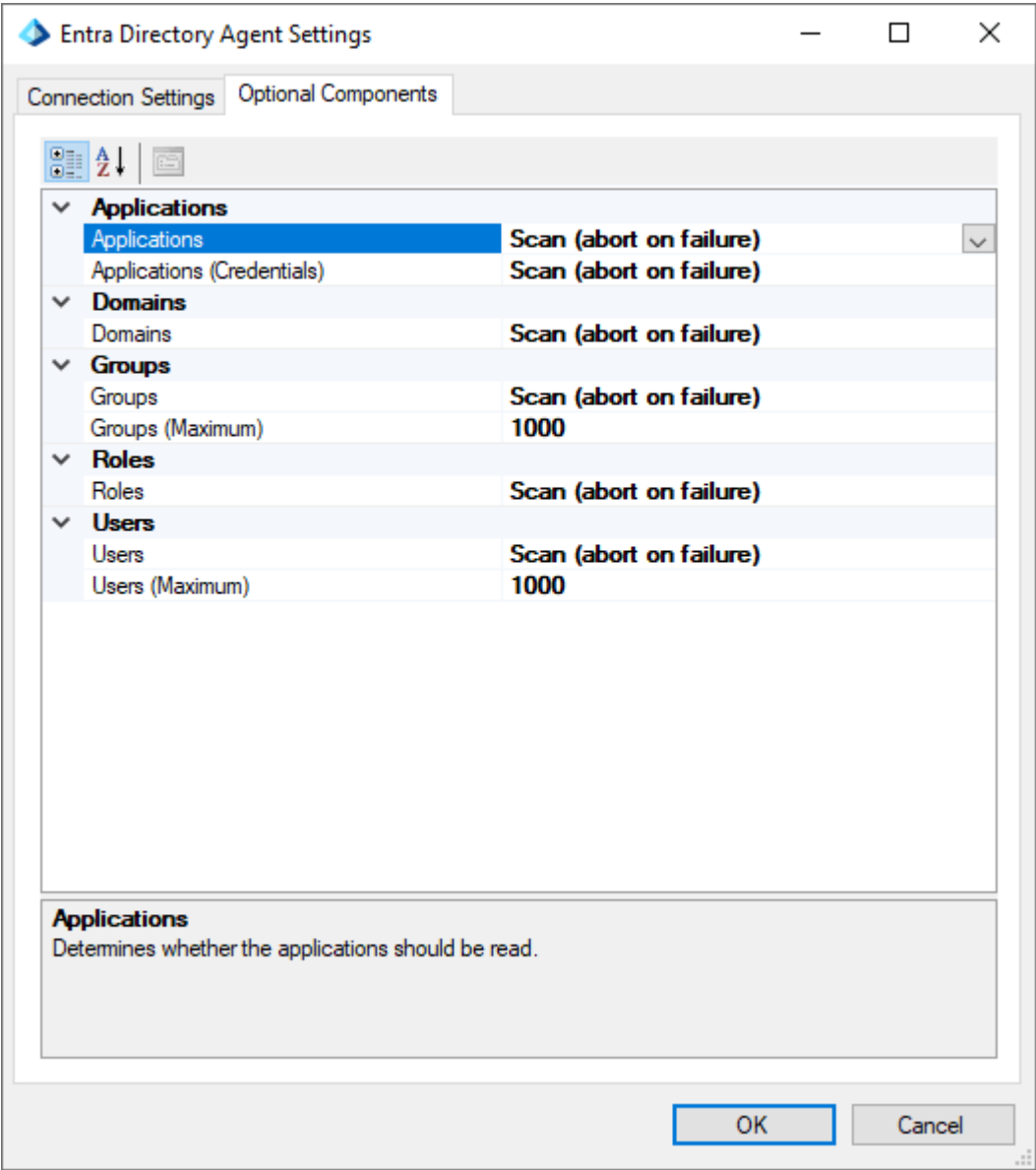
Environment

The environment to connect to.

Tenant (optional)

The name or unique identifier of the tenant organization to connect to - for example "contoso.onmicrosoft.com".

Optional Components

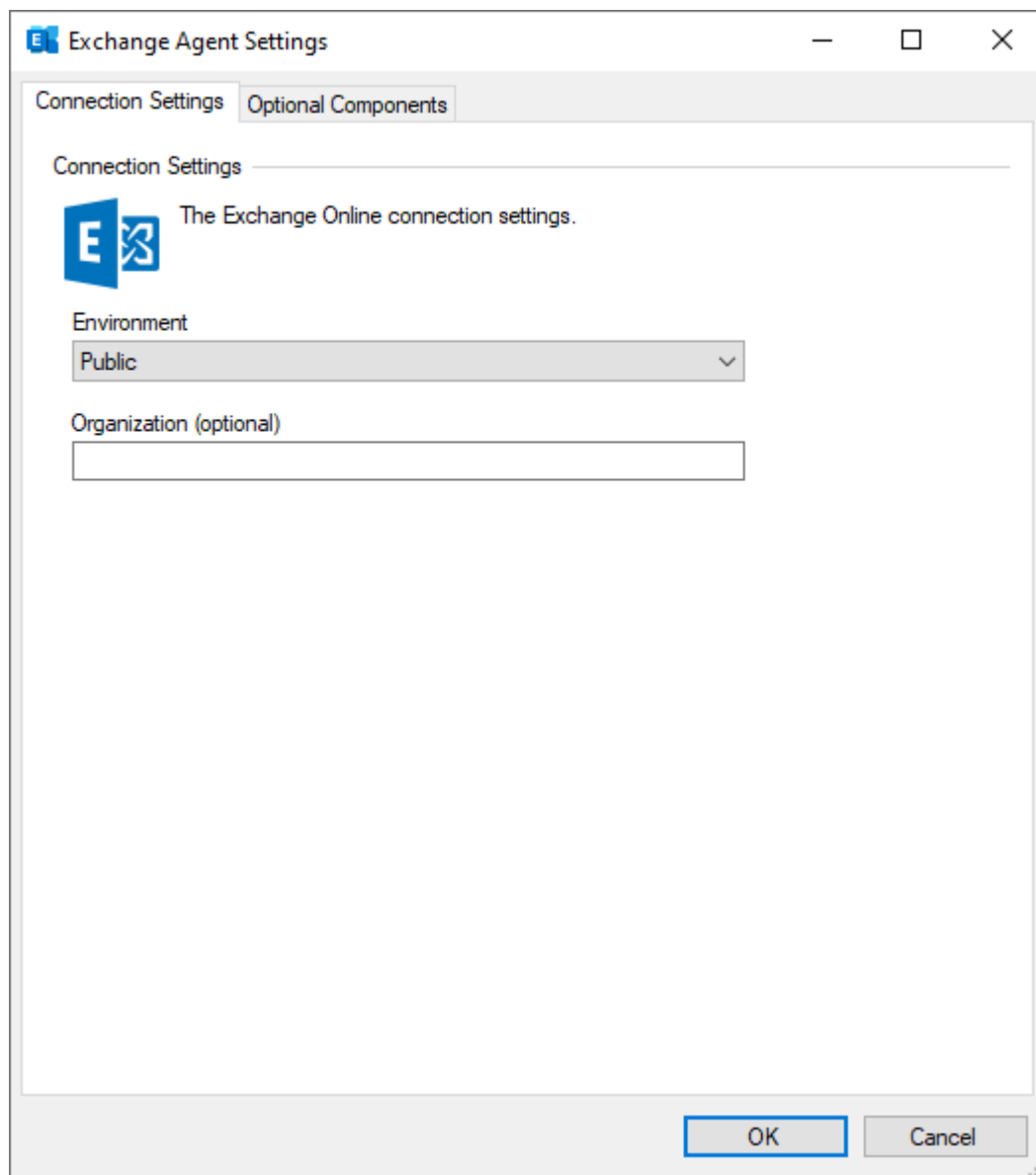


Optional Components

This determines the optional components of the scan.

For more information see the [optional components](#) section of the [Entra directory agent](#).

Exchange Online Agent Settings Dialog



The image shows the 'Exchange Agent Settings' dialog box. It has two tabs: 'Connection Settings' (selected) and 'Optional Components'. The 'Connection Settings' tab contains the following elements:

- A header section with the Exchange Online logo and the text 'The Exchange Online connection settings.'
- An 'Environment' dropdown menu currently set to 'Public'.
- An 'Organization (optional)' text input field.
- 'OK' and 'Cancel' buttons at the bottom right.

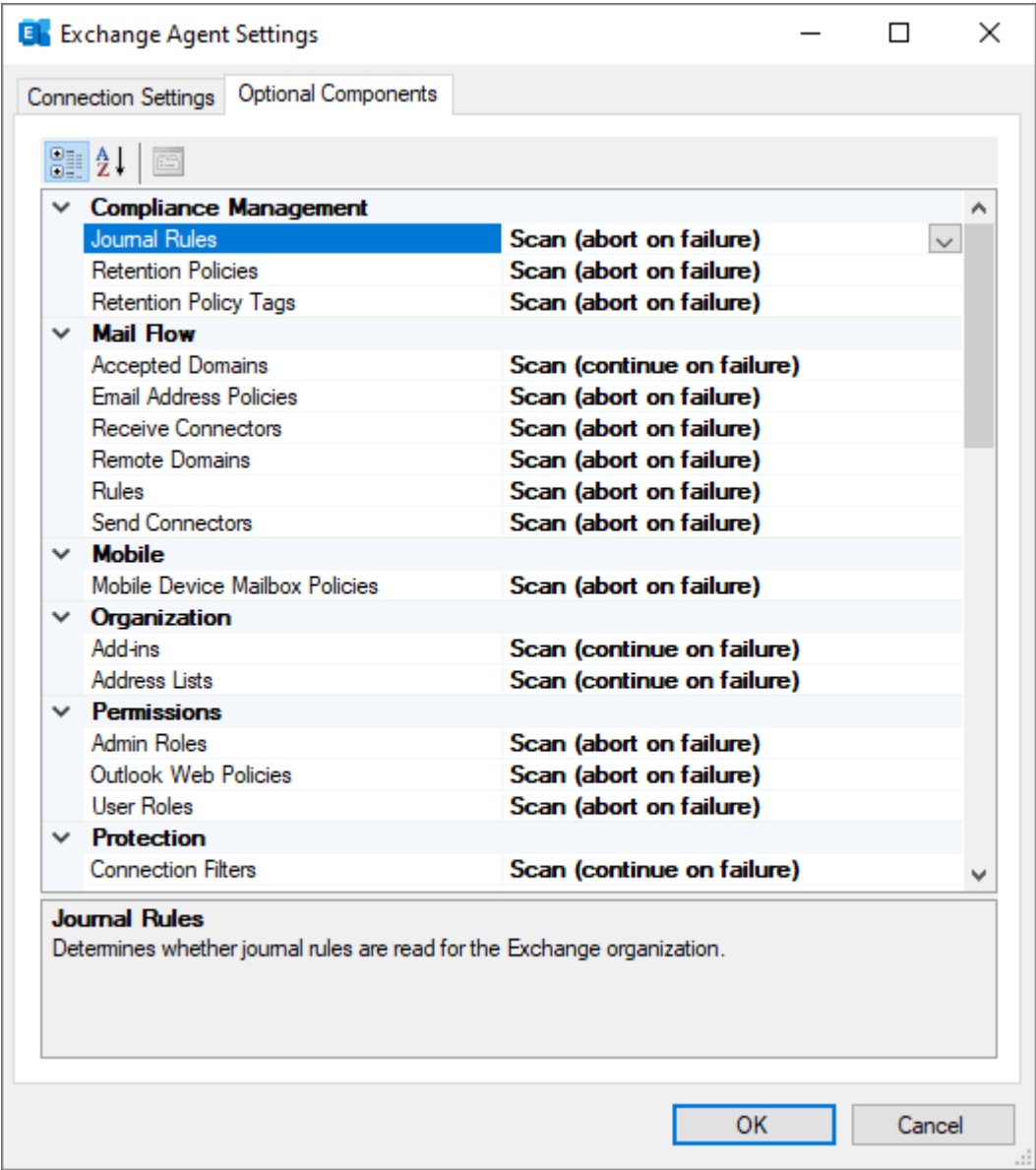
Environment

The [Exchange Online](#) environment to connect to.

Organization (optional)

The name of the [Exchange Online](#) organization to connect to - for example "contoso.onmicrosoft.com".

Optional Components



Optional Components

This determines the optional components of the scan.

For more information see the [optional components](#) section of the [Exchange organization agent](#).

Menu

The drop down menu displayed in the [Microsoft Online Agent UI](#).

File Menu

Reset Settings

Resets the settings to the default values.

Save Settings

Saves the current settings.

Exit

Exits the tool.

Tools Menu

Agent Settings > Azure Tenant Agent Settings

Displays the [Azure tenant agent settings dialog](#).

Agent Settings > Entra Directory Agent Settings

Displays the [Entra directory agent settings dialog](#).

Agent Settings > Exchange Agent Settings

Displays the [Exchange Online agent settings dialog](#).

Install Exchange Online PowerShell Cmdlets

Opens a PowerShell prompt to install the Exchange Online PowerShell cmdlets.

For more information see the [Installing Exchange Online PowerShell Cmdlets](#) section.

Diagnostics > Enable Diagnostics

Enables the diagnostics log for the [Exchange Online Agent UI](#).

Diagnostics > Open Diagnostics Folder

Opens the folder that contains the diagnostics log for the [Exchange Online Agent UI](#).

Help Menu

Contents and Index

Displays this help.

Requirements

For more information about the requirements of the Azure tenant scan see the [Azure tenant agent requirements](#).

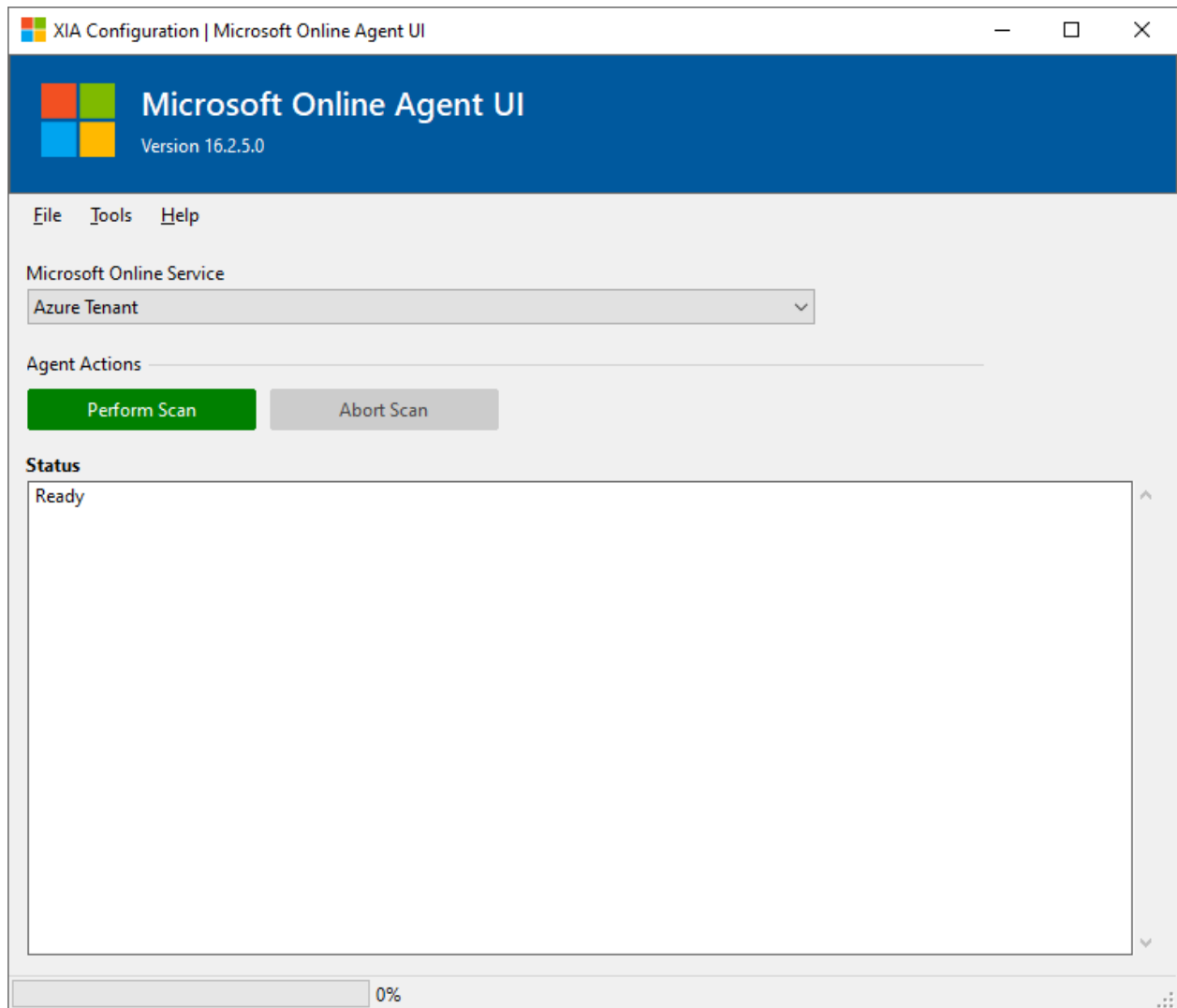
For more information about the requirements of the Entra directory scan see the [Entra directory agent requirements](#).

For more information about the requirements of the Exchange Online scan see the [Exchange organization agent requirements](#).

Performing a Scan

To perform a scan using the [Microsoft Online Agent UI](#) follow these steps.

- Ensure the [requirements](#) have been met.
- Start the [Microsoft Online Agent UI](#) from the [tools menu](#) of the [XIA Configuration Client administration tools](#).



- Optionally set the [agent settings](#) by clicking agent settings on the [tools menu](#).
- Select the type of Microsoft online service to scan.
- Click the perform scan button.
- When prompted enter your credentials.

Sign in to your account

Microsoft

Sign in

Email address or phone number

Can't access your account?

Back

Next

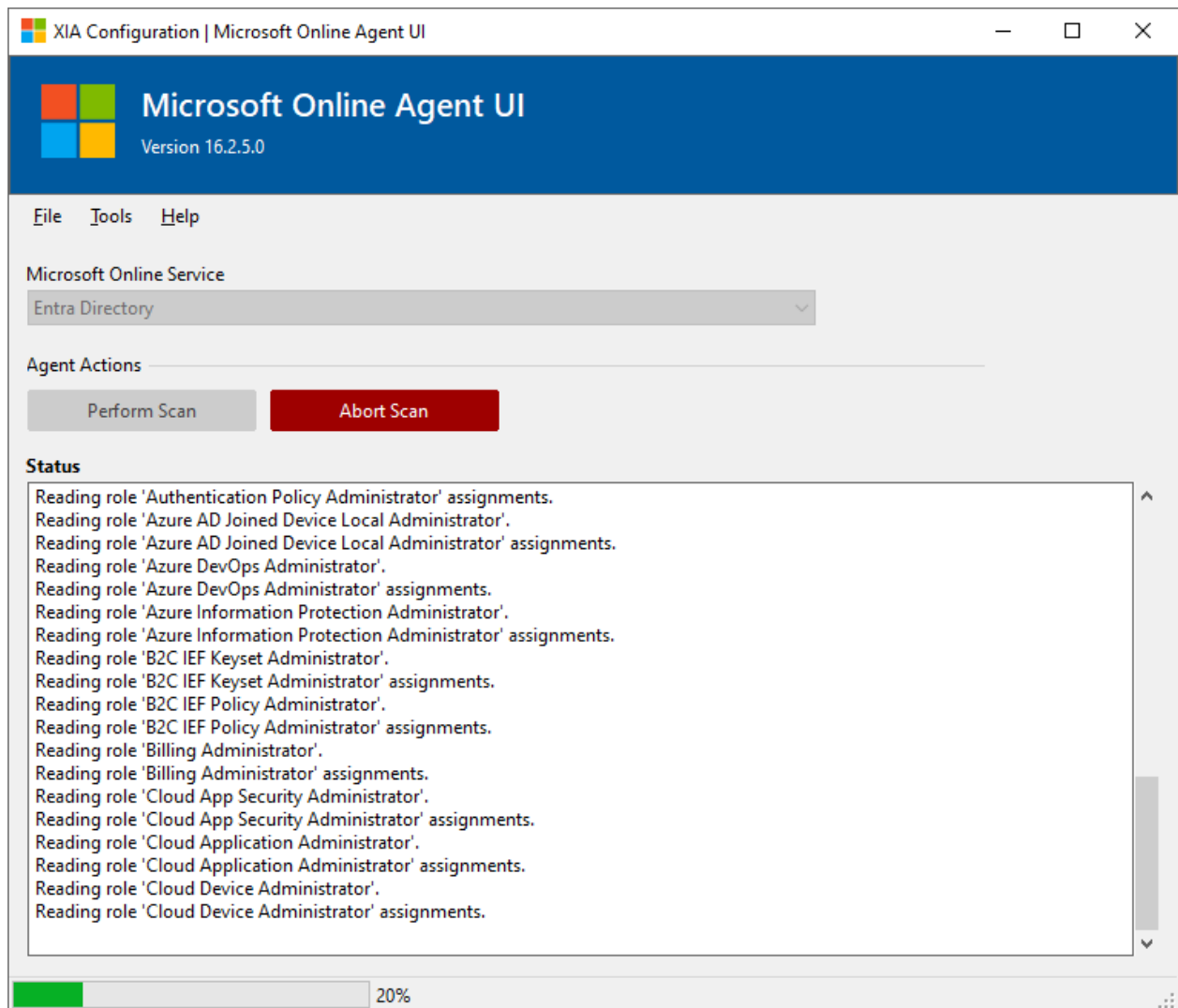
 Sign-in options

Terms of use

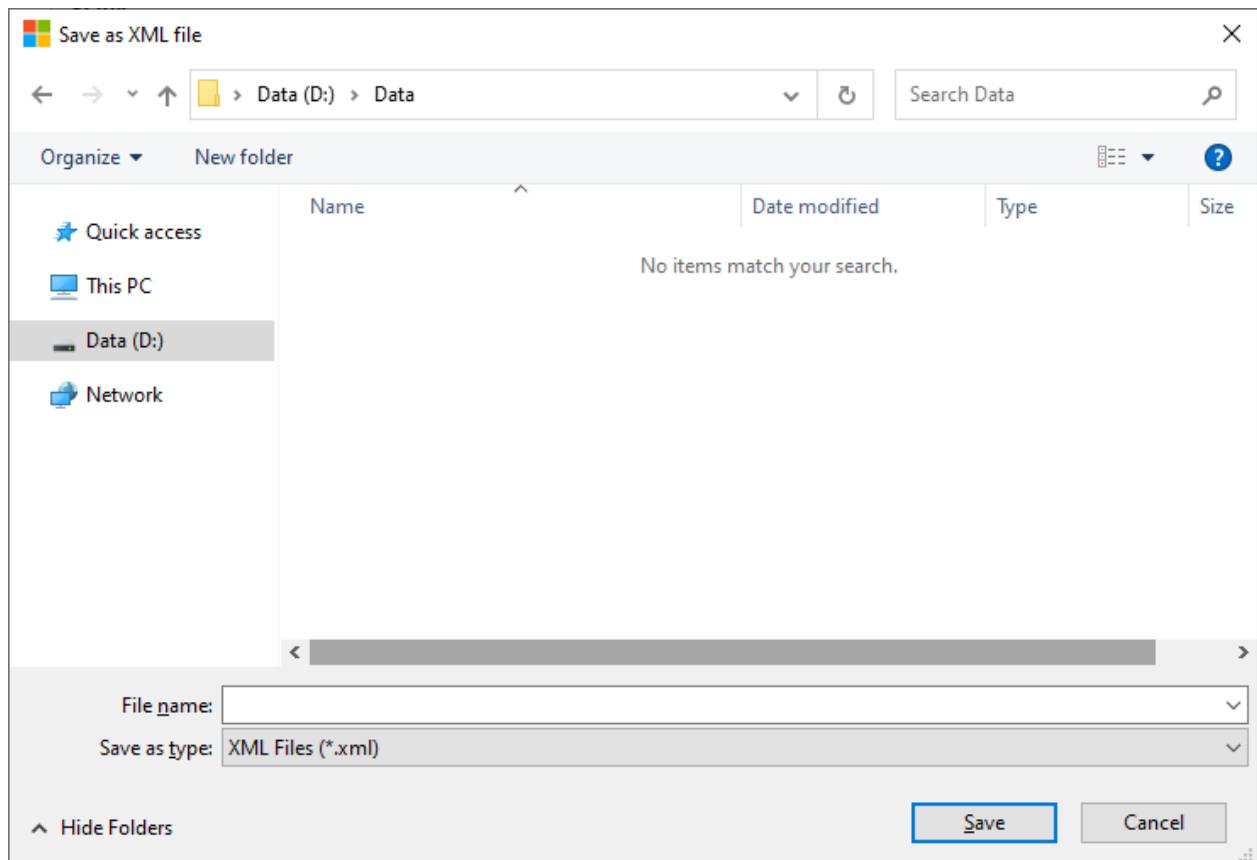
Privacy & cookies

...

- The scan will proceed, you can click the abort scan button at any time.



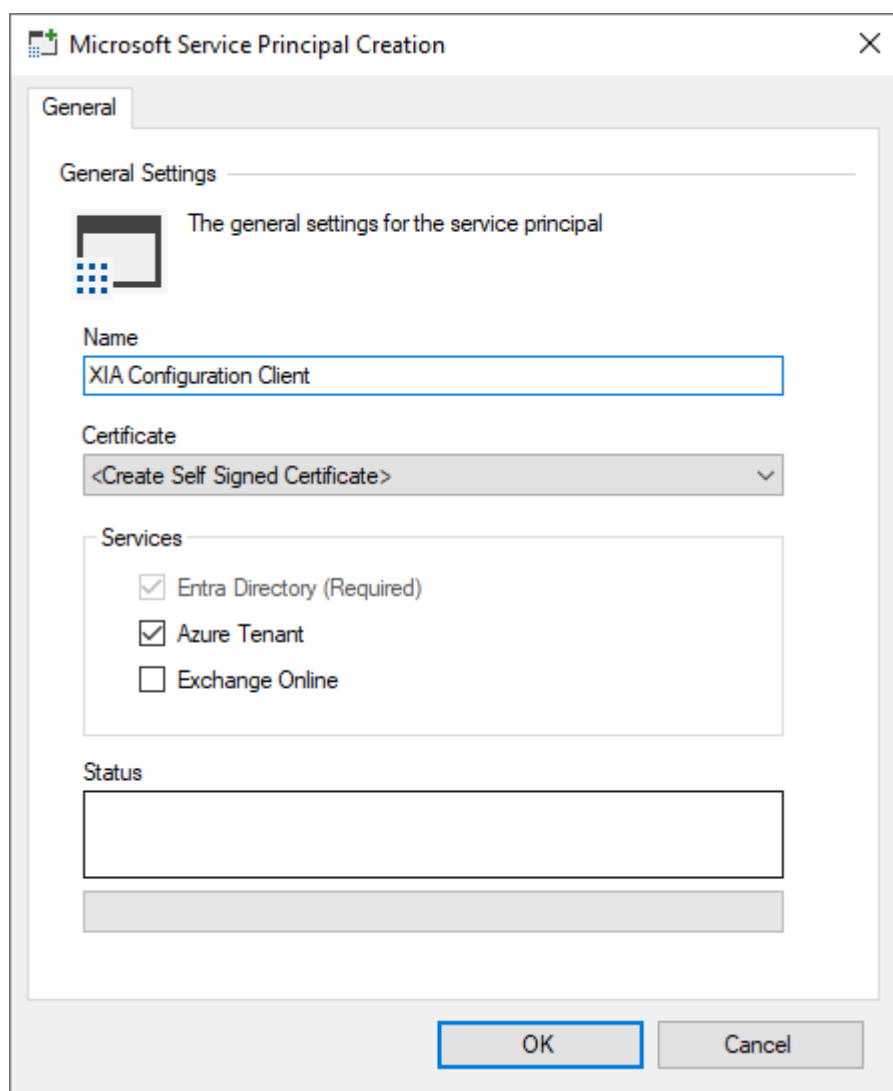
- When the scan is complete you will be prompted to save the output.



- The data file can be [manually uploaded](#) into [XIA Configuration Server](#).

Microsoft Service Principal Creation Tool

The Microsoft service principal creation tool automatically creates a service principal in the [Entra](#) directory and optionally creates and assigns a self-signed certificate to use for authentication.



The screenshot shows the 'Microsoft Service Principal Creation' dialog box. It has a 'General' tab selected. Under 'General Settings', there is a description 'The general settings for the service principal' with a small icon. Below this, the 'Name' field contains 'XIA Configuration Client'. The 'Certificate' dropdown menu is set to '<Create Self Signed Certificate>'. Under the 'Services' section, there are three checkboxes: 'Entra Directory (Required)' (checked), 'Azure Tenant' (checked), and 'Exchange Online' (unchecked). At the bottom, there is a 'Status' field which is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

Name

The name of the service principal to create.

Certificate

The certificate to use for authentication. The certificate must be installed in the user store of the [XIA Configuration Client service account](#) and support client authentication. Alternatively selecting "<Create Self Signed Certificate>" will create and install a new certificate in the user store of the [XIA Configuration Client service account](#) that supports client authentication.

Services

The services that the service principal will support.

Services > Entra Directory (Required)

Configures the [permissions required](#) to read information from an [Entra directory](#), this is required regardless of the service being scanned.

Services > Azure Tenant

Configures the [permissions required](#) to read information from an [Azure tenant](#).

Services > Exchange Online

Configures the [permissions required](#) to read information from an [Exchange Online organization](#).

Status

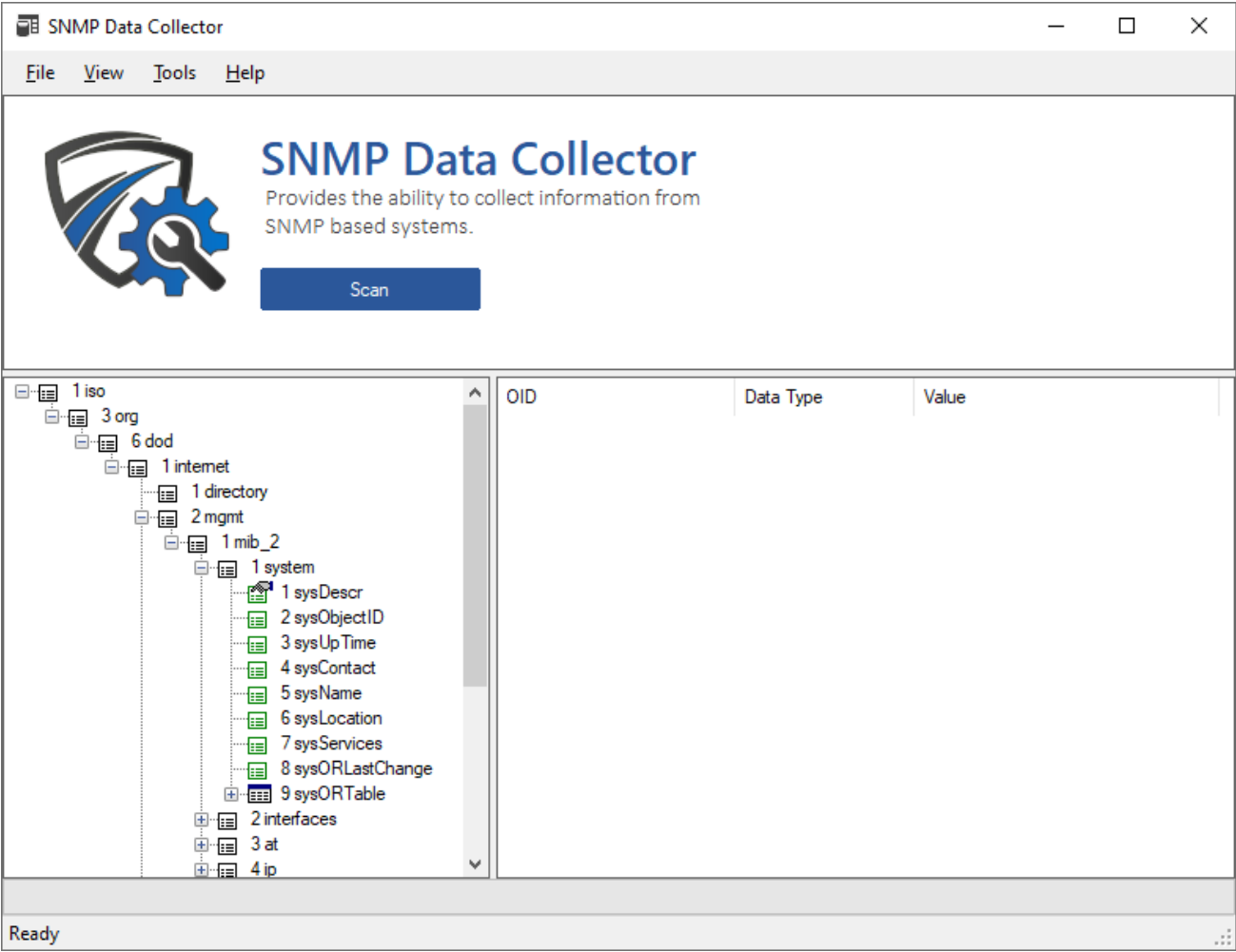
The status of the creation.

NOTE: There may be a delay whilst the service principal and permissions are replicated in Azure before you can successfully complete a scan.

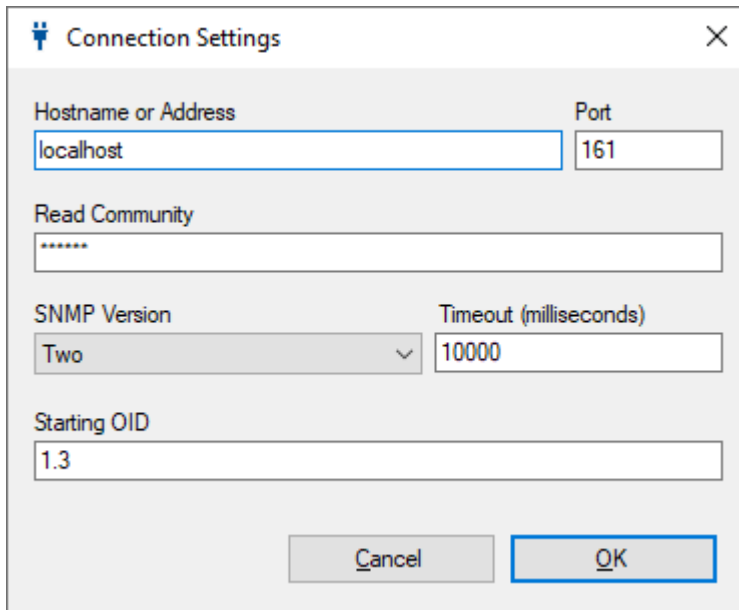
SNMP Data Collector

The SNMP Data Collector is a tool that allows the collection and analysis of SNMP data from remote machines. This can be used for diagnostics purposes and to provide information to [CENTREL Solutions](#) when adding support for new device types or device manufacturers.

To being a scan click the **scan** button which displays the [connection settings dialog](#).



Connection Settings

A screenshot of the 'Connection Settings' dialog box. The dialog has a title bar with a network icon and a close button. It contains several input fields: 'Hostname or Address' with 'localhost', 'Port' with '161', 'Read Community' with a masked string '*****', 'SNMP Version' with a dropdown menu showing 'Two', 'Timeout (milliseconds)' with '10000', and 'Starting OID' with '1.3'. At the bottom are 'Cancel' and 'OK' buttons.

Connection Settings	
Hostname or Address	Port
localhost	161
Read Community	

SNMP Version	Timeout (milliseconds)
Two	10000
Starting OID	
1.3	
Cancel	OK

Hostname or Address

The name or IP address of the device or machine to connect to.

Port

The port on which SNMP is listening on the remote machine. By default, this is 161.

Read Community

The SNMP read community string to use to connect to the device.

SNMP Version

The SNMP version to use to connect to the device. By default, this is version 2.

Timeout (milliseconds)

The connection timeout in milliseconds.

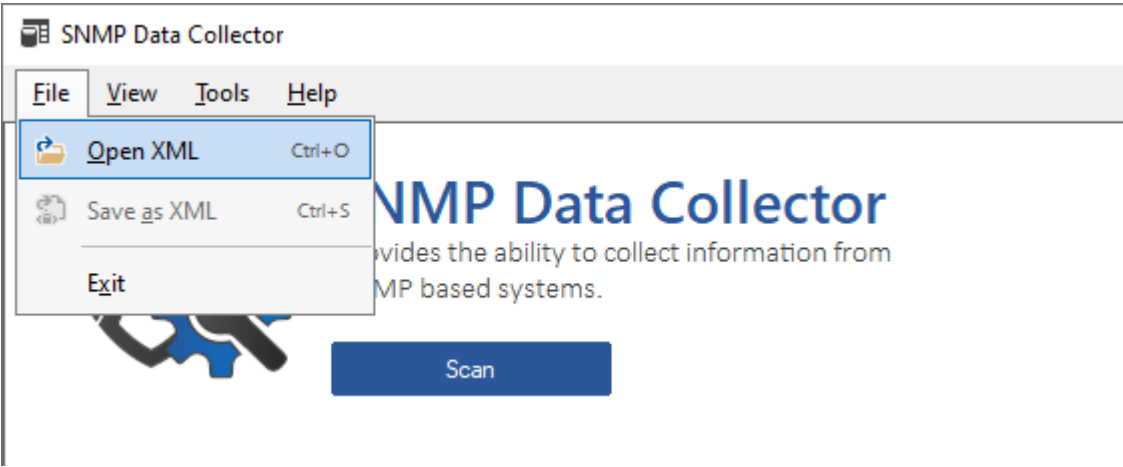
Starting OID

The object identifier (OID) from which to start collecting data. By default, this is 1.3.

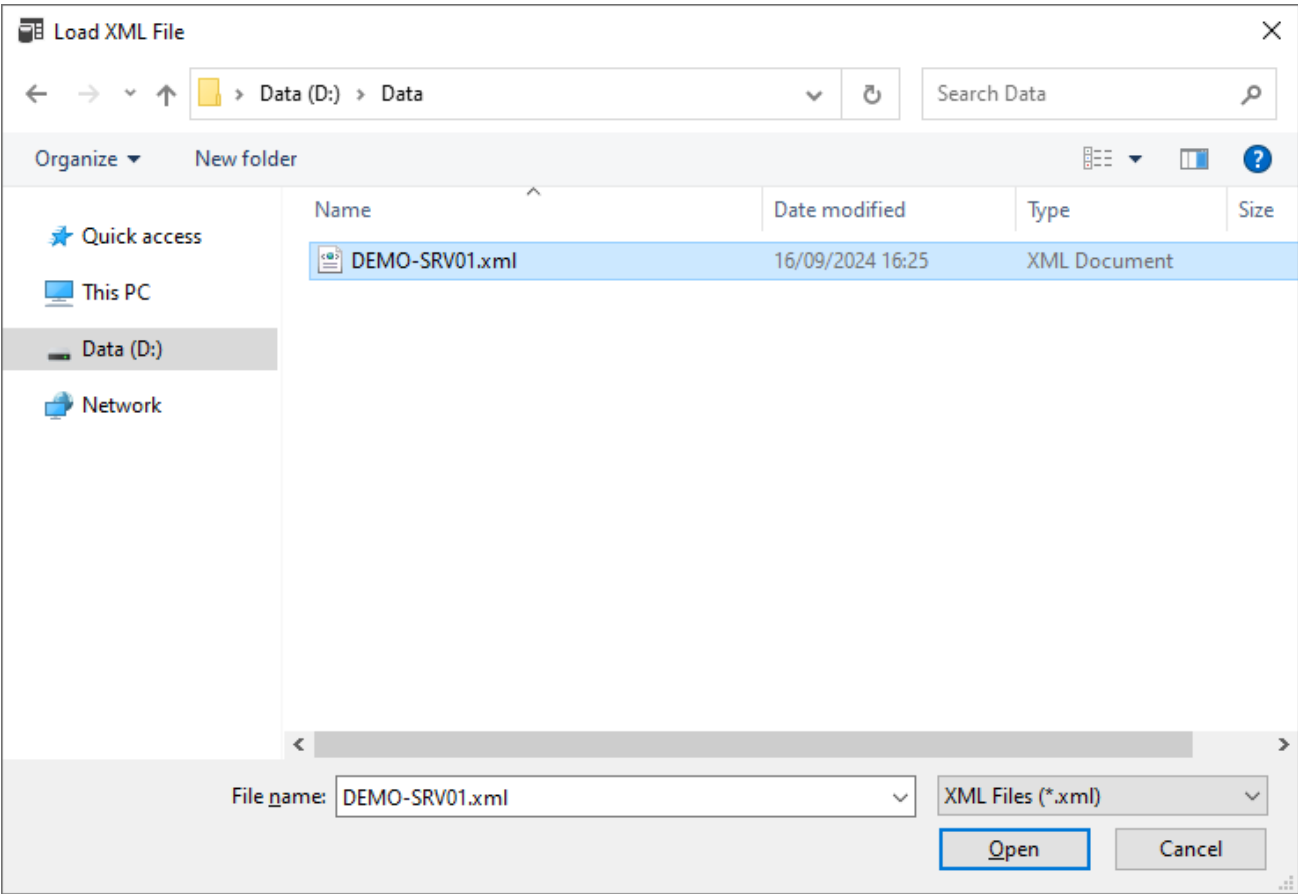
Loading and Saving Data

Data from the [SNMP Data Collector](#) can be loaded from and saved to XML.

Select the **Open XML** or **Save as XML** from the **file** menu.



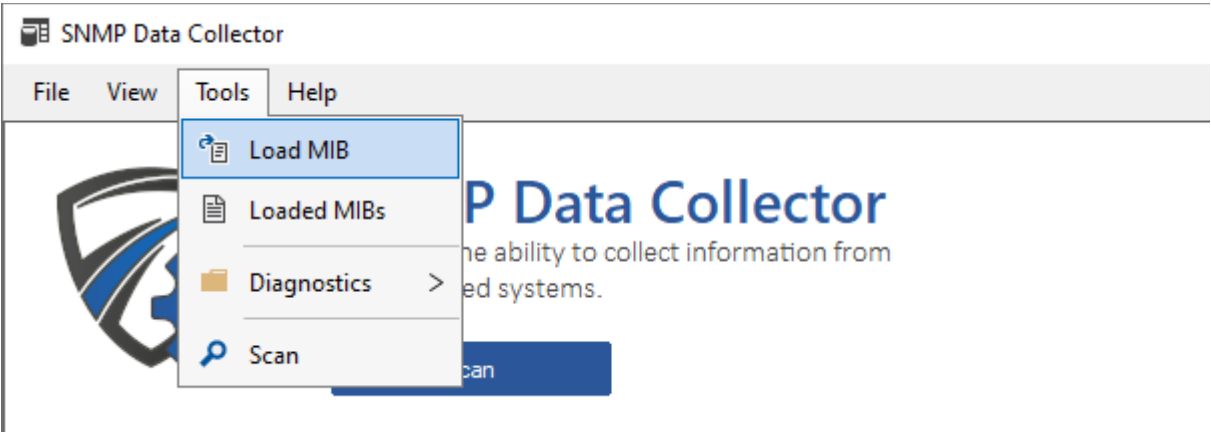
Select the filename.



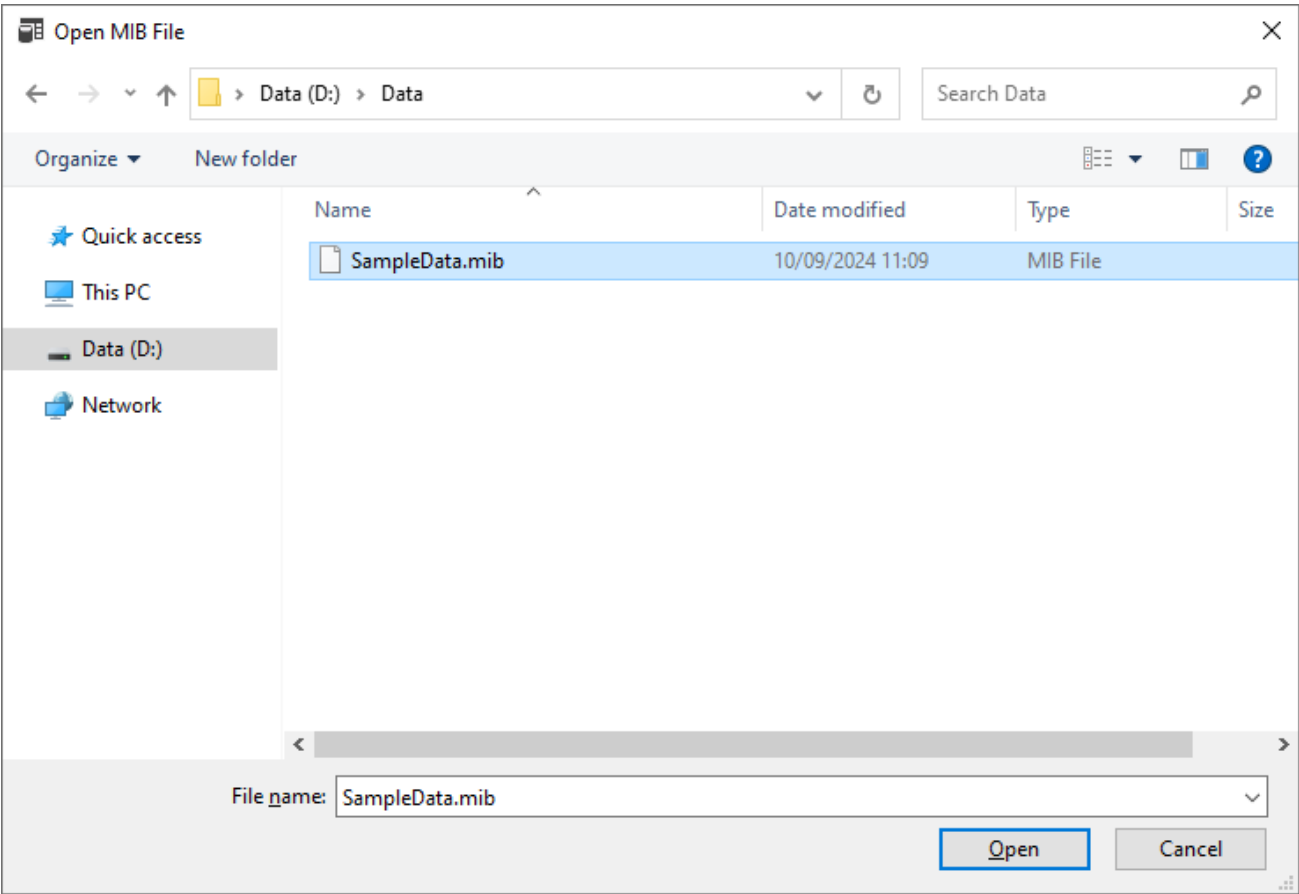
MIB Files

A management information base (MIB) is a file that contains definition information for the simple network management protocol (SNMP).

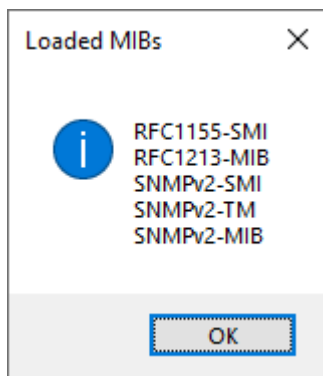
Data from the [SNMP Data Collector](#) automatically loads commonly used MIB files, and additional MIBs can be loaded by selecting **Load MIB** from the **Tools** menu.



Select the MIB file to load.

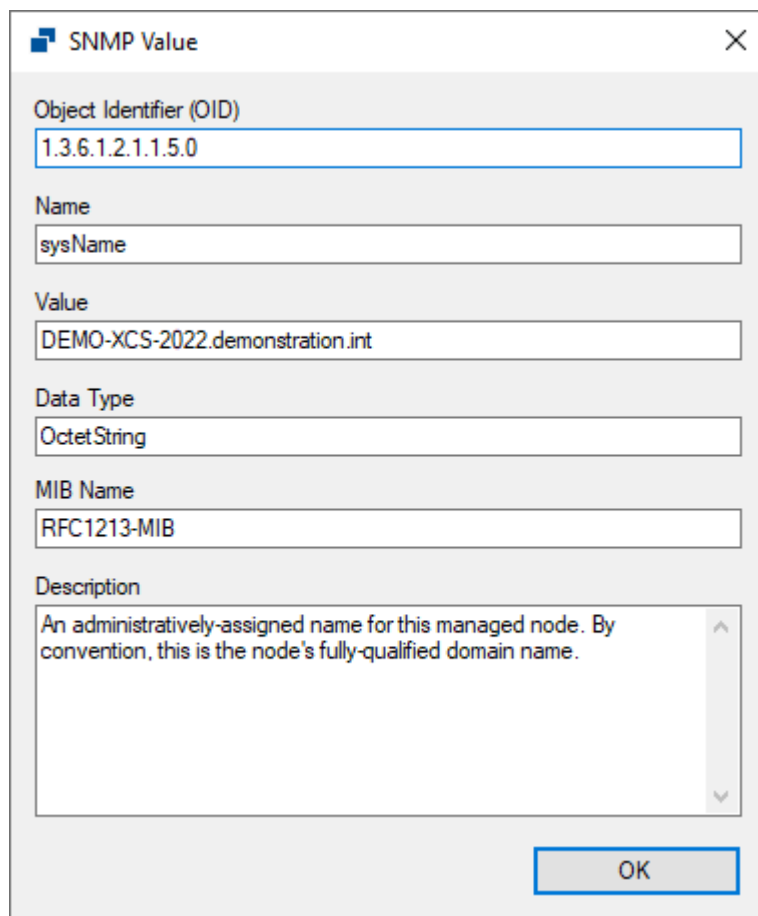


Clicking **Loaded MIBs** displays all currently loaded MIBs.



Viewing Results

Double clicking a result displays the full details for that result.



The image shows a dialog box titled "SNMP Value" with a close button (X) in the top right corner. The dialog contains several labeled text input fields and a description area. The fields are: "Object Identifier (OID)" with the value "1.3.6.1.2.1.1.5.0", "Name" with the value "sysName", "Value" with the value "DEMO-XCS-2022.demonstration.int", "Data Type" with the value "OctetString", and "MIB Name" with the value "RFC1213-MIB". Below these fields is a "Description" section containing a text area with the text: "An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name." At the bottom right of the dialog is an "OK" button.

Object Identifier (OID)	1.3.6.1.2.1.1.5.0
Name	sysName
Value	DEMO-XCS-2022.demonstration.int
Data Type	OctetString
MIB Name	RFC1213-MIB
Description	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.

Object Identifier (OID)

The unique identifier for this result.

Name

The display name of the SNMP object if this has been resolved by a [MIB File](#).

Value

The value of this SNMP object.

Data Type

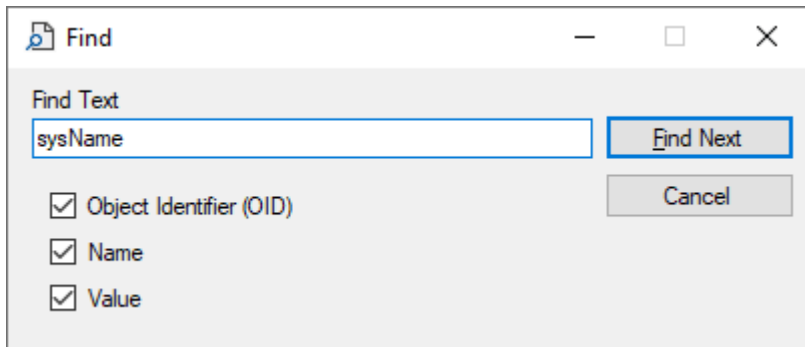
The type of data.

Description

The description of the SNMP object if this has been resolved by a [MIB File](#).

Finding Results

To find data within the SNMP Data Collector's results, select **Find** from the **View** menu or press CTRL + F.



Enter the search text and select the options within the dialog.

Object Identifier (OID)

Results will be found that match the object identifier specified.

Name

Results will be found that match the name specified - for example "sysUpTime".

Value

Results will be found that contain the value specified - for example "DEMO-SRV01".

Troubleshooting

The following chapters cover the troubleshooting and diagnostics of the [XIA Configuration Client](#).

Diagnostics Trace

The [XIA Configuration Client](#) allows the output of information to a trace file to enable detailed diagnostics.

Enabling trace on a computer running the [XIA Configuration Client](#) can be achieved in one of two ways.

- Accessing the [diagnostics log viewer](#).
- By modifying a registry key as follows

WARNING Using Registry Editor incorrectly can cause serious problems with your operating system.

- Open regedit.exe.
- Browse to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\CENTREL Solutions\XIA Configuration Service
- Set the value *EnableTrace* to a value of 1.
- Please note that diagnostics tracing can consume large amounts of disk space, tracing should therefore be disabled when not required by setting the EnableTrace value to 0.

Windows Management Instrumentation (WMI)

Overview

Windows Management Instrumentation WMI is a Microsoft Technology that allows the management of local and remote machines. It is used extensively by the XIA Configuration Service to collect information. WMI uses RPC to execute the commands on remote machines.

Installation

WMI is a core Operating System component and will typically already be installed with the Operating System however it may need to be installed on older Windows NT4 machines. WMI Core 1.5 for Windows NT 4.0 can be downloaded from the following Microsoft Web Site

<http://www.microsoft.com/downloads/details.aspx?familyid=C174CFB1-EF67-471D-9277-4C2B1014A31E&displaylang=en>

Errors caused by WMI

Typically, WMI errors are caused by insufficient permissions on the remote machine or because WMI is not installed or the ports required by WMI are being blocked by a firewall device or the Windows Firewall Service. The XIA Configuration Client Service will test WMI connectivity before starting a Scan and may report errors such as the following

Could not connect to WMI on the remote machine The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)

Troubleshooting WMI Issues

- Ensure that the user account that the XIA Configuration Service is running on has the appropriate permissions to execute WMI on the Remote machine. By default, this is local Administrator permissions.
- Ensure that there is no Firewall between the XIA Configuration Service and the remote machine.
- Execute wbmtest on the machine running the XIA Configuration Service (see steps below) and attempt to connect to the remote machine.
- Execute wbmtest locally on the remote machine if this succeeds it indicates that WMI is correctly installed and running.
- Ensure that the Remote Procedure Call (RPC) Service is started on the Remote Machine

Troubleshoot with wbmtest.exe

It is possible to run queries against the local or remote WMI system using wbmtest. For more information see [Test WMI with wbmtest.exe](#).

Troubleshoot with PowerShell

It is possible to run queries against the local or remote WMI system using Windows PowerShell. For more information see [Test WMI with PowerShell](#).

WMI Stability HotFix

For Windows XP and Windows Server 2003 the following HotFix may help improve WMI stability
<http://support.microsoft.com/kb/933061>

Other Tools

The Microsoft WMI Diagnosis Utility, Version 2.0 may assist with troubleshooting. This tool can be downloaded from Microsoft at the following location.

<http://www.microsoft.com/downloads/details.aspx?familyid=d7ba3cd6-18d1-4d05-b11e-4c64192ae97d&displaylang=en>

Class does not exist (0x80070583)

Symptoms

When performing a scan with an agent that uses WMI you may see the error "Class does not exist" with an error code of 0x80070583.

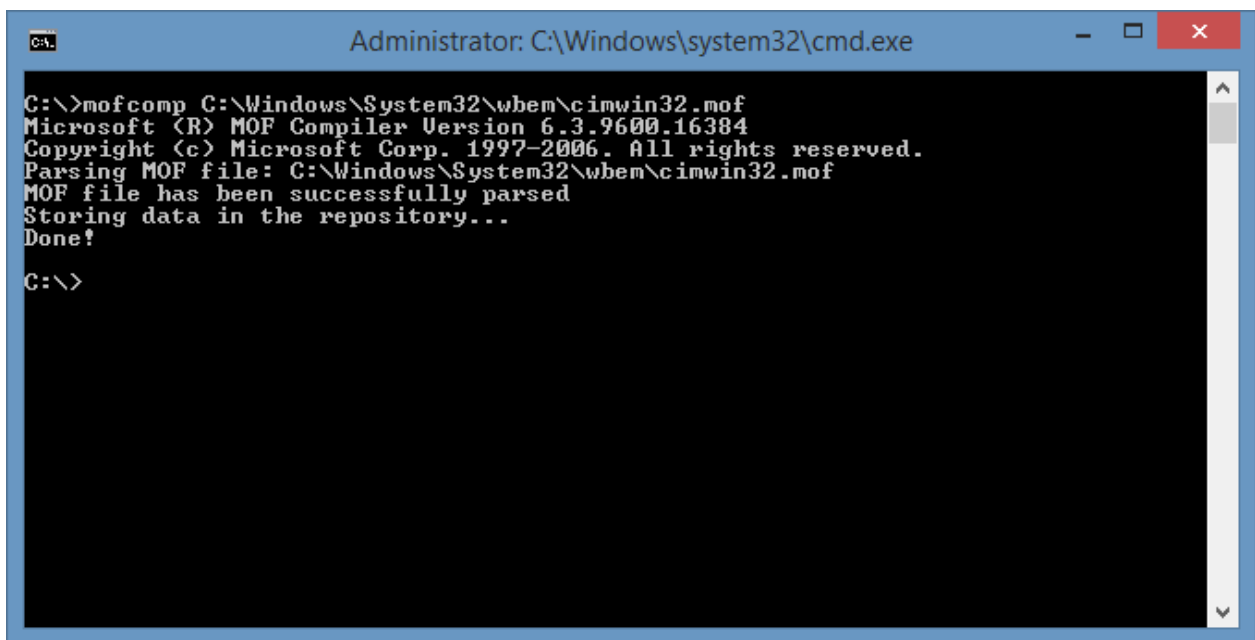
Cause

This can be caused by a corrupt WMI database on the target machine.

Resolution

- View the full exception of the error within the [scan result details](#) dialog, this should include information about the underlying component that caused the error.
- Ensure you have a **full backup** of the target system where the issue was reported.
- Logon to the target system where the issue was reported as an **administrator**.
- If the issue is caused by one of the standard WMI classes enter the following [mofcomp](#) command to rebuild the WMI.

```
mofcomp C:\Windows\System32\wbem\cimwin32.mof
```



```
Administrator: C:\Windows\system32\cmd.exe

C:\>mofcomp C:\Windows\System32\wbem\cimwin32.mof
Microsoft (R) MOF Compiler Version 6.3.9600.16384
Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.
Parsing MOF file: C:\Windows\System32\wbem\cimwin32.mof
MOF file has been successfully parsed
Storing data in the repository...
Done!
C:\>
```

RPC Server is Unavailable

Symptoms

An agent scan fails and the following message is reported

The *SQL Instance* Agent encountered an exception when Testing WMI connection - Could not connect to WMI on the remote machine.

Could not return the initial result from the query 'SELECT * FROM Win32_OperatingSystem'. There was an error performing the query 'SELECT * FROM Win32_OperatingSystem'. The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)

Issue

There was an issue connecting to the remote machine using WMI

Resolution

Though this issue is typically caused by a firewall blocking the remote connection it can also be caused by the service account not having sufficient permissions.

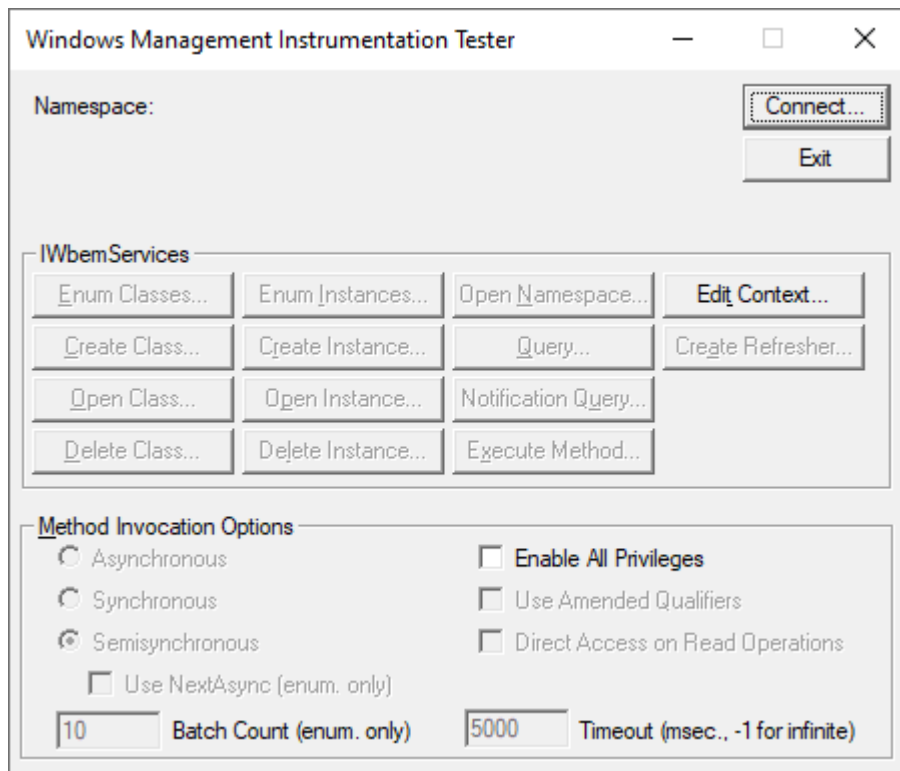
Please follow the troubleshooting tips in the [WMI Issues](#) section.

Test WMI with wbemtest.exe

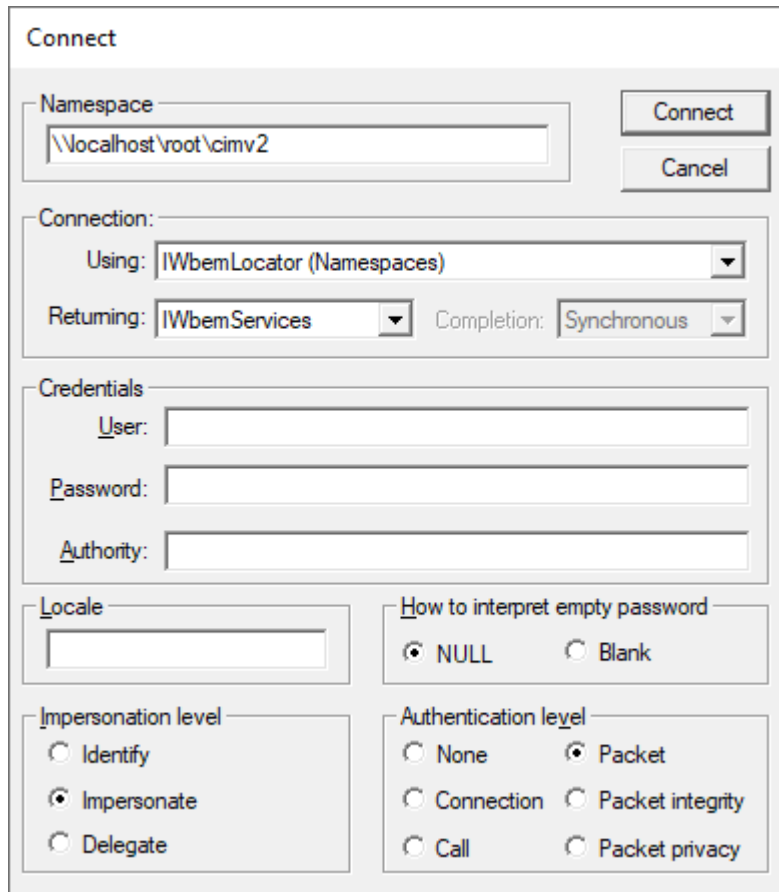
Wbemtest.exe is a tool that is included as part of the WMI installation that helps to troubleshoot WMI issues.

To use **wbemtest** complete the following steps

- Click start, then run and enter **wbemtest** and click OK.
- Click the connect button.



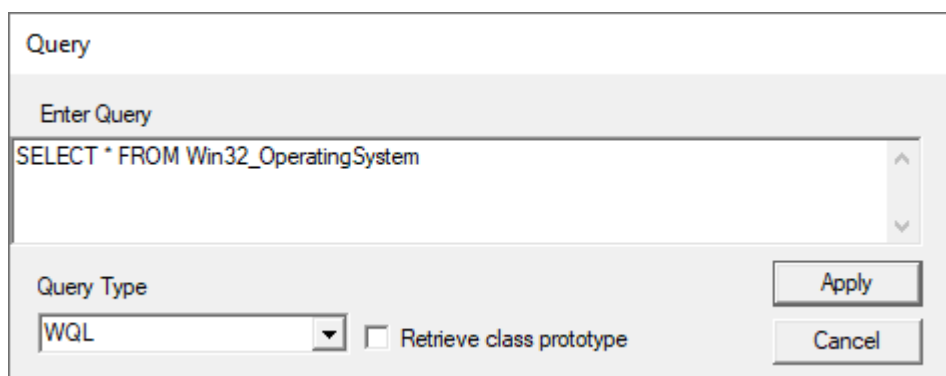
- In the namespace box enter `\\servername\root\cimv2`, where servername is the name of the server to connect to.



The 'Connect' dialog box is used to establish a connection to a WMI namespace. It contains the following fields and options:

- Namespace:** A text box containing the path `\\localhost\root\cimv2`.
- Buttons:** 'Connect' and 'Cancel' buttons are located to the right of the Namespace field.
- Connection:** A section containing:
 - Using:** A dropdown menu set to 'IWbemLocator (Namespaces)'.
 - Returning:** A dropdown menu set to 'IWbemServices'.
 - Completion:** A dropdown menu set to 'Synchronous'.
- Credentials:** A section with three text boxes for 'User:', 'Password:', and 'Authority:'.
- Locale:** A text box for specifying a locale.
- How to interpret empty password:** Two radio buttons: 'NULL' (selected) and 'Blank'.
- Impersonation level:** Three radio buttons: 'Identify', 'Impersonate' (selected), and 'Delegate'.
- Authentication level:** Six radio buttons: 'None', 'Packet' (selected), 'Connection', 'Packet integrity', 'Call', and 'Packet privacy'.

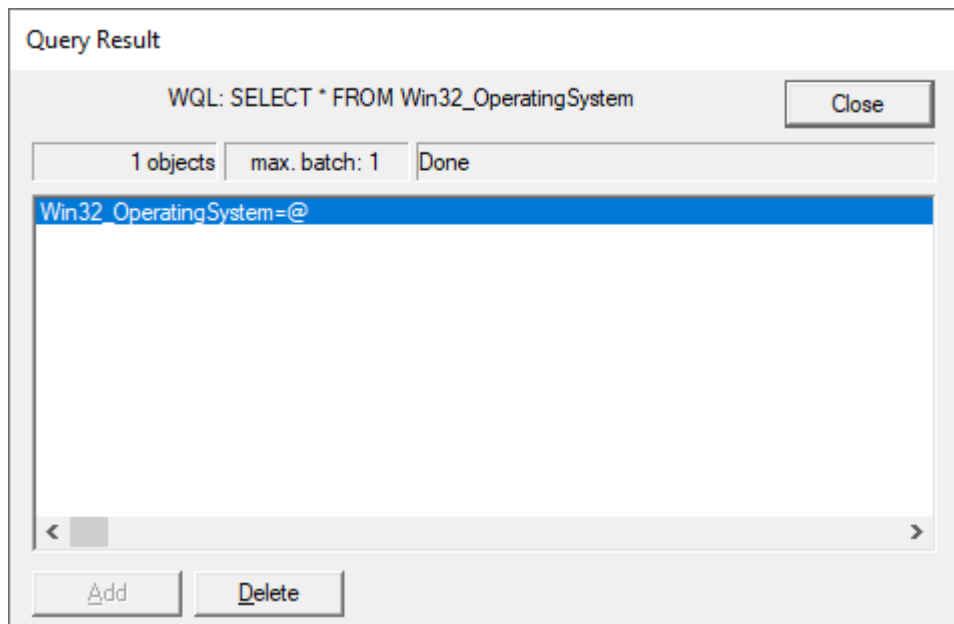
- Click connect.
- Click the query button.
- In the query field enter `SELECT * FROM Win32_OperatingSystem`.



The 'Query' dialog box is used to execute a WQL query. It contains the following fields and options:

- Enter Query:** A large text area containing the query `SELECT * FROM Win32_OperatingSystem`.
- Query Type:** A dropdown menu set to 'WQL'.
- Retrieve class prototype:** An unchecked checkbox.
- Buttons:** 'Apply' and 'Cancel' buttons are located at the bottom right.

- Click the apply button.
- A single result should be returned, otherwise an error message will be displayed.



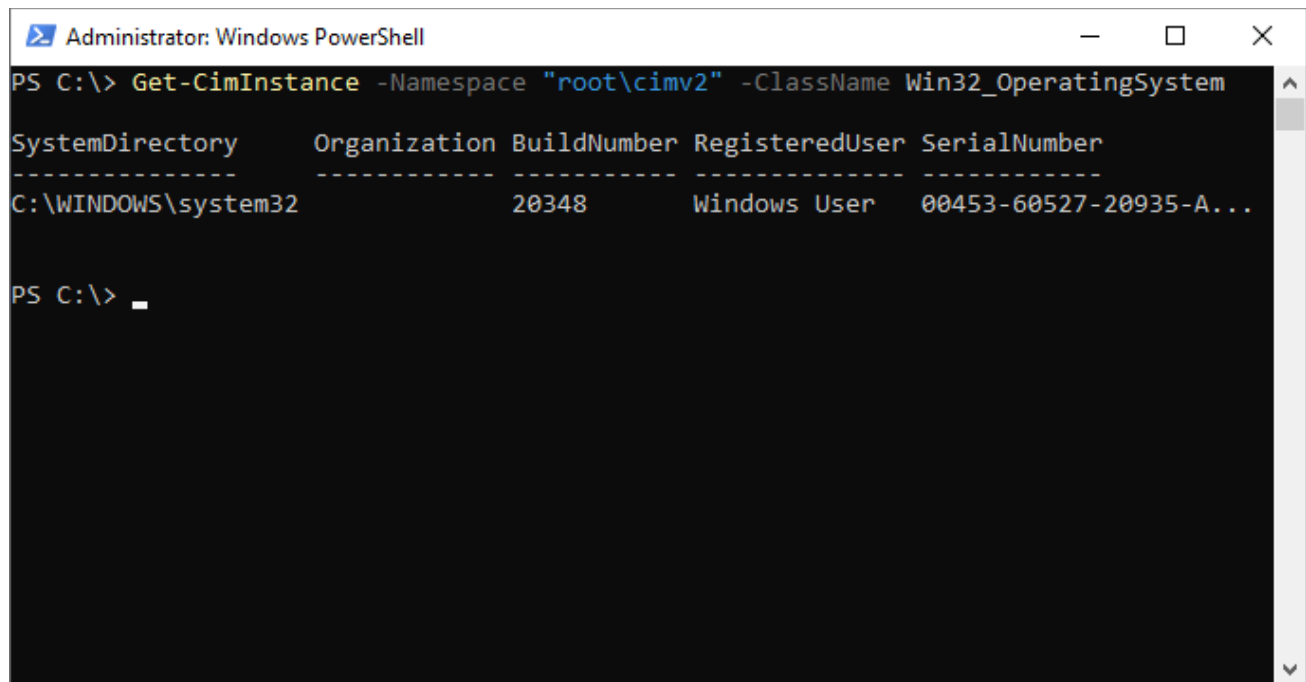
Test WMI with PowerShell

Windows PowerShell includes the ability to query WMI on the local and remote machines using the `Get-CimInstance` cmdlet.

Local Machine

Simply enter the command replacing the query as required.

`Get-CimInstance -Namespace "root\cimv2" -ClassName Win32_OperatingSystem`



```
Administrator: Windows PowerShell
PS C:\> Get-CimInstance -Namespace "root\cimv2" -ClassName Win32_OperatingSystem

SystemDirectory      Organization BuildNumber RegisteredUser SerialNumber
-----
C:\WINDOWS\system32      20348      Windows User  00453-60527-20935-A...
```

Remote Machine

Simply enter the required query and provide the ComputerName parameter.

`Get-CimInstance -Namespace "root\cimv2" -ClassName Win32_OperatingSystem -ComputerName computer name`

Troubleshooting

It is possible to see any errors within the PowerShell output.

```
Administrator: Windows PowerShell
PS C:\> Get-CimInstance -ComputerName "DEMO-SRV01" -Namespace "root\cimv2" -ClassName Win32_OperatingSystem
Get-CimInstance : WinRM cannot process the request. The following error occurred while using Kerberos authentication: Cannot find the computer DEMO-SRV01. Verify that the computer exists on the network and that the name provided is spelled correctly.
At line:1 char:1
+ Get-CimInstance -ComputerName "DEMO-SRV01" -Namespace "root\cimv2" -C ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (root\cimv2:Win32_OperatingSystem:String) [Get-CimInstance], CimException
+ FullyQualifiedErrorId : HRESULT 0x80070035,Microsoft.Management.Infrastructure.CimCmdlets.GetCimInstanceCommand
+ PSComputerName        : DEMO-SRV01
PS C:\>
```

Common Issues

This section highlights common issues.

Accessing the Administration Tools is slow in a disconnected environment

Issue

When accessing the [administration tools](#) in a disconnected environment where the computer running the [XIA Configuration Client](#) does not have internet access you may find that the [administration tools](#) user interface may be slow to load or respond.

Cause

The [administration tools](#) are digitally signed using a DigiCert certificate and this issue is seen when the computer running [XIA Configuration Client](#) cannot check the certificate revocation list (CRL) for the digital certificate.

Resolution 1 (Recommended)

Ensure that the computer running the [XIA Configuration Client](#) has internet access.

Resolution 2

NOTE: The following steps are for reference only. Please review the following Microsoft documentation and ensure you understand the risks and issues associated with changes to the security settings on Windows.

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn265983\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn265983(v=ws.11))

- On a computer with internet access create a directory for example C:\CTL
- In a command prompt run the following command.
certutil -syncWithWU C:\CTL
- Download the DigiCert certificate revocation list (CRL) files to the CTL directory.
<http://crl3.digicert.com/sha2-assured-cs-g1.crl>
<http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl>
- Once the certificates are downloaded copy the C:\CTL directory to the computer in the disconnected environment.
- On the computer in the disconnected environment open regedit and set the following registry key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
RootDirURL (REG_SZ)
C:\CTL
- Install the DigiCert certificate revocation list (CRL) files by either

Right click the CRL files and select *Install CRL*

- or -

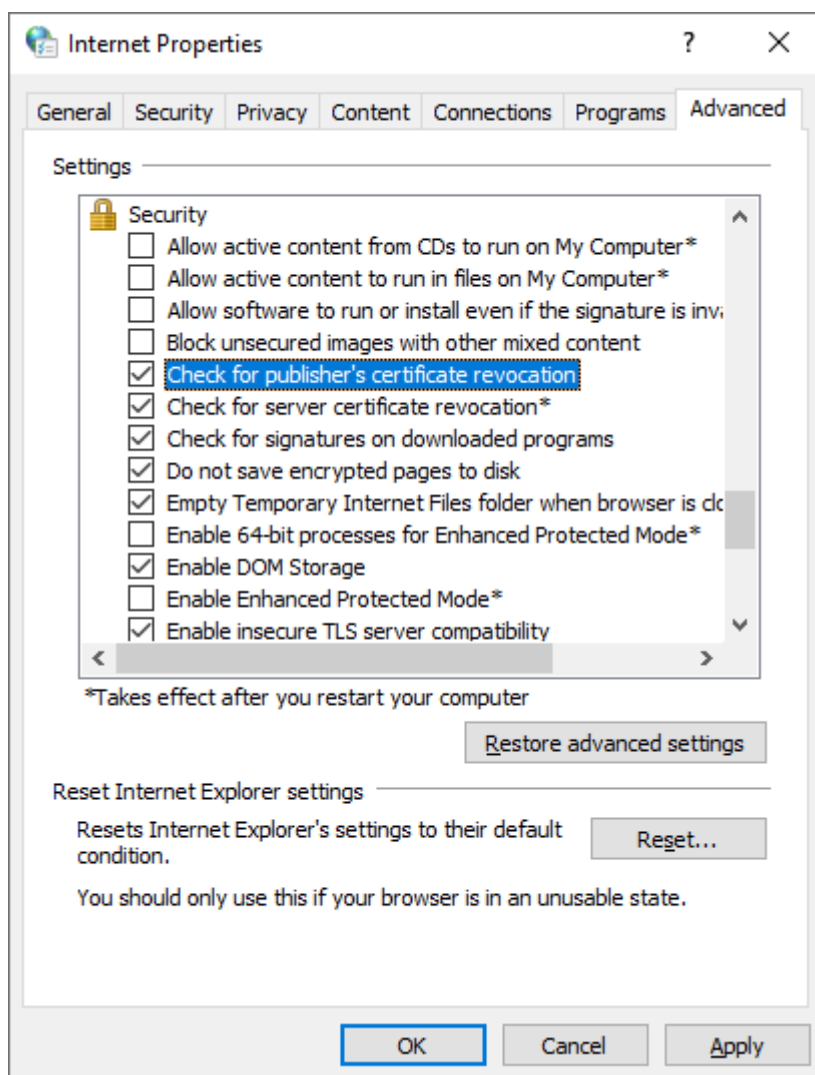
```
certutil -addstore CA C:\CTL\sha2-assured-cs-g1.crl
certutil -addstore ROOT C:\CTL\sha2-assured-cs-g1.crl
certutil -addstore CA C:\CTL\DigiCertAssuredIDRootCA.crl
certutil -addstore ROOT C:\CTL\DigiCertAssuredIDRootCA.crl
```

NOTE: The trusted and untrusted CTLs can be updated on a daily basis, so ensure that you keep the files synchronized by using a scheduled task or another method.

Resolution 3

NOTE: This resolution is not recommended as this reduces security.

- Go to Control Panel > Internet Options.
- On the Advanced tab uncheck the *Check for publisher's certificate revocation* checkbox.
- Click OK



Client certificates not available

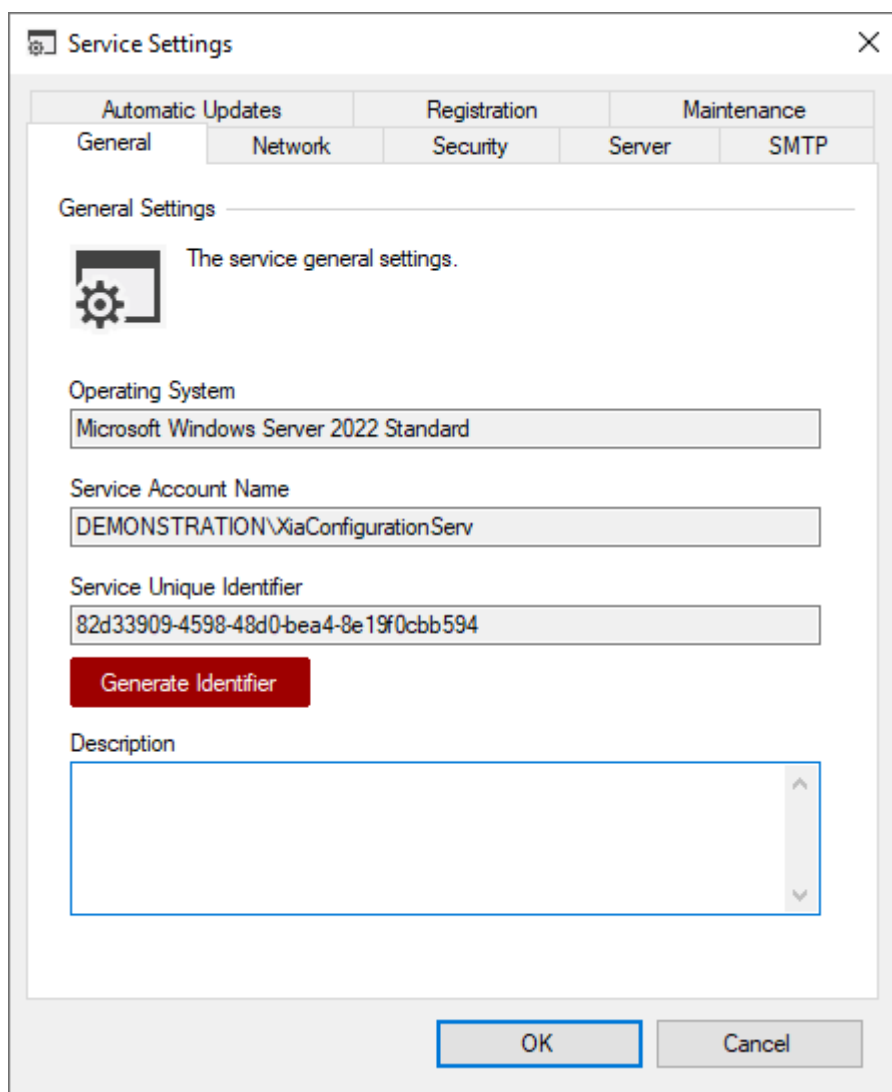
Symptoms

When trying to select a certificate in the [administration tools](#) you find that the expected certificate is not available in the drop down list.

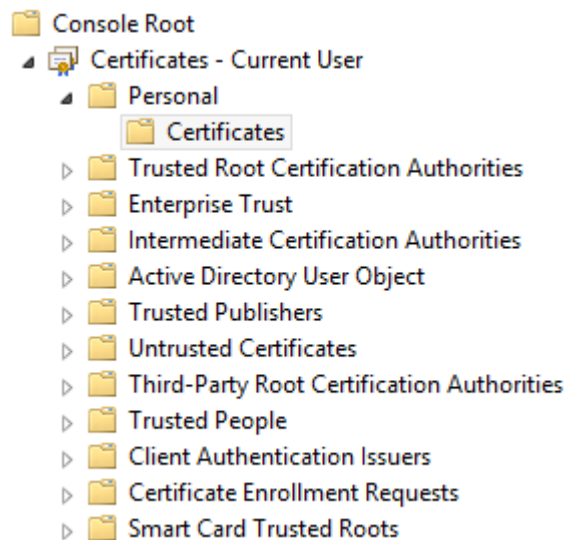
Cause

The certificate may not be available for one of the following reasons.

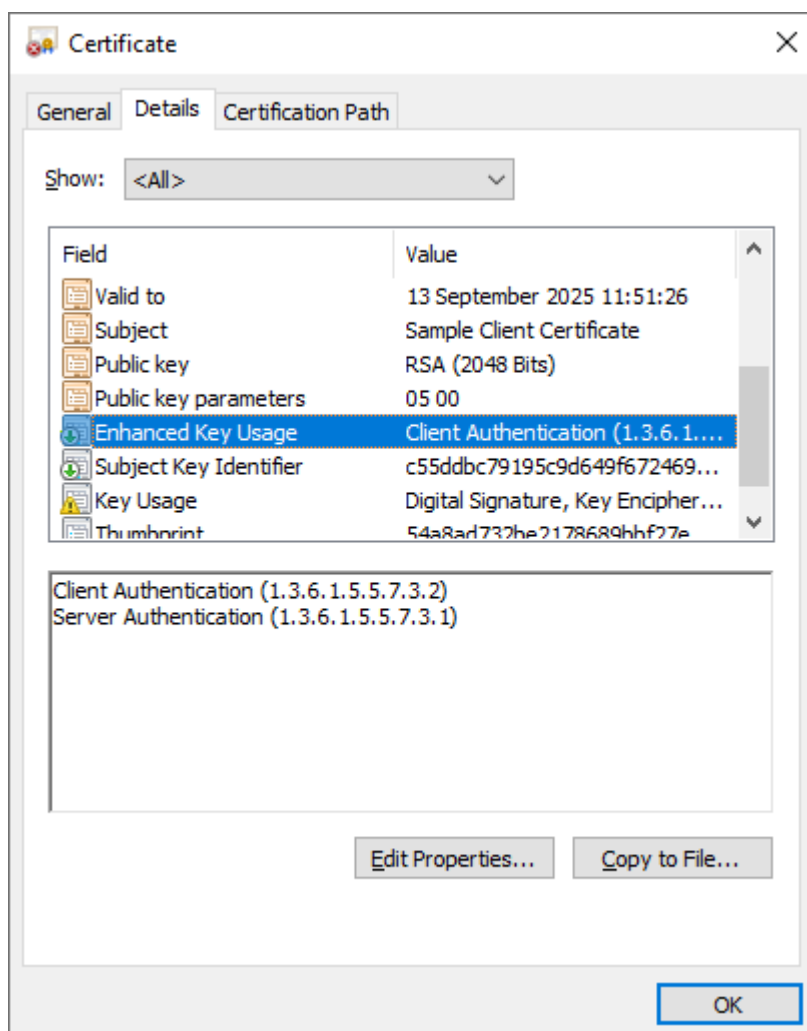
- The certificate is not installed in the certificate store for the [service account](#) running the [XIA Configuration Client](#) service.



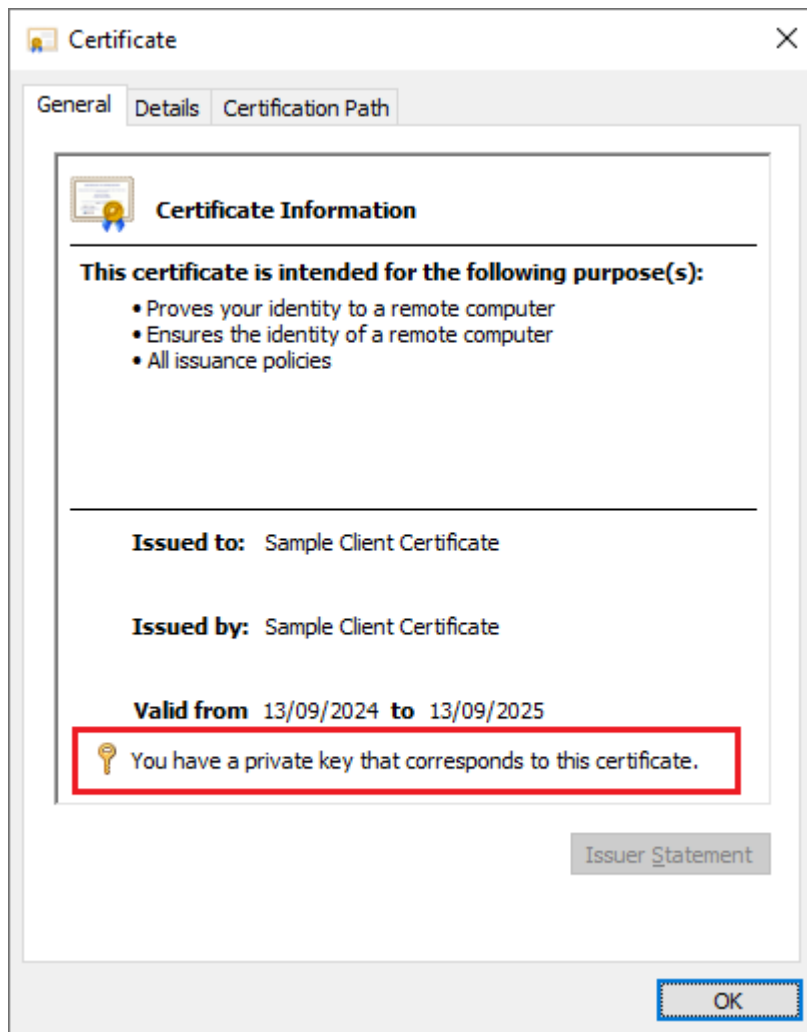
- The certificate is not installed in the **Personal** store.



- The certificate does not support the **Client Authentication (1.3.6.1.5.5.7.3.2)** enhanced key usage.



- The certificate does not have the corresponding private key.



Resolution

- Ensure that the certificate meets all of the requirements above.
- or -
- Use the [Microsoft service principal creation tool](#) to create a new certificate.

Error Outputting to Disk

Symptoms

When scanning any item type and the client is configured to write data to the disk you receive an error "Error outputting to disk - could not find part of the path *Pathname.xml*"

Cause

The configuration client deletes the data directory found within the XIA Configuration Service installation directory when a scan is started. If the folder is open in Windows Explorer when the scan is started the folder cannot be correctly deleted and recreated.

Resolution

- When starting a scan, ensure that the Data folder is not open in Windows Explorer.
- Alternatively, you can disable the output to disk on the Scan Profile settings if output to disk is not required.

Failed to connect to an IPC Port: Access is denied

Symptoms

When [connecting](#) to the [XIA Configuration Client](#) service you receive the error Failed to connect to an IPC Port: Access is denied.

Cause

The user connecting to the [XIA Configuration Client](#) service is not a member of the IPC Authorized Users group specified in the [security settings](#).

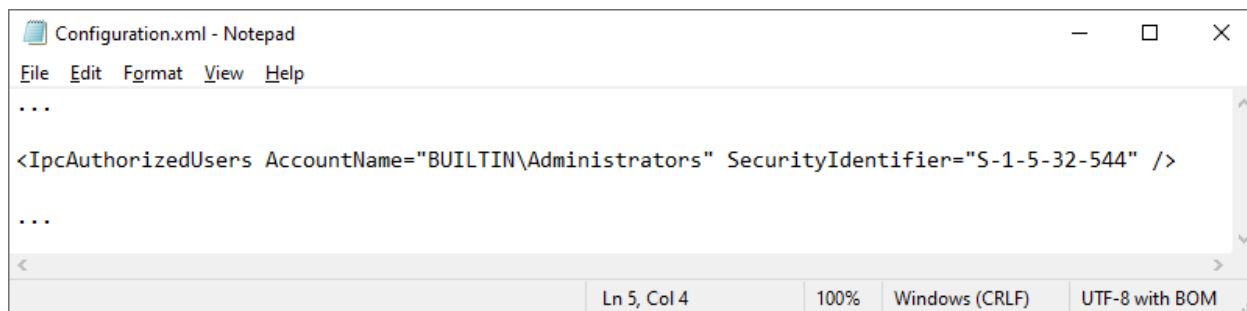
Resolution

Log on as a user who is a member of the IPC Authorized Users group

- or -

If the group is unknown or has an issue you can correct it manually

- Make a backup copy of the client configuration file, which is by default found in the following location
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Configuration\Configuration.xml
- Open the Configuration.xml file in a text editor.
- Modify the **IpcAuthorizedUsers** property.



- Restart the XIA Configuration Service.

Hexadecimal value {value}, is an invalid character

Issue

When uploading data to the XIA Configuration Server, or saving data to XML you see the following error. The hexadecimal value seen may vary.

There was an error generating the XML document. ---> System.ArgumentException: '-', hexadecimal value 0x1F, is an invalid character.

Cause

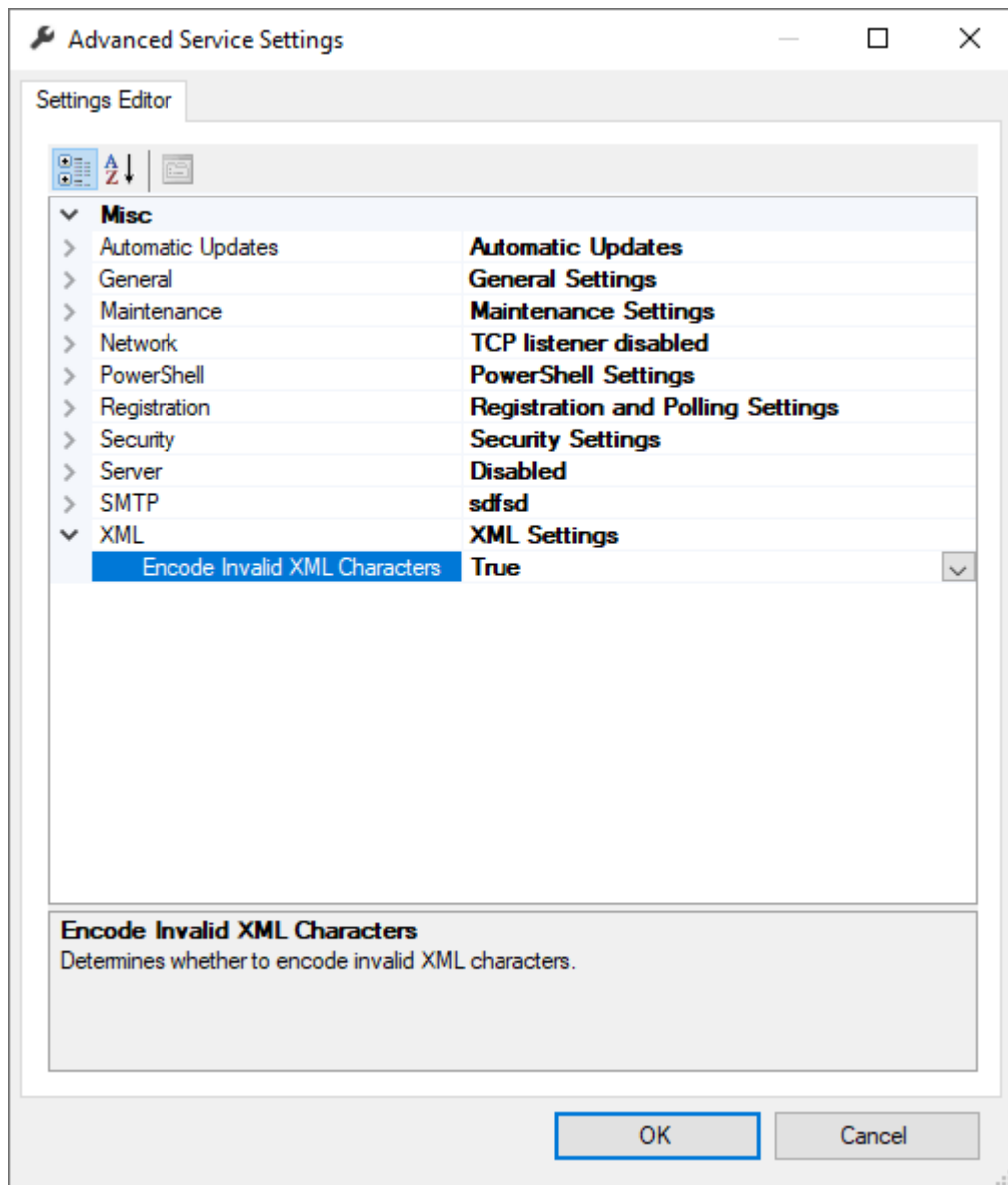
This error can be caused when one of the [scan tasks](#) is reading data from the [target item](#) that contains characters that are invalid in the destination XML document.

Resolution

To resolve the issue please log a support call.

The following method can be used to help diagnose where the invalid characters are found.

- Log-on to the machine running the [XIA Configuration Client](#) as an administrator.
- Click *Tools > Advanced > Advanced Service Settings* to open the [service advanced settings editor](#).
- Set the XML > *Encode invalid XML characters* setting to *True*.



- Click the *OK* button.
- Click the *Save Configuration* button.
- Create a new [scan profile](#), and modify its properties
 - Ensure the *Inherit service settings* and *Connect to server* settings are **unchecked** on the [server upload](#) tab.
 - Ensure the *Save to filesystem* setting is **checked** on the [file output](#) tab.
 - Ensure the *RSA sign document* setting is **unchecked** on the [file output](#) tab.
- Create a [scan task](#) that matches the [task](#) that is failing.
- Start a scan of [scan profile](#).
- When the scan is complete the data file created can be found in the following directory by

default

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service\Data

- The invalid data can be seen in the data file as encoded XML, for example
<Name>DEMO-SRV01</Name>
- Provide the data file as part of the support call.
- Open the [Service Advanced Settings Editor](#), and set the XML > *Encode invalid XML characters* setting to *False*.
- Click the *OK* button.
- Delete the [scan profile](#) you created in the previous steps.
- Click the *Save Configuration* button.

Operation Aborted by User

Symptoms

When viewing the scan results, the agent reports "Operation Aborted By User"

Cause

This is caused by the user clicking the "Abort" action point within the [Scan Monitor](#). The behaviour is by design.

Resolution

No resolution required.

Temporary files are created during a scan on the target machine

Symptoms

When performing a scan temporary files with a .tmp extension are created and subsequently deleted on the target machine.

Cause

Some of the [scan tasks](#) use custom code that is generated with the [Add-Type](#) PowerShell cmdlet on the target machine.

The [Add-Type](#) cmdlet creates temporary files using the csc.exe compiler as part of this process. The files are automatically deleted when the process is complete.

Resolution

This behavior is by design.

"There was an error starting the Secondary Logon service" when using custom credentials

Issue

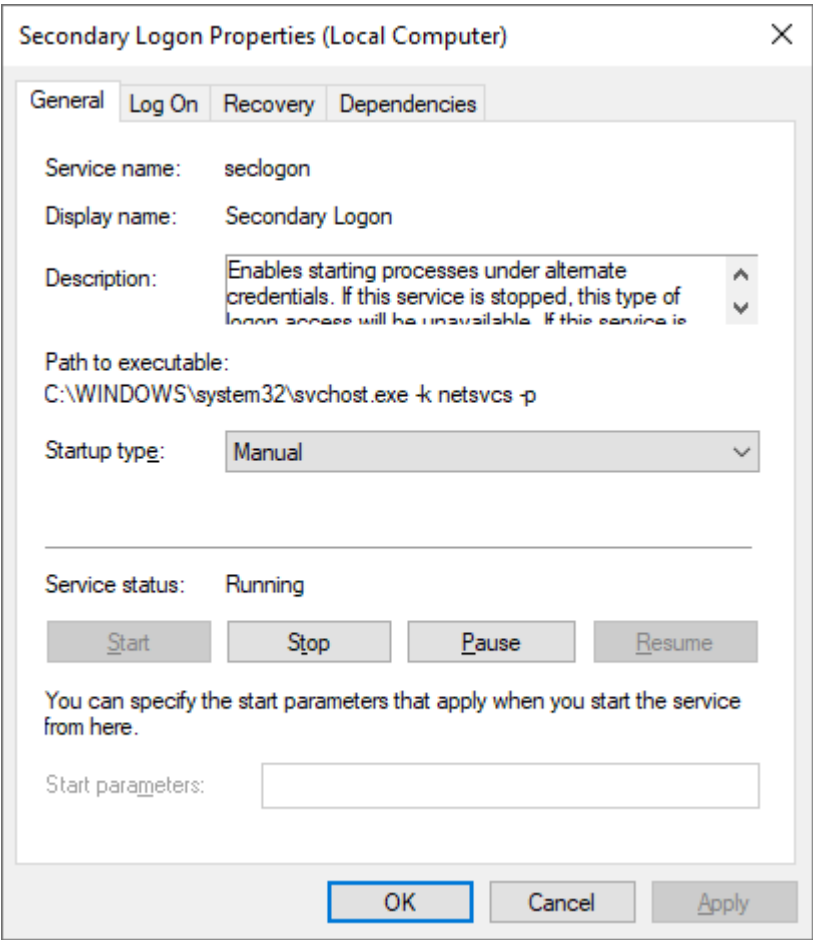
When performing a scan using custom credentials the following error is seen
"There was an error starting the Secondary Logon service, please ensure that this service is not disabled."

Cause

This error can be seen if the "Secondary Logon" (seclogon) service is disabled.

Resolution

Ensure that the "Secondary Logon" service is not disabled.



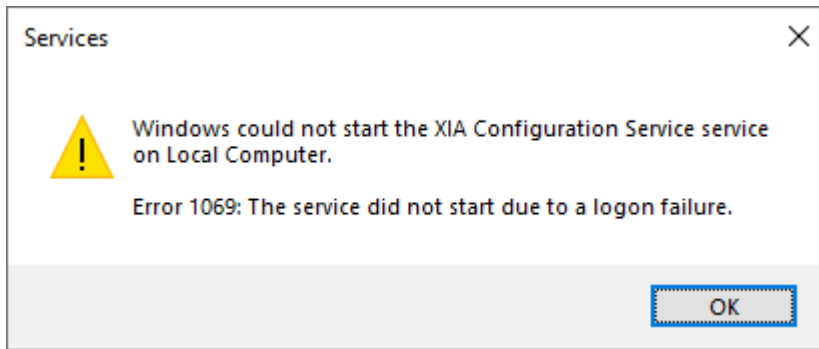
Windows could not start the XIA Configuration Service (Logon Failure)

Symptoms

When attempting to start the [XIA Configuration Client](#) service (XIAConfigurationSvc) you see the following error.

Windows could not start the XIA Configuration Service service on Local Computer.

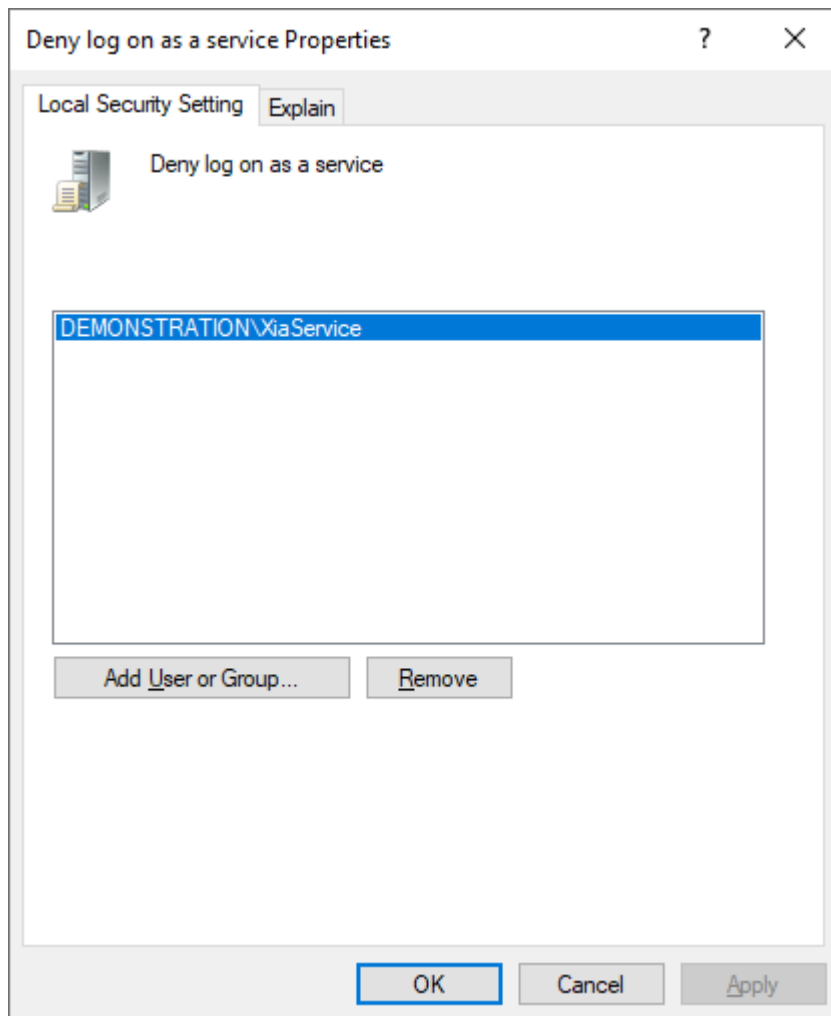
Error 1069: The service did not start due to a logon failure.



Issue

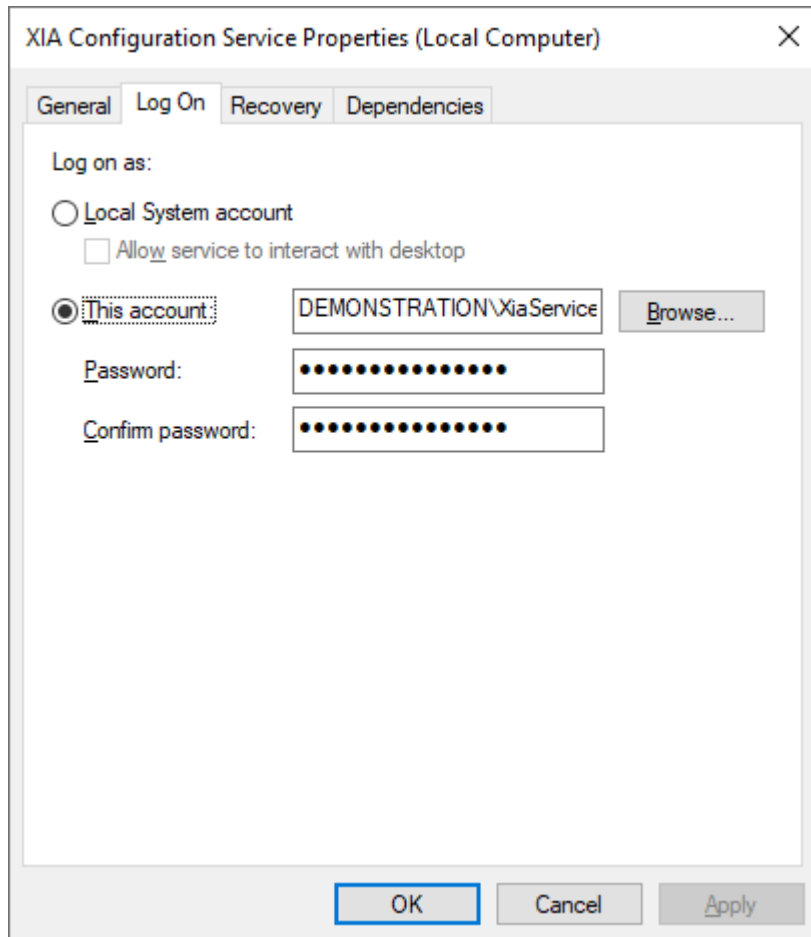
There are several possible causes of this issue

- The password for the [service account](#) has expired.
- The account is disabled.
- The account is locked out.
- The [service account](#) has not been assigned the [Log on as a service](#) right.
- The [service account](#) has been assigned the [Deny log on as a service](#) right.



Resolution

- Open *Windows Event Viewer* and check for any log on related errors.
- [Change the service account password](#) if it has expired.



- Ensure the account is not disabled.
- Unlock the account.
- Ensure that the [service account](#) has been assigned the [Log on as a service right](#). This is automatically granted by the [installation](#), however can be overridden by the Group Policy configuration within your organization.
- Ensure that the [service account](#) has not been assigned the [Deny log on as a service right](#).

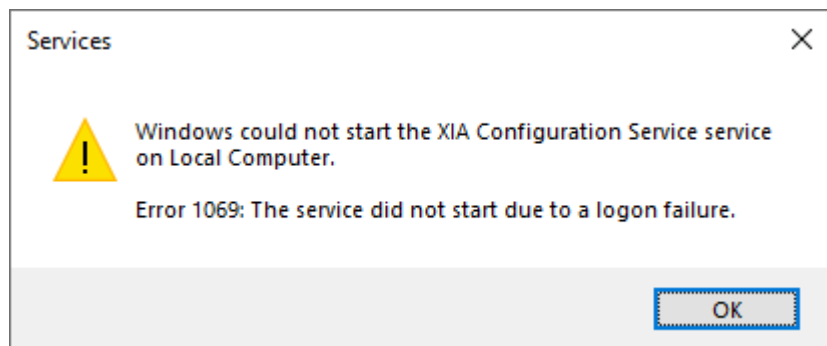
Windows could not start the XIA Configuration Service (Access Denied)

Symptoms

When attempting to start the [XIA Configuration Client](#) service (XIAConfigurationSvc) you see the following error.

Windows could not start the XIA Configuration Service service on Local Computer.

Error 5: Access is denied



Issue

This error can occur if the [service account](#) does not have access to the [XIA Configuration Client](#) installation directory.

Resolution

Review the NTFS permissions of the [XIA Configuration Client](#) installation directory - by default this is the following directory:

C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Service

Ensure that the [service account](#) has the appropriate permissions.

More Information

If the service account has been manually changed, ensure that you have followed the instructions for [changing the service account](#). This provides information for changing the NTFS permissions for the service account.

You do not have permission to perform this command

Issue

When you attempt to start a [scan profile](#) using [custom credentials](#) the following error is seen where profile name is the name of the [scan profile](#) being run.

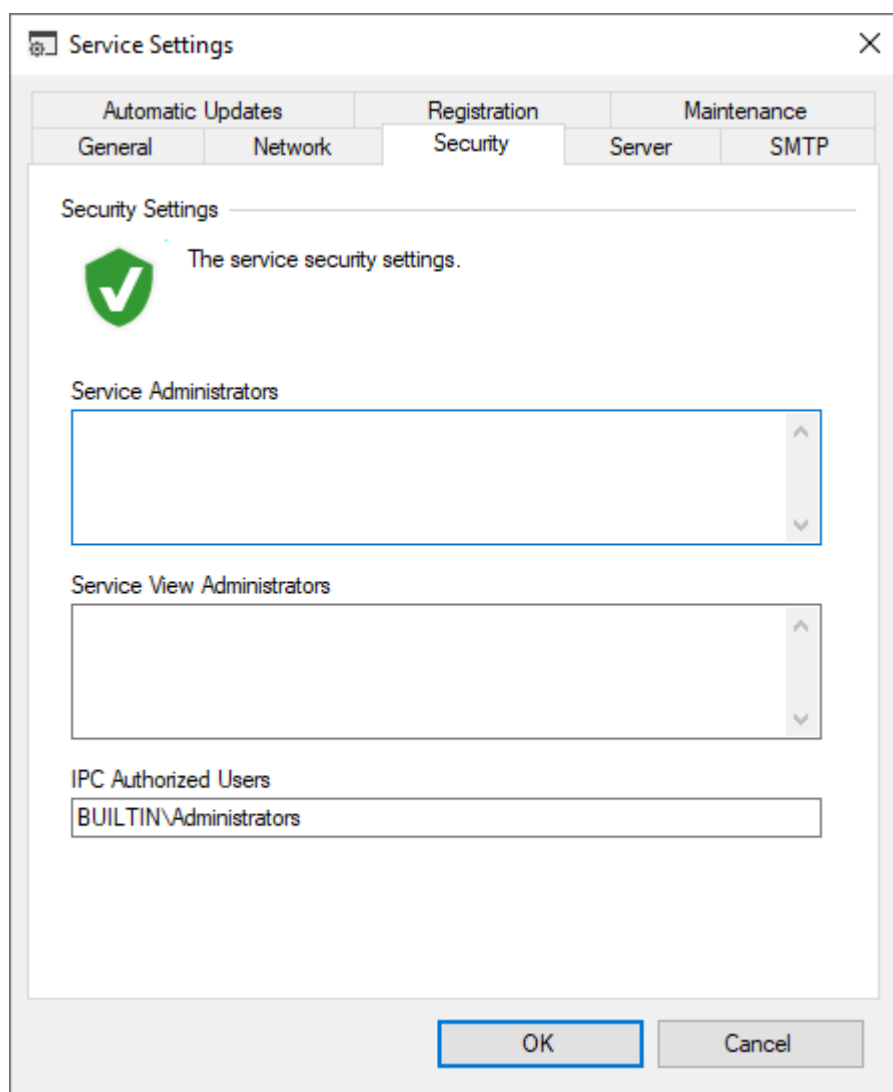
"Could not start the scan profile 'profile name'. You do not have permission to perform this command."

Cause

This error can be seen if the [service account](#) does not have permissions to start a scan profile.

Resolution

By default the [service account](#) is made a local administrator, however if the account does not have these permissions it must be manually given service administrator or service view administrator rights in the [security](#) settings.



More Information

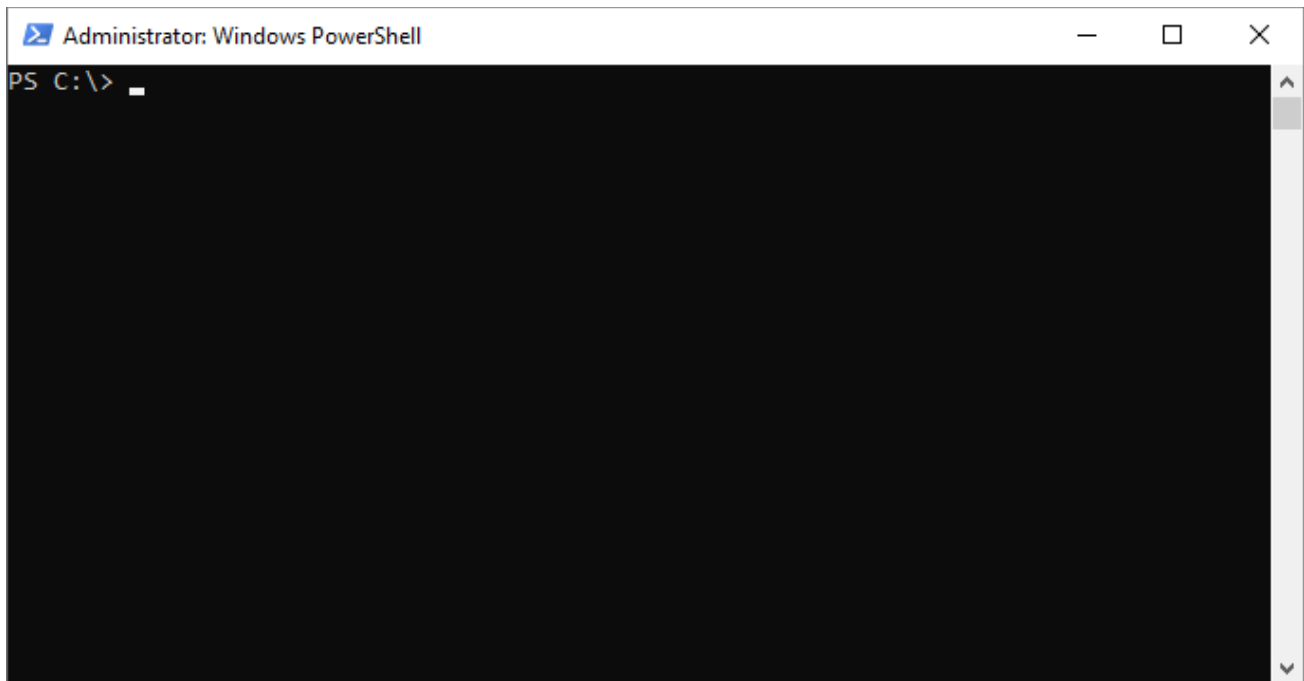
This is an added level of security in place to the scan host that is used when running [scan profiles](#) with [custom credentials](#).

PowerShell Remoting

Windows [PowerShell remoting](#) allows PowerShell [cmdlets](#) to be run on remote machines.

The WS-Management protocol and [Windows Remote Management \(WinRM\)](#) provide the technology that underpins [PowerShell remoting](#).

This section provides details on the support and troubleshooting of PowerShell remoting including how to [enable PowerShell Remoting](#), and resolve [access is denied](#) errors.



Access is denied

Symptoms

When using an agent that uses [PowerShell remoting](#) you see the following error

"Connecting to remote server failed with the following error message: Access is denied. For more information, see the [about_Remote_Troubleshooting Help](#) topic."

Cause

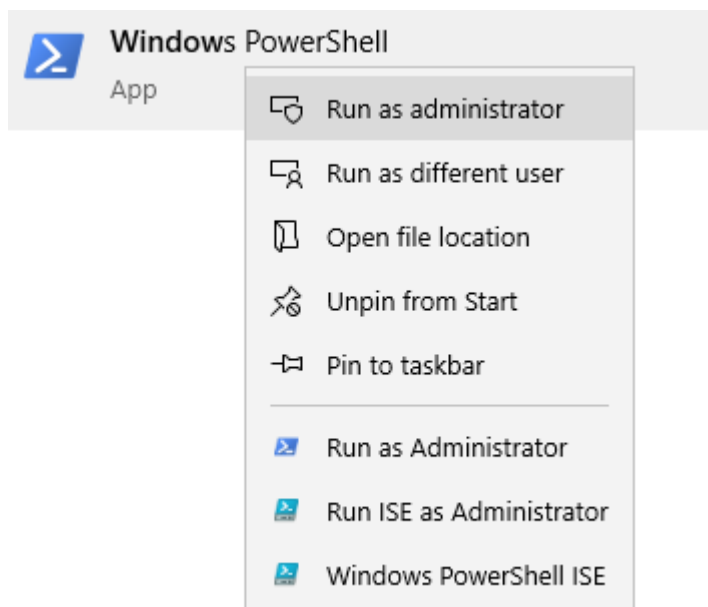
The [XIA Configuration Client](#) service account (or the [custom credentials](#) in use) do not have permissions to create a PowerShell remoting session to the remote machine.

Resolution

- Use a user account that has permissions to connect to [PowerShell remoting](#).

or

- Open a PowerShell console as Administrator



- Execute the following command to display the PowerShell security descriptor
`Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell`
- Modify the permissions as required.

Permissions for http://schemas.microsoft.com/powershell/Microsoft.PowerShell

http://schemas.microsoft.com/powershell/Microsoft.PowerShell

Group or user names:

- Administrators (DEMONSTRATION\Administrators)
- Remote Management Users (DEMONSTRATION\Remote ...)
- INTERACTIVE

Add... Remove

Permissions for Administrators	Allow	Deny
Full Control(All Operations)	☒	☐
Read(Get,Enumerate,Subscribe)	☐	☐
Write(Put,Delete,Create)	☐	☐
Execute(Invoke)	☐	☐
Special permissions	☐	☐

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply

Enable PowerShell Remoting

Certain agents require that the [PowerShell remoting](#) is enabled. This allows PowerShell commands to be executed on the remote machines where this command is executed.

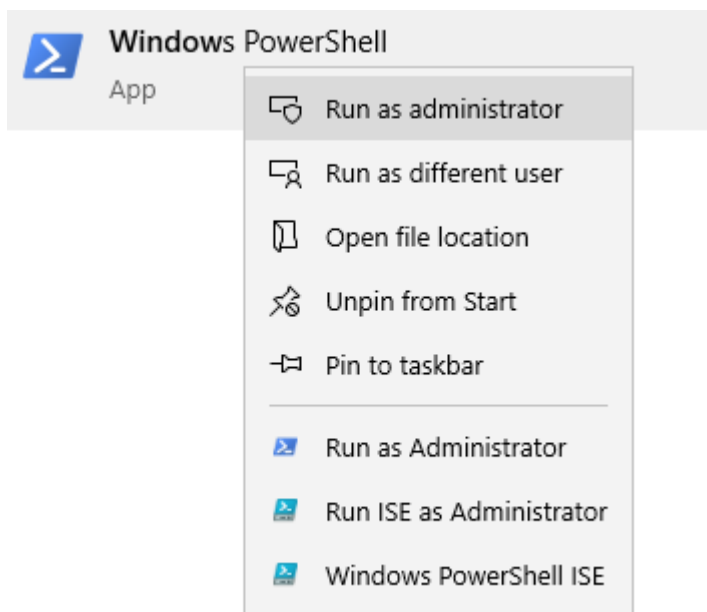
- Start PowerShell as an Administrator
- Run the [Enable-PSRemoting](#) cmdlet
- You may be prompted to confirm the change to the machine.

Error "...only if the target machine is part of the TrustedHosts list"

When using an agent that requires [PowerShell Remoting](#) and you are using [custom credentials](#) you may see the following error message

The *agent name* agent encountered an exception when 'Connecting using negotiate authentication'. Connecting to remote server failed with the following error message: The WinRM client cannot process the request. Default credentials with Negotiate over HTTP can be used only if the target machine is part of the TrustedHosts list or the Allow implicit credentials for Negotiate option is specified.

To enable the computer running the [XIA Configuration Client](#) to **trust** the remote machine, on the computer running the [XIA Configuration Client](#) open PowerShell as an **Administrator**



- Enter the following command to determine the current TrustedHosts value *
`Get-Item WSMan:\localhost\Client\TrustedHosts`
- If there is an existing value you can add a new value by entering the following command where **<ServerMachineName>** is the name of the remote server and **<OldValue>** is the current value.
`Set-Item WSMan:\localhost\Client\TrustedHosts -Value "<ServerMachineName>, <OldValue>" -Force`
- Enter the following command where **<ServerMachineName>** is the name of the remote server
`Set-Item WSMan:\localhost\Client\TrustedHosts -Value <ServerMachineName> -Force`
- To trust **any** machine, use the following command:
`Set-Item WSMan:\localhost\Client\TrustedHosts -Value * -Force`

* **NOTE:** If you do not run the PowerShell prompt as an administrator you may see the following error

Get-Item : Cannot find path 'WSMan:\localhost\Client' because it does not exist.

Install-Package : No match was found for the specified search criteria

Issue

When attempting to install a module using [Windows PowerShell](#) using the [Install-Module](#) cmdlet as an Administrator you see the error

PackageManagement\Install-Package : No match was found for the specified search criteria and module name 'module name'.

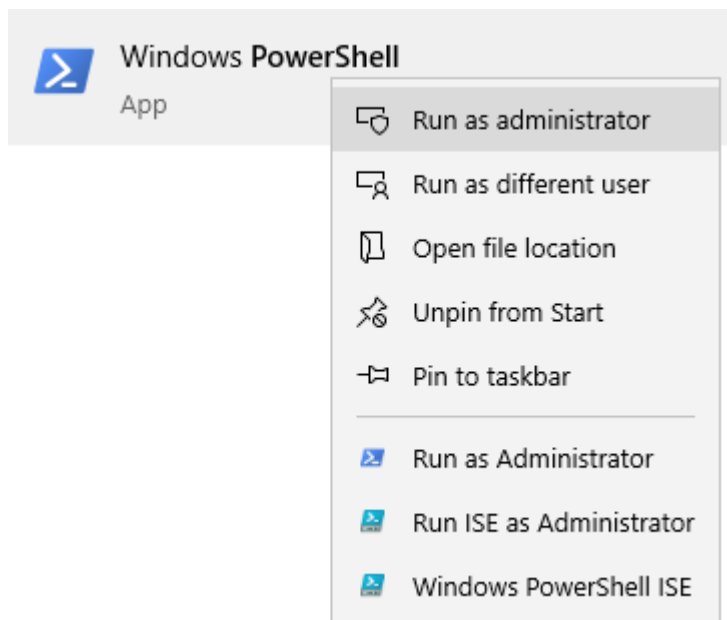
Try Get-PSRepository to see all available registered module repositories.

Cause

This error can be seen if the default PSGallery PowerShell repository is not correctly registered.

Resolution

- Start [Windows PowerShell](#) as an Administrator



- Restore the default repository by executing the [Register-PSRepository](#) cmdlet.
Register-PSRepository -Default
- Ensure the default repository is installed with the [Get-PSRepository](#) cmdlet.
Get-PSRepository

More Information

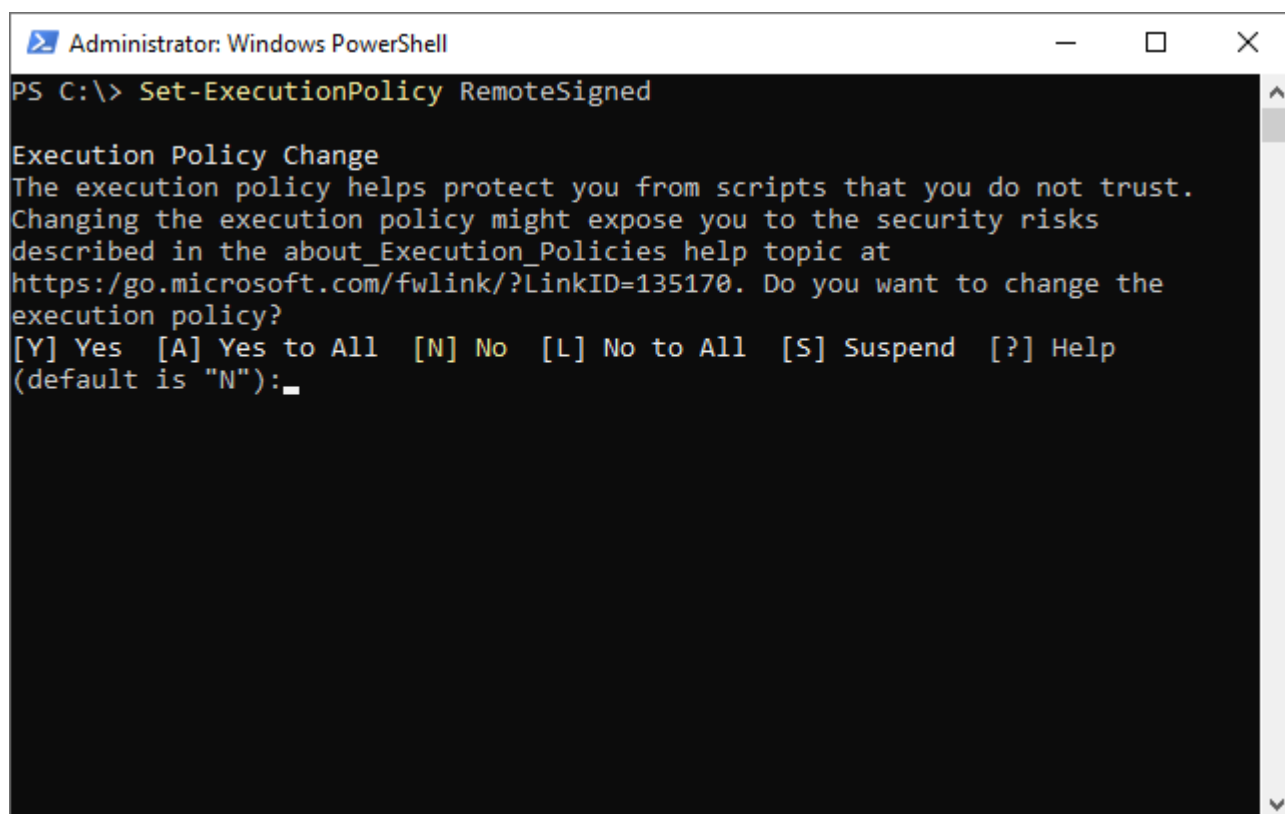
If the repository is not restored ensure the system is configured to use TLS version 12.
For more information see the [Unable to download the list of available providers](#) section.

Set Execution Policy to RemoteSigned

Certain agents require that the PowerShell execution policy be set to **RemoteSigned** or above.

This allows PowerShell scripts to be executed however they must be signed by a trusted publisher.

- Start PowerShell as an Administrator
- Run the [Set-ExecutionPolicy](#) cmdlet with the parameter RemoteSigned
Set-ExecutionPolicy RemoteSigned
- You may be prompted to confirm the change of policy.



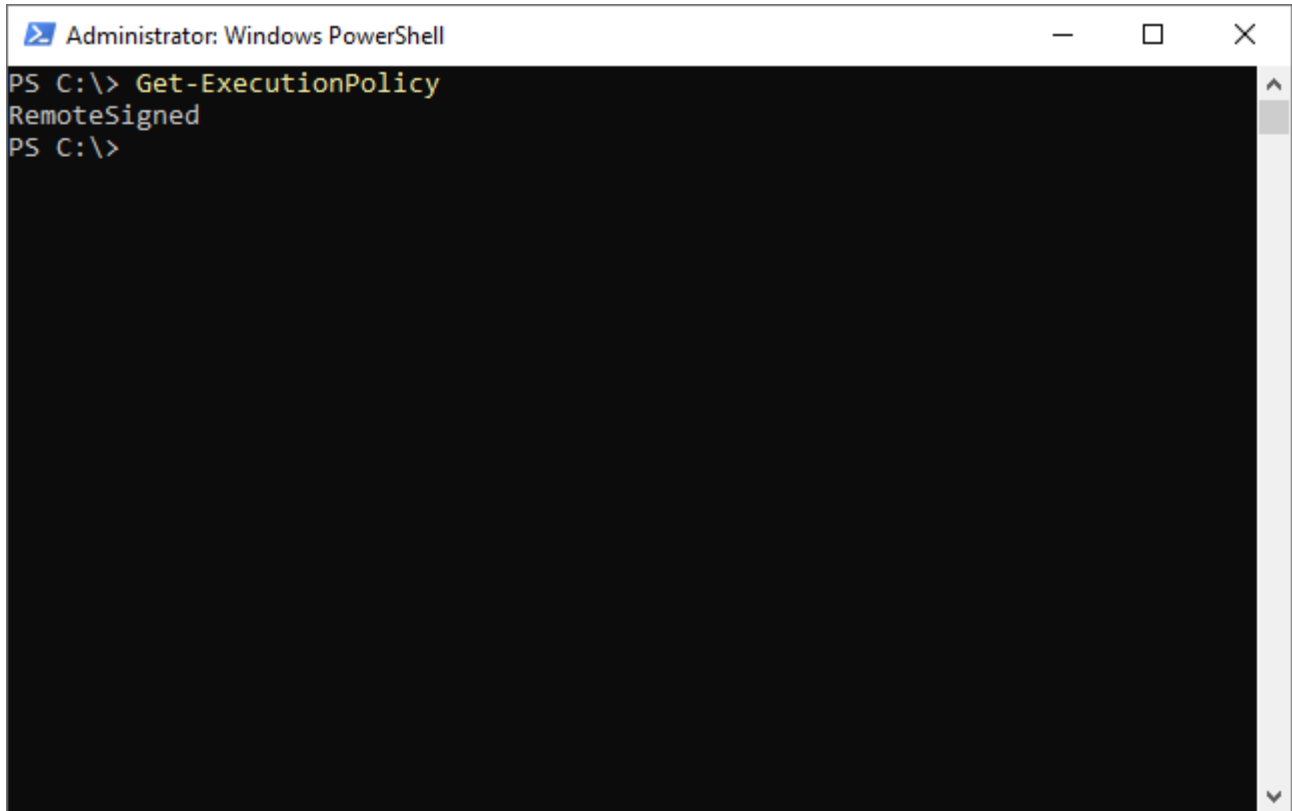
```
Administrator: Windows PowerShell
PS C:\> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks
described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "N"):_
```

Checking Current Policy

To determine the current execution policy

- Start PowerShell as an Administrator
- Run the [Get-ExecutionPolicy](#) cmdlet



```
Administrator: Windows PowerShell
PS C:\> Get-ExecutionPolicy
RemoteSigned
PS C:\>
```

The authentication mechanism requested by the client is not supported

Issue

When scanning using an [agent](#) that uses [PowerShell remoting](#) you may see the following error

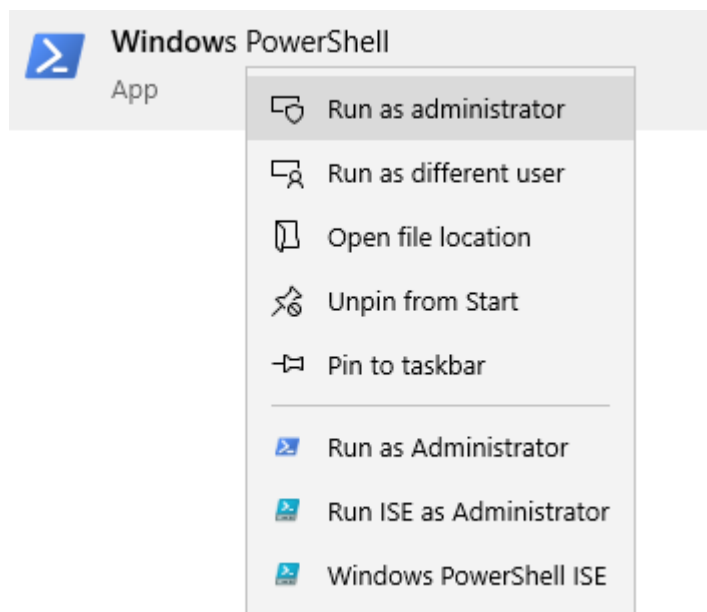
The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server.

Cause

This error can be seen when Kerberos (or Negotiate when using [custom credentials](#)) authentication is disabled in the WinRM configuration on the machine being scanned.

Resolution

Confirm that the appropriate authentication setting is enabled by executing the following command as an Administrator



```
winrm get winrm/config/service
```

A screenshot of a Windows PowerShell terminal window titled 'Administrator: Windows PowerShell'. The terminal shows the command `winrm get winrm/config/service` being executed. The output displays the configuration for the WinRM service, including the RootSDDL, various operation limits, authentication settings, and default ports.

```
PS C:\> winrm get winrm/config/service
Service
  RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXG
W;;;WD)
  MaxConcurrentOperations = 4294967295
  MaxConcurrentOperationsPerUser = 1500
  EnumerationTimeoutms = 240000
  MaxConnections = 300
  MaxPacketRetrievalTimeSeconds = 120
  AllowUnencrypted = false
  Auth
    Basic = false
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
  DefaultPorts
    HTTP = 5985
    HTTPS = 5986
  IPv4Filter = *
  IPv6Filter = *
  EnableCompatibilityHttpListener = false
```

The client cannot connect to the destination specified in the request.

Symptoms

When using an agent that uses [PowerShell remoting](#) you see the following error

Connecting to remote server `machine name` failed with the following error message : The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig". For more information, see the [about_Remote_Troubleshooting Help](#) topic.

Cause

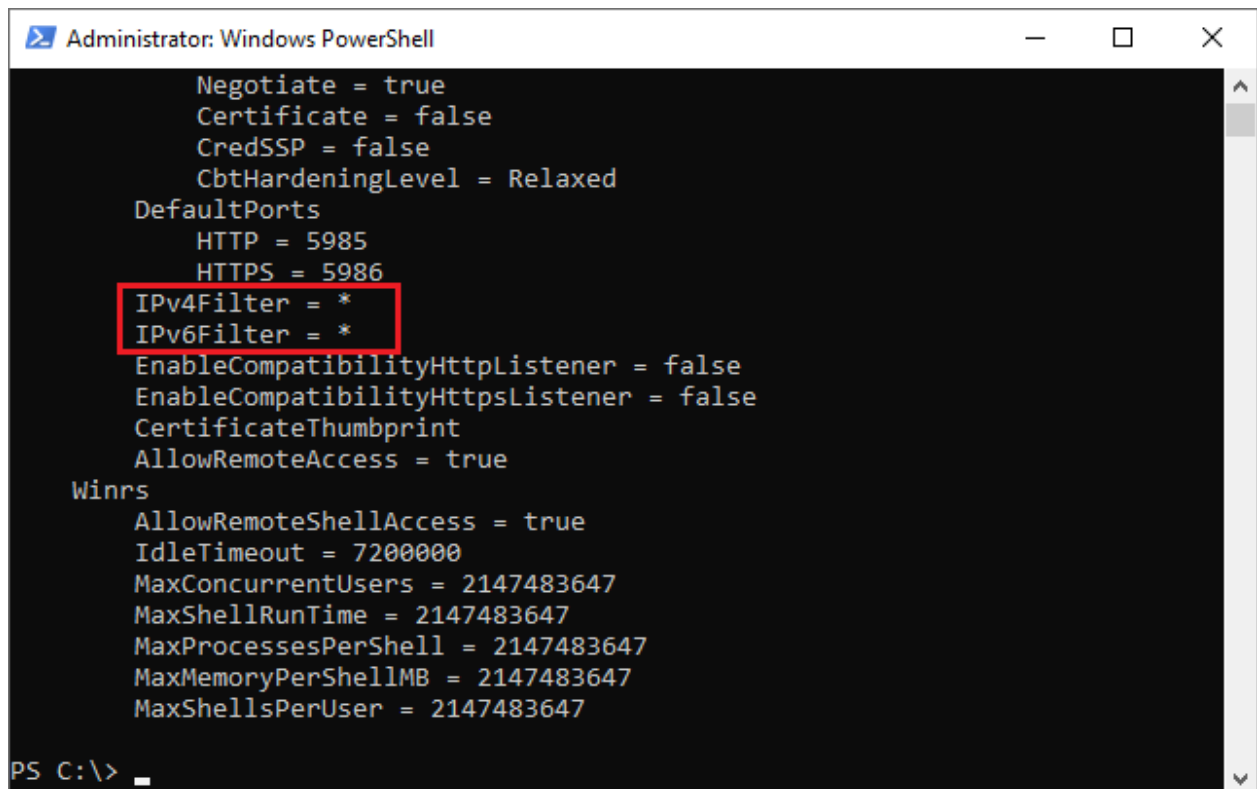
This issue can be caused by several issues.

- [PowerShell remoting](#) is not enabled on the remote machine.
- The Windows Remote Management (WS-Management) service is stopped.
- Firewalls are blocking the connection.
- IP filtering is configured to block the IP address of the machine running the [XIA Configuration Client](#).
- The IP listen list is configured to not listen for HTTP requests on the specified IP address.

Resolutions

- [Enable PowerShell remoting](#).
- Ensure that the Windows Remote Management (WS-Management) service is started.
- Ensure that firewalls allow the PowerShell remoting connection.
- Run a command prompt as Administrator and enter the following command and confirm whether the **IPv4Filter** or **IPv6Filter** is configured to block the IP of the machine running the [XIA Configuration Client](#).

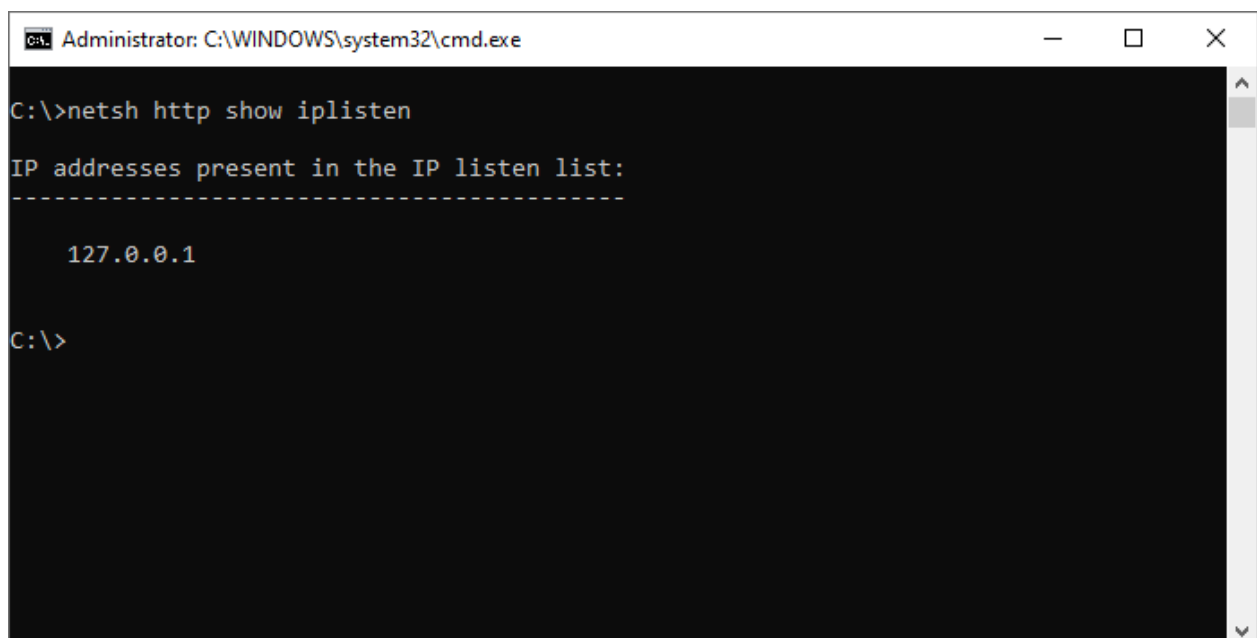
```
winrm get winrm/config
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a black background with white text. It displays the configuration for the netsh http service. The configuration includes: Negotiate = true, Certificate = false, CredSSP = false, CbtHardeningLevel = Relaxed, DefaultPorts: HTTP = 5985, HTTPS = 5986, IPv4Filter = *, IPv6Filter = * (these two lines are highlighted with a red rectangle), EnableCompatibilityHttpListener = false, EnableCompatibilityHttpsListener = false, CertificateThumbprint, AllowRemoteAccess = true, and a Winrs section with: AllowRemoteShellAccess = true, IdleTimeout = 7200000, MaxConcurrentUsers = 2147483647, MaxShellRunTime = 2147483647, MaxProcessesPerShell = 2147483647, MaxMemoryPerShellMB = 2147483647, and MaxShellsPerUser = 2147483647. The prompt "PS C:\>" is visible at the bottom left.

```
Negotiate = true
Certificate = false
CredSSP = false
CbtHardeningLevel = Relaxed
DefaultPorts
  HTTP = 5985
  HTTPS = 5986
  IPv4Filter = *
  IPv6Filter = *
EnableCompatibilityHttpListener = false
EnableCompatibilityHttpsListener = false
CertificateThumbprint
AllowRemoteAccess = true
Winrs
  AllowRemoteShellAccess = true
  IdleTimeout = 7200000
  MaxConcurrentUsers = 2147483647
  MaxShellRunTime = 2147483647
  MaxProcessesPerShell = 2147483647
  MaxMemoryPerShellMB = 2147483647
  MaxShellsPerUser = 2147483647
PS C:\>
```

- Check the IP listen list with the following [netsh http](#) command - the command should either return no results (in which case HTTP will listen on all IP addresses), or all required IP addresses should be in the list.

netsh http show iplisten

A screenshot of a Windows Command Prompt window titled "Administrator: C:\WINDOWS\system32\cmd.exe". The window has a black background with white text. It shows the command "C:\>netsh http show iplisten" being executed. The output is "IP addresses present in the IP listen list:" followed by a dashed line and the IP address "127.0.0.1". The prompt "C:\>" is visible at the bottom left.

```
C:\>netsh http show iplisten
IP addresses present in the IP listen list:
-----
127.0.0.1
C:\>
```

More Information

For further information open the Windows Event Viewer, and select the System event log. Look for error messages that have "Windows Remote Management" as the source.

The service is configured to not accept any remote shell requests

Symptoms

When using an agent that uses [PowerShell remoting](#) you see the following error
"The WS-Management service cannot process the request. The service is configured to not accept any remote shell requests."

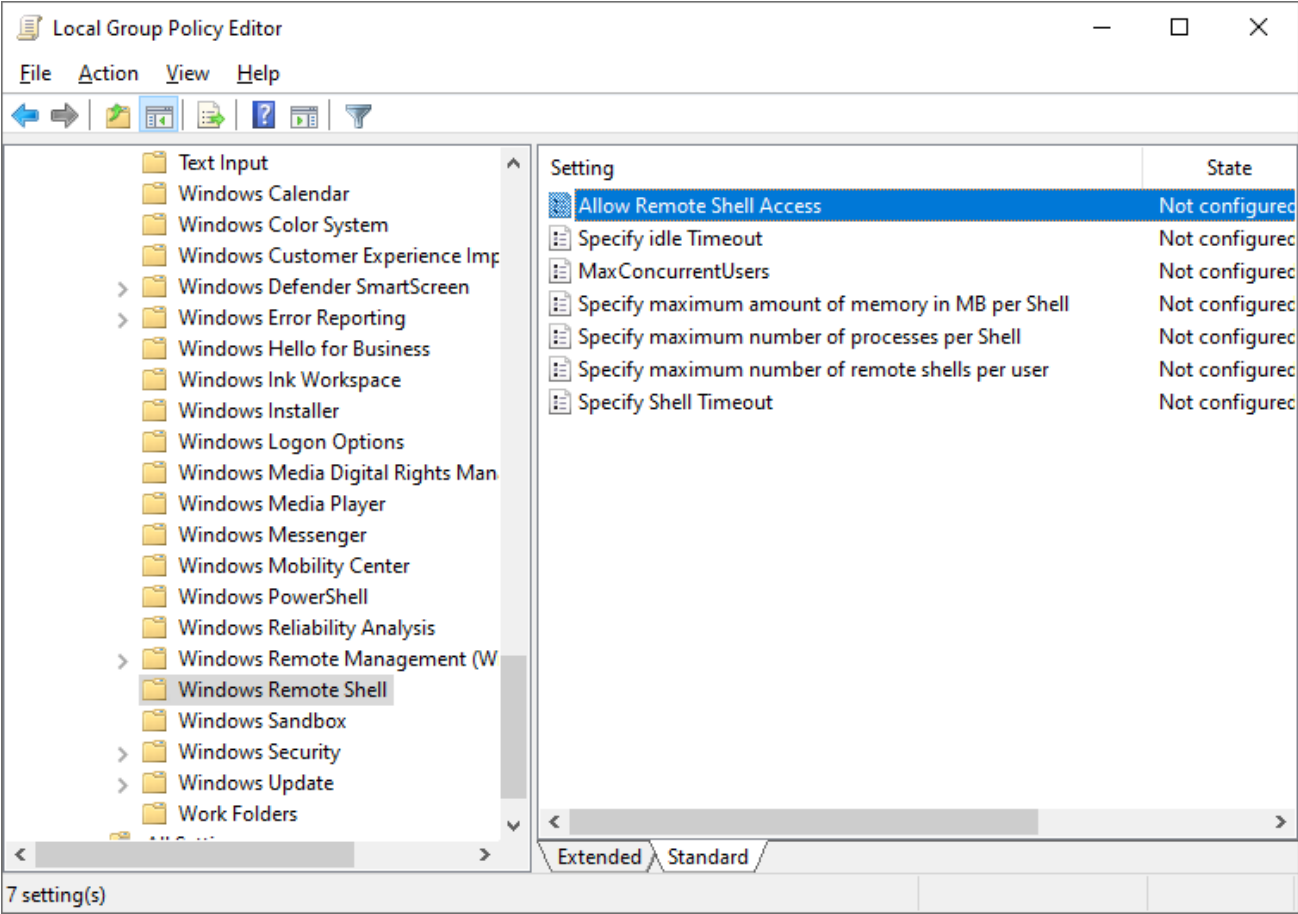
Cause

The *Allow Remote Shell Access* group policy setting has been disabled.

Resolution

Review and configure the following setting
`Get-Item WSMan:\localhost\Shell\AllowRemoteShellAccess`

The setting can be located in the following group policy path
Computer Configuration > Administrative Templates > Windows Components > Windows Remote Shell > Allow Remote Shell Access



The WSMAN provider host process did not return a proper response

When using an agent that requires [PowerShell Remoting](#) you may see one of the following error messages

Processing data from remote server failed with the following error message: The WSMAN provider host process did not return a proper response.

- or -

Exception of type 'System.OutOfMemoryException' was thrown.

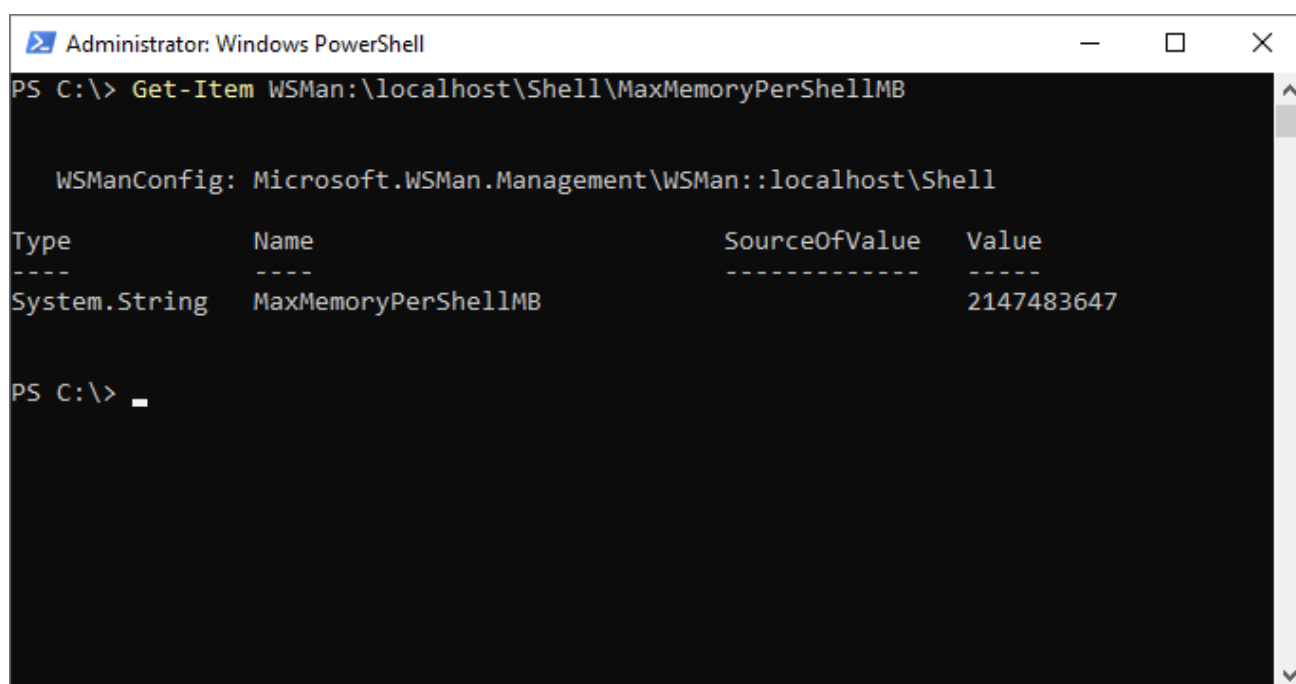
- or -

New-PSSession : [SEVERNAME] Remoting data is missing TargetObject property.

This error can occur when the MaxMemoryPerShellMB setting is not configured with a high enough value.

To determine the current value run the following command in a PowerShell prompt on the **remote** machine you are trying to scan:

```
Get-Item WSMAN:\localhost\Shell\MaxMemoryPerShellMB
```



```
Administrator: Windows PowerShell
PS C:\> Get-Item WSMAN:\localhost\Shell\MaxMemoryPerShellMB

WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Shell

Type      Name                      SourceOfValue      Value
----      -
System.String MaxMemoryPerShellMB      2147483647

PS C:\> _
```

A new value can then be configured using the following command:

```
Set-Item WSMAN:\localhost\Shell\MaxMemoryPerShellMB newvalue -Force
```

Unable to download the list of available providers

Symptoms

When attempting to install a module using [Windows PowerShell](#) using the [Install-Module](#) cmdlet as an Administrator you see the error

"WARNING: Unable to download the list of available providers. Check your internet connection."

Cause

This can occur when the machine is not configured to connect to the server using TLS version 1.2.

Resolution

- Set the current [Windows PowerShell](#) session to use TLS version 1.2 by executing the following command in the [Windows PowerShell](#).

```
[System.Net.ServicePointManager]::SecurityProtocol =  
[System.Net.SecurityProtocolType]::Tls12;
```

- or -

- To set this for all .NET Framework 4 applications, set the following registry key

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319  
"SchUseStrongCrypto" = dword:00000001
```

More Information

For more information see the following article.

<https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client>

Using Custom Credentials and PowerShell Remoting

When scanning using an agent that uses PowerShell remoting using [custom credentials](#) negotiate authentication is used and the computer running the [XIA Configuration Client](#) must trust the remote machine before a remote PowerShell session can be established.

For more information see the following article

[Error "...only if the target machine is part of the TrustedHosts list"](#)

Server Connections

This section provides information for the troubleshooting of the connection to the [XIA Configuration Server](#), configured on the [server settings](#) section.

The request failed with HTTP status 403: Forbidden

The request failed with HTTP status 403: Forbidden

Symptoms

When connecting to the [XIA Configuration Server](#), the system reports
The request failed with HTTP status 403: Forbidden

Issue

The issue can be caused when the Internet Information Server (IIS) is configured to require an SSL connection, however the [server settings](#) are configured to use a HTTP connection or a client certificate is required by IIS.



SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

☒ **Require SSL**

Client certificates:

- ☐ Ignore
- ☐ Accept
- ☒ Require

Resolution

Confirm that the [server settings](#) are configured to use a HTTPS connection to the server

- and -

If a client certificate is required that this is specified on the [server settings](#) section [advanced settings tab](#).

The request failed with HTTP status 413: Request Entity Too Large

Symptoms

When uploading data to the [XIA Configuration Server](#) using SSL the system reports Error uploading to XIA Configuration at address '*server address*'. The request failed with HTTP status 413: Request Entity Too Large.

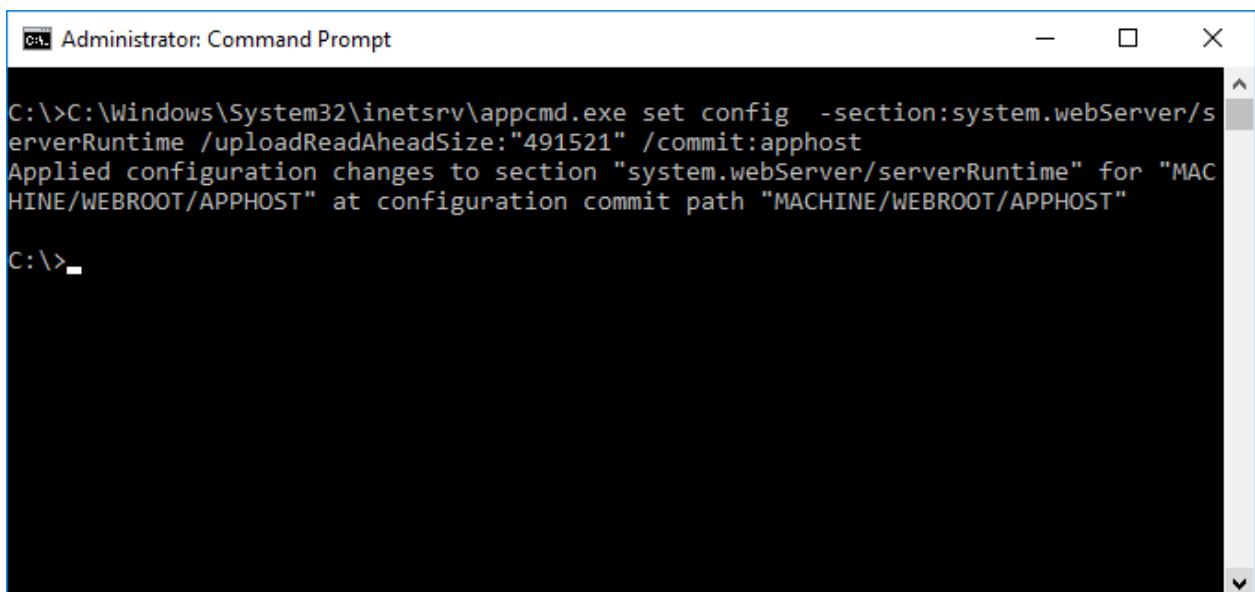
Issue

This issue can occur because of the way data is sent using an SSL connection and is limited by the **uploadReadAheadSize** setting.

Resolution

- Review the [uploadReadAheadSetting](#) documentation on the [Microsoft Server Runtime settings page](#).
- Start a command prompt as an Administrator and enter the following command, replacing the value with the maximum size in bytes between 0 and 2147483647 that will allow the data required.

```
C:\Windows\System32\inetsrv\appcmd.exe set config -  
section:system.webServer/serverRuntime /uploadReadAheadSize:"value" /commit:apphost
```



```
Administrator: Command Prompt  
C:\>C:\Windows\System32\inetsrv\appcmd.exe set config -section:system.webServer/s  
erverRuntime /uploadReadAheadSize:"491521" /commit:apphost  
Applied configuration changes to section "system.webServer/serverRuntime" for "MAC  
HINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT/APPHOST"  
C:\>_
```

The underlying connection was closed: An unexpected error occurred on a receive

Symptoms

When uploading data from the [XIA Configuration Client](#) to the [XIA Configuration Server](#) using SSL the system reports

The underlying connection was closed: An unexpected error occurred on a receive.

The error is also shown when testing the server connection.

Cause

This error can occur when the computer running [XIA Configuration Server](#) has been configured to allow only TLS 1.2 connections, however the machine running the [XIA Configuration Client](#) is not configured to use TLS 1.2.

More Information

Viewing the [diagnostics log](#) displays additional information.

The client and server cannot communicate, because they do not possess a common algorithm

Resolution

- Ensure you are running the latest version of [XIA Configuration Server](#), and [upgrade](#) if required.
- Ensure you have a full system backup on the machine running the [XIA Configuration Client](#).
- Apply the following registry settings, then reboot the machine running the [XIA Configuration Client](#).

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
```

```
"SystemDefaultTlsVersions"=dword:00000001
```

```
"SchUseStrongCrypto"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
```

```
"Enabled"=dword:ffffffff
```

```
"DisabledByDefault"=dword:00000000
```


XIA Configuration Local Service

The [XIA Configuration Client](#) does not require any additional software to be installed on remote machines for the collection of data as it uses remoting technologies appropriate for connecting to different target systems such as [PowerShell remoting](#) for [Windows machines](#) and [SQL Server Management Objects \(SMO\)](#) for [SQL Instances](#).

These technologies require certain levels of permissions on the remote machine and certain TCP ports to be open.

Where these requirements are prohibitive - perhaps because of firewall or user account constraints the [XIA Configuration Local Service](#) can be installed on these machines.

The [XIA Configuration Local Service](#) has the following attributes:

- ✔ Operates on a single TCP port (by default 8092).
- ✔ Runs as a Windows service under the [Local System Account](#).
- ✔ Is configured using [Group Policy](#) either locally with the local Group Policy editor or using [Active Directory Group Policy](#).
- ✔ Can be configured to accept connections only from specified user accounts.
- ❗ Must be installed and updated on each target machine.
- ❗ Is only available for [Microsoft Windows](#) based target systems.

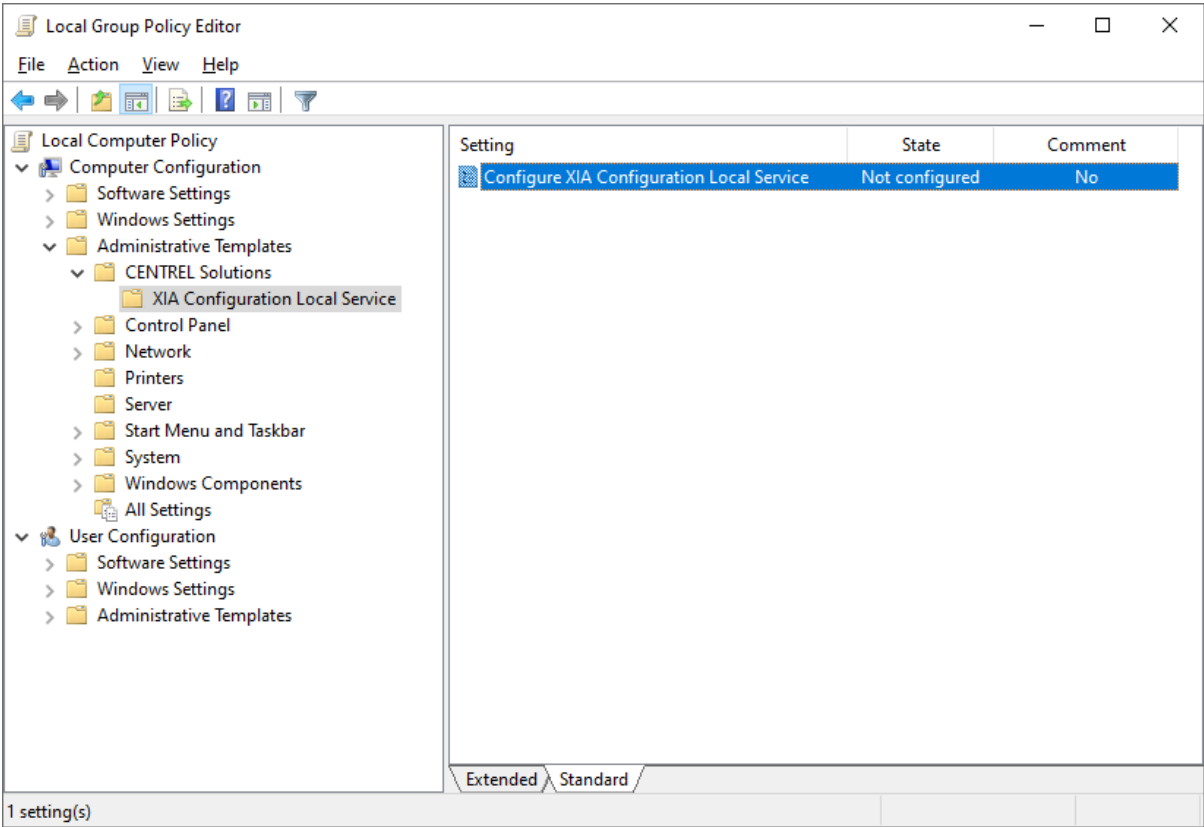
NOTE: Whilst the [XIA Configuration Local Service](#) does provide a solution to the scenarios detailed above it is generally recommended that items are scanned using the [XIA Configuration Client](#) remotely using [PowerShell remoting](#).

Group Policy

The [XIA Configuration Local Service](#) can be easily configured using [Microsoft Group Policy](#) and the provided Administrative Template ADMX file.

NOTE: For more information on Active Directory and [Group Policy](#) best practices please refer to the Microsoft documentation for your version of Windows.

- Firstly access the [Group Policy template files](#), these include the ADMX, and ADML files.
- The files can be installed into the [Central Store for Group Policy Administrative Templates](#).
- The settings can be found within the Computer Configuration > Administrative Templates > CENTREL Solutions > XIA Configuration Local Service.



- The [Group Policy settings](#) can be configured as required.

Group Policy Settings

Configure XIA Configuration Local Service

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on:

Options:

TCP Port

Permitted Accounts (DomainName\UserName)

Show...

☐ Enable Trace Logging

Help:

Allows the configuration of the XIA Configuration Local Service.

TCP Port
Configures the TCP port on which the XIA Configuration Local Service listens. This must be a valid port number that is not already in use by other applications.

Permitted Accounts (DomainName\UserName)
Configures the list of user accounts in the format "DomainName\Username" that are permitted to connect to, and execute scans using the XIA Configuration Local Service. By default, only local Administrators may connect.

Enable Trace Logging
Determines if diagnostics trace logging should be enabled for the XIA Configuration Local Service. This information is useful when attempting to resolve issues, however may consume large amounts of disk space over time.

OK Cancel Apply

TCP Port

Configures the TCP port on which the [XIA Configuration Local Service](#) listens. This must be a valid port number that is not already in use by other applications.

Permitted Accounts (DomainName\UserName)

Configures the list of user accounts in the format "DomainName\Username" that are permitted to connect to, and execute scans using the [XIA Configuration Local Service](#). By default, only local Administrators may connect.

Enable Trace Logging

Determines if diagnostics trace logging should be enabled for the **XIA Configuration Local Service**. This information is useful when attempting to resolve issues, however may consume large amounts of disk space over time so should be disabled when not in use.

Group Policy Template Files

The [XIA Configuration Local Service Group Policy](#) Administrative Template can be found in the following locations

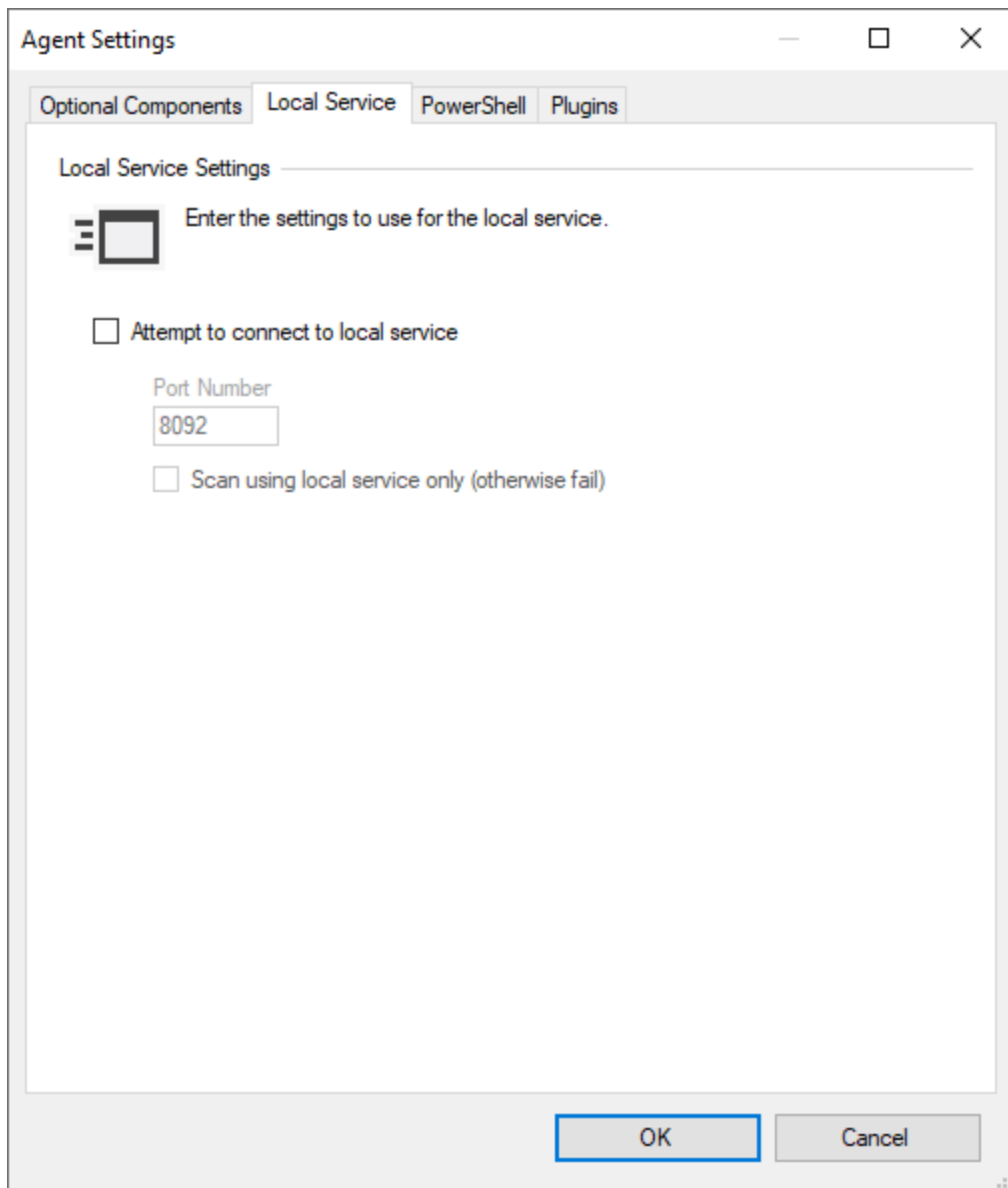
- In the [XIA Configuration Server](#) select Tools > Download Installers from the menu and click "Local Service Group Policy Template".

- or -
- In the [XIA Configuration Server](#) installation directory, by default
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration
Server\App_Data\Installers\LocalClient\XIA Configuration Local Service Group Policy
Template.zip

- or -
- Within the [XIA Configuration Local Service](#) installation directory, by default
C:\Program Files\CENTREL Solutions\XIA Configuration\XIA Configuration Local Service\Group
Policy\XIA Configuration Local Service Group Policy Template.zip

Local Service Settings

The local service settings are available for any agent that supports the [XIA Configuration Local Service](#).



The image shows a Windows-style dialog box titled "Agent Settings". It has four tabs: "Optional Components", "Local Service", "PowerShell", and "Plugins". The "Local Service" tab is selected. Inside the dialog, there is a section titled "Local Service Settings" with a sub-header "Enter the settings to use for the local service." Below this, there is a checkbox labeled "Attempt to connect to local service". Underneath this checkbox is a text box labeled "Port Number" containing the value "8092". Below the port number is another checkbox labeled "Scan using local service only (otherwise fail)". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Attempt to Connect to local service

Instructs the agent to attempt to use the local service connection before trying to use the agentless method of obtaining the information.

Port Number

Determines the TCP port to use when attempting to connect to the local service, by default this is port 8092.

Scan using local service only (otherwise fail)

Determines whether, if the [XIA Configuration Local Service](#) scan fails, the [XIA Configuration Client](#) should attempt to perform the scan using a direct agent-less connection or to immediately fail the scan.

Requirements

This section describes the requirements for the installation of the [XIA Configuration Local Service](#).

Operating Systems (Server)

The following operating systems are supported for the installation of a production version of the [XIA Configuration Local Service](#).

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Desktop Operating Systems

The following operating systems are supported for the installation of a production version of the [XIA Configuration Local Service](#).

- Windows 11 Pro (64-bit)
- Windows 10 Pro Anniversary Edition (64-bit)

.NET Framework

- [.NET Framework 4.8](#) *

** Please see the [Microsoft .NET Framework 4.8 installation requirements](#) for further information*

Troubleshooting

The following chapters cover the troubleshooting and diagnostics of the [XIA Configuration Local Service](#).

You do not have permissions to access the local service on a WORKGROUP

Symptoms

When attempting to connect to the [XIA Configuration Local Service](#) on a machine that is a member of a WORKGROUP the connection fails with the following error, even though the user is a member of the Administrators group.

You do not have permissions to access the local service.

Cause

This can be caused by the [User Access Control \(UAC\)](#) settings on the WORKGROUP machine which removes Administrator privileges from remote user accounts by default.

Resolution

There are two options to resolve this issue.

- Enable [diagnostics trace logging](#) on the machine running the [XIA Configuration Local Service](#) to confirm the account name that is being evaluated - for example:

Access denied for user 'CORP-SRV01\adminaccount'.

Explicitly add the user account to the [access list](#) setting in the [Group Policy settings](#).

- or -

- Change the following registry key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System  
LocalAccountTokenFilterPolicy = 1
```

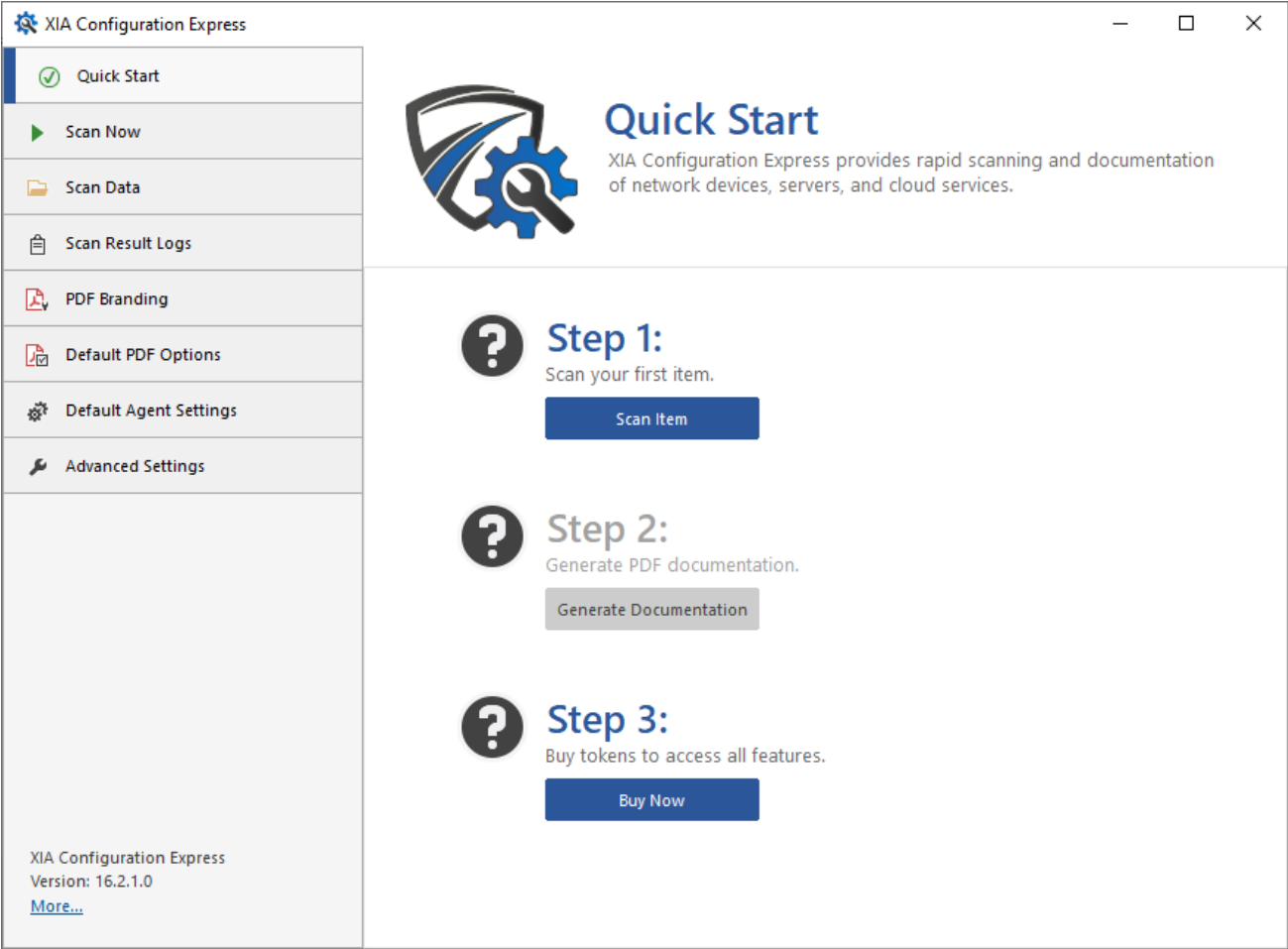
WARNING: This change affects the security level.

More Information

For more information see the [Access is denied scanning WORKGROUP machines](#) article.

XIA Configuration Express

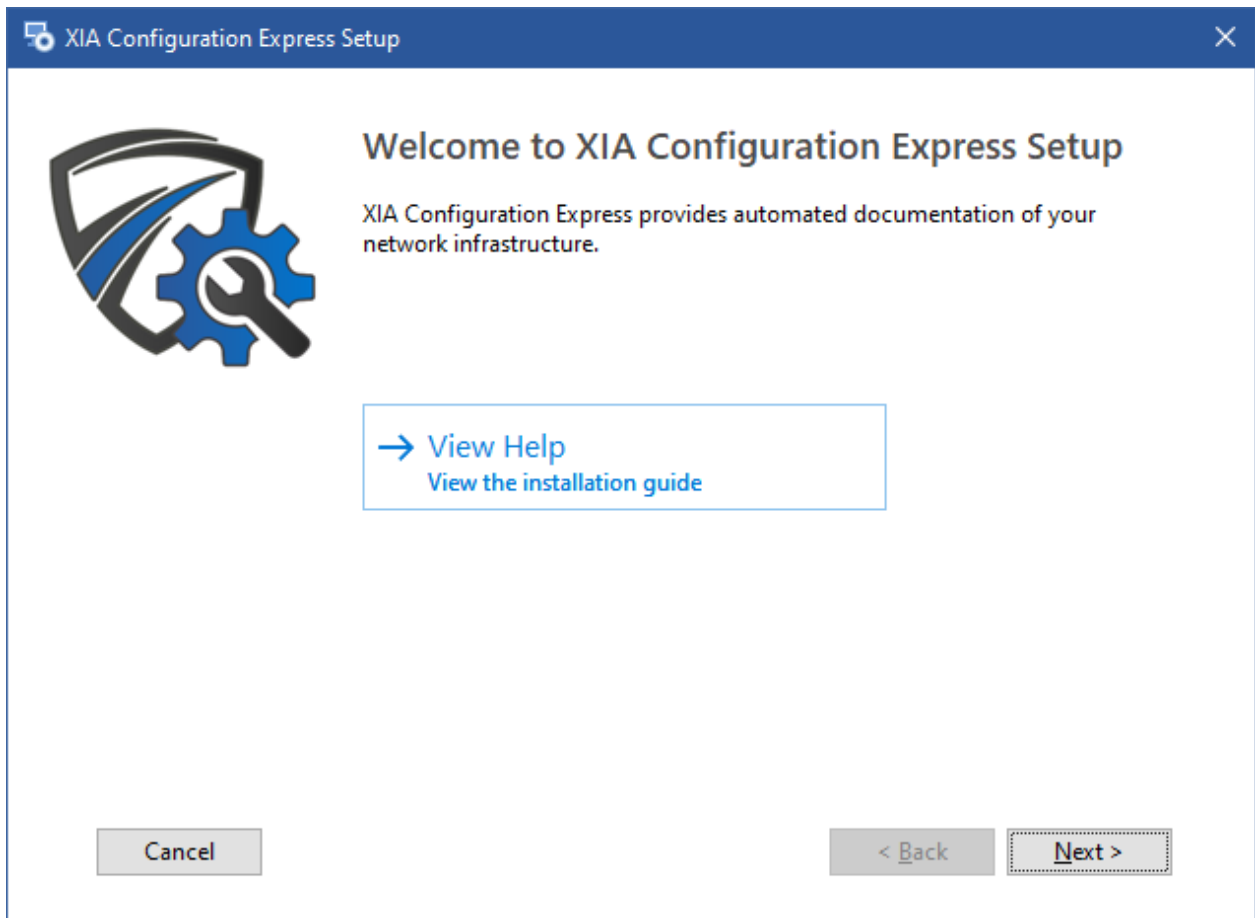
XIA Configuration Express is a fast and simple way to document your IT infrastructure and compare items that uses technology from [XIA Configuration Server](#) and the [XIA Configuration Client](#).



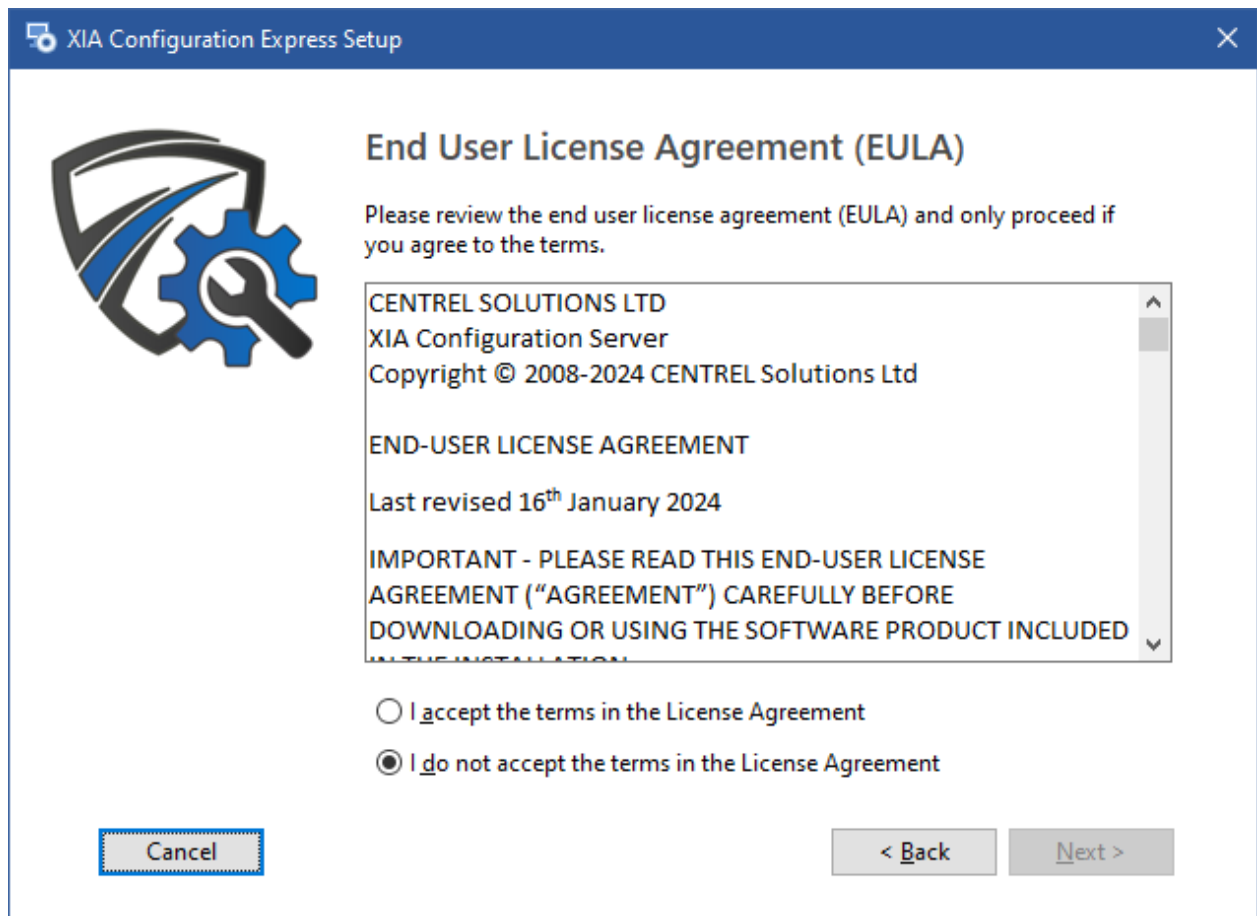
Installation

This section describes the installation process of [XIA Configuration Express](#). For information about the removal of the product see the [uninstallation](#) section.

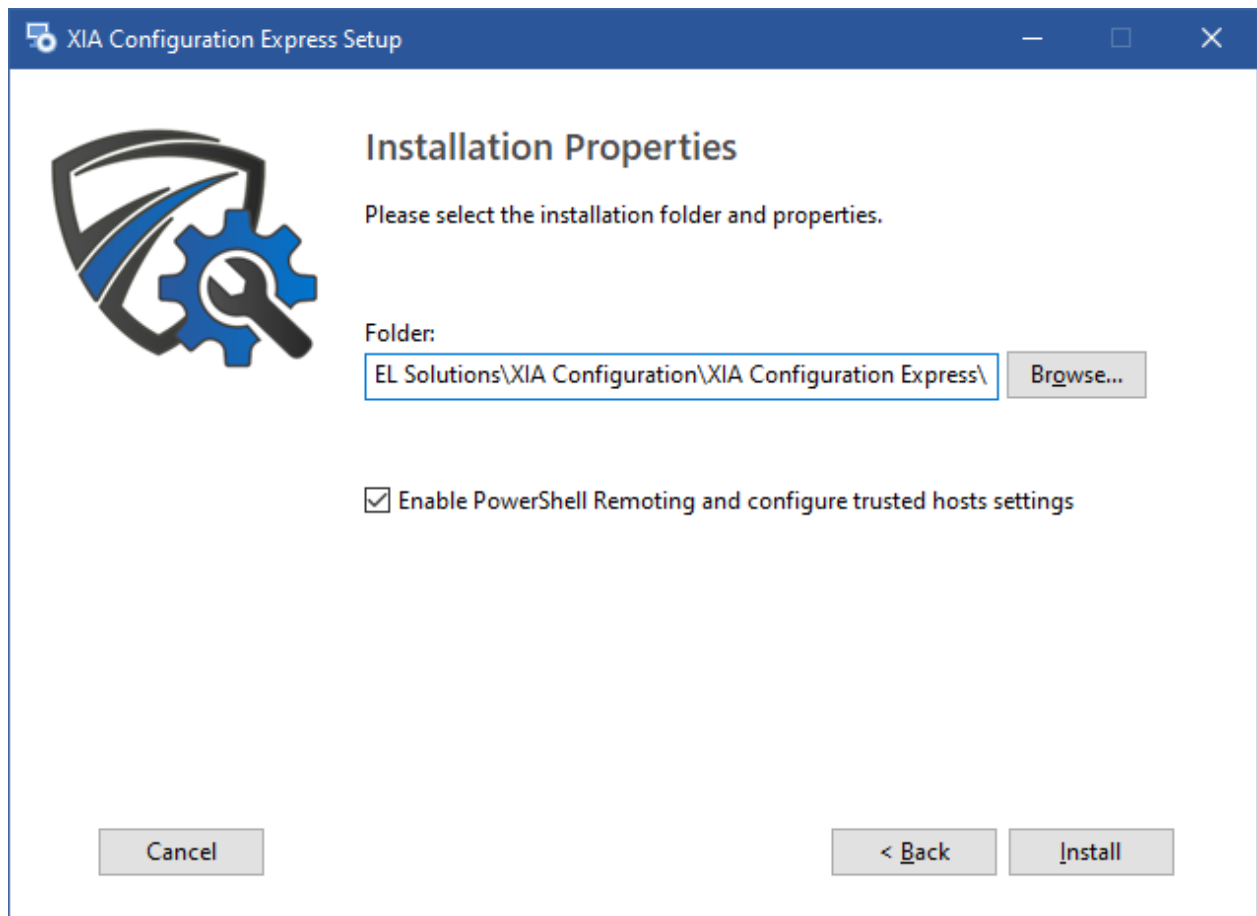
- Download the latest [installation package](#).
- Check that the system you are installing on meets the [system requirements](#).
- Start the installer.



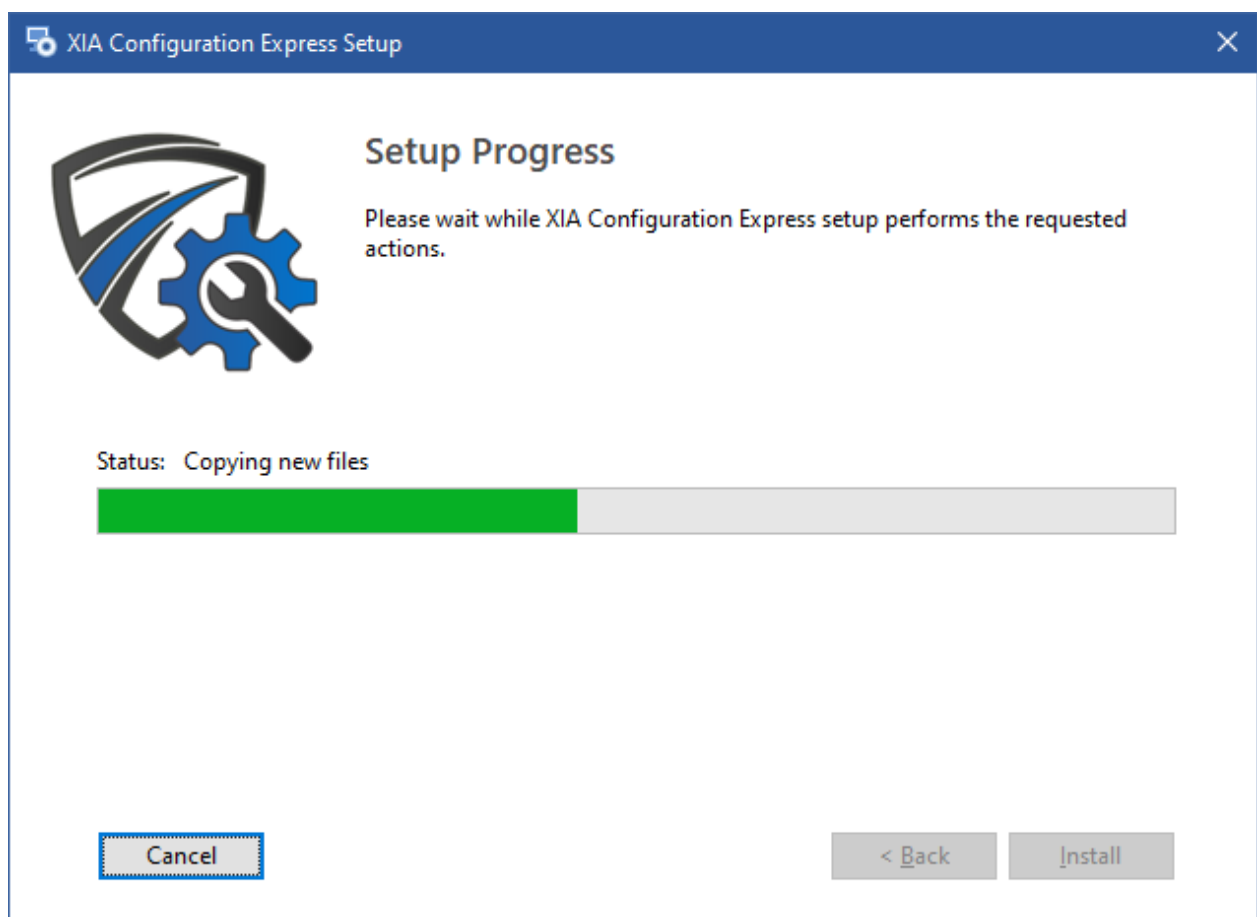
- Review the [End User License Agreement \(EULA\)](#) and only accept if you agree to the terms. If you do not accept the terms of the agreement please cancel the installation.



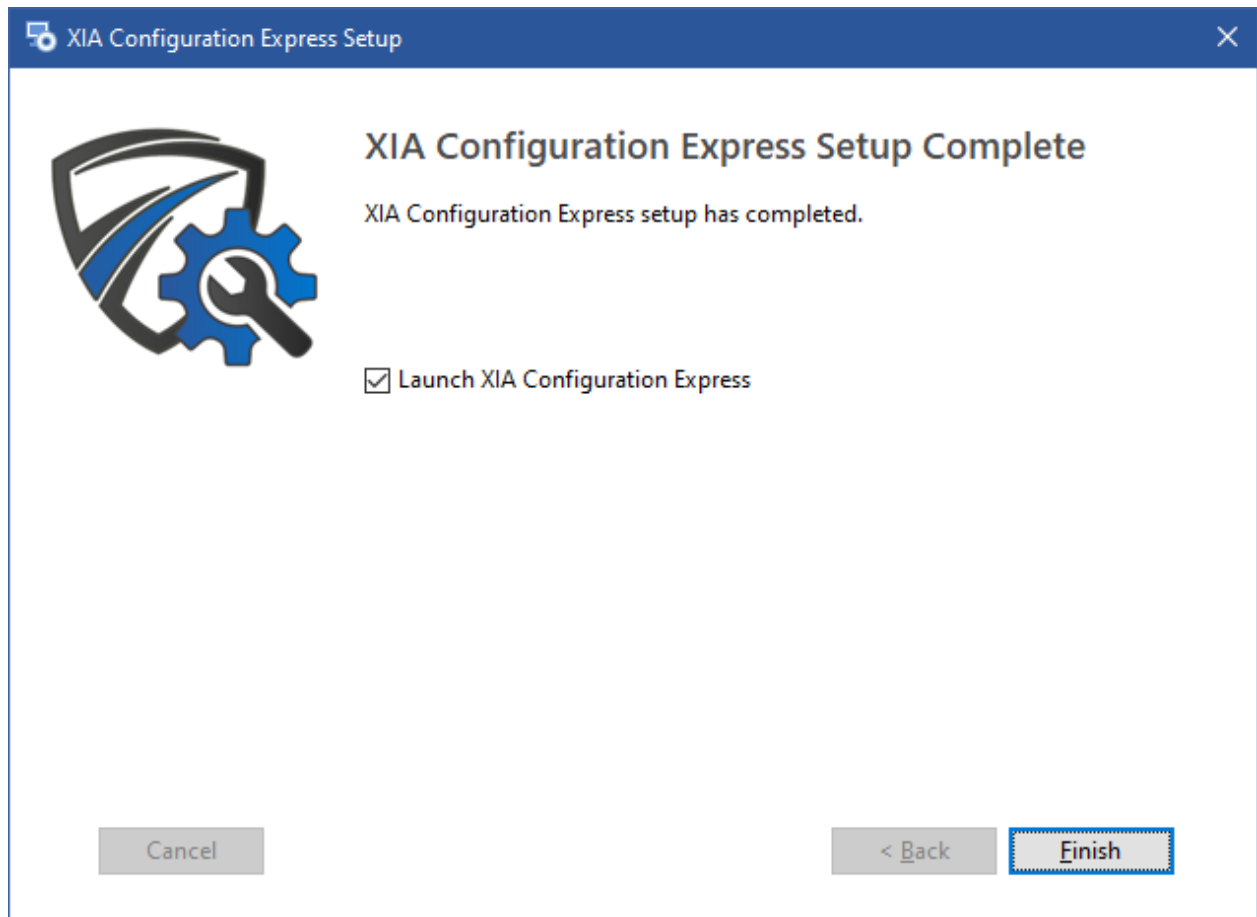
- Review the installation properties setting the folder if required and whether to enable [PowerShell remoting](#) on the local machine, and configure the [trusted hosts](#) setting to allow connections to any host.



- The installation progress will be shown.



- Click finish to complete the installation. By default [XIA Configuration Express](#) will automatically be started when the installation completes.



System Requirements

This section describes the requirements for the [installation](#) of [XIA Configuration Express](#).

Operating Systems

The following operating systems are supported for the installation of [XIA Configuration Express](#):

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 11 Pro (64-bit)
- Windows 10 Pro Anniversary Edition (64-bit)

.NET Framework

- [.NET Framework 4.8](#)

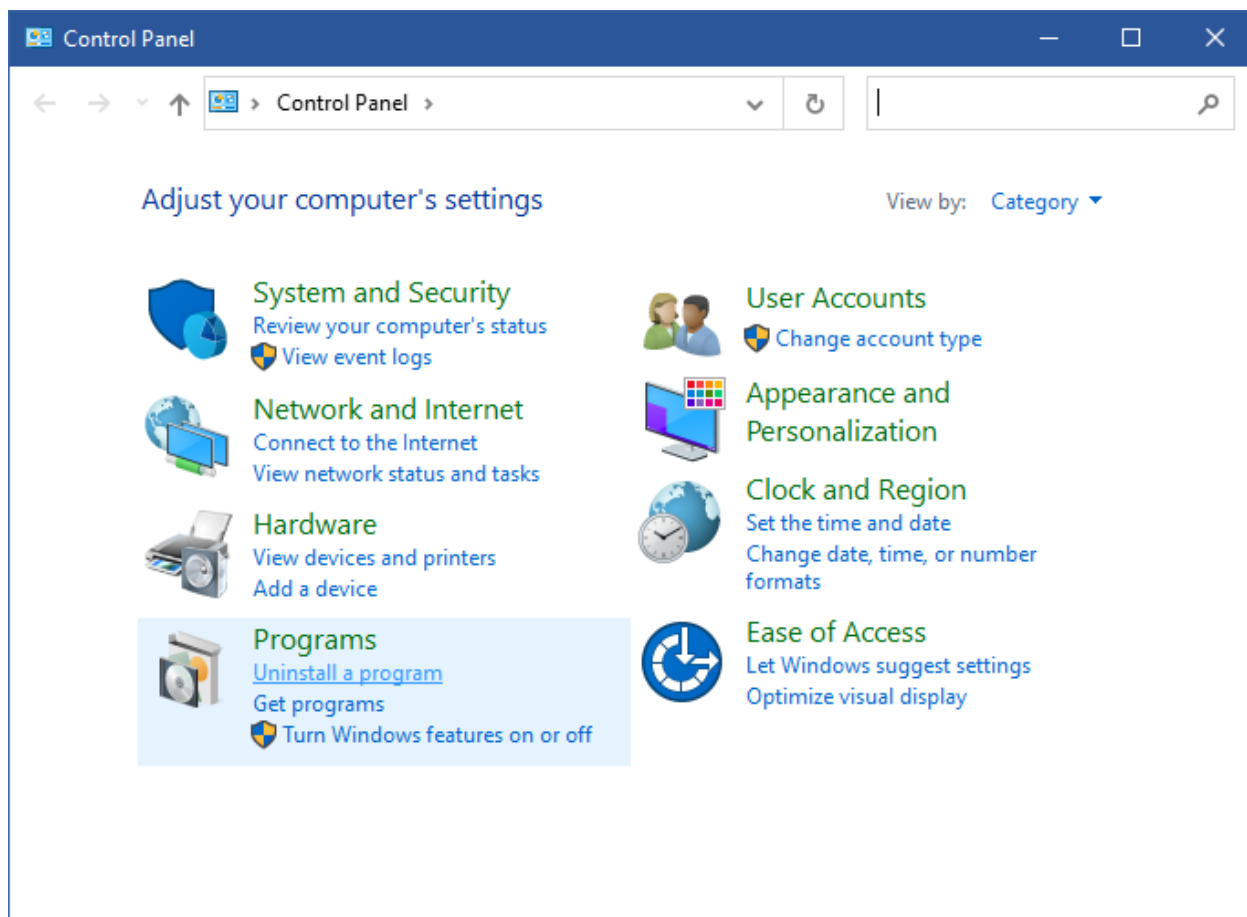
Windows Management Framework

- [Window Management Framework 5.1](#) (pre-installed on Windows 10, Windows Server 2016 and above).

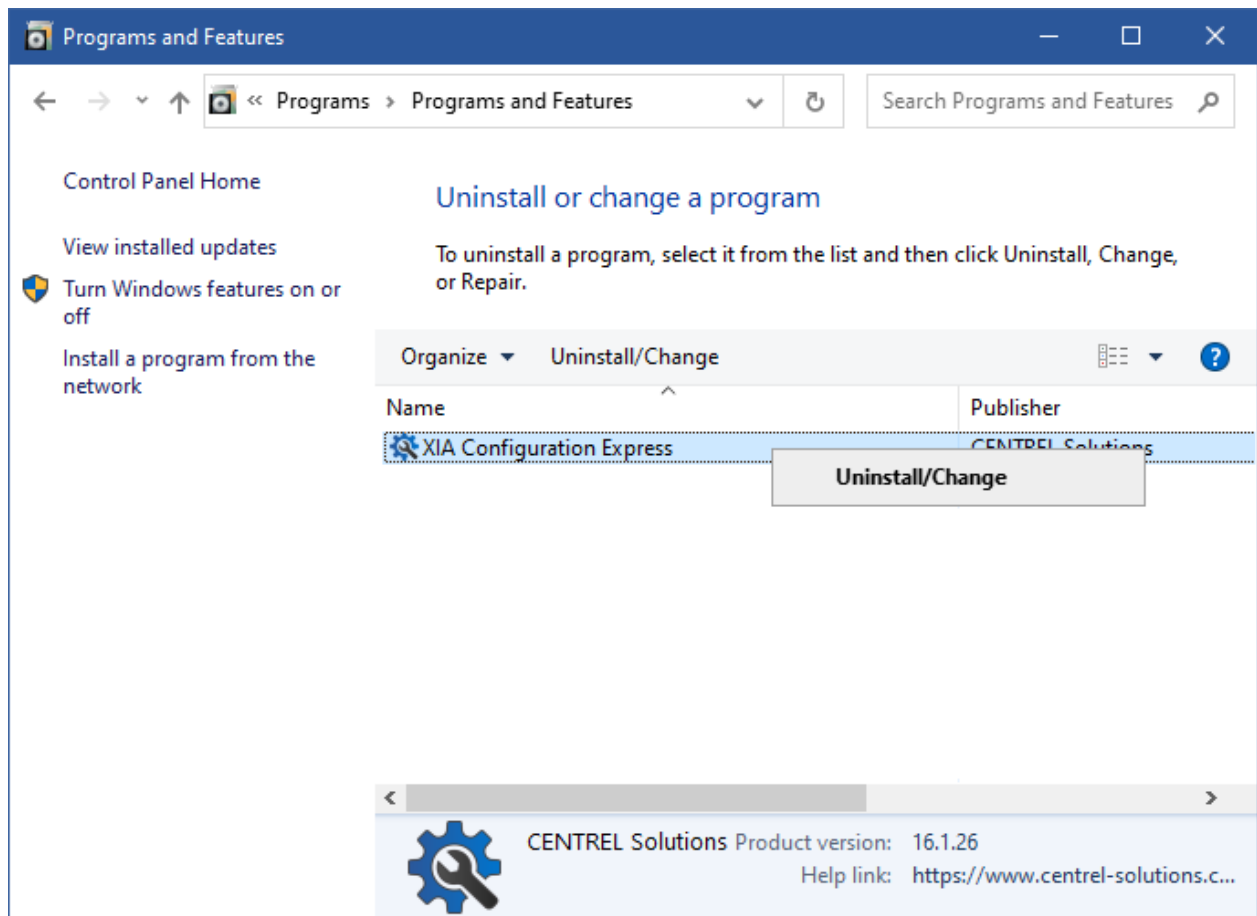
Uninstallation

To uninstall XIA Configuration Express

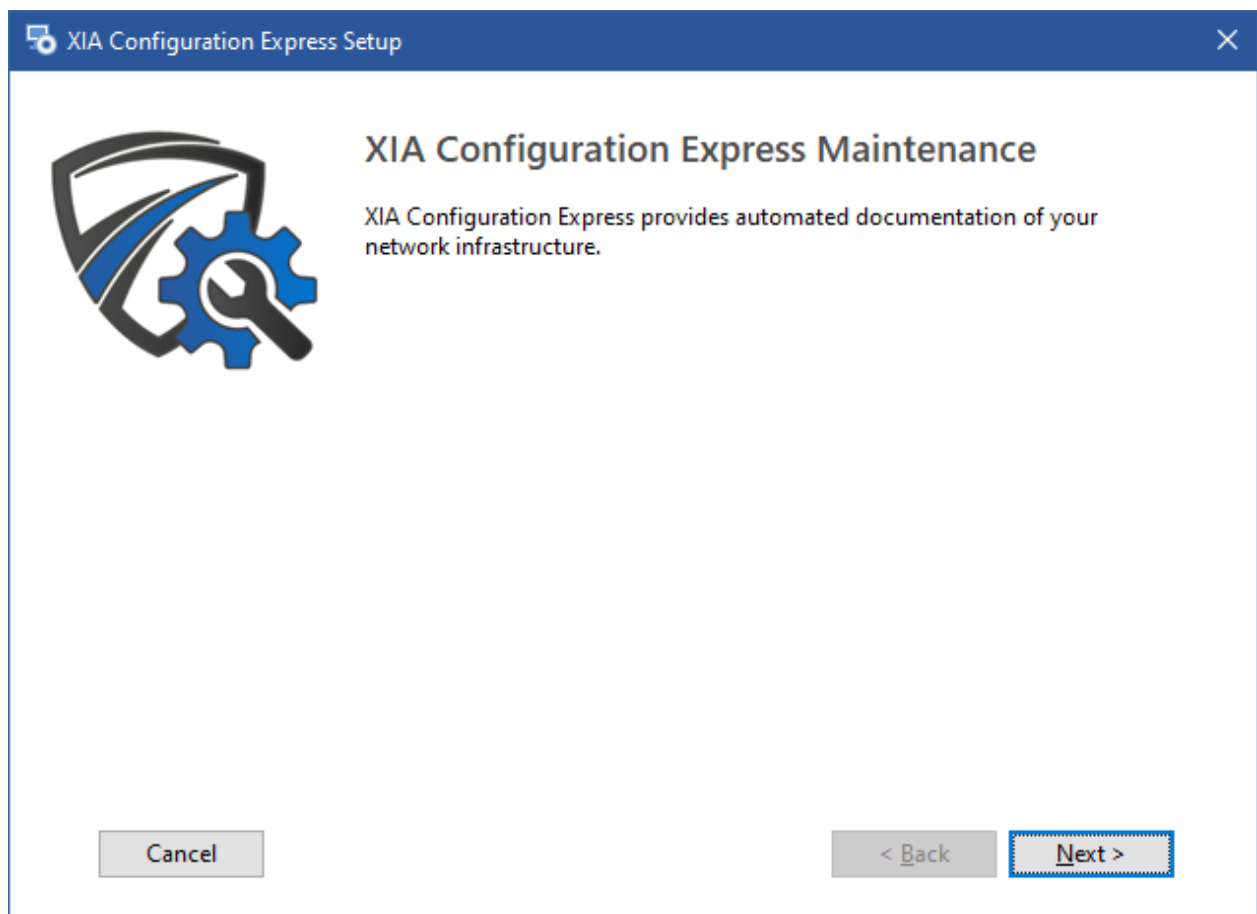
- Go to Control Panel, *Programs*, *Uninstall a program*.



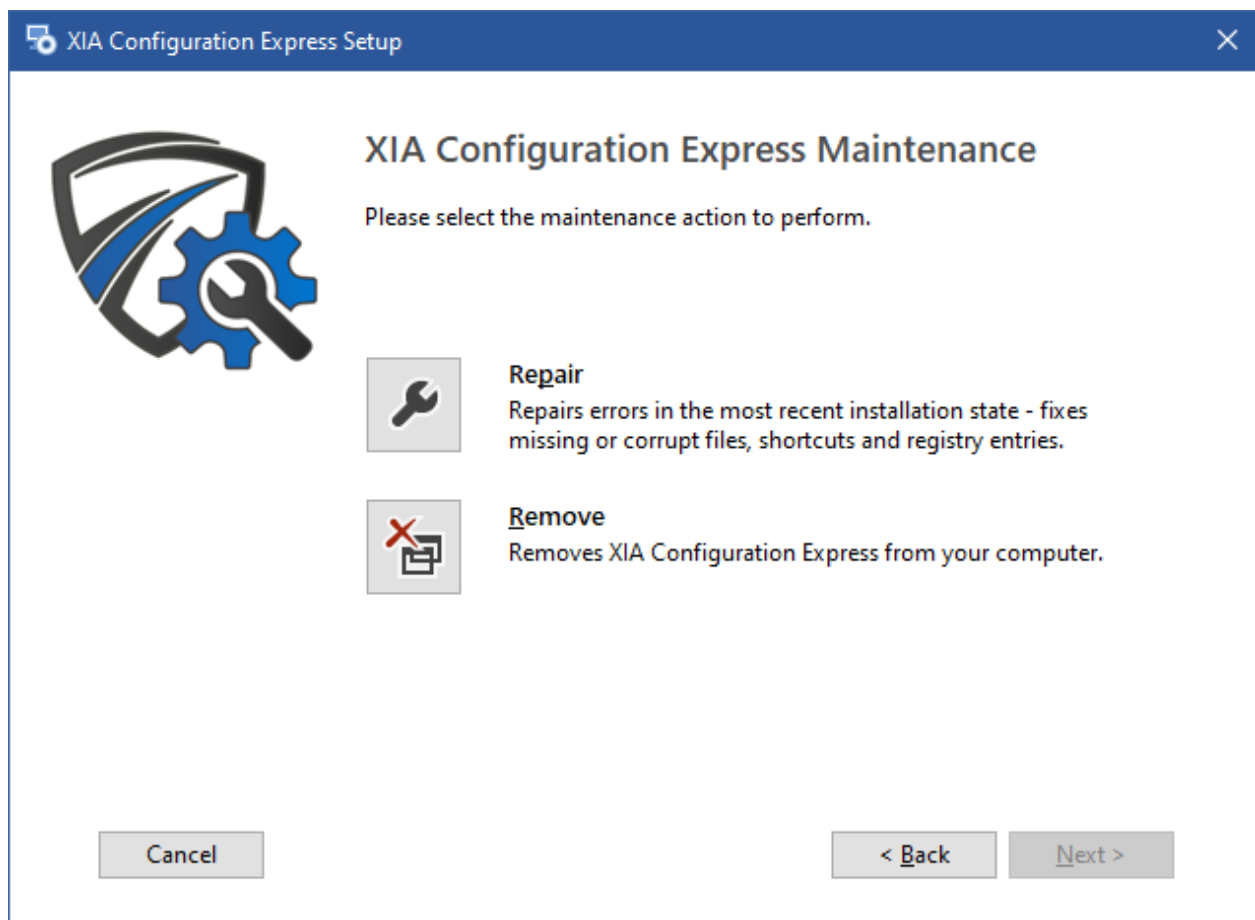
- Right click *XIA Configuration Express* and select *Uninstall/Change*



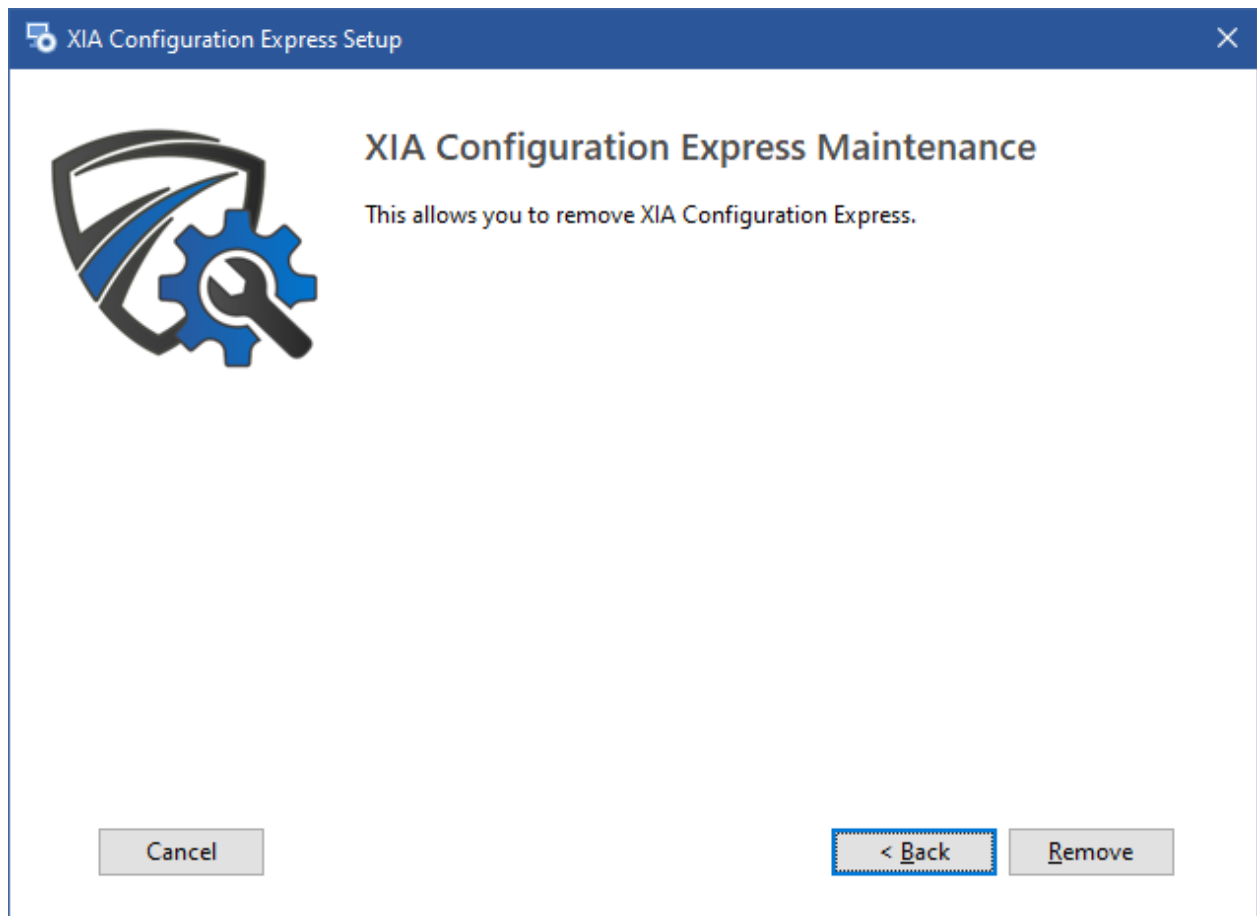
- The welcome screen will be displayed.



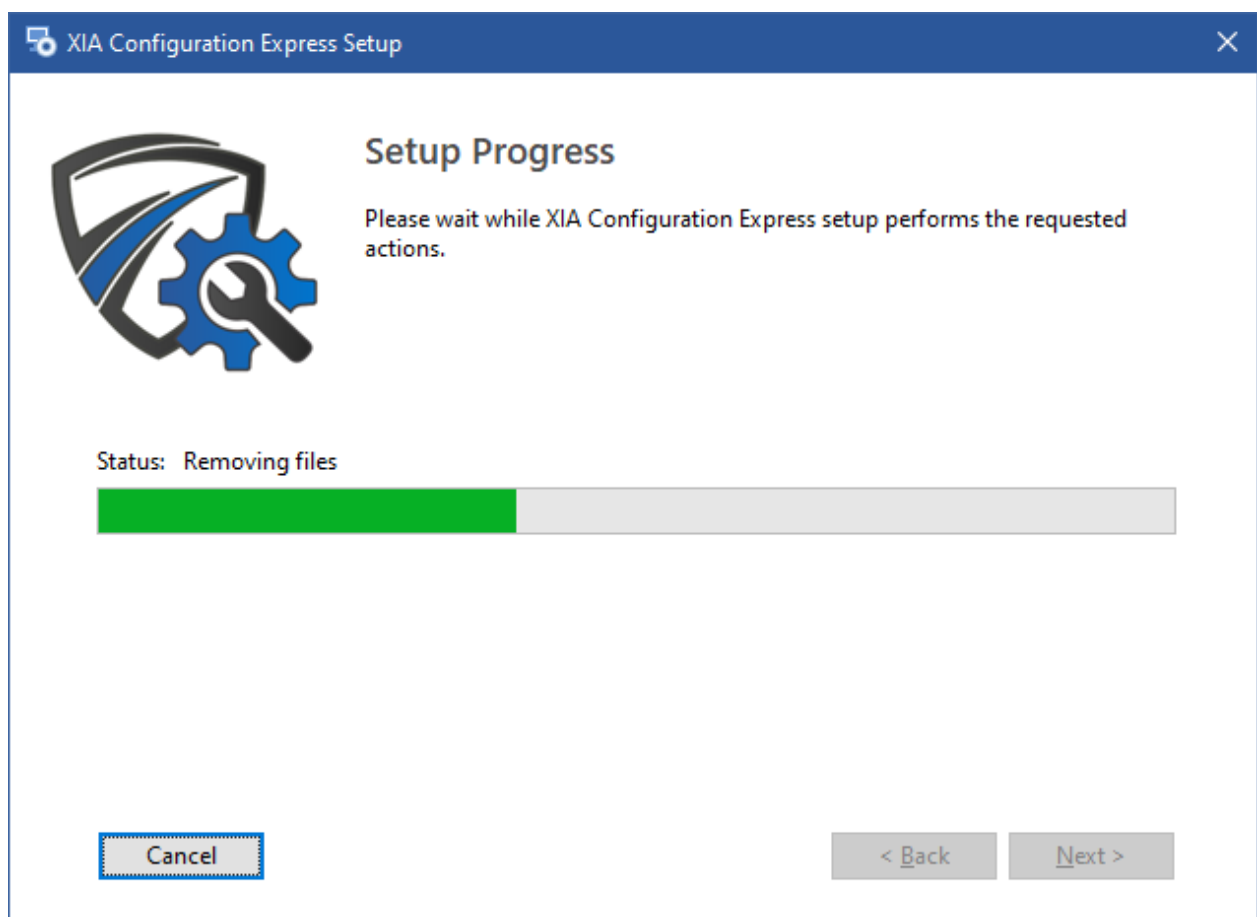
- Select Remove.



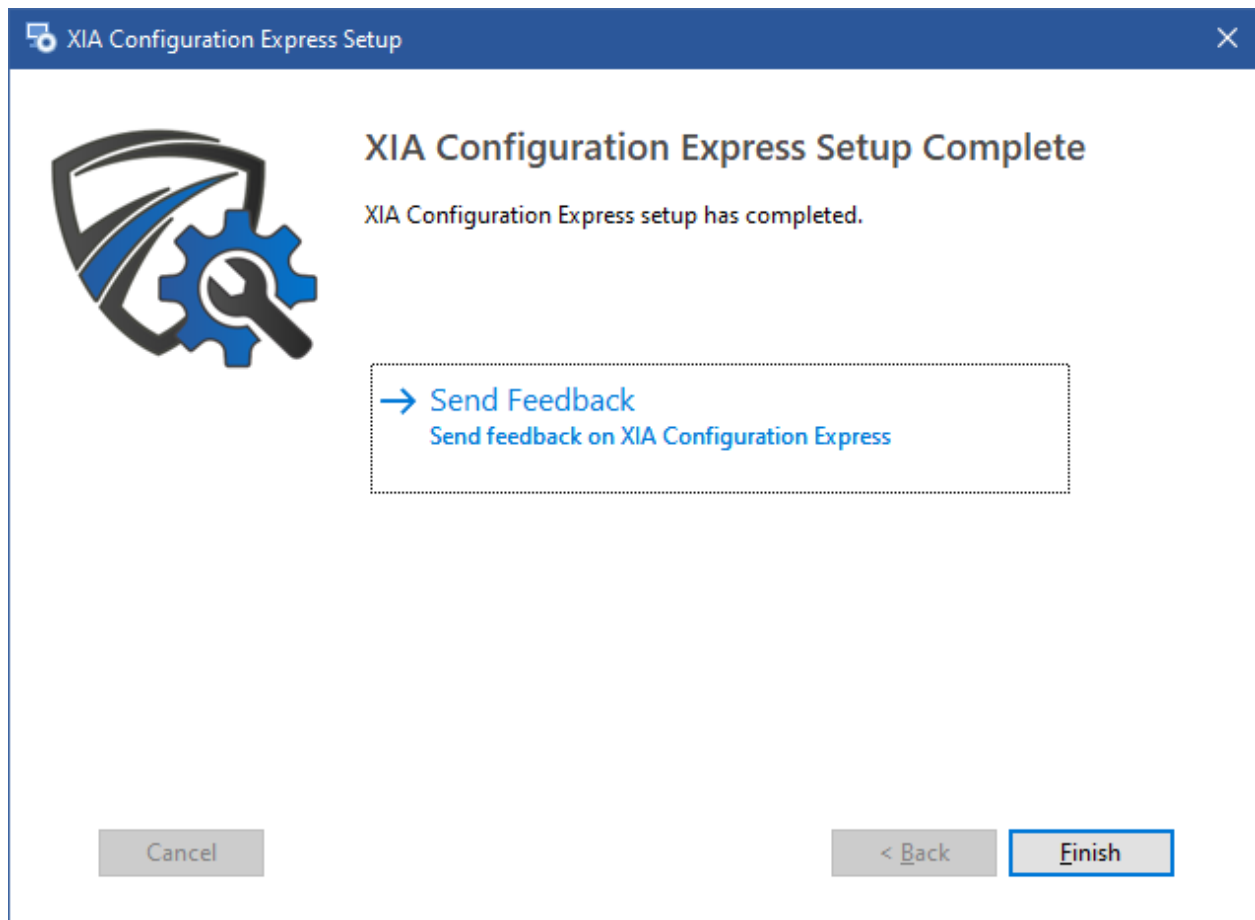
- Click Remove to begin the uninstallation.



- The progress will be displayed.

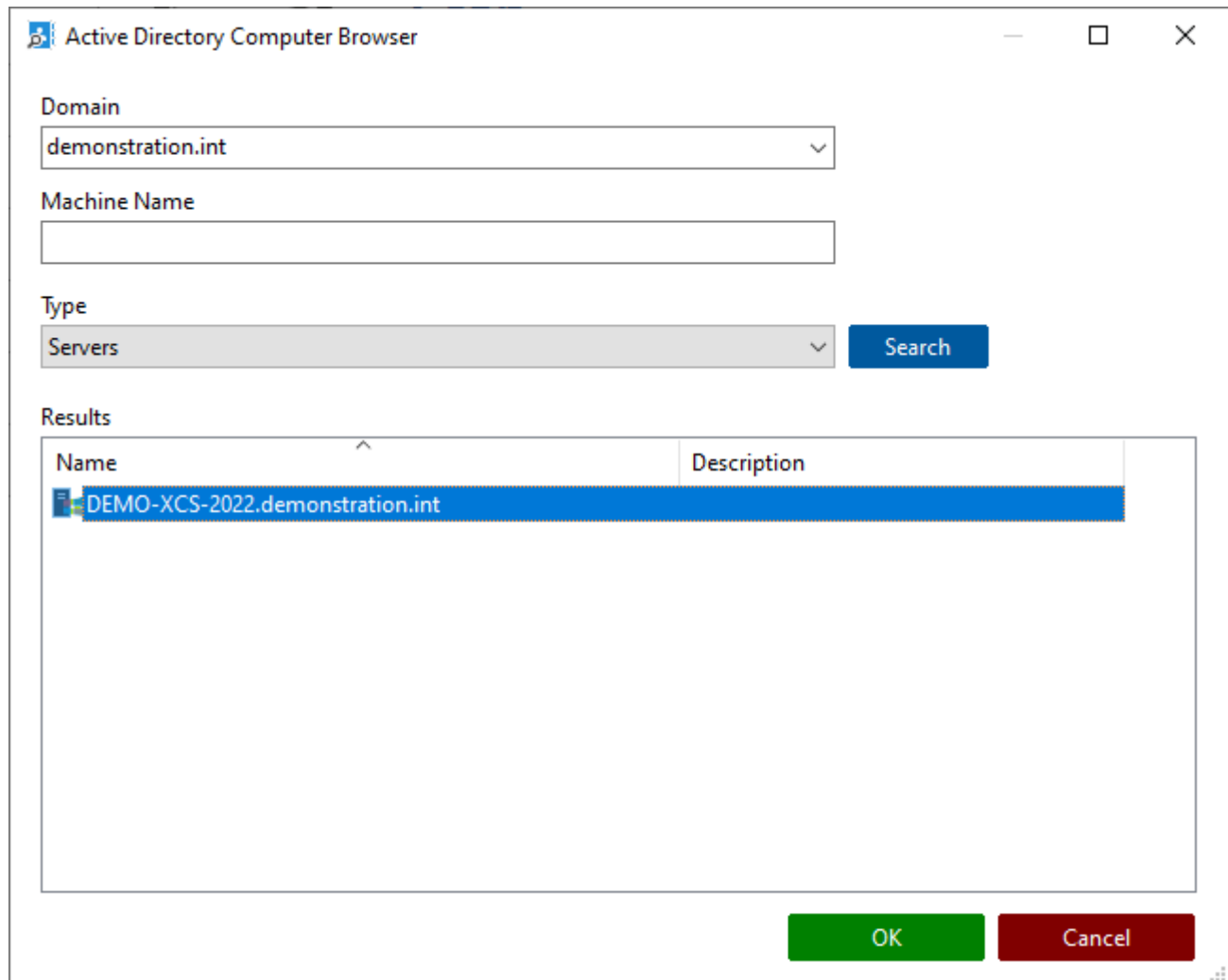


- The complete screen will be displayed allowing you to optionally send feedback.



Active Directory Computer Browser

The Active Directory computer browser simplifies the selection of a computer or server that is a member of an on-premises [Active Directory](#) domain.



The screenshot shows the 'Active Directory Computer Browser' dialog box. It has a title bar with a minimize button, a maximize button, and a close button. The dialog contains the following fields and controls:

- Domain:** A dropdown menu with 'demonstration.int' selected.
- Machine Name:** An empty text input field.
- Type:** A dropdown menu with 'Servers' selected.
- Search:** A blue button to the right of the 'Type' dropdown.
- Results:** A table with two columns: 'Name' and 'Description'. The first row is highlighted in blue and contains the text 'DEMO-XCS-2022.demonstration.int'.
- OK:** A green button at the bottom right.
- Cancel:** A red button at the bottom right.

Domain

The domain in which to locate the computers.

Machine Name

The name of the machine to locate. This can include wildcards for example "DEMO*".

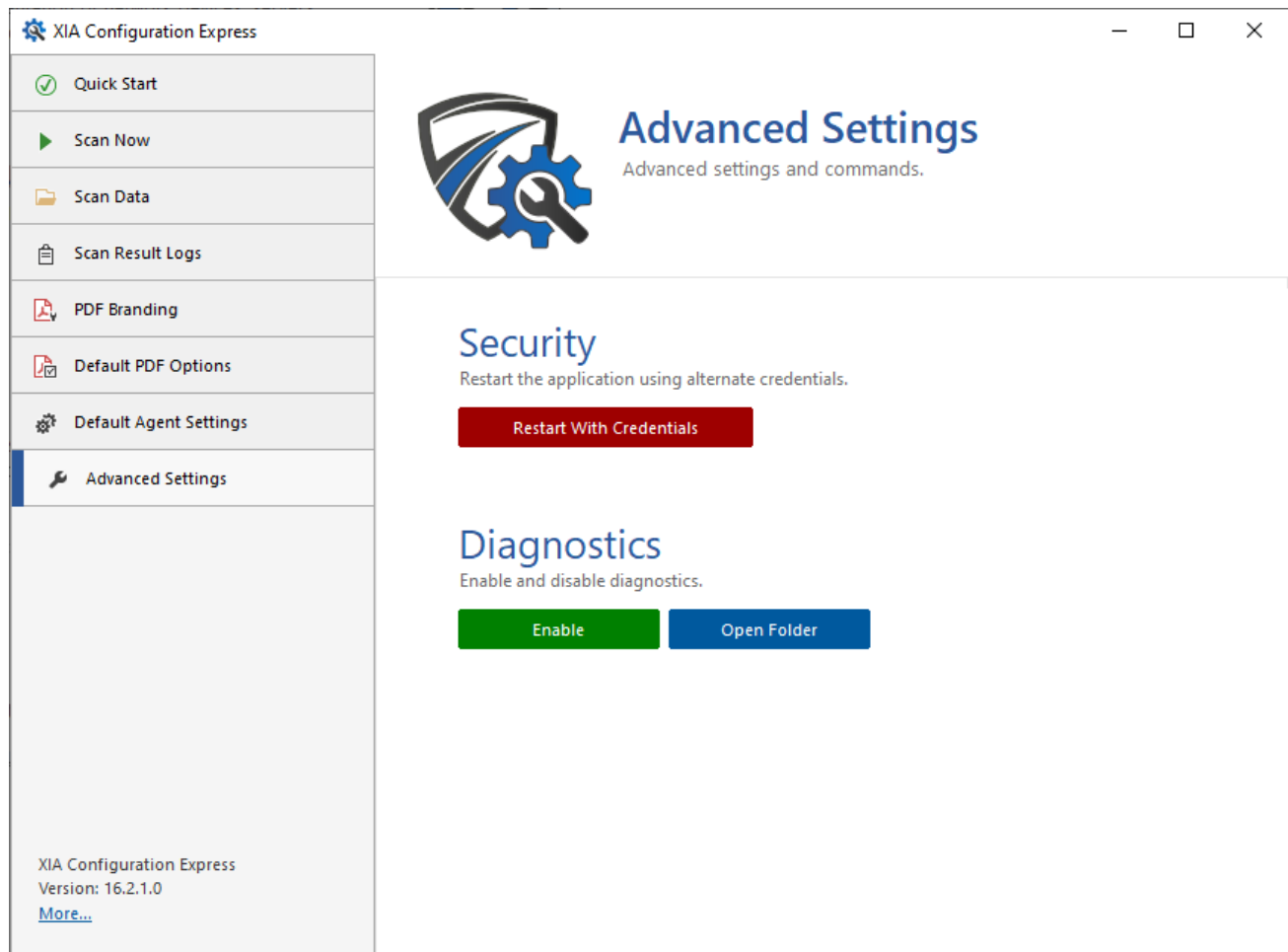
Type

The computer type - which can include workstations, servers or both.

Results

The search results.

Advanced Settings



Restart With Credentials

Displays the [credentials form](#) allowing [XIA Configuration Express](#) to be restarted with alternative credentials.

Diagnostics > Enable

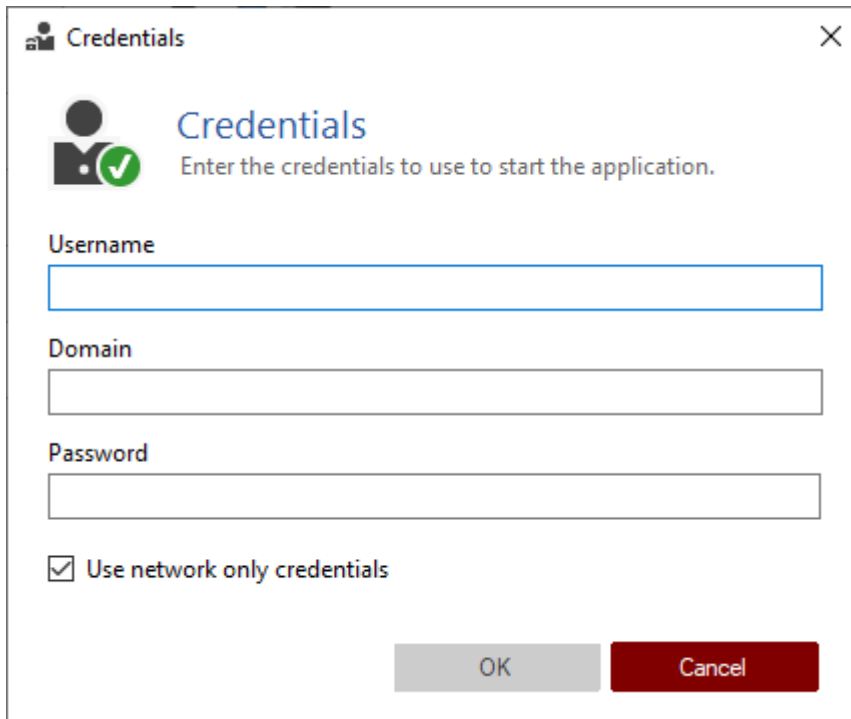
Enables the trace diagnostics log.

Diagnostics > Option Folder

Open the folder where the diagnostics log is stored.

Credentials Form

The credentials form allows you to restart [XIA Configuration Express](#) with the specified credentials.

The image shows a Windows-style dialog box titled "Credentials" with a close button (X) in the top right corner. Inside the dialog, there is a user icon with a green checkmark and the text "Credentials" followed by "Enter the credentials to use to start the application." Below this, there are three text input fields labeled "Username", "Domain", and "Password". At the bottom left, there is a checkbox labeled "Use network only credentials" which is currently checked. At the bottom right, there are two buttons: "OK" (grey) and "Cancel" (red).

Username

The username to use.

Domain

The Active Directory domain name to use either in NetBIOS format or the fully qualified domain name of the domain.

Password

The password to use.

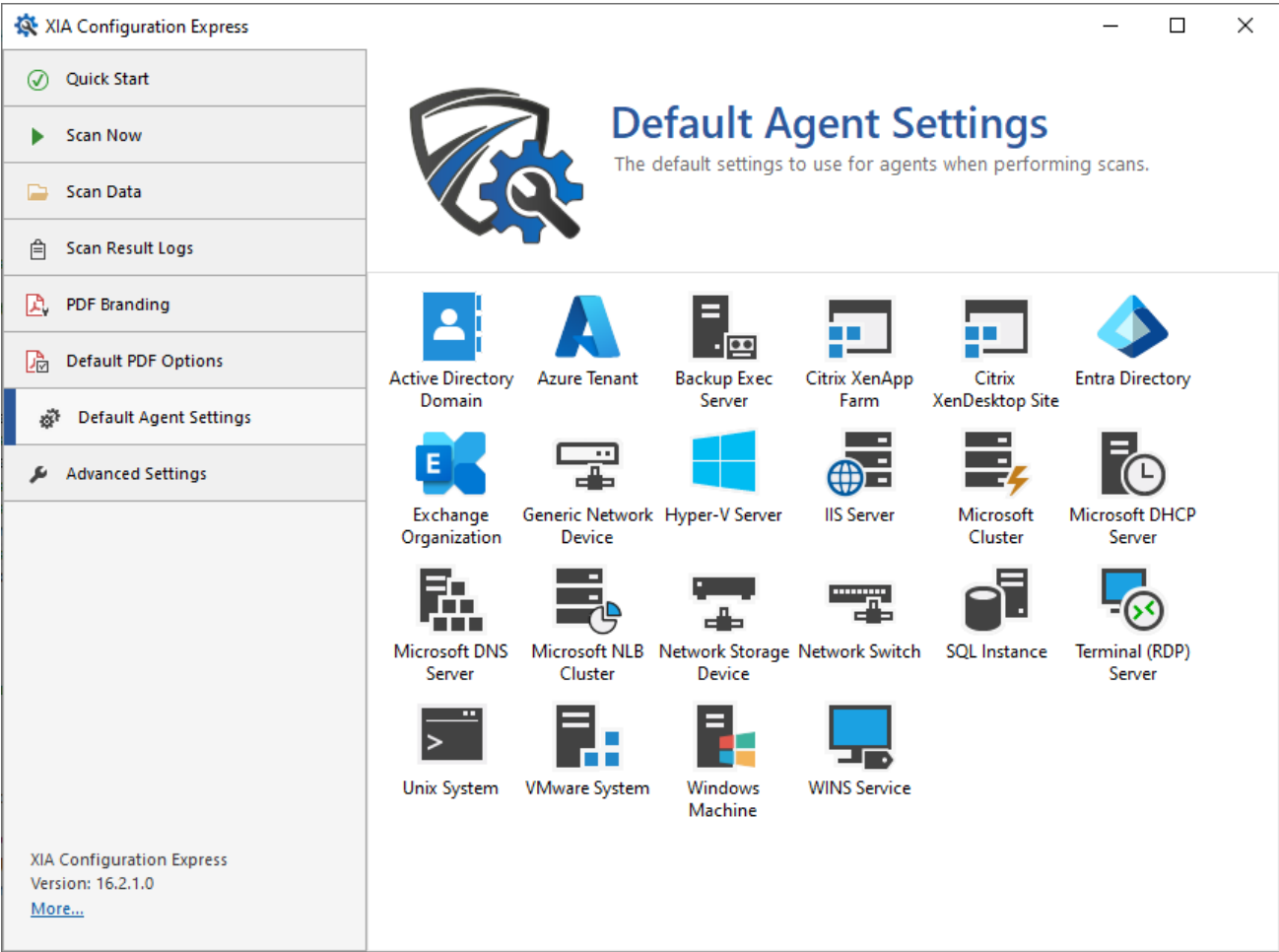
Use Network Only Credentials

Determines whether to restart [XIA Configuration Express](#) with the alternative credentials but only use them when making connections to network resources. This allows credentials to be used when the computer running [XIA Configuration Express](#) need to use credentials in an untrusted domain or workgroup.

This uses the LOGON_NETCREDENTIALS_ONLY parameter of the [CreateProcessWithLogonW](#) method.

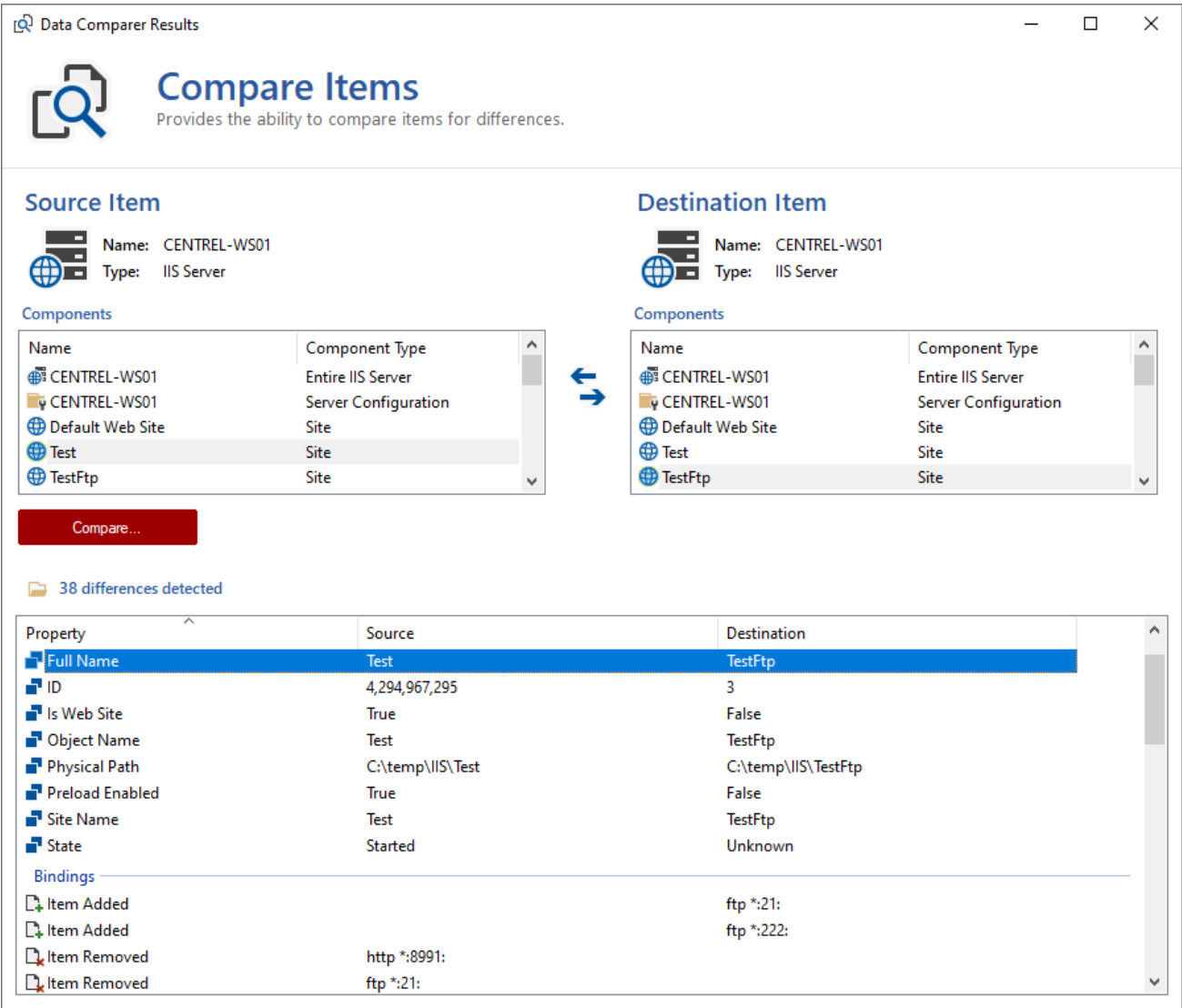
Default Agent Settings

The default agent settings allows the user to view and modify the default settings the agents use when performing a [scan](#).



Compare Items

The compare items user interface allows the comparing two [scan data items](#) or their components.



Source Item

The source [scan data item](#) to compare.

Destination Item

The destination [scan data item](#) to compare.

Components

Certain [scan data items](#) have components that can be compared in addition to the entire [scan data item](#).

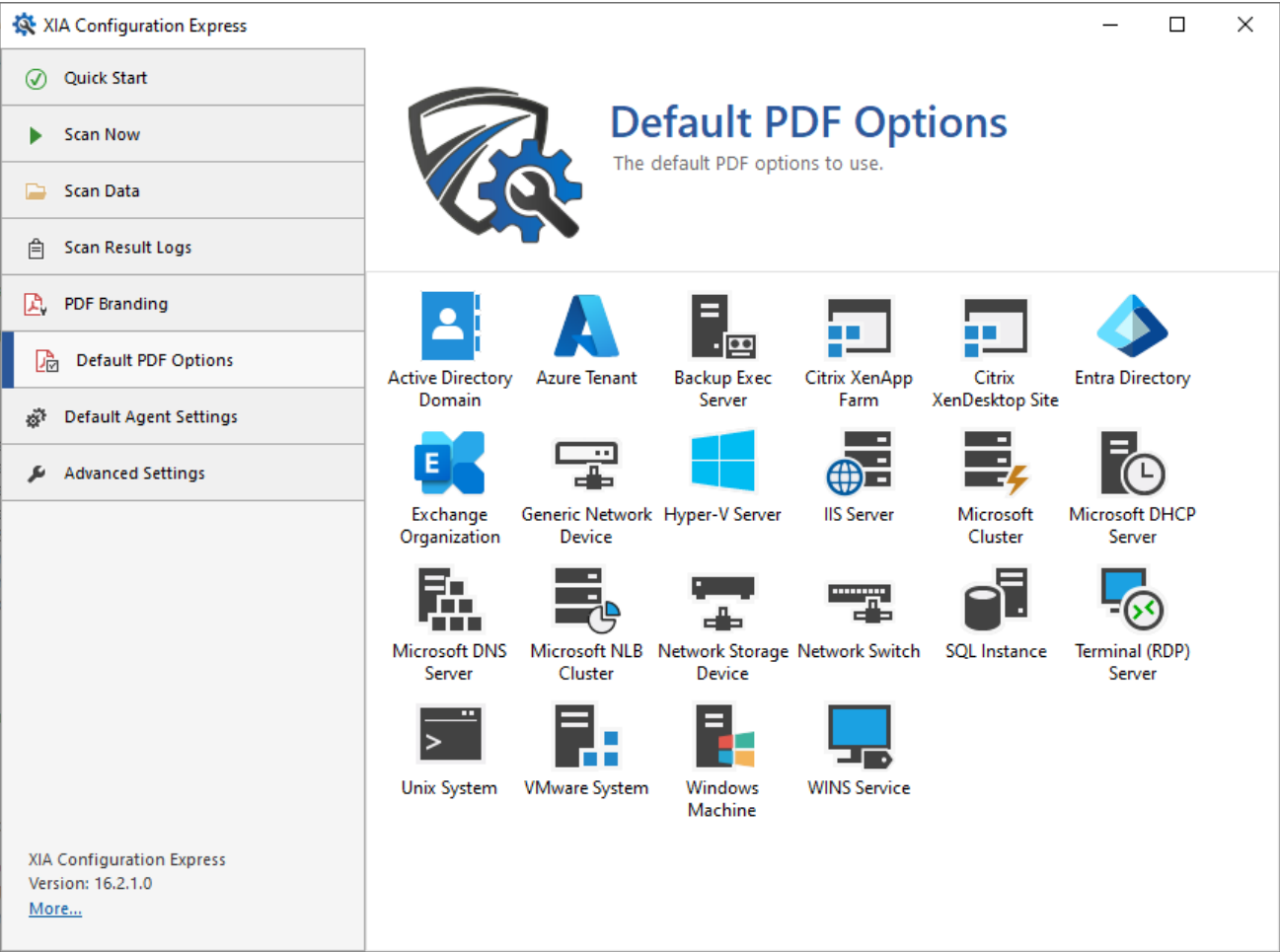
Compare

Clicking the compare button shows the context menu that allows comparing and sending the results

to the screen, a PDF file or an XML file.

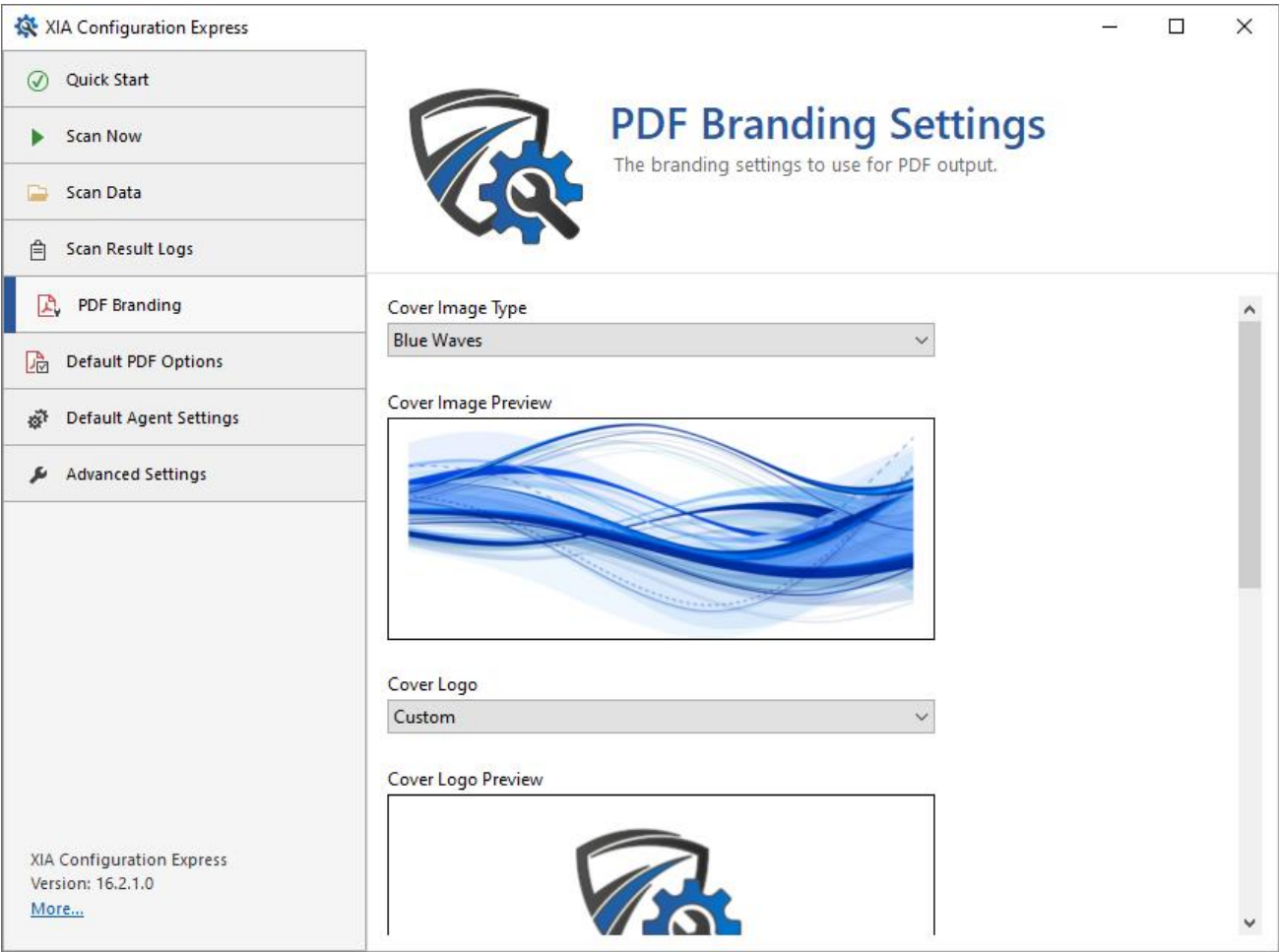
Default PDF Options

The default options to use when generating a PDF of a [scan data item](#).



PDF Branding Settings

The PDF branding settings to use when generating a PDF of a [scan data item](#).



Cover Image Type

The type of image to use on the cover page of the PDF.

Cover Logo

The type of logo to use on the cover page of the PDF.

Disclaimer

The disclaimer text to use for the PDF.

Confidentiality Level

The confidentiality level of the document.

Footer Text

The footer text to display in the PDF document.

Character Support

The character support to use for the PDF.

Watermark

The watermark to use for the PDF.

Edit Colors

Displays the [PDF colors](#) dialog.

PDF Colors

Determines the colors that are used for the [PDF branding settings](#).

PDF Colors



Colors

Select the colors to use for PDF output.

 Restore Defaults

General

Heading



#2354A6

Table Heading Cell



#0054A6

Cover Page

Cover Page Background



#FFFFFF

Footer Background



#FFFFFF

Heading



#2354A6

OK

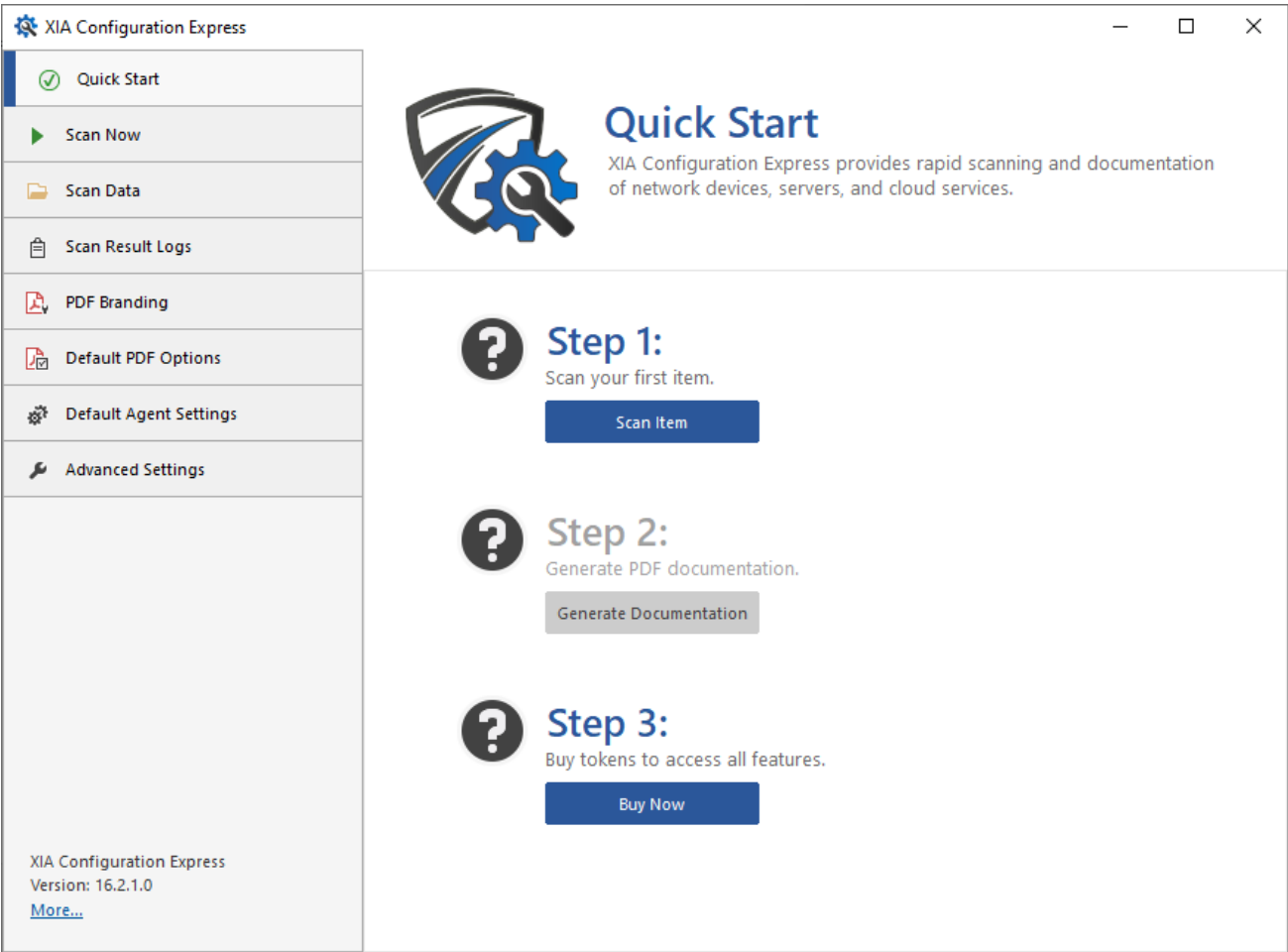
Cancel

Page 1508 of 1553

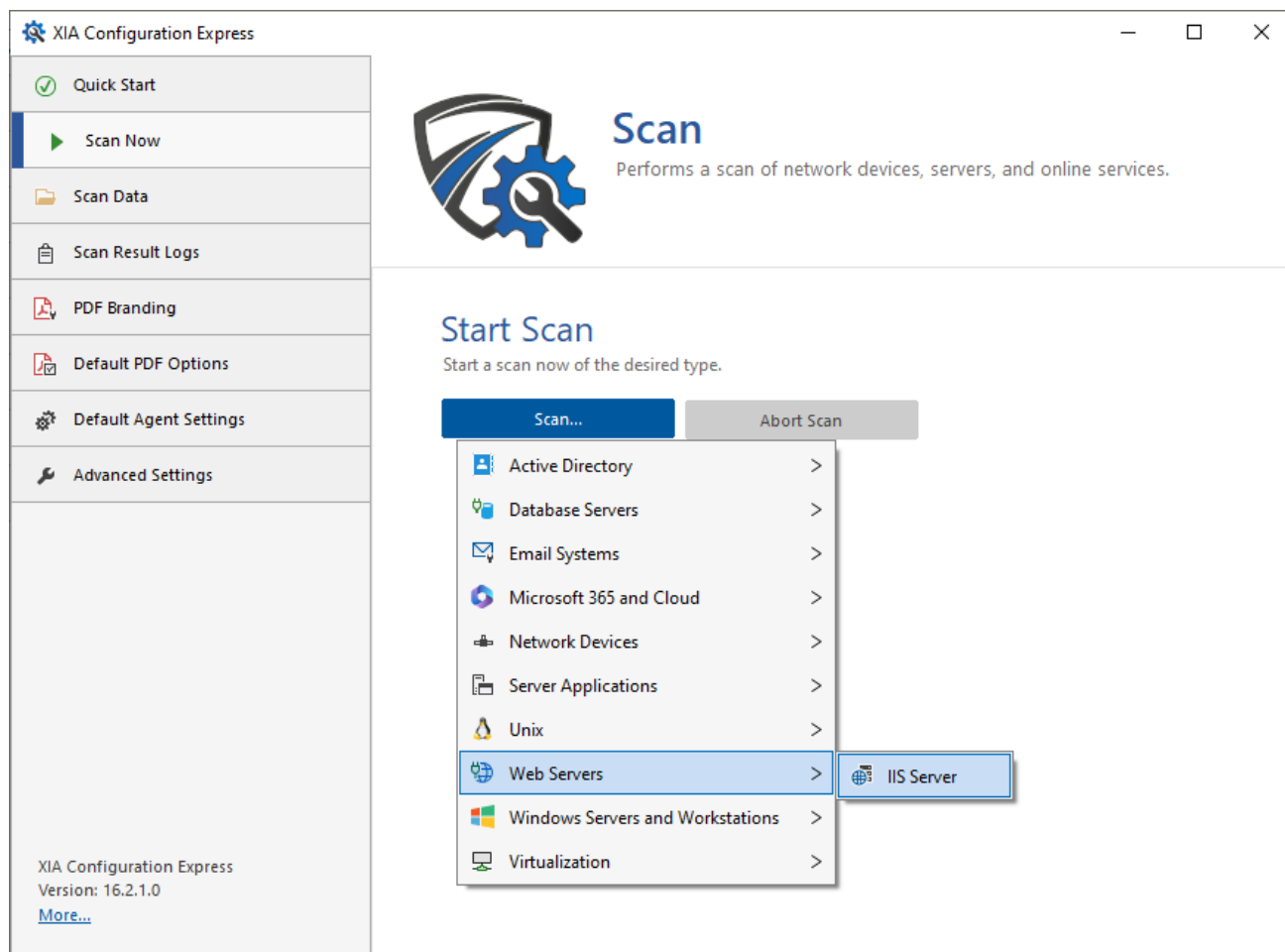
XIA Configuration Administrator's Guide

Quick Start

The Quick Start screen helps you get up and running quickly with [XIA Configuration Express](#).



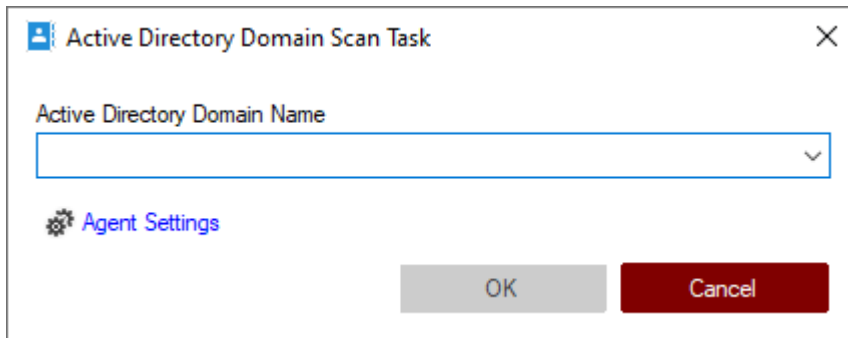
Scanning



Clicking the scan button displays the context menu which displays the types of devices, servers, and cloud services that can be scanned.

Active Directory Domain

The Active Directory domain scan task is able to scan a Microsoft on-premises [Active Directory](#) domain running on [Windows Server](#) 2012 and above using [PowerShell](#).



Active Directory Domain Scan Task

Active Directory Domain Name

Agent Settings

OK Cancel

Active Directory Domain Name

The name of the [Active Directory](#) domain to scan. The name of a domain controller may also be used to perform the scan against a specific machine. The drop down includes the names of detected domains.

Agent Settings

See the [agent settings](#) section.

Requirements

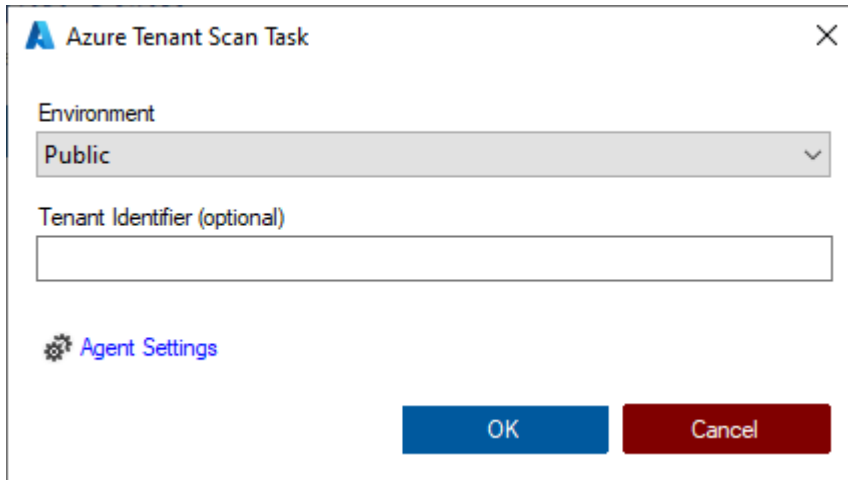
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Azure Tenant

The Azure tenant scan task is able to scan a [Microsoft Azure tenant](#).

The image shows a dialog box titled "Azure Tenant Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Environment" with a dropdown menu currently showing "Public". Below this is a section labeled "Tenant Identifier (optional)" with an empty text input field. At the bottom left, there is a link with a gear icon labeled "Agent Settings". At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (red).

Environment

The [environment](#) to connect to.

Tenant Identifier (Optional)

The optional name or identifier of the tenant (organization).

Agent Settings

See the [agent settings](#) section.

Requirements

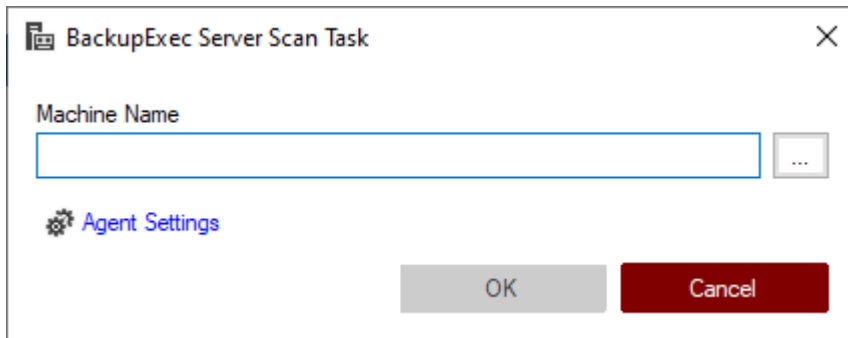
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

BackupExec Server

The [Backup Exec](#) server scan task is able to scan a Backup Exec server version 14.0 and above using [PowerShell](#) remoting.



Machine Name

The name of the [Backup Exec](#) server to scan. Clicking the browse button displays the [Active Directory](#) computer browser.

Agent Settings

See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

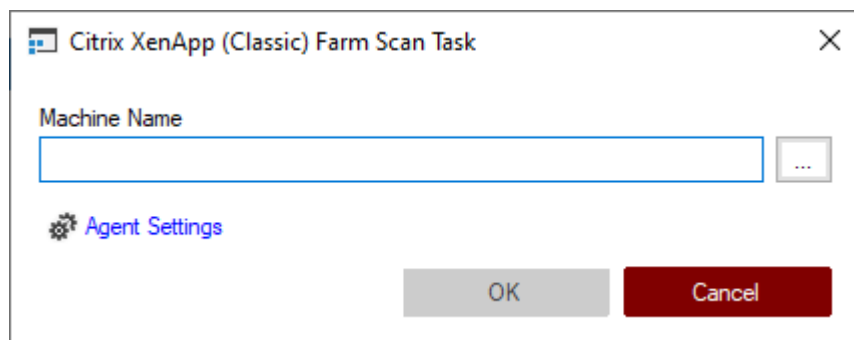
Troubleshooting

See the [troubleshooting](#) section.

Citrix XenApp (Classic) Farm

The Citrix XenApp Farm scan task is able to scan a Citrix XenApp 6.0 or 6.5 farm using [PowerShell remoting](#).

For newer versions of Citrix XenApp and XenDesktop (known as Citrix App and Desktop Virtualization) please see the [Citrix XenDesktop Site](#) scan task.



Machine Name

The name of the server participating in the Citrix XenApp 6.0 or 6.5 farm to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

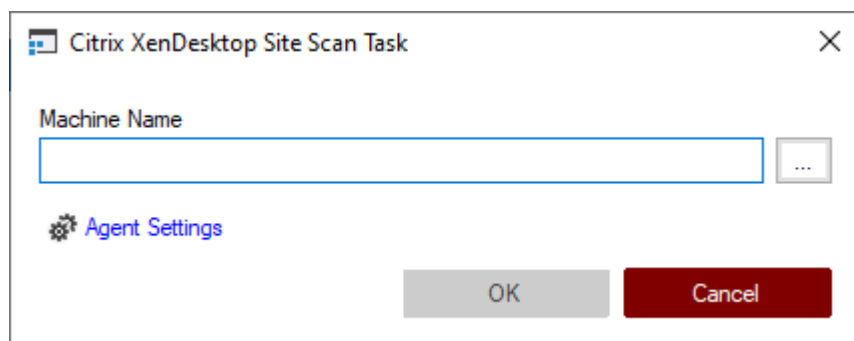
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Citrix XenDesktop Site

The Citrix XenDesktop site scan task is able to scan a Citrix XenDesktop ([Citrix Virtual Apps and Desktops](#)) site using [PowerShell remoting](#).

A screenshot of a Windows-style dialog box titled "Citrix XenDesktop Site Scan Task". It features a close button (X) in the top right corner. Below the title bar, there is a label "Machine Name" above a text input field. To the right of the input field is a small square button with three dots "...". Below the input field, there is a gear icon followed by the text "Agent Settings". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Machine Name

The name of a delivery controller in the Citrix XenDesktop ([Citrix Virtual Apps and Desktops](#)) site to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

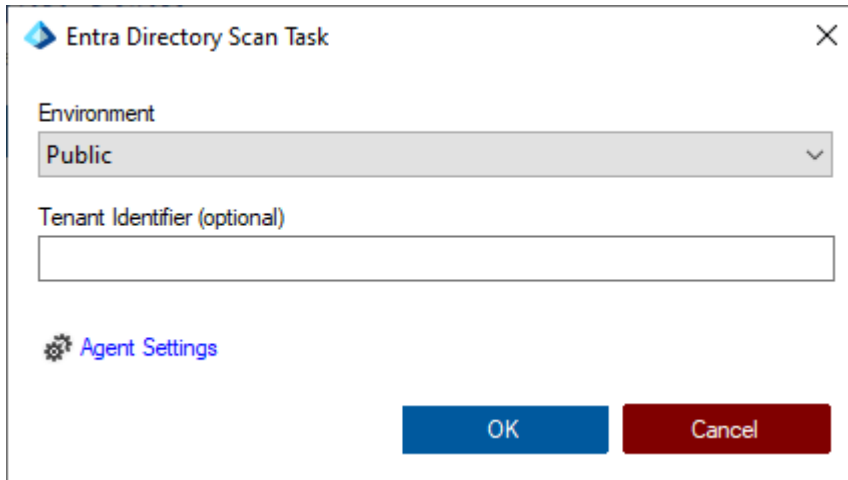
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Entra Directory

The Entra directory scan task is able to scan an [Entra directory](#) also known as a tenant.

A screenshot of a dialog box titled "Entra Directory Scan Task". The dialog has a close button (X) in the top right corner. It contains a label "Environment" above a dropdown menu showing "Public". Below this is a label "Tenant Identifier (optional)" above a text input field. At the bottom left is a link "Agent Settings" with a gear icon. At the bottom right are two buttons: "OK" and "Cancel".

Entra Directory Scan Task

Environment

Public

Tenant Identifier (optional)

Agent Settings

OK Cancel

Environment

The [environment](#) to connect to.

Tenant Identifier (Optional)

The optional name or identifier of the tenant (organization).

Agent Settings

See the [agent settings](#) section.

Requirements

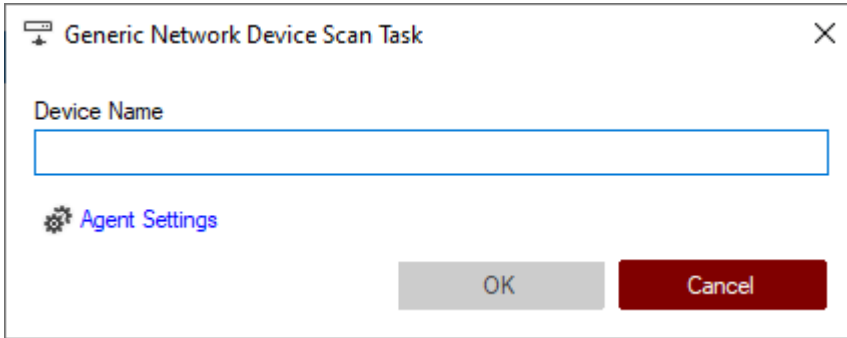
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Generic Network Device

The generic network device scan task is able to scan a network device which is SNMP enabled.



Generic Network Device Scan Task

Device Name

 [Agent Settings](#)

OK Cancel

Device Name

The name or IP address of the device to scan.

Agent Settings

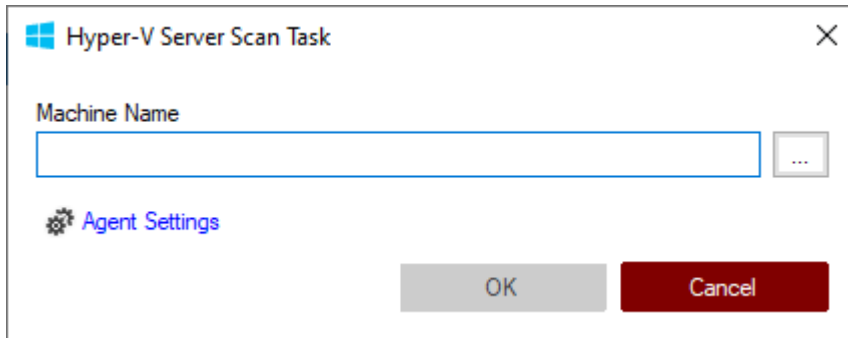
See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

Hyper-V Server

The Hyper-V server scan task is able to scan a [Microsoft Hyper-V server](#).



Machine Name

The name of the [Hyper-V server](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

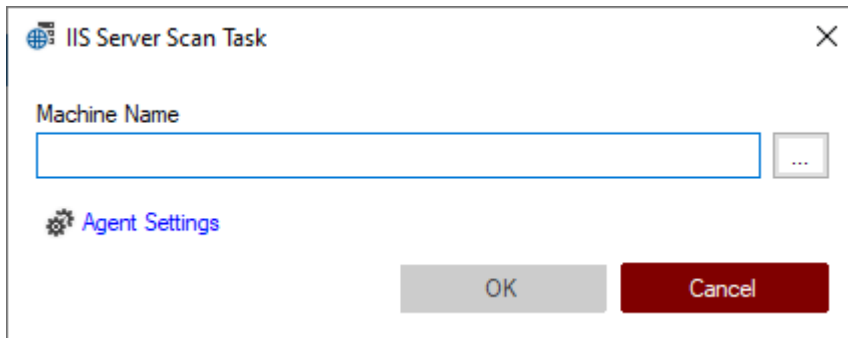
See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

IIS Server

The IIS server scan task is able to scan a [Microsoft Internet Information Services \(IIS\) Server](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).



Machine Name

The name of the [IIS Server](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

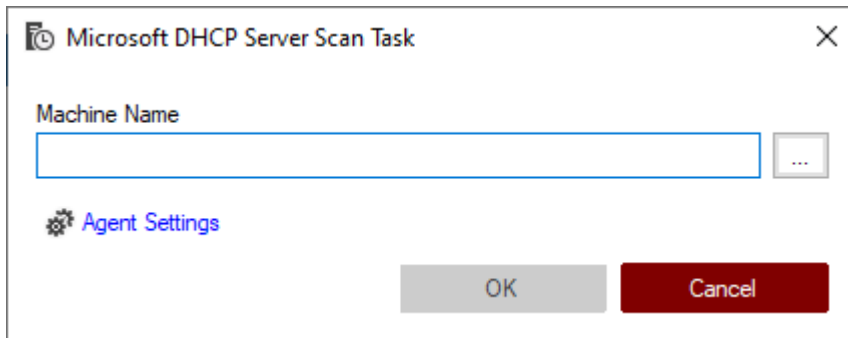
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Microsoft DHCP Server

The Microsoft DHCP server scan task is able to scan a [Microsoft DHCP server](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).

The image shows a dialog box titled "Microsoft DHCP Server Scan Task". It has a close button (X) in the top right corner. Below the title bar, there is a label "Machine Name" followed by a text input field. To the right of the input field is a small square button with three dots "...". Below the input field, there is a gear icon followed by the text "Agent Settings". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Machine Name

The name of the [Microsoft DHCP server](#) to scan. Clicking the browse button displays the [Active Directory](#) computer browser.

Agent Settings

See the [agent settings](#) section.

Requirements

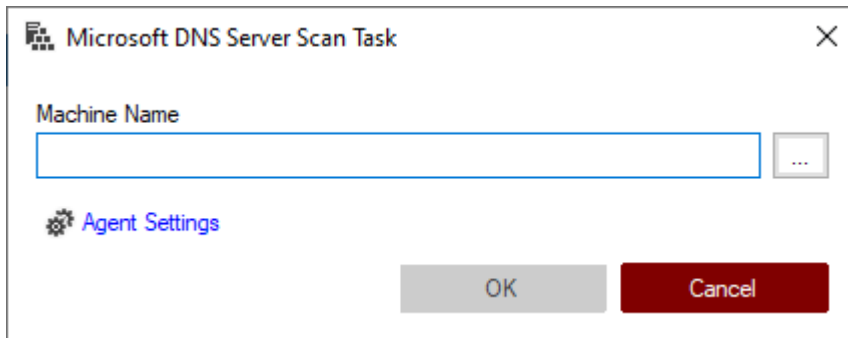
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Microsoft DNS Server

The Microsoft DNS server scan task is able to scan a [Microsoft DNS server](#) running on [Windows Server](#) 2012 and above using [PowerShell remoting](#).



Machine Name

The name of the [Microsoft DNS server](#) to scan. Clicking the browse button displays the [Active Directory](#) computer browser.

Agent Settings

See the [agent settings](#) section.

Requirements

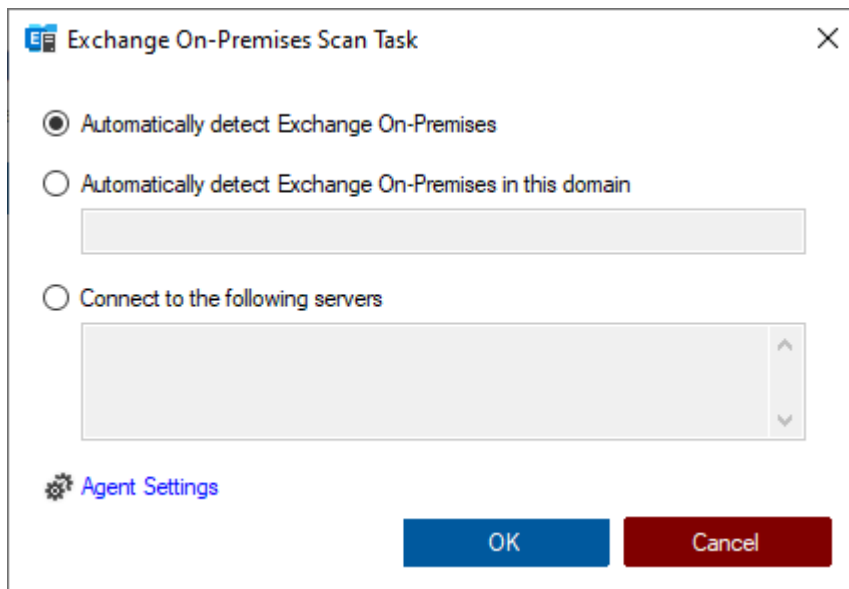
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Microsoft Exchange On-Premises

The Microsoft Exchange on-premises scan task is able to scan a Microsoft Exchange on-premises organization.



Automatically detect Exchange On-Premises

The agent will automatically detect, and attempt to connect to Exchange Servers in the forest of which the computer running [XIA Configuration Express](#) is a member. Server connections are attempted in order of Exchange version number, highest first.

Automatically detect Exchange On-Premises in this domain

The agent will automatically detect, and attempt to connect to Exchange Servers in the parent forest of the specified domain. Server connections are attempted in order of Exchange version number, highest first.

Connect to the following servers

The agent will attempt to connect to the Exchange Servers specified. Server connections are attempted in the order specified.

Agent Settings

See the [agent settings](#) section.

Requirements

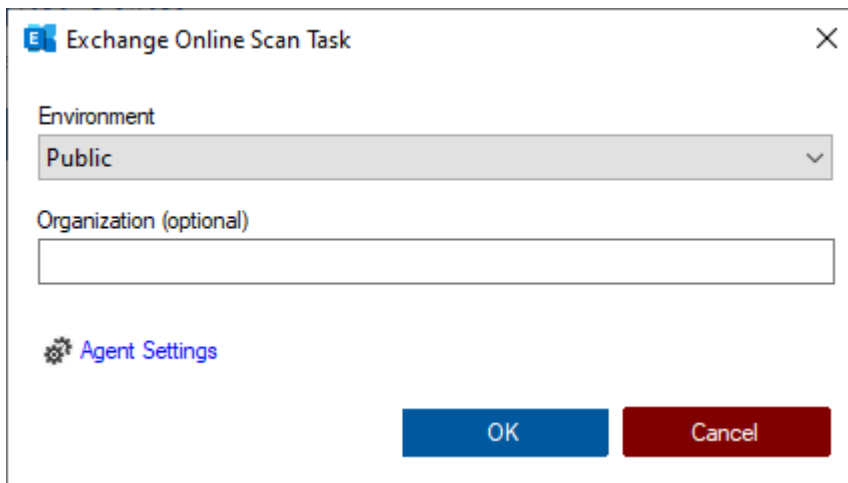
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Microsoft Exchange Online

The Microsoft Exchange Online scan task is able to scan a Microsoft [Exchange Online](#) organization.



The screenshot shows a dialog box titled "Exchange Online Scan Task". It features a close button (X) in the top right corner. Below the title bar, there is a section labeled "Environment" with a dropdown menu currently showing "Public". Underneath this is a section labeled "Organization (optional)" with an empty text input field. Further down is a link labeled "Agent Settings" accompanied by a gear icon. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Environment

The [environment](#) to connect to.

Organization (Optional)

The optional name of the organization (tenant).

Agent Settings

See the [agent settings](#) section.

Requirements

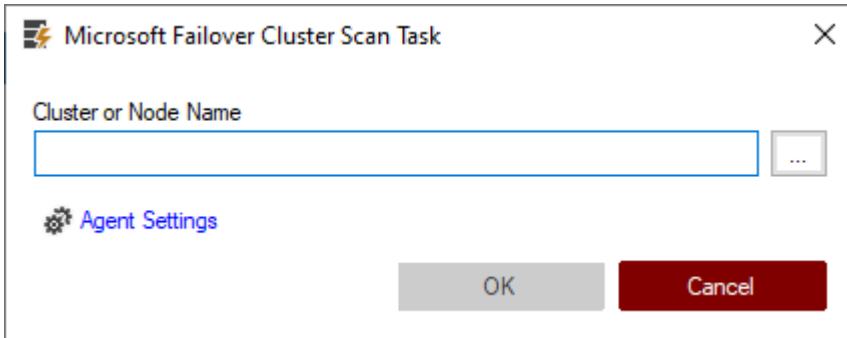
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Microsoft Failover Cluster

The Microsoft failover cluster scan task is able to scan a [Microsoft failover cluster](#) running on [Windows Server](#) 2012 and above.

The image shows a dialog box titled "Microsoft Failover Cluster Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a label "Cluster or Node Name" above a text input field. To the right of the input field is a small square button with three dots "...". Below the input field, there is a link "Agent Settings" preceded by a gear icon. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Cluster or Node Name

The cluster name or the name of any node in the [Microsoft failover cluster](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

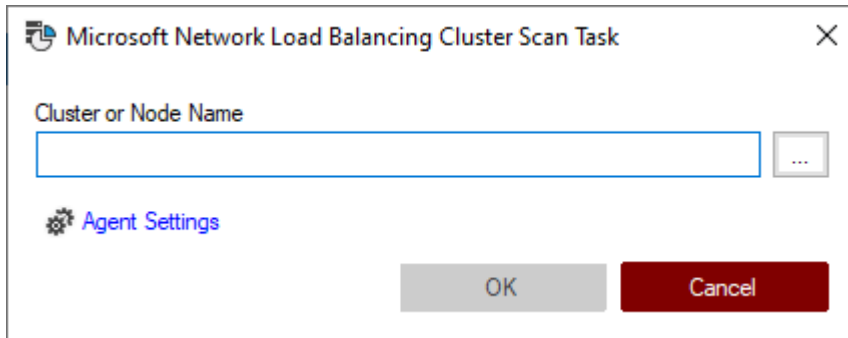
Troubleshooting

See the [troubleshooting](#) section.

Microsoft Network Load Balancing Cluster

The Microsoft network load balancing cluster scan task is able to scan a [Microsoft network load balancing cluster](#) running on [Windows Server](#) 2003 and above.

For information about Microsoft failover clustering support see the [Microsoft failover cluster](#) section.



Cluster or Node Name

The cluster name or the name of any node in the [Microsoft network load balancing cluster](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

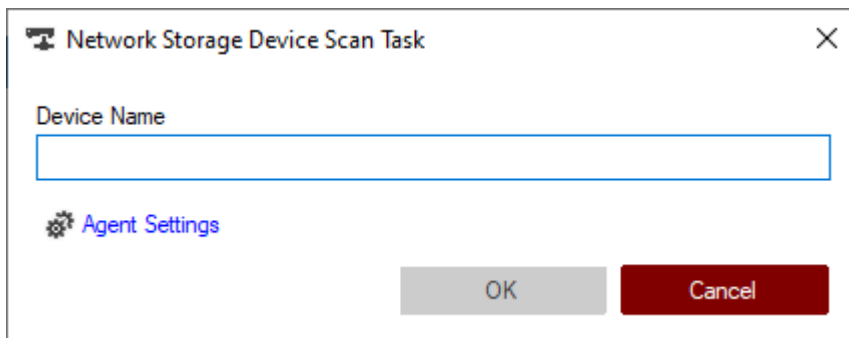
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Network Storage Device

The network storage device scan task is able to scan a [supported](#) network storage device.



The screenshot shows a dialog box titled "Network Storage Device Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a label "Device Name" above a text input field. Below the input field, there is a link "Agent Settings" preceded by a gear icon. At the bottom right of the dialog, there are two buttons: "OK" (gray) and "Cancel" (red).

Device Name

The name or IP address of the network storage device to scan.

Agent Settings

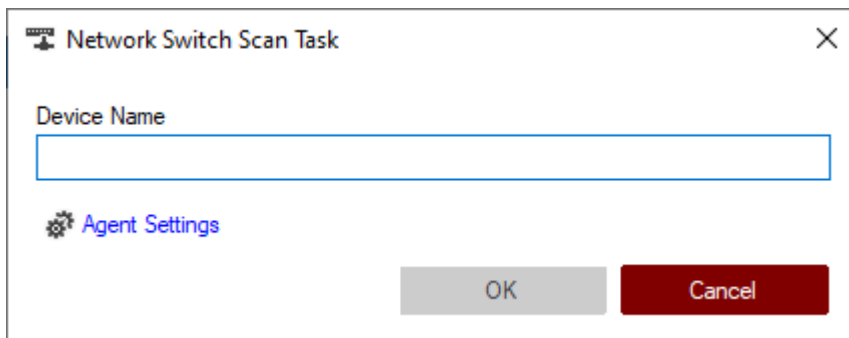
See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

Network Switch

The network switch scan task is able to scan a network switch.



The screenshot shows a dialog box titled "Network Switch Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a label "Device Name" above a text input field. Below the input field, there is a link labeled "Agent Settings" with a gear icon. At the bottom right of the dialog, there are two buttons: "OK" (gray) and "Cancel" (red).

Device Name

The name or IP address of the network switch to scan.

Agent Settings

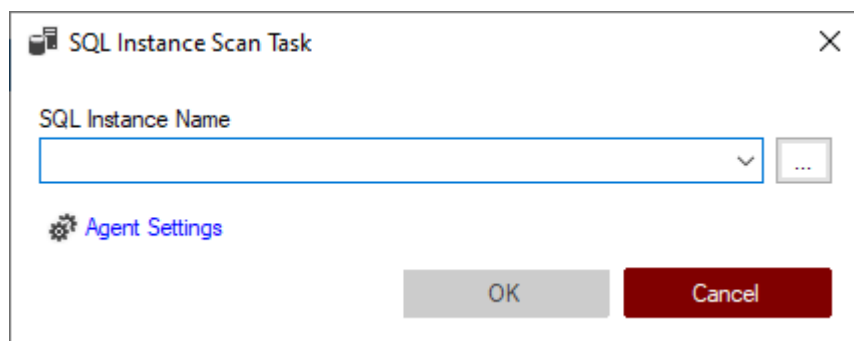
See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

SQL Instance

The SQL instance scan task is able to scan a [Microsoft SQL Server](#) on-premises instance or [Microsoft Azure SQL Server](#).



The screenshot shows a dialog box titled "SQL Instance Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a label "SQL Instance Name" above a text input field. To the right of the input field is a small square button with three dots "...". Below the input field, there is a link "Agent Settings" preceded by a gear icon. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

SQL Instance Name

The instance name of the [Microsoft SQL Server](#) on-premises instance or [Microsoft Azure SQL Server](#) name. Clicking the browse button displays the [Active Directory computer browser](#).

When scanning an [Microsoft Azure SQL Server](#) you may need to provide alternative credentials on the [credentials tab](#) of the [agent settings](#).

Agent Settings

See the [agent settings](#) section.

Requirements

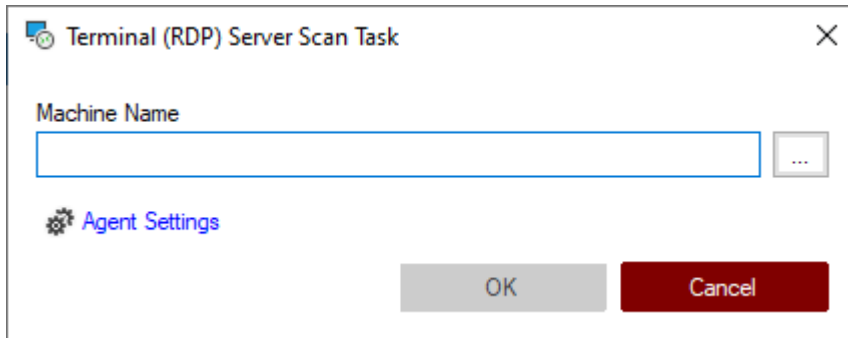
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Terminal (RDP) Server

The Terminal (RDP) Server scan task is able to scan a [Microsoft Remote Desktop session host](#) server.



Machine Name

The name of the [Microsoft Remote Desktop session host](#) server to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

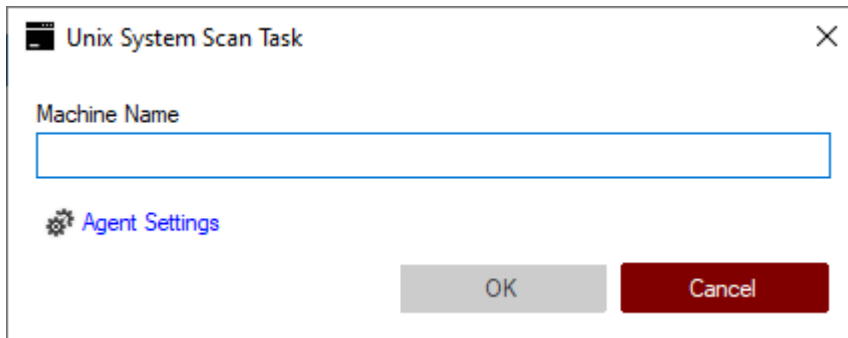
See the [agent settings](#) section.

Requirements

See the [requirements](#) section.

Unix System

The Unix system scan task is able to scan a Unix and Linux platform running [NetBSD](#), [Solaris](#), [RedHat Enterprise Linux](#), [Ubuntu](#), [Fedora](#), and [Debian](#) using [SNMP](#) and [SSH](#).



Unix System Scan Task

Machine Name

Agent Settings

OK Cancel

Machine Name

The name or IP address of the Unix or Linux system to scan.

Agent Settings

See the [agent settings](#) section.

Requirements

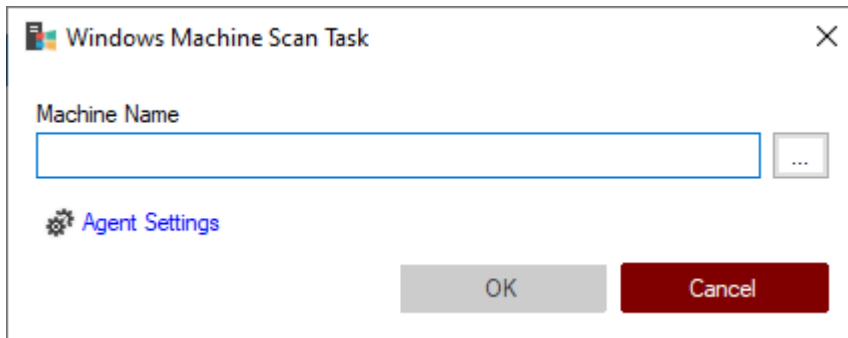
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Windows Machine

The Windows machine scan task is able to scan a [Microsoft Windows server](#) or workstation using classic technologies or [PowerShell remoting](#).



Machine Name

The name of the [Microsoft Windows server](#) or workstation to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

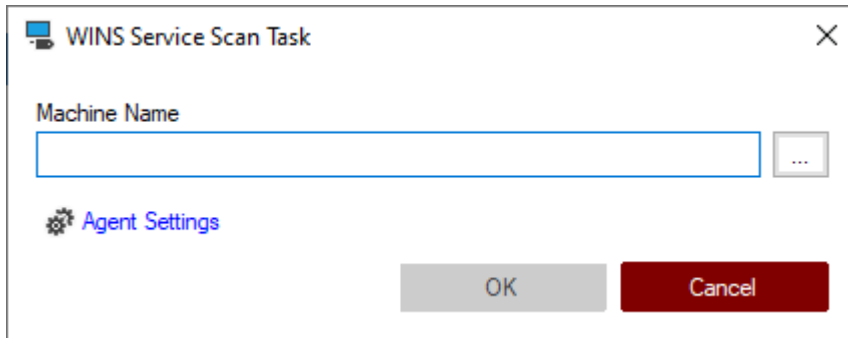
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

WINS Service

The WINS service scan task is able to scan a [WINS service](#).



Machine Name

The name of the [WINS server](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Agent Settings

See the [agent settings](#) section.

Requirements

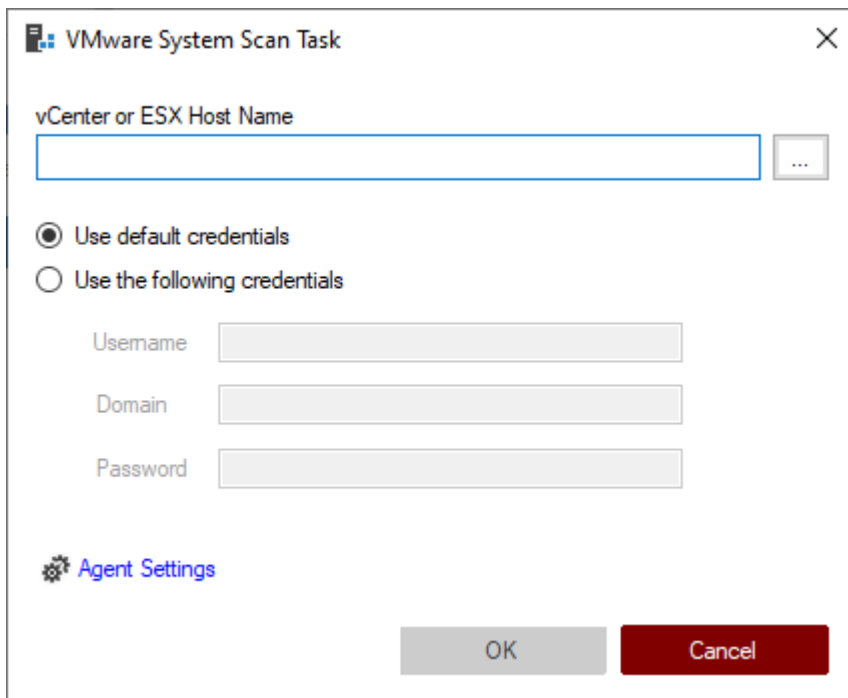
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

VMware System

The VMware system scan task is able to scan a [VMware vCenter server](#) or [ESXi host](#).



The screenshot shows a dialog box titled "VMware System Scan Task" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "vCenter or ESX Host Name" with a browse button (three dots) to its right. Below this, there are two radio buttons: "Use default credentials" (which is selected) and "Use the following credentials". Under the "Use the following credentials" option, there are three text input fields labeled "Username", "Domain", and "Password". At the bottom left, there is a link labeled "Agent Settings" with a gear icon. At the bottom right, there are two buttons: "OK" and "Cancel".

vCenter or ESX Host Name

The name of the [VMware vCenter server](#) or [ESXi host](#) to scan. Clicking the browse button displays the [Active Directory computer browser](#).

Use Default Credentials

The currently logged on user's credentials are used to connect to the vCenter server. This setting does not apply when connecting directly to an ESXi host.

Use Specific Credentials

Determines the credentials to use when connecting to the [VMware vCenter server](#) or [ESXi host](#).

Agent Settings

See the [agent settings](#) section.

Requirements

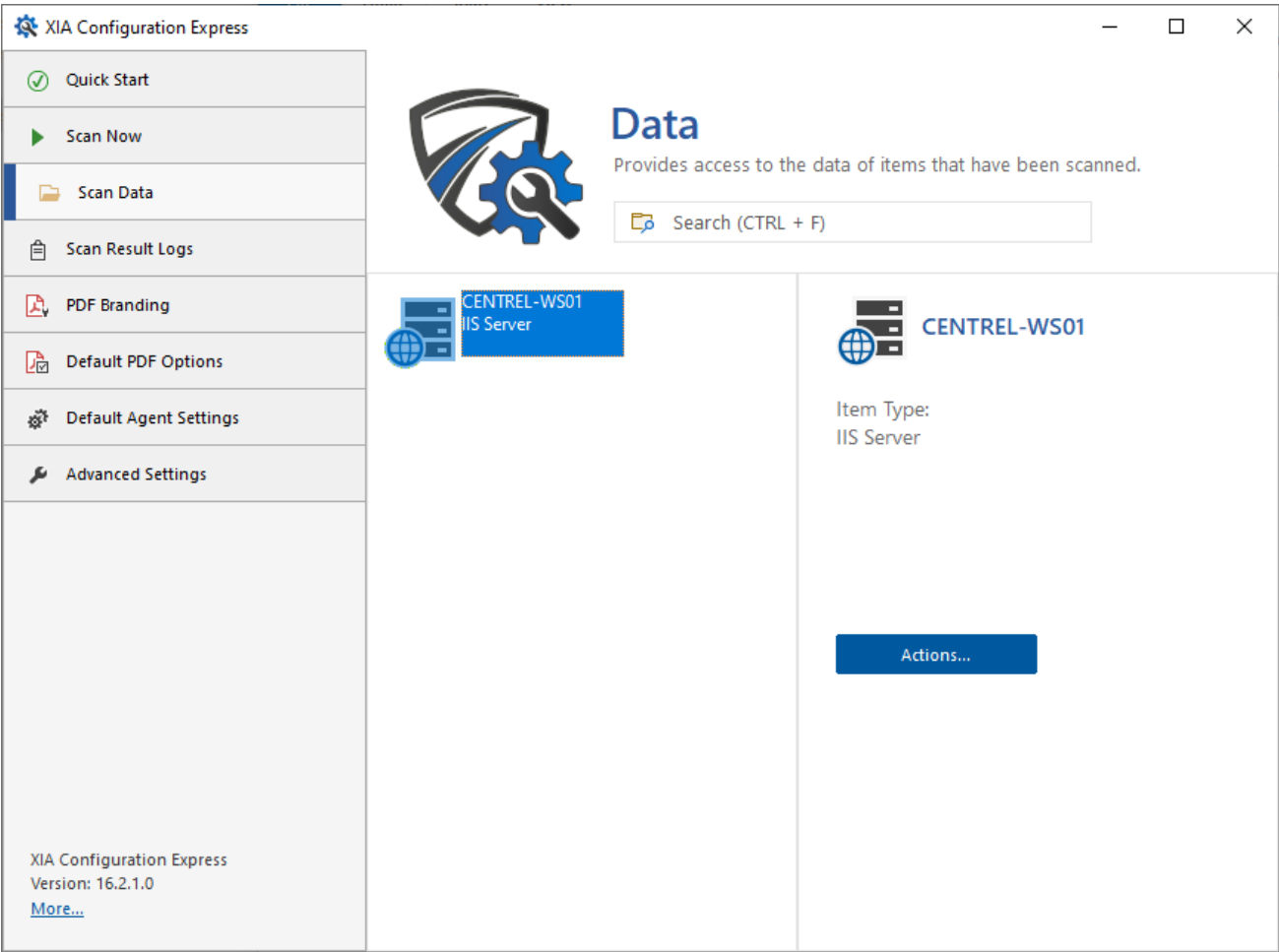
See the [requirements](#) section.

Troubleshooting

See the [troubleshooting](#) section.

Scan Data

The scan data displays the information that has been collected by the [scans](#).



Item Name

The name of the item that was [scanned](#).

Item Type

The type of item that was [scanned](#).

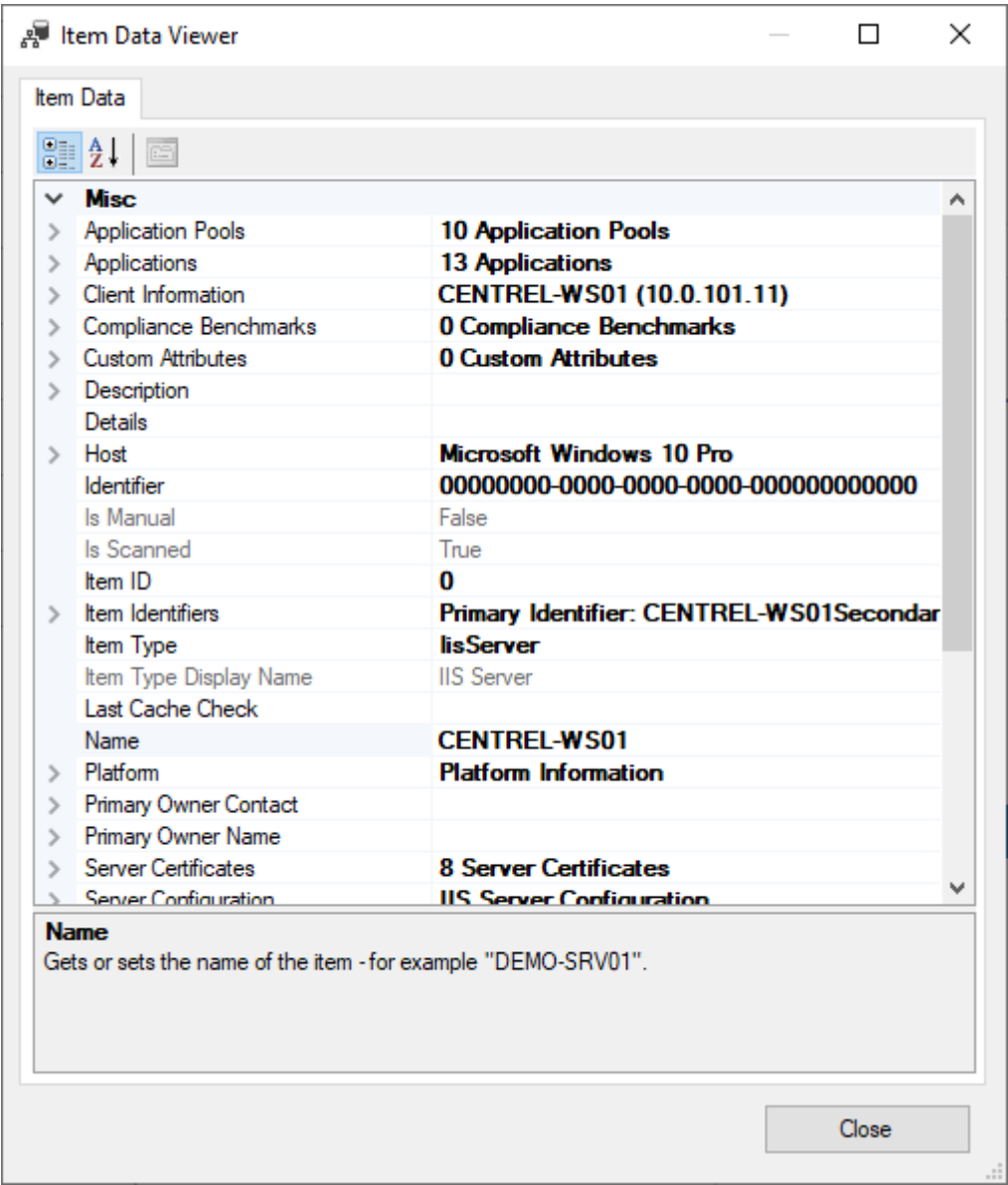
Actions

Clicking the actions button displays the [scan data actions context menu](#).

Right clicking an item displays the [scan data context menu](#).

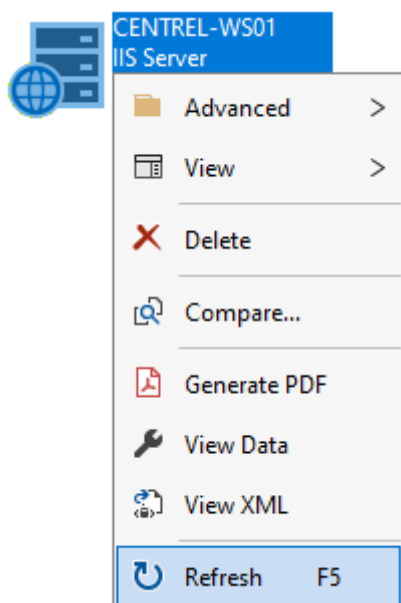
Item Data Viewer

The item data viewer displays the information from an item in the [scan data](#) user interface.



Scan Data Context Menu

The scan data context menu is displayed when a user right clicks an item in the [scan data](#) user interface.



Advanced > Open Folder In Explorer

Opens the folder that holds the scan data in Windows explorer.

Advanced > Rebuild Index

Re-reads the data files in the scan data folder and rebuilds the index.

View > Details

Displays the results in details view.

View > Tiles

Displays the results as tiles.

Delete

Deletes the currently selected scan data item(s).

Compare

Opens the currently selected item(s) in the [compare items dialog](#). This menu item is only available when either a single item or two items of the same type are selected. When a single item is selected you are able to compare components within the item with other components of this item.

Generate PDF

Generates PDF documentation of the currently selected item. This only applies when a single item is selected.

View Data

Displays the item in the [item data viewer](#).

View XML

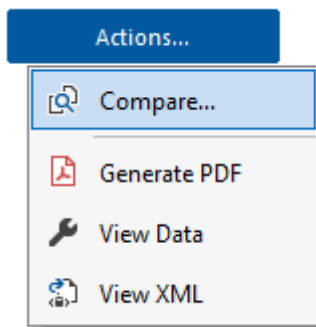
Displays the scan data item in XML format.

Refresh

Refreshes the view.

Scan Data Actions Context Menu

The scan data context menu is displayed when a user clicks the actions button in the [scan data](#) user interface.



Compare

Opens the currently selected item(s) in the [compare items dialog](#). This menu item is only available when either a single item or two items of the same type are selected. When a single item is selected you are able to compare components within the item with other components of this item.

Generate PDF

Generates PDF documentation of the currently selected item. This only applies when a single item is selected.

View Data

Displays the item in the [item data viewer](#).

View XML

Displays the scan data item in XML format.

Scan Result Logs

The scan results logs display information about the [scans](#) that have been performed and any issues encountered.

XIA Configuration Express

Quick Start

Scan Now

Scan Data

Scan Result Logs

PDF Branding

Default PDF Options

Default Agent Settings

Advanced Settings

XIA Configuration Express

Version: 16.2.1.0

[More...](#)



Scan Result Logs

The results of previous scans.

Item Name	Item Type	Finish Time	Scan Time	Status
 localhost	IIS Server	04 September 2024 15:34:08	32 seconds ...	Success (Warnings)

Item Name

The name of the item that was [scanned](#).

Item Type

The type of item that was [scanned](#).

Finish Time

The date and time the [scan](#) completed.

Scan Time

The total time that elapsed during the [scan](#).

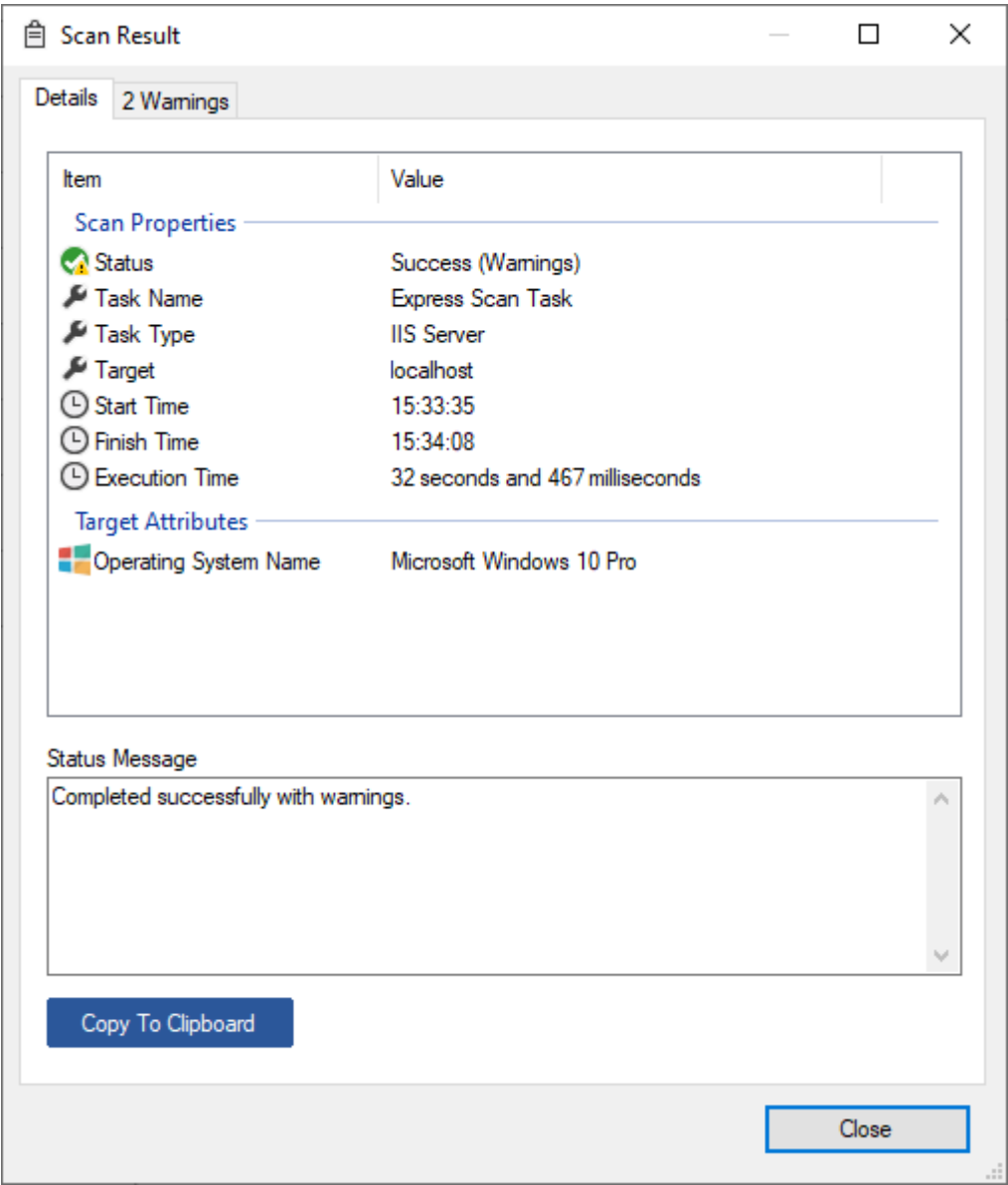
Status

The status of the [scan](#).

Right clicking a scan result log displays the [scan result log context menu](#).

Scan Result Details

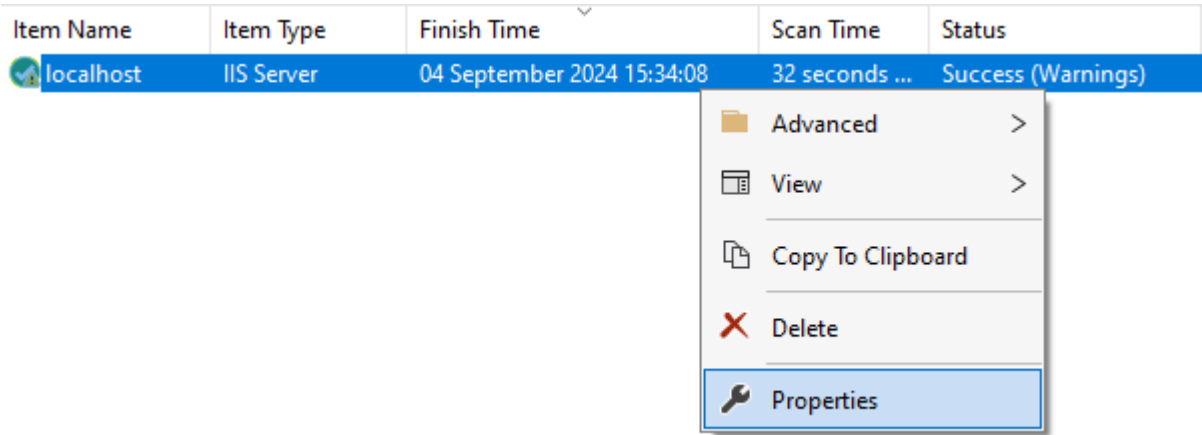
The scan result details dialog displays the full information about the [scan result](#).



For more information see the [scan result details](#) section.

Scan Result Log Context Menu

The scan result log context menu is displayed when a user right clicks a [scan result log](#) in the user interface.



Advanced > Open Folder In Explorer

Opens the folder that holds the scan results in Windows explorer.

View > Details

Displays the results in details view.

View > Tiles

Displays the results as tiles.

Copy To Clipboard

Copies the details of the selected scan results(s) to the clipboard.

Delete

Deletes the selected scan result(s).

Properties

Displays the properties of the scan result in the [scan result details dialog](#).

End User License Agreement

(EULA)

CENTREL SOLUTIONS LTD

XIA Configuration Server

Copyright © 2008-2025 CENTREL Solutions Ltd

END-USER LICENSE AGREEMENT

Last revised 15th January 2025

IMPORTANT - PLEASE READ THIS END-USER LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE PRODUCT INCLUDED IN THE INSTALLATION.

This CENTREL Solutions Ltd ("CENTREL SOLUTIONS") AGREEMENT constitutes a legally binding agreement between you or the business and/or entity which you represent ("YOU" or "LICENSEE") and CENTREL SOLUTIONS for the XIA Configuration Server product and related demonstration code, intermediate files, and documentation ("SOFTWARE PRODUCT") included in the installation.

By purchasing, installing, copying, or otherwise using the SOFTWARE PRODUCT, YOU acknowledge that YOU have read this AGREEMENT and YOU agree to be bound by its terms and conditions. If YOU are representing a business and/or entity, YOU acknowledge that YOU have the legal authority to bind the business and/or entity YOU are representing to all the terms and conditions of this AGREEMENT.

If YOU do not agree to any of the terms and conditions of this AGREEMENT or if YOU do not have the legal authority to bind the business and/or entity YOU are representing to any of the terms and conditions of this AGREEMENT, DO NOT INSTALL, COPY, USE, EVALUATE, OR REPLICATE IN ANY MANNER, ANY PART, FILE OR PORTION OF THE SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE.

Subject to all the terms and conditions of this AGREEMENT, CENTREL SOLUTIONS grants the LICENSEE a non-exclusive, non-transferable license to install and use the SOFTWARE PRODUCT included in the installation as authorized in this section.

The SOFTWARE PRODUCT stores information about individual items (“ITEMS”) including, but not limited to, network switches, network storage devices, Microsoft® Windows® servers, and Microsoft® SQL databases.

1.1 ENTERPRISE LICENSE.

YOU may install, copy, and use the SOFTWARE PRODUCT by purchasing an ENTERPRISE LICENSE from CENTREL SOLUTIONS or its authorized resellers.

The number of ITEMS permitted will be specified by count in the LICENSE. The LICENSEE must not attempt to exceed the number of ITEMS specified in the LICENSE.

The SOFTWARE PRODUCT of a version released prior to the SUPPORT expiry date specified in the LICENSE may be installed on a single machine in the Active Directory domain specified in the LICENSE, or on the machine with the NetBIOS name specified in the LICENSE.

The SOFTWARE PRODUCT may be installed on an additional machine in the Active Directory domain of the name specified in the LICENSE for the purposes of resilience as long as this does not permit the LICENSEE from exceeding the number of ITEMS specified in the LICENSE.

1.2 UNLIMITED LICENSE.

YOU may install, copy, and use the SOFTWARE PRODUCT by purchasing an UNLIMITED LICENSE from CENTREL SOLUTIONS or its authorized resellers.

The LICENSEE must only store information about ITEMS that are owned by the LICENSEE, or where the LICENSEE is a managed service provider (MSP) and is the primary technical support provider for the ITEM.

If the LICENSE stipulates additional terms such as, but not limited to, a geographical or project based limitation of use, these will be visible in the “Notes” field of the LICENSE and the LICENSEE must adhere to these additional terms.

The SOFTWARE PRODUCT of a version released prior to the SUPPORT expiry date specified in the LICENSE may be installed on a single machine in the Active Directory domain specified in the LICENSE, or on the machine with the NetBIOS name specified in the LICENSE.

The SOFTWARE PRODUCT may be installed on an additional machine in the Active Directory domain named in the LICENSE for the purposes of resilience only.

The price of the UNLIMITED LICENSE is based on information about the organization named in the LICENSE which is provided by the LICENSEE.

If the information provided by the LICENSEE to CENTREL SOLUTIONS is found to contain inaccuracies including, but not limited to, Windows server, customer, or virtualization host numbers, CENTREL SOLUTIONS shall be entitled to charge, and the LICENSEE shall pay, an amount equal to such underpayment as calculated in accordance with the price of the SOFTWARE PRODUCT had such information provided by the LICENSEE been correct. If the LICENSEE fails to pay such additional fees CENTREL SOLUTIONS will terminate this AGREEMENT. In such events, the LICENSEE must destroy all copies of the SOFTWARE PRODUCT and all of its component parts including any related documentation.

The LICENSEE agrees to periodically provide information about their usage of the SOFTWARE PRODUCT to ensure that the terms of the UNLIMITED LICENSE are met.

The LICENSEE may not assign or transfer the LICENSE to succeeding parties in the case of a merger, acquisition or change of control of the LICENSEE (within the meaning of section 1124 of the Corporation Tax Act 2010). CENTREL SOLUTIONS should be notified in writing within ninety (90) days of such an eventuality. A new UNLIMITED LICENSE should be purchased for the succeeding parties, or the SOFTWARE PRODUCT must be uninstalled and all copies destroyed.

1.3 TECHNICIAN LICENSE.

YOU may install, copy, and use the SOFTWARE PRODUCT by purchasing a TECHNICIAN LICENSE from CENTREL SOLUTIONS or its authorized resellers. YOU may install, copy, and use the SOFTWARE PRODUCT for 12 months from the date that the LICENSE is purchased ("USAGE PERIOD"). Upon expiration of the USAGE PERIOD, a new LICENSE should be purchased, or the SOFTWARE PRODUCT must be uninstalled and all copies destroyed.

The SOFTWARE PRODUCT of a version not exceeded by the LICENSE may be installed on the single machine named in the LICENSE.

The SOFTWARE PRODUCT may ONLY be used by the individual named in the LICENSE.

The SOFTWARE PRODUCT may ONLY be accessed from the machine named in the LICENSE.

1.4 EVALUATION (TRIAL) USE LICENSE.

If the LICENSE YOU have obtained is marked as a "TRIAL" or "EVALUATION", YOU may install the SOFTWARE PRODUCT for evaluation purposes only, for the period set within the LICENSE

("EVALUATION PERIOD"). Upon expiration of the EVALUATION PERIOD, a LICENSE should be purchased, or the SOFTWARE PRODUCT must be uninstalled and all copies destroyed.

YOU MAY NOT CREATE or ATTEMPT TO CREATE final end user documentation using the SOFTWARE PRODUCT under the terms of the EVALUATION (TRIAL) USE LICENSE.

YOU MAY NOT REDISTRIBUTE files or other outputs created by the SOFTWARE PRODUCT if using an EVALUATION (TRIAL) USE LICENSE.

1.5 WORKGROUP LICENSE.

If the LICENSE YOU have obtained is marked as a "Workgroup" or "WORKGROUP EDITION", YOU may install the SOFTWARE PRODUCT without charge, for the period set within the LICENSE ("LICENSE PERIOD").

The SOFTWARE PRODUCT may ONLY be used by the organization named in the LICENSE.

The number of ITEMS permitted will be specified by count in the LICENSE. The LICENSEE must not attempt to exceed the number of ITEMS specified in the LICENSE.

The number of ITEMS permitted may be revised in future versions of the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT of a version not exceeded by the LICENSE may be installed on a single machine with the NetBIOS name specified in the LICENSE.

The SOFTWARE PRODUCT may exhibit additional limitations of functionality compared to other LICENSE types.

1.6 PRE-RELEASE SOFTWARE

The SOFTWARE PRODUCT marked as PRE-RELEASE (including but not limited to the designation of BETA, Community Technology Preview "CTP", or Release Candidate "RC") may contain deficiencies and as such, should not be considered for use in any production environment.

CENTREL SOLUTIONS may, at its sole discretion, discontinue availability of the PRE-RELEASE software, limit or modify PRE-RELEASE software functionality, or eliminate SUPPORT SERVICES for the PRE-RELEASE software at any time.

2. LIMITATIONS ON REVERSE ENGINEERING, DECOMPIlation, AND DISASSEMBLY.

YOU may not reverse engineer, decompile, create derivative works or disassemble the SOFTWARE PRODUCT. If the SOFTWARE PRODUCT is purchased by YOU with the intent to reverse engineer, decompile, create derivative works, or the exploitation and unauthorized transfer of any CENTREL SOLUTIONS intellectual property and trade secrets, to include any exposed methods or source code where provided, no licensed right of use shall exist and any PRODUCT(s) created as a result shall be judged illegal by definition.

Any sale or resale of intellectual property or created derivatives so obtained will be prosecuted to the fullest extent of all local, federal and international law.

3. SEPARATION OF COMPONENTS.

The SOFTWARE PRODUCT is licensed as a single PRODUCT. The SOFTWARE PRODUCT and its constituent parts may not be reverse engineered, decompiled, disassembled or separated for use on more than one computer, nor placed for distribution, sale, or resale as individual creations by the LICENSEE.

4. RENTAL.

YOU may not rent, lease, or lend the SOFTWARE PRODUCT.

5. TRANSFER.

Notwithstanding the provisions in clause 1.2, YOU may NOT permanently or temporarily transfer ANY of YOUR rights under this AGREEMENT to any individual, business, government entity or other organization without prior written approval from CENTREL SOLUTIONS.

6. COPYRIGHT.

YOU acknowledge that CENTREL SOLUTIONS is the owner or licensor of all intellectual property rights in the SOFTWARE PRODUCT anywhere in the world, that rights in the SOFTWARE PRODUCT are licensed (not sold) to you, and that you have no rights in, or to, the SOFTWARE PRODUCT other than the right to use them in accordance with the terms of this AGREEMENT and the relevant LICENSE.

YOU acknowledge that you have no right to have access to the SOFTWARE PRODUCT in source code form.

7. TWELVE (12) MONTH SUPPORT AND UPDATES.

CENTREL SOLUTIONS licenses the SOFTWARE PRODUCT on a subscription basis. A subscription lasts for a 12 month period from the date of purchase. The LICENSEE will be eligible to receive all major and minor updates for the SOFTWARE PRODUCT during this 12 month period.

Upon expiration of a subscription, the LICENSEE can optionally renew the SOFTWARE PRODUCT subscription for an additional 12 month period (and each subsequent year thereafter) in order to continue receiving major and minor updates of the SOFTWARE PRODUCT from CENTREL SOLUTIONS.

Pricing for the 12 month SOFTWARE PRODUCT subscription is charged at 20% of the total cost of the LICENSE. CENTREL SOLUTIONS reserves the right to change the price of any subsequent renewal of the SOFTWARE PRODUCT subscription.

The LICENSEE must maintain the 12 month SOFTWARE PRODUCT subscriptions contiguously with a break of no more than 31 days. If the break exceeds 31 days the LICENSEE must purchase a new LICENSE to renew the SOFTWARE PRODUCT subscription.

CENTREL SOLUTIONS does not provide SUPPORT when the SOFTWARE PRODUCT is used in conjunction with a LICENSE which is marked as a "Workgroup" or "WORKGROUP EDITION" LICENSE.

When the SOFTWARE PRODUCT is used in conjunction with a TECHNICIAN LICENSE, CENTREL SOLUTIONS will only provide SUPPORT to the individual named on the LICENSE.

CENTREL SOLUTIONS reserves the right to discontinue the SOFTWARE PRODUCT or its constituents, at any time. The LICENSEE will be entitled to use the legacy version of the SOFTWARE PRODUCT in perpetuity but at the LICENSEE's own risk.

8. DOWNLOAD of SOFTWARE PRODUCT.

The SOFTWARE PRODUCT will be made available for download from the CENTREL SOLUTIONS web site exclusively.

9. DISCLAIMER OF WARRANTY.

CENTREL SOLUTIONS expressly disclaims any warranty for the SOFTWARE PRODUCT. THE SOFTWARE PRODUCT (INCLUDING ANY THIRD PARTY CONTROLS), AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. CENTREL SOLUTIONS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS

OF THE USE, OF THE SOFTWARE PRODUCT IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT REMAINS WITH YOU. No oral or written information or advice given by CENTREL SOLUTIONS or its employees shall create a warranty or in any way increase the scope of this warranty.

9.1. VIRUSES.

CENTREL SOLUTIONS will make commercially reasonable efforts to ensure that the SOFTWARE PRODUCT as delivered by CENTREL SOLUTIONS will not contain any virus, or other software designed to permit unauthorized access to, or to erase or otherwise harm, the LICENSEE's software, hardware, or data.

10. LIMITATIONS ON LIABILITY.

YOU acknowledge that the SOFTWARE PRODUCT has not been developed to meet your individual requirements, including any particular cybersecurity requirements you might be subject to under law or otherwise, and that it is therefore YOUR responsibility to ensure that the facilities and functions of the SOFTWARE PRODUCT meet your requirements. CENTREL SOLUTIONS will not be responsible for any failure or fault of the SOFTWARE PRODUCT where such failure results from YOU having altered, modified or misused the SOFTWARE PRODUCT.

The LICENSEE understands that the SOFTWARE PRODUCT may produce inaccurate result due to a failure by the LICENSEE to properly use and/ or deploy the SOFTWARE PRODUCT. The LICENSEE assumes full and sole responsibility for any use of the SOFTWARE PRODUCT. CENTREL SOLUTIONS' maximum aggregate liability under or in connection with this AGREEMENT whether in contract, tort (including negligence) or otherwise, shall in all circumstances be limited to a sum equal to the price paid to CENTREL SOLUTIONS for the SOFTWARE PRODUCT.

Nothing in this AGREEMENT shall limit or exclude CENTREL SOLUTIONS' liability for death or personal injury resulting from its negligence; fraud or fraudulent misrepresentation; or any other liability that cannot be excluded or limited by English law.

11. SUPPORT SERVICES.

CENTREL SOLUTIONS may provide YOU with support services related to the SOFTWARE PRODUCT ("SUPPORT SERVICES"). Use of SUPPORT SERVICES is governed by CENTREL SOLUTIONS policies and programs described in the product documentation, in online documentation and/or other CENTREL SOLUTIONS provided materials. CENTREL SOLUTIONS may restrict or otherwise discontinue SUPPORT SERVICES provided to the LICENSEE if YOUR use of the SUPPORT SERVICES is deemed by

CENTREL SOLUTIONS, in its sole and reasonable discretion, to be excessive and beyond the scope of fair use.

Any supplemental SOFTWARE PRODUCT(S) provided to YOU as part of the SUPPORT SERVICES shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this AGREEMENT. With respect to technical information YOU provide to CENTREL SOLUTIONS as part of the SUPPORT SERVICES, CENTREL SOLUTIONS may use such information for its business purposes, including for SOFTWARE PRODUCT support and development.

Should the LICENSEE wish to report an issue relating to the SOFTWARE PRODUCT, the LICENSEE agrees to report the issue using the “Log Support Call” page of the CENTREL SOLUTIONS web site.

The LICENSEE agrees to use the TeamViewer product from TeamViewer GmbH, for remote support. More information on TeamViewer can be found at <https://www.teamviewer.com>.

CENTREL SOLUTIONS may restrict or otherwise discontinue SUPPORT SERVICES provided to the LICENSEE if the SOFTWARE PRODUCT installed by the LICENSEE is more than one major release behind the currently available version of the SOFTWARE PRODUCT.

12. TERMINATION.

Without prejudice to any other rights or remedies, CENTREL SOLUTIONS may terminate this AGREEMENT immediately by written notice to YOU if YOU commit a material or persistent breach of this AGREEMENT which YOU fail to remedy (if remediable) within 14 days after the service of written notice requiring YOU to do so.

On termination for any reason, the LICENSEE must destroy all copies of the SOFTWARE PRODUCT and all of its component parts including any related documentation.

13. TAX.

CENTREL SOLUTIONS delivers its software electronically. YOU should confirm that YOUR local, state, or federal government does not impose any sales or use tax on electronically delivered software. YOU are entirely liable for any such sales or use tax.

14. PERSONAL DATA.

CENTREL SOLUTIONS does not lend, lease, sell, or market information it obtains from its customers or those who provide us personally identifiable information. CENTREL SOLUTIONS does not disclose purchase information or licensing information to third parties.

CENTREL SOLUTIONS collects personally identifiable information whenever YOU purchase/license a CENTREL SOLUTIONS product or service. Information includes Name, Address, Phone Number, Email address, Product Purchases, Licenses Owned, Employee/Contact Details, etc. The information we collect allows CENTREL SOLUTIONS to communicate with YOU regarding upcoming product updates, new product releases, company news and other important business matters.

CENTREL SOLUTIONS may disclose or report Confidential Information in limited circumstances where it believes in good faith that disclosure is required under the law.

The CENTREL SOLUTIONS privacy policy can be viewed online at the following address
<https://www.centrel-solutions.com/company/privacy-policy.aspx>

15. USE OF YOUR ACCOUNT

YOUR election to use the SOFTWARE PRODUCT indicates YOUR acceptance of the terms of this AGREEMENT. YOU are responsible for maintaining confidentiality of YOUR username, password and other sensitive information. YOU are responsible for all activities that occur in YOUR user account and in case of any unauthorized activity on YOUR account, YOU agree to inform CENTREL SOLUTIONS immediately by any method listed on the CENTREL SOLUTIONS website's Contact page.

CENTREL SOLUTIONS is not responsible for any loss or damage to YOU or to any third party incurred as a result of any unauthorized access and/or use of YOUR user account, or otherwise.

16. THIRD PARTY CONTROLS

The SOFTWARE PRODUCT contains the following third-party software, use of which is subject to the terms noted below

CodeMirror (Open Source - MIT License)

Copyright © 2017 by Marijn Haverbeke (marijnh@gmail.com) and others

<https://codemirror.net/LICENSE>

17. AGREEMENT

This AGREEMENT constitutes the entire agreement between us and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between us, whether written or oral, relating to its subject matter. YOU agree that YOU shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this AGREEMENT. YOU agree that you shall have no

claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this AGREEMENT.

This AGREEMENT, its subject matter and its formation (and any non-contractual disputes or claims) are governed by English law. CENTREL SOLUTIONS and YOU both irrevocably agree to the exclusive jurisdiction of the courts of England and Wales.

18. MISCELLANEOUS

This AGREEMENT may only be modified or amended by YOU if the modification or amendment is approved in writing and signed by an authorized officer of CENTREL SOLUTIONS. If any provision of this AGREEMENT is found void or unenforceable, the remainder will remain valid and enforceable according to its terms. If any remedy provided is determined to have failed for its essential purpose, all limitations of liability and exclusions of damages set forth in the Limited Warranty shall remain in effect.

If we have to contact YOU, we will do so by email or post to the address YOU provided in accordance with your purchase of the LICENSE.

Any notice given by CENTREL SOLUTIONS to YOU will be deemed received and properly served 24 hours after an email is sent, or three days after the date of posting of any letter. Any notice given by YOU to CENTREL SOLUTIONS will be deemed received and properly served three days after the date of posting of any letter.

CENTREL SOLUTIONS reserves all rights not specifically granted in this AGREEMENT.

Should YOU have any questions concerning this AGREEMENT, contact us directly on +44 (0)1865 589216 or write to

CENTREL Solutions Ltd
Innovation House
John Smith Drive
Oxford
United Kingdom
OX4 2JY

All trademarks and registered trademarks are property of their respective owners.