XIA Configuration Server

Version 14.1 Upgrade Notes





Wednesday, 17 August 2022

Table of Contents

XIA Configuration Version 14.1	3
Upgrading from a version older than v14.0?	3
T00942 - Az PowerShell module version 8.1.0	4
T00948 - Remote Settings Data Model	5
T00955 – Windows Events Data Model	6
T00956 - Windows Basic Compliance Benchmark Settings	7

XIA Configuration Version 14.1

XIA Configuration Server version 14.1 includes many security related improvements including

- The Windows Basic Compliance Benchmark was updated to version 5.0.
- The Windows Basic Compliance Benchmark now includes 340+ tests.
- Improved support for reading Event Logs on Windows machines.
- The ability to read audit rules on NTFS and ReFS filesystems on Windows machines.
- The ability to read the security descriptor for Event Logs on Windows machines.
- Improved support for reading security descriptors for registry keys on Windows machines.

Upgrading from a version older than v14.0?

If you're upgrading from a version older than v14.0, please also check the previous version upgrade notes.

- <u>Version 14.0 upgrade notes</u>
- Version 13.1 upgrade notes
- Version 13.0 upgrade notes
- Version 12.2 upgrade notes
- Version 12.1 upgrade notes
- Version 12.0 upgrade notes
- <u>Version 11.1 upgrade notes</u>
- Version 11.0 upgrade notes

T00942 - Az PowerShell module version 8.1.0

The new Azure tenant agent now requires the <u>Azure Az PowerShell module</u> version 8.1.0 or above.

The <u>Azure Az PowerShell module</u> must be upgraded using the PowerShell command

Update-Module Az

T00948 - Remote Settings Data Model

The data model for Windows machines has been updated. Windows machines must be rescanned using the latest version of the XIA Configuration Client.

Windows machines scanned with a previous version of the XIA Configuration Client will not display information for the "Remote Desktop" and "Remote Assistance" sections.

EMO-20 Windows Server 39820
Remote Desktop
Remote Desktop allows users running an appropriate version of the Remote Desktop client to connect to a remote machine and access the desktop or published applications using the Remote Desktop Protocol (RDP).
Remote Desktop Settings
This section does not contain any information.

T00955 – Windows Events Data Model

The data model for Windows machines has been updated. Windows machines must be rescanned using the latest version of the XIA Configuration Client.

Windows machines scanned with a previous version of the XIA Configuration Client will not display certain information for the "Events logs" section.

EMO-20 Windows Server 39820				
Event Logs				
The event logging service records e	vents from various sou	rces and stores them in a sin	gle collection called an event log	
			0.0	
9 Event Logs				
 Name 	Туре	Maximum File Size	Retention Policy	
Application	Unknown	20,480 KB	Overwrite events as needed	
Forwarded Events	Unknown	20,480 KB	Archive the log when full	
Hardware Events	Unknown	20,480 KB	Overwrite events as needed	
f Internet Explorer	Unknown	1,028 KB	Overwrite events as needed	
Key Management Service	Unknown	20,480 KB	Overwrite events as needed	
Security	Unknown	20,480 KB	Do not overwrite events	
f Setup	Unknown	0 KB	Do not overwrite events	
System	Unknown	20,480 KB	Overwrite events as needed	
Windows PowerShell	Unknown	15,360 KB	Overwrite events as needed	

T00956 - Windows Basic Compliance Benchmark Settings

The data model for the Windows Basic Compliance Benchmark has been updated. This is to facilitate the large number of additional benchmark tests added to the Windows Basic Compliance Benchmark version 5.0.0.

Customers are advised to review the new format of the settings and ensure that their configuration meets their requirements.

🕒 Windows Machine Agent Settings – 🗖 🗙				
Local Service Files Registry Tolerance SNMF Scan Method Basic Compliance Benchmark Option	Plugins PowerShell WMI nal Components Agent Detection			
Use Basic Compliance Benchmark Custom Settings				
13.41 Replace a process level token	User Right Setting			
13.42 Restore files and directories	User Right Setting			
13.43 Shut down the system	User Right Setting			
13.44 Synchronize directory service data	User Right Setting			
13.45 Take ownership of files or other objects	User Right Setting			
Section 14: Windows Firewall Domain Profile	Domain Profile			
14.04 Display Notification	False 🗸			
14.06 Log File Path	SystemRoot %\System32\Log			
14.08 Log File Size Limit	16384			
14.09 Log Successful Connections	True			
 Section 15: Windows Firewall Private Profile 	Private Profile			
15.04 Display Notification	False			
15.06 Log File Path	SystemRoot %\System32\Log			
15.08 Log File Size Limit	16384			
15.09 Log Successful Connections	True			
Section 16: Windows Firewall Public Profile	Public Profile			
16.04 Display Notification	False			
16.06 Log File Path %SystemRoot%\System32\Lo				
16.08 Log File Size Limit	16384 🗸			
14.04 Display Notification The desired value for 14.04 "Windows Firewall Domain Profile 'Display a notification' setting".				
	Cancel OK			