

# Knowledge Base Article

KB1077



CONTOSO  
TECHNICAL  
SERVICES

<b>Date</b>	30/01/2020 11:43:43
<b>Author</b>	DEMO2012R2\sysadmin
<b>Version</b>	1.02
<b>Product</b>	XIA Configuration Server [12.0.15.20336]

# Table of Contents

Disclaimer

Knowledge Base Article Information

Relationships 5

Relationship Map 6

Knowledge Base Article Content

Summary 7

Cause 7

Resolution 8

More Information 8

Version History

# Disclaimer

This document is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and, or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

# Knowledge Base Article

## Information

Provides general information for this item.

---

### General Information

Name	KB1077
Description	You receive an "HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials" error message when you try to access a Web site that is part of an IIS 6.0 application pool
Primary Owner Name	Technical Services
Primary Owner Contact	support@contosotechnicalservices.com

---


### System Information


Item Path	Contoso Technical Services
Item ID	1077
Version ID	1.02
CheckOut Status	Available

# Relationships

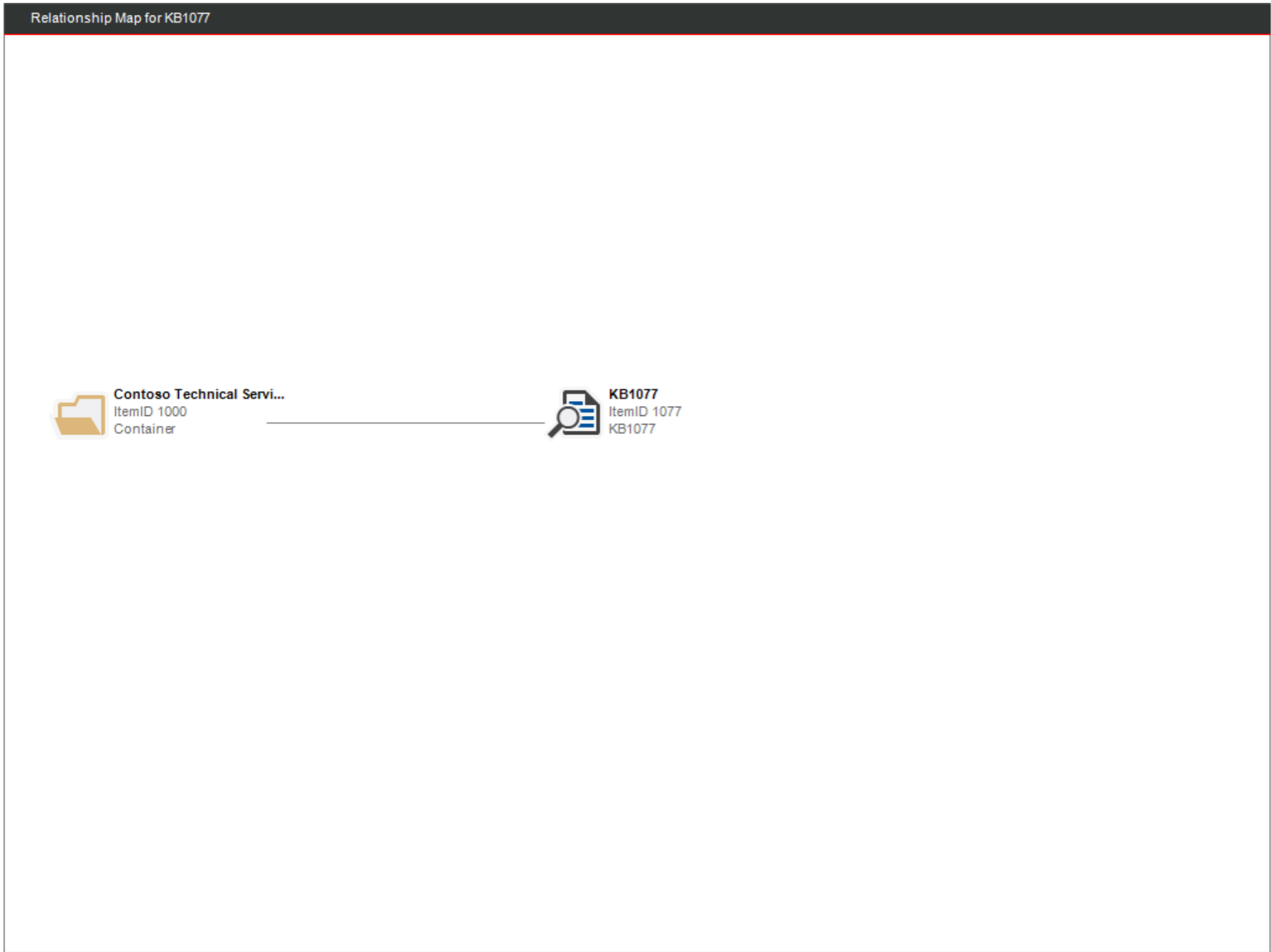
Provides a summary of the relationships between this item and other items in the environment.

---

 1 Relationships

Item ID	Direction	Name	Type	Relationship Type
 1000	Outbound	Contoso Technical Services	Container	Contained Within

# Relationship Map



# Knowledge Base Article Content

You receive an "HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials" error message when you try to access a Web site that is part of an IIS 6.0 application pool

## Summary

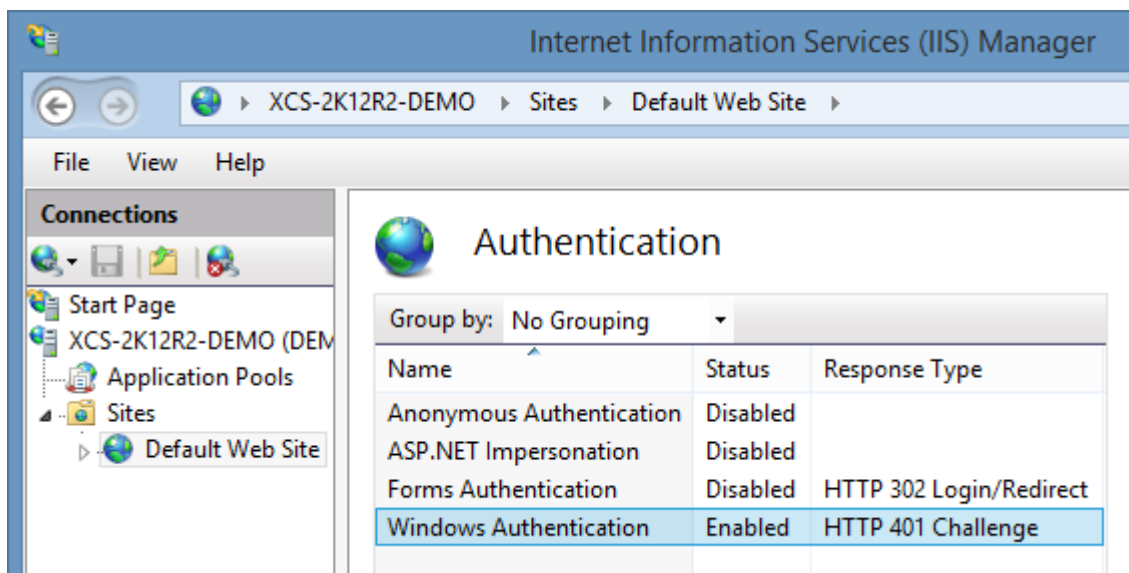
When you try to access a Microsoft Internet Information Services (IIS) 6.0 Web site that is configured to use Integrated Windows authentication only, you are prompted for your user credentials. When you try to log on, you receive the logon prompt again. After you try to log on three times, you receive the following error message:

HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials.

## Cause

This behavior may occur if the following conditions are true:

- The IIS 6.0 Web site is part of an IIS application pool.
- The application pool is running under a local account or under a domain user account.
- The Web site is configured to use Integrated Windows authentication only.



In this scenario, when Integrated Windows authentication tries to use Kerberos, Kerberos authentication may not work. To use Kerberos authentication, a service must register its service principal name (SPN) under the account in the Active Directory directory service that the service is running under. By default, Active Directory registers the network basic input/output system (NetBIOS) computer name. Active Directory also permits the Network Service or the Local System account to use Kerberos.

# Resolution

If this behavior occurs when the application pool is running under a local account, follow the steps in the "Workaround" section.

To resolve this behavior when the application pool is running under a domain user account, set up an HTTP SPN with the NetBIOS name and the fully qualified domain name (FQDN) of the domain user account that the application pool is running under. To do this, follow these steps on a domain controller:

**Important** An SPN for a service can only be associated with one account. Therefore, if you use this suggested resolution, any other application pool that is running under a different domain user account cannot be used with Integrated Windows authentication only.

1. Install the Setspn.exe tool. To obtain the Setspn.exe tool for Microsoft Windows Server 2003, click the following article number to view the article in the Microsoft Knowledge Base:

[970536](#) Setspn.exe support tool update for Windows Server 2003

2. Start a command prompt, and then change to the directory where you installed Setspn.exe.
3. At the command prompt, type the following commands. Press ENTER after each command:

```
setspn.exe -S http/IIS_computer's_NetBIOS_name DomainName\UserName
```

```
setspn.exe -S http/IIS_computer's_FQDN DomainName\UserName
```

**Note:** **UserName** is the user account that the application pool is running under. Also note that if you are running the setspn.exe command on a Windows 2000 machine, use the -A switch instead of the -S switch.

After you set the SPN for the HTTP service to the domain user account that the application pool is running under, you can successfully connect to the Web site without being prompted for your user credentials.

## More Information

If you set the SPN by using only the FQDN of the server that is running IIS, you will be prompted for your user credentials after 30 minutes. The 30-minute time-out occurs because of the way that Internet Explorer caches Domain Name System (DNS) information. After 30 minutes, Internet Explorer reverts to the NetBIOS name. Therefore, you must make sure that you also register the SPN by using the NetBIOS name of the server that is running IIS to avoid being prompted for your user credentials. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

[263558](#) How Internet Explorer uses the cache for DNS host entries

To verify the registered SPNs for the user account that your application pool is running under, start a command prompt, type the following command from the directory where Setspn.exe is installed, and then press ENTER:

```
setspn.exe -I UserName
```

A list of the registered SPNs for the user account is returned.




## Internet Information Services (IIS) 7.0

The topics discussed in this article can also apply to IIS 7.0 if one of the following conditions is true:

- Kernel Mode Authentication is disabled.
- Kernel Mode Authentication is enabled, and the useAppPoolCredentials attribute is set to TRUE.

# Version History

The version history displays the changes that have been made to the documentation of this item over time - either automatically when a change has been detected, or manually by users of the system.

 3 versions

Version	Username	Date	Time	Description
 1.02	DEMO2012R2\sysadmin	30 January 2020	11:43	Updated Windows Authentication image.
 1.01	DEMO2012R2\sysadmin	30 January 2020	11:07	Updated by the new item interface.
 1.00	DEMO2012R2\sysadmin	30 January 2020	11:06	Item created.