

Microsoft SharePoint Authentication

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up Microsoft SharePoint authentication for MS SharePoint 2010, 2013, 2016 and 2019.

A few things to consider

Do I have to use authentication?

Yes, authentication is required for compliance scans. Choose the type of authentication you want to perform: Windows or MS SQL Database. If you choose Windows, provide the name of the Windows domain where the account is stored. The domain name is required because the scanning engine must associate the operating system account with the MS SQL Server database account for authentication.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

[Authentication Technologies Matrix](#)

What are the steps?

First, set up a user account and privileges on target hosts (we'll help you with this below). Then, using Qualys Policy Compliance, complete these steps: 1) Add Windows and Microsoft SharePoint authentication records. 2) Launch a compliance scan. 3) Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

Scan User Privileges and Configurations

Follow detailed instructions in these sections of the document:

[Part 1: System Configuration Requirements](#)

[Part 2: Scan User Privileges \(Windows and MS SQL Database\)](#)

[Part 3: Verify Scan User Membership and Test Connection by PowerShell Script](#)

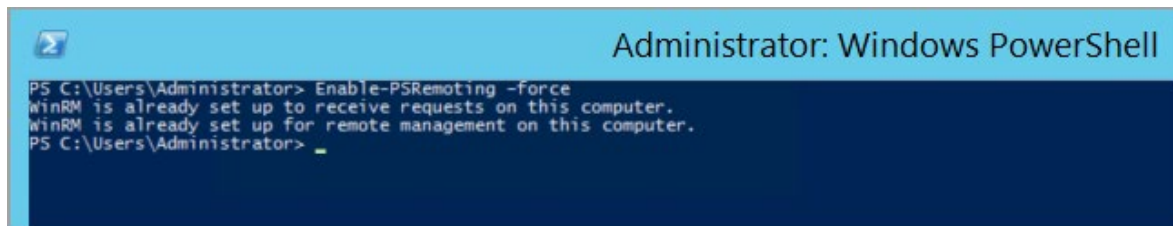
Part 1: System Configuration Requirements

- Set PowerShell Execution Policies
- Verify WinRM IIS Extensions
- Enable Windows Authentication for PowerShell Virtual Directory

1) Open a Windows PowerShell window. Open by selecting Run as administrator and run the command as shown:

```
Set-ExecutionPolicy RemoteSigned
```

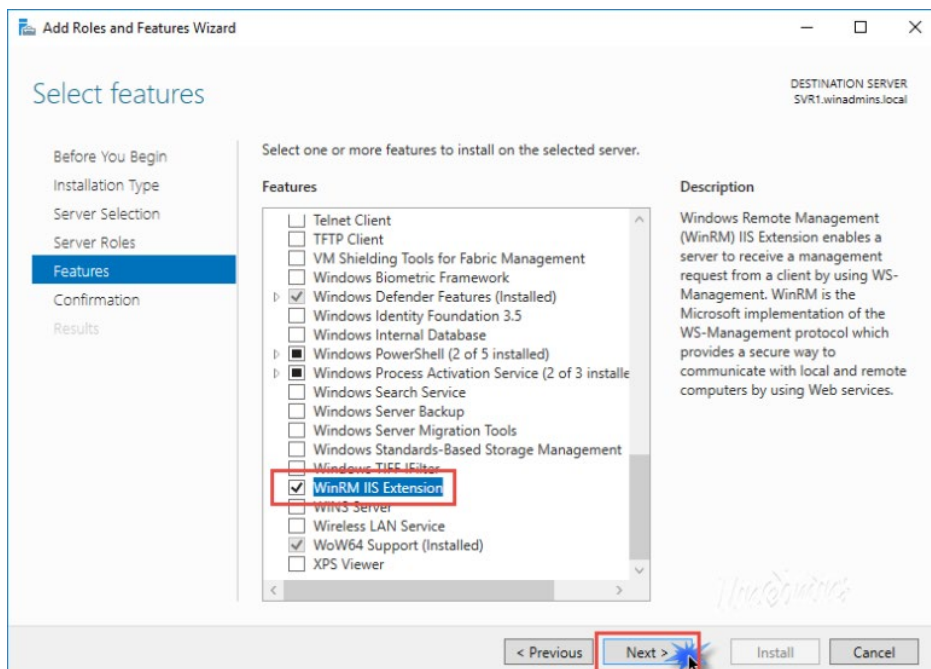
Also check if Remote PowerShell is Enabled on the host:

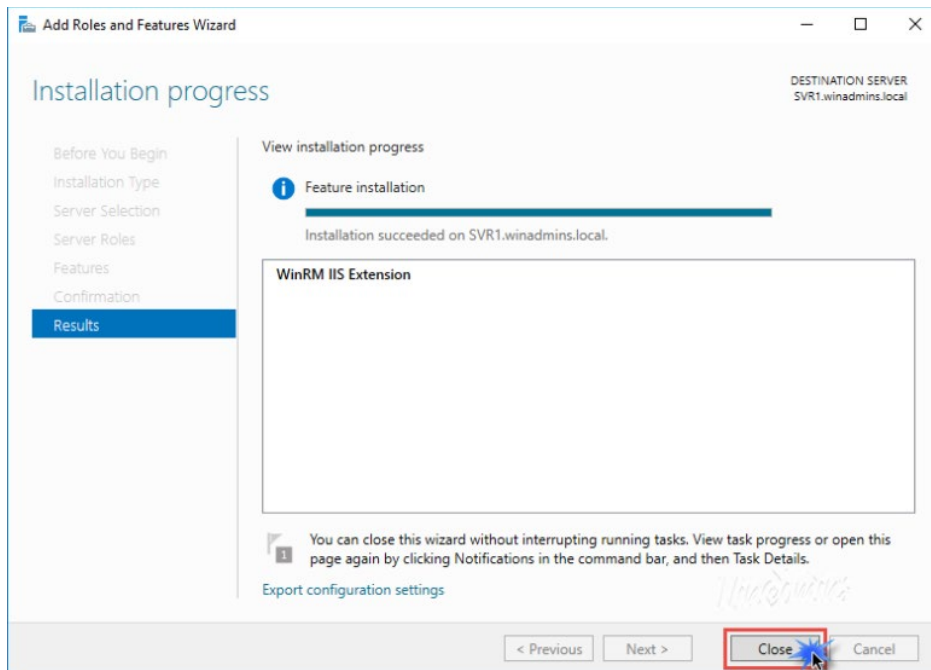


2) Enable the WinRM IIS Extensions under Add Roles and Features in Server Manager.

Windows Remote Management (WinRM) IIS Extension enables a server to receive a management request from a client computer by using the WS-Management protocol. WinRM is the Microsoft implementation of the WS-Management protocol. This helps secure communication between local and remote computers by using Web-based services.

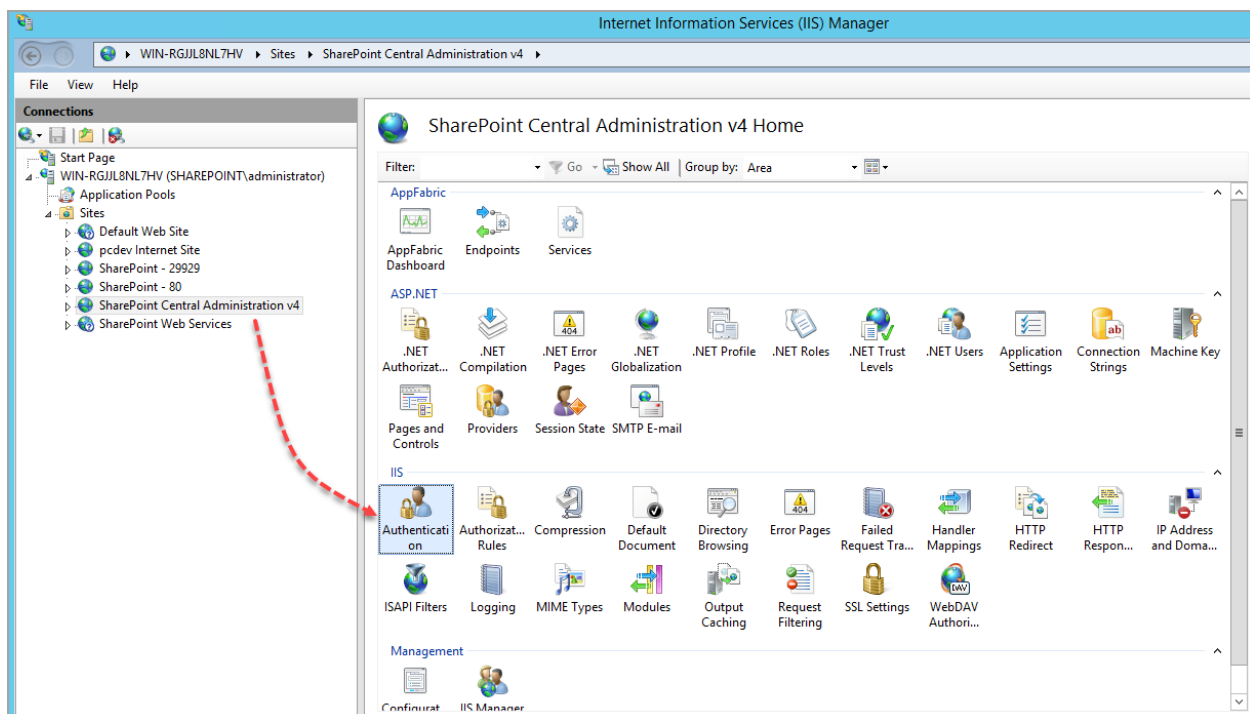
Steps shown in the images below:



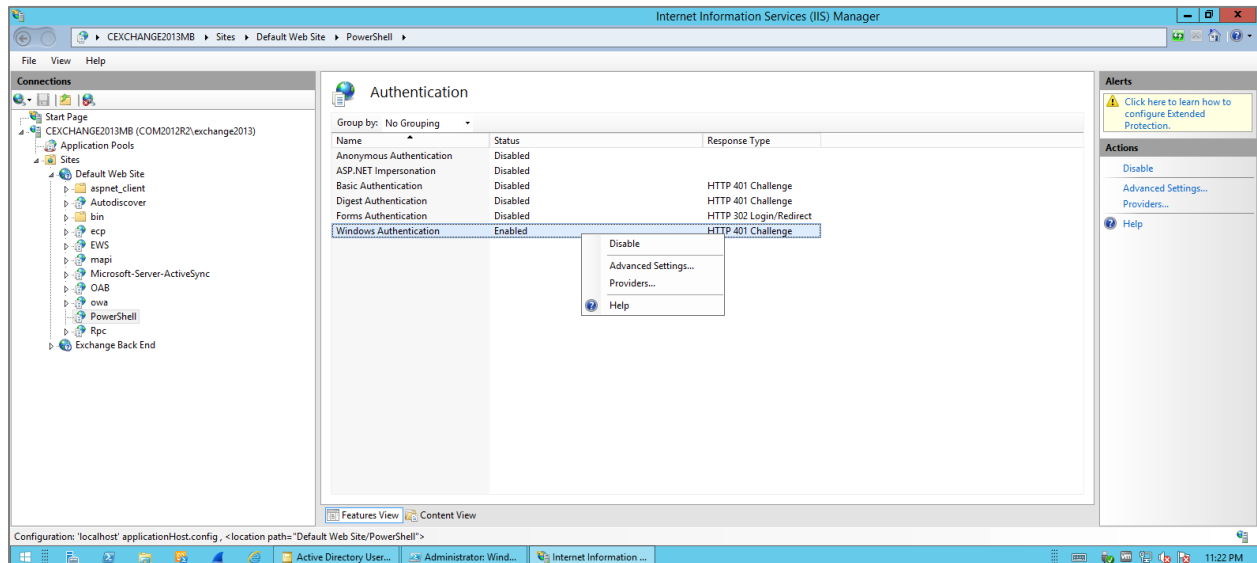


3) Log in to your Sharepoint 2010+ server and enable the Windows Authentication on the PowerShell site.

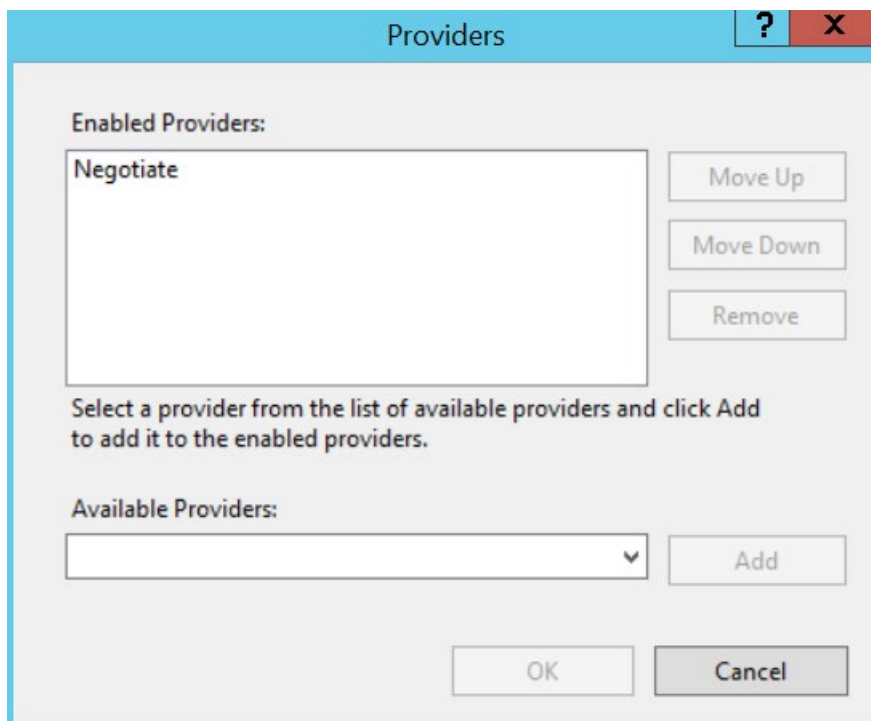
- Open the Internet Information Services (IIS) Manager console.
- Connect to the SharePoint Server.
- Open Sites > SharePoint Central Administration > PowerShell, and open Authentication.



Enable Windows Authentication. Right click on Windows Authentication and select Providers as NTLM or Negotiate.



Providers:



Part 2: Scan User Privileges (Windows and MS SQL Database)

Pre-requisites

SharePoint Farm Scan User account

The server farm account requires the following permissions:

- It must have domain user account permissions.
- Additional permissions are automatically granted to the SharePoint Farm Service account on SharePoint servers that are joined to a server farm.

1) After you run Setup, machine-level permissions include:

- Membership in the WSS_ADMIN_WPG Windows security group for the SharePoint Timer Service.
- Membership in WSS_RESTRICTED_WPG for the Central Administration and Timer service application pools.
- Membership in WSS_WPG for the Central Administration application pool.

2) After you run the configuration wizards, SQL Server and database permissions include:

- Membership in the WSS_CONTENT_APPLICATION_POOLS role for the SharePoint server farm configuration database.
- Membership in the WSS_CONTENT_APPLICATION_POOLS role for the SharePoint_Admin content database.

If these permissions are not satisfied, contact your Setup administrator or SQL Server administrator to request these permissions.

Adding scan user as a SharePoint Shell Admin

Add-SPShellAdmin

- Adds a user to the SharePoint_Shell_Access role for the specified database.
- If you specify only the user, the user is added to the role for the farm configuration database.

C:\PS>Add-SPShellAdmin -UserName DOMAIN\qualys_scan

This example adds a new user named “qualys_scan” to the SharePoint_Shell_Access role in the farm configuration database only, and also ensures the user is added to the WSS_Admin_WPG local group on each server in the farm.

Using the database parameter the user is added to the role on the farm configuration database, the Central Administration content database and the specified database.

C:\PS>Add-SPShellAdmin -UserName DOMAIN\qualys_scan -database <DB GUID>

This example adds a new user named “qualys_scan” to the SharePoint_Shell_Access role in both the specified content database and the configuration database by passing a database GUID to the cmdlet.

Using the database parameter is the preferred method because most of the administrative operations require access to the Central Administration content database

Minimum privilege needed to scan the SQL Server portion of SharePoint controls with restricted/read-only account

Please run the scripts provided below, in the order shown.

If creating a Windows authentication on the SQL Server, start with Step 1a.

If creating a SQL Server authentication on the SQL Server, start with Step 1b.

1a) Create a Windows Authentication Login for the Scan Account

This script creates a domain login for the user account to be used for scanning. Provide a domain name or local user account, and name of the target database before running the script. Tip – An admin needs to create the account on the host first. We recommend creating an account called QUALYS_SCAN.

```
USE [master]
GO
CREATE LOGIN [domain\QUALYS_SCAN] FROM WINDOWS WITH DEFAULT_DATABASE=master
GO
```

1b) Create a SQL Server Authentication Login for the Scan Account

This script creates a database login for the user account to be used for scanning. Please provide a password and the name of the target database before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

```
USE [master]
GO
CREATE LOGIN QUALYS_SCAN WITH PASSWORD=N'[password]', DEFAULT_DATABASE=master,
CHECK_EXPIRATION=ON, CHECK_POLICY=ON
GO
```

2) Create a User Account

```
USE [master]
GO
CREATE USER [qualys_scan] FOR LOGIN [username created in Step 1]
GO
```

```
grant SELECT on sys.all_objects to qualys_scan;
grant SELECT on sys.configurations to qualys_scan;
grant SELECT on sys.databases to qualys_scan;
grant SELECT on sys.database_permissions to qualys_scan;
grant SELECT on sys.syslogins to qualys_scan;
grant SELECT on sys.trace_events to qualys_scan;
grant SELECT on sys.traces to qualys_scan;
grant SELECT on sys.sysaltfiles to qualys_scan;
grant SELECT on sys.server_principals to qualys_scan;
grant VIEW ANY DEFINITION TO qualys_scan;
GO
```

3) Verify Privileges on the Scan Account

Verify that the QUALYS_SCAN account has all the privileges in the database in order to run a successful compliance scan. Log into the database using the “QUALYS_SCAN” account, then run the following queries to see if access is available to the account.

Query	Expected Results
select top 1 1 permission from sys.all_objects	1
select top 1 1 permission from sys.configurations	1
select top 1 1 permission from sys.databases	1
select top 1 1 permission from sys.database_permissions	1
select top 1 1 permission from sys.syslogins	1
select top 1 1 permission from sys.trace_events	1
select top 1 convert(char(20),serverproperty('productversion')) permission	13.0.1601.5

Did you get different results? Contact your SQL Server DBA to ensure that privileges are set up correctly.

Part 3: Verify Scan User Membership and Test Connection by PowerShell Script

Connecting to MS SharePoint Server via PowerShell

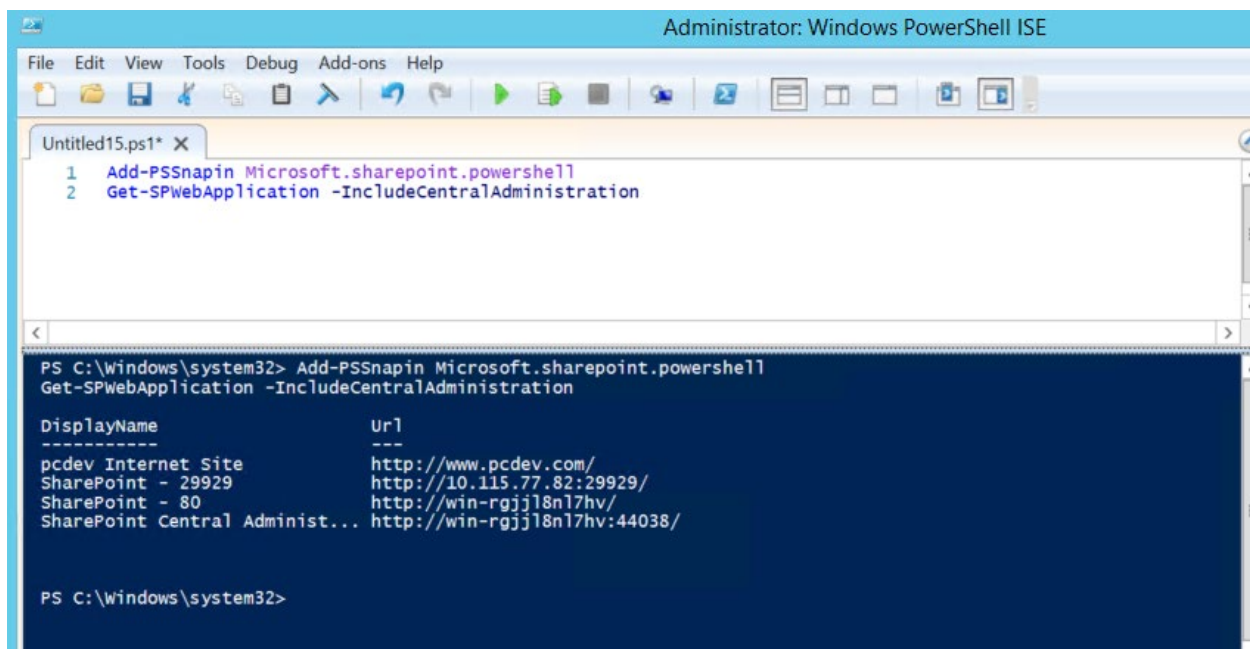
Here are the steps required to connect to PowerShell Virtual Directory using a PowerShell script.

1) Open PowerShell or PowerShell ISE and insert below code as shown :

```
Add-PSSnapin Microsoft.sharepoint.powershell
```

```
Get-SPWebApplication -IncludeCentralAdministration
```

2) Run the above code with correct input details as per your host setup and you should be able to see the connection result as follows. Following image shows an example scenario.



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled15.ps1* X
1 Add-PSSnapin Microsoft.sharepoint.powershell
2 Get-SPWebApplication -IncludeCentralAdministration

PS C:\Windows\system32> Add-PSSnapin Microsoft.sharepoint.powershell
Get-SPWebApplication -IncludeCentralAdministration

   DisplayName                                     Url
   -----
pcdev Internet Site                             http://www.pcdev.com/
SharePoint - 29929                             http://10.115.77.82:29929/
SharePoint - 80                                http://win-rgjj18n17hv/
SharePoint Central Administration                http://win-rgjj18n17hv:44038/

PS C:\Windows\system32>
```

This ensures you are able to connect the PowerShell Virtual Directory using PowerShell with the Scan User specified.

Additional References

<https://docs.microsoft.com/en-us/sharepoint/install/account-permissions-and-security-settings-in-sharepoint-2013>

<https://docs.microsoft.com/en-us/sharepoint/install/account-permissions-and-security-settings-in-sharepoint-server-2016>

<https://docs.microsoft.com/en-us/powershell/sharepoint/sharepoint-server/sharepoint-server-cmdlets?view=sharepoint-ps>

Last updated: May 27, 2022