MS Exchange Server Authentication – Scan User Privileges and Configuration

This document provides system configuration requirements and scan user privileges needed to authenticate to a Microsoft Exchange Server running on a Windows host and scan it for compliance.

Table of Contents

System Configuration Requirements (when using a Cloud Agent)

If you're using Qualys Cloud Agent, the agent will run and scan using the local **System** user by default. It runs Get-* cmdlets from scripts, which require the "View-Only Organization Management Role" for the Exchange host.

Make sure the Exchange host meets the following minimum requirements for agent scans:

- On **Exchange Servers DC**, go to **Active Directory Users and Groups** > **Microsoft Exchange Security Groups** > **View-Only Organization Management** > **Members** > **Add** > Select **Object types** as "**Computers**" > Enter the **Exchange Server Hostname** and **Apply**.
- PowerShell Version 3.0 and above. Our PS scripts mostly support commands that are used in PowerShell 3.0 and above.
- Our scripts are signed by Qualys Trusted Certificates. Make sure the PowerShell Execution Policy or any third-party tool does not block our PS scripts from running.

Note that Cloud Agent scans do not require authentication records because agents are installed directly on the host being scanned. For agent scans, there are no additional steps needed.

System Configuration Requirements (when using a Scanner)

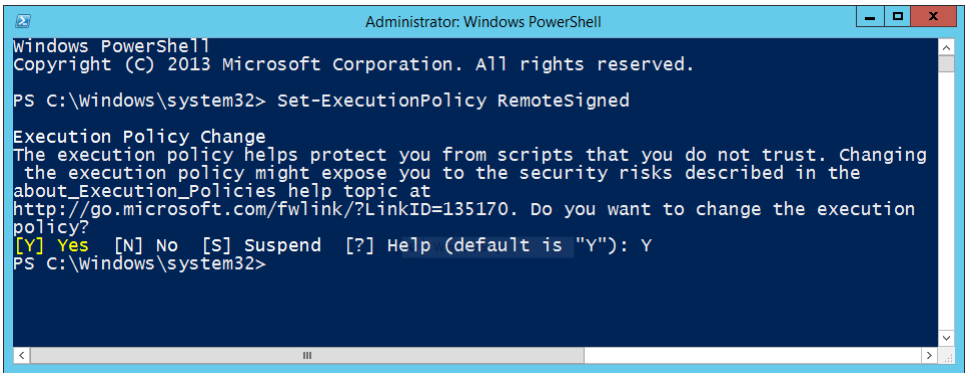
If you're using a Scanner, then you'll need to complete these system configuration requirements:

- Set PowerShell Execution Policies
- Verify WinRM IIS Extensions
- Enable Windows Authentication for PowerShell Virtual Directory
- Verify SSL setting for PowerShell Virtual Directory
- Verify the application pool for PowerShell Virtual Directory
- Verify the Security for PowerShell Virtual Directory

Follow the steps below for system configuration:

1) Open a **Windows PowerShell** window by selecting **Run as administrator**. Then run the command below:

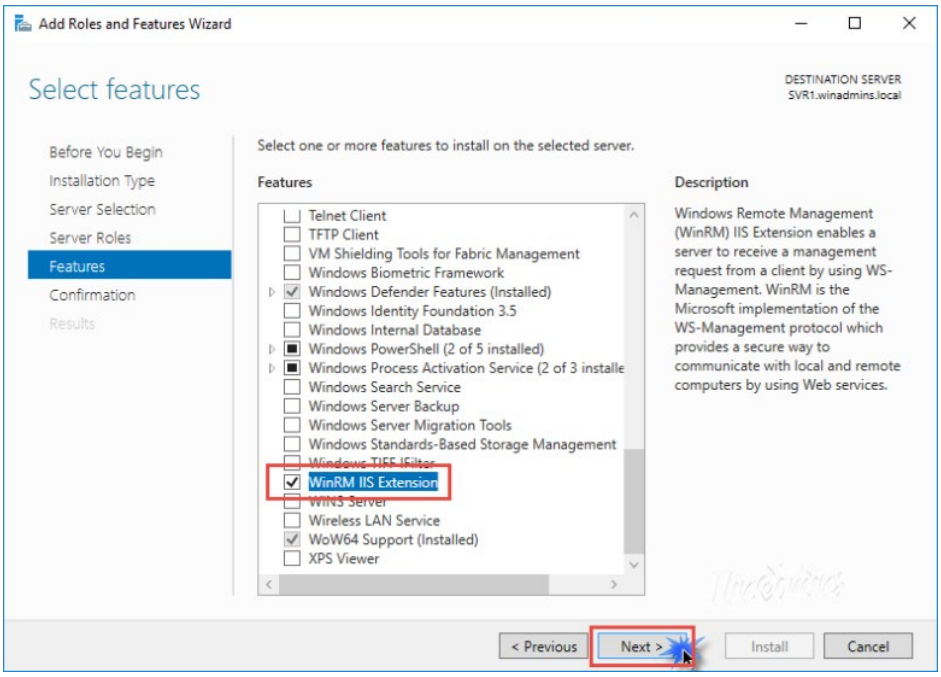
```
Set-ExecutionPolicy RemoteSigned
```



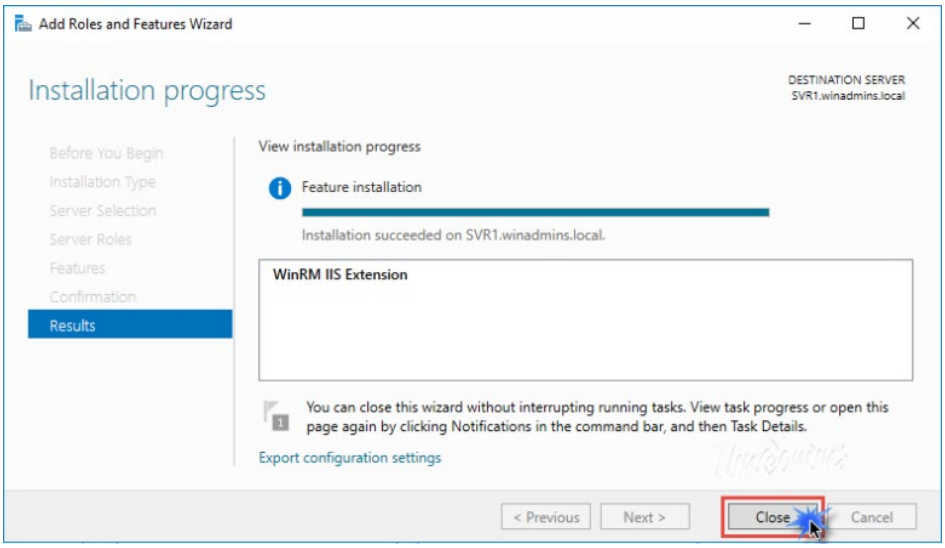
2) Enable the **WinRM IIS Extension** under **Add Roles and Features** in **Server Manager**.

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.

2a) In the **Add Roles and Features Wizard**, select **WinRM IIS Extension** and click **Next**.



2b) View installation progress for the WinRM IIS Extension, and click **Close**.

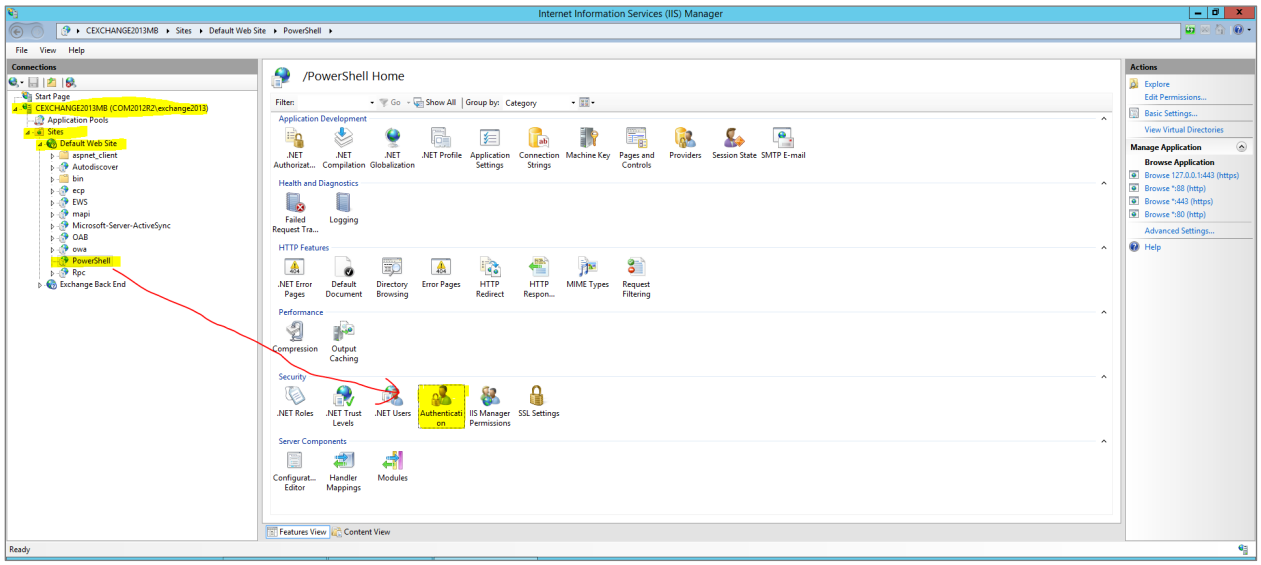


3) Log in to your Exchange 2010+ server and enable **Windows Authentication** on the **PowerShell** site.

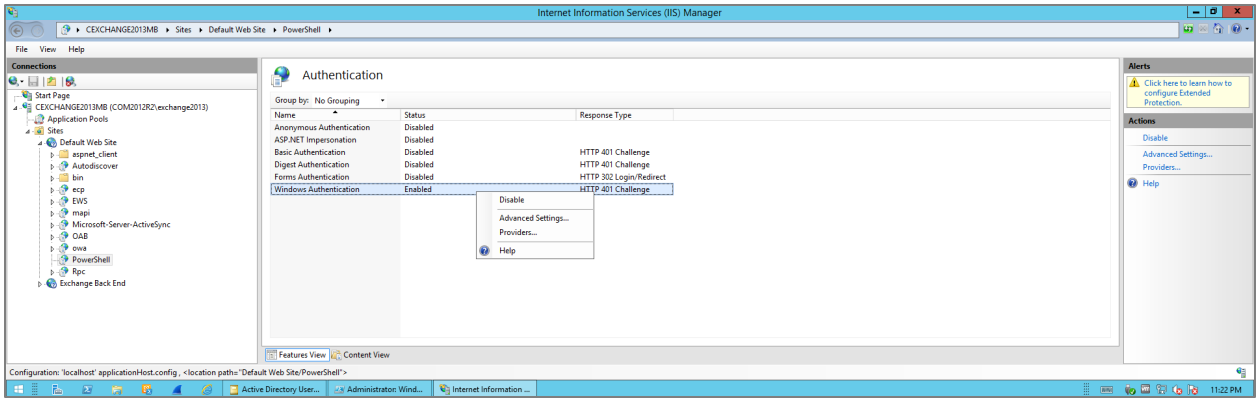
3a) Open the **Internet Information Services (IIS) Manager** console.

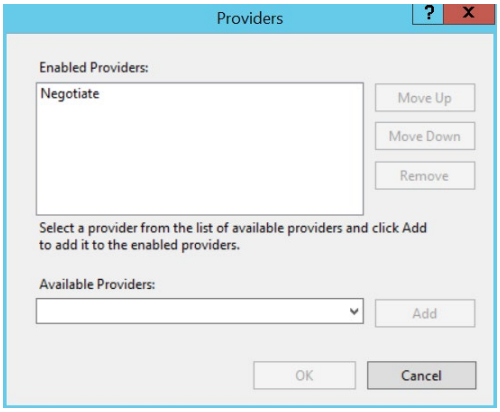
3b) Connect to the **Exchange Server**.

3c) Open **Sites** > **"Name of your Exchange Site"** > **PowerShell**, and open **Authentication**.



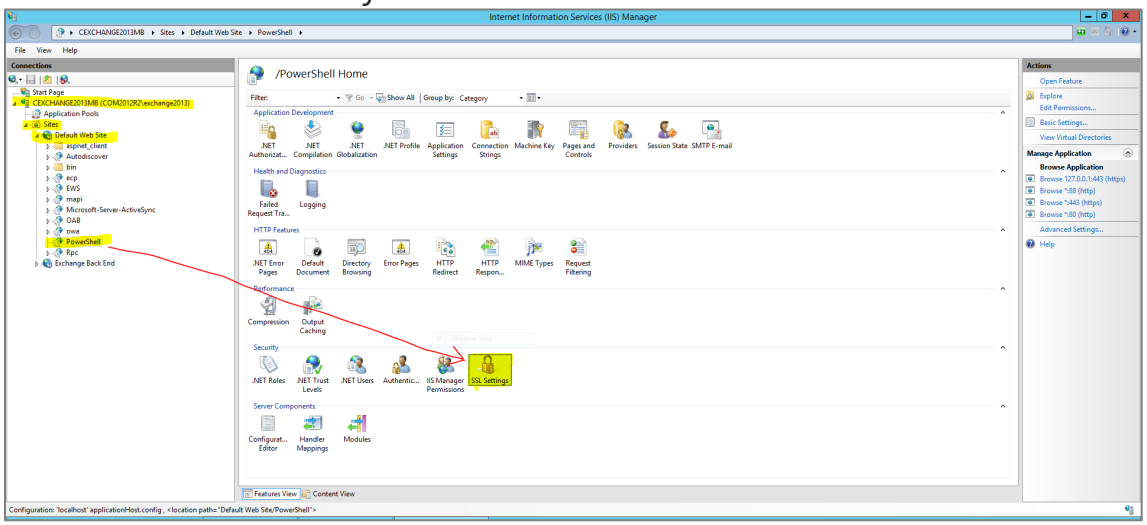
3d) Enable **Windows Authentication**. Right click on **Windows Authentication** and select **Providers** as **Negotiate**.



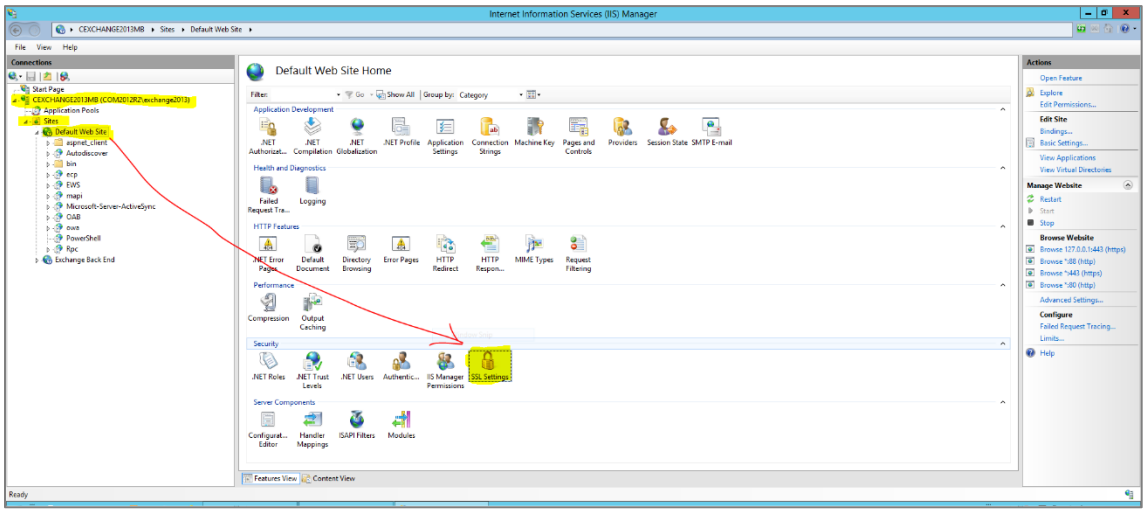


4) For using HTTP URI to access PowerShell Virtual Directory, you must disable the SSL checking (with Ignore) for the PowerShell Virtual Directory and for the Default IIS Web Site, as shown in the images below. Make sure you click **Apply** to save your changes.

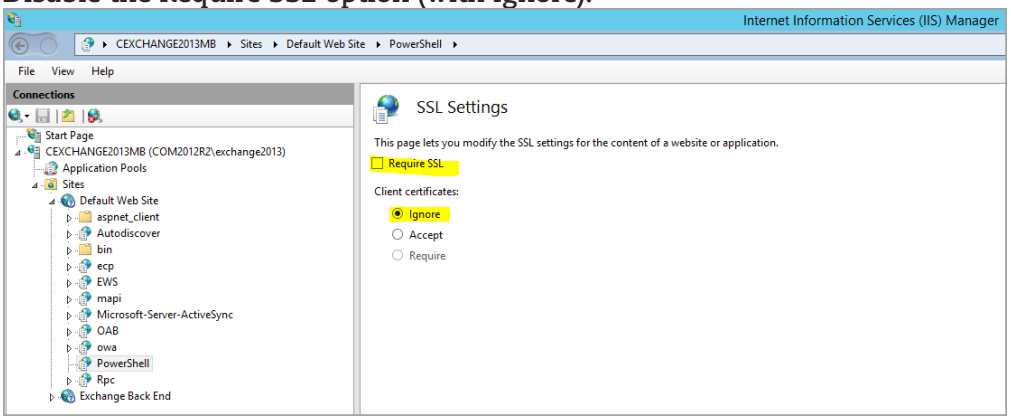
PowerShell Virtual Directory:



Default Web Site:



Disable the Require SSL option (with Ignore):

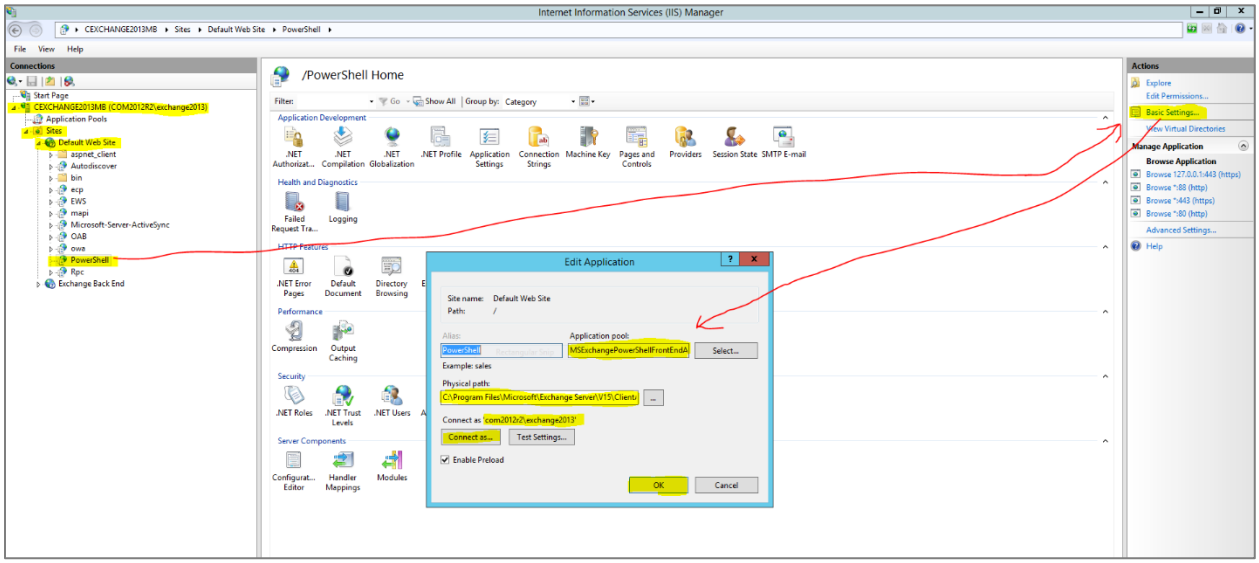


5) Go to **Powershell Virtual Directory** > **Basic Settings**. Make sure you have the correct **Application pool** and **Physical path** selected to access the PowerShell virtual directory on the host under IIS root.

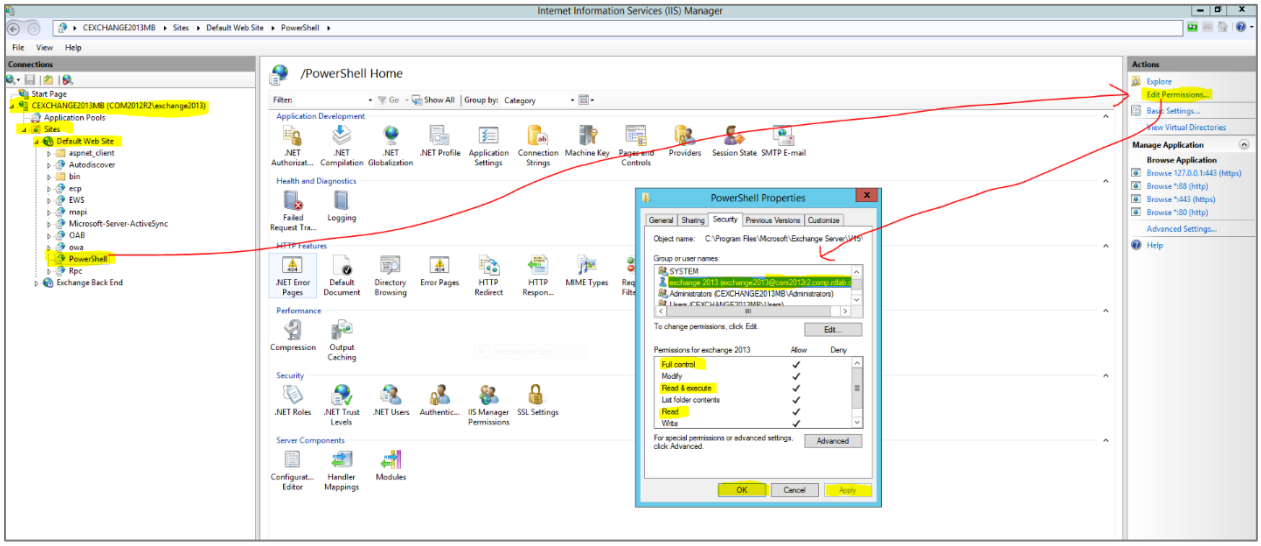
Use these settings:

Application pool: MSExchangePowerShellAppPool or MSExchangePowerShellFrontEndAppPool

Physical path: C:\Program Files\Microsoft\Exchange Server\V<Exchange Version>\ClientAccess\PowerShell



6) Make sure the Exchange user has Read permissions on the Physical path specified. To do this, go to **PowerShell Virtual Directory** > **Edit Permissions**. Select the **Security** tab. Assign **Read** permissions to the user performing the scan, as shown in the image below.



Scan User Privileges Required (when using a Scanner)

The user account provided for authentication must have certain privileges. We'll help you with the steps.

- Add new user account in Active Directory
- Add Roles/Group membership for newly created user account
- Enable Remote PowerShell for newly created user account

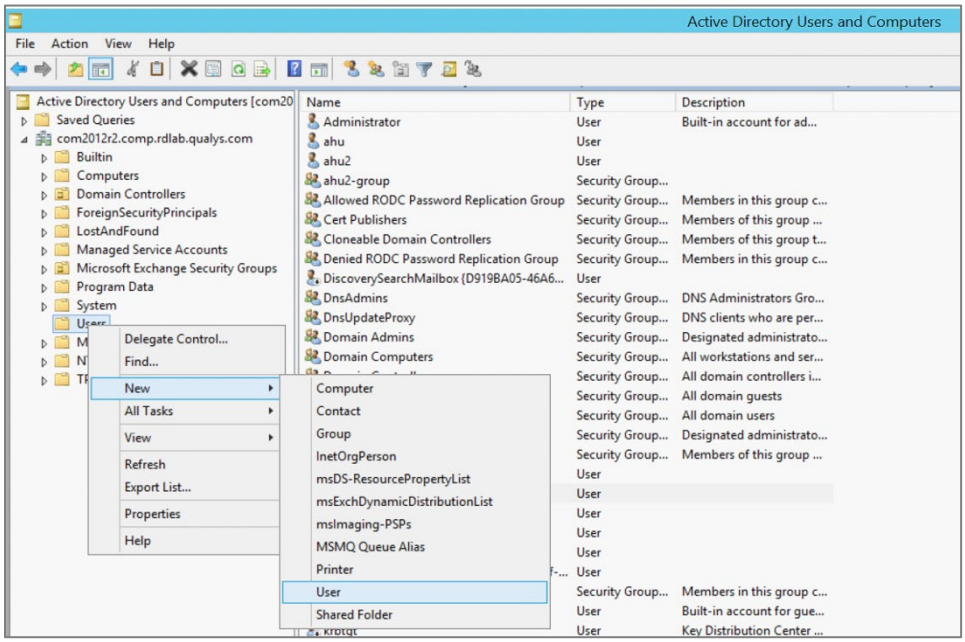
Create New User Account as MS Exchange Scan User in Active Directory

Follow these steps to create the new user account:

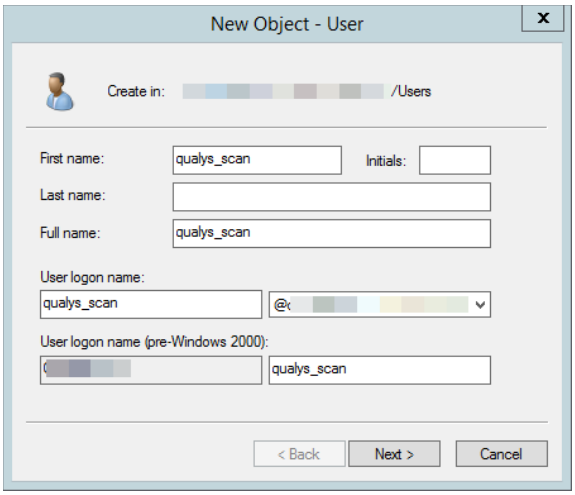
1) Open **Server Manager** and select **Active Directory Users and Computers** (ADUC) from the **Tools** menu.

2) In the left pane, expand your domain and click the **Users** container.

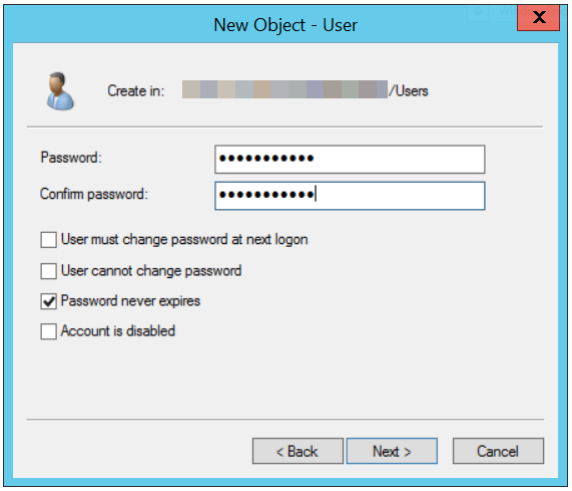
3) In the right pane, right click some empty space and select **New** > **User** from the menu.



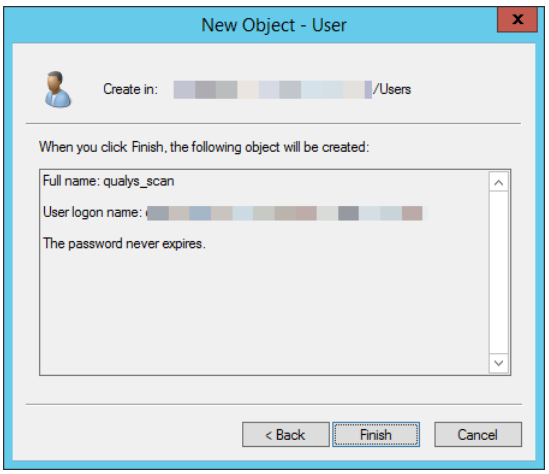
4) In the **New Object – User** window, enter a First name, Last name, User logon name, and then click **Next** to continue.



5) Type and confirm a **Password**, then click **Next**.



6) Check the information for the new user on the confirmation screen and click **Finish**.



Add Roles/Group Membership for Newly Created User Account

The user performing the scan should be an Exchange AD user with the following Roles/Group membership configurations to run specific Exchange PowerShell Cmdlets. Make sure the user is a part of Exchange Management Role Groups to run specific sets of Exchange PowerShell cmdlets as mentioned below.

Follow the steps below using Domain Administrator user:

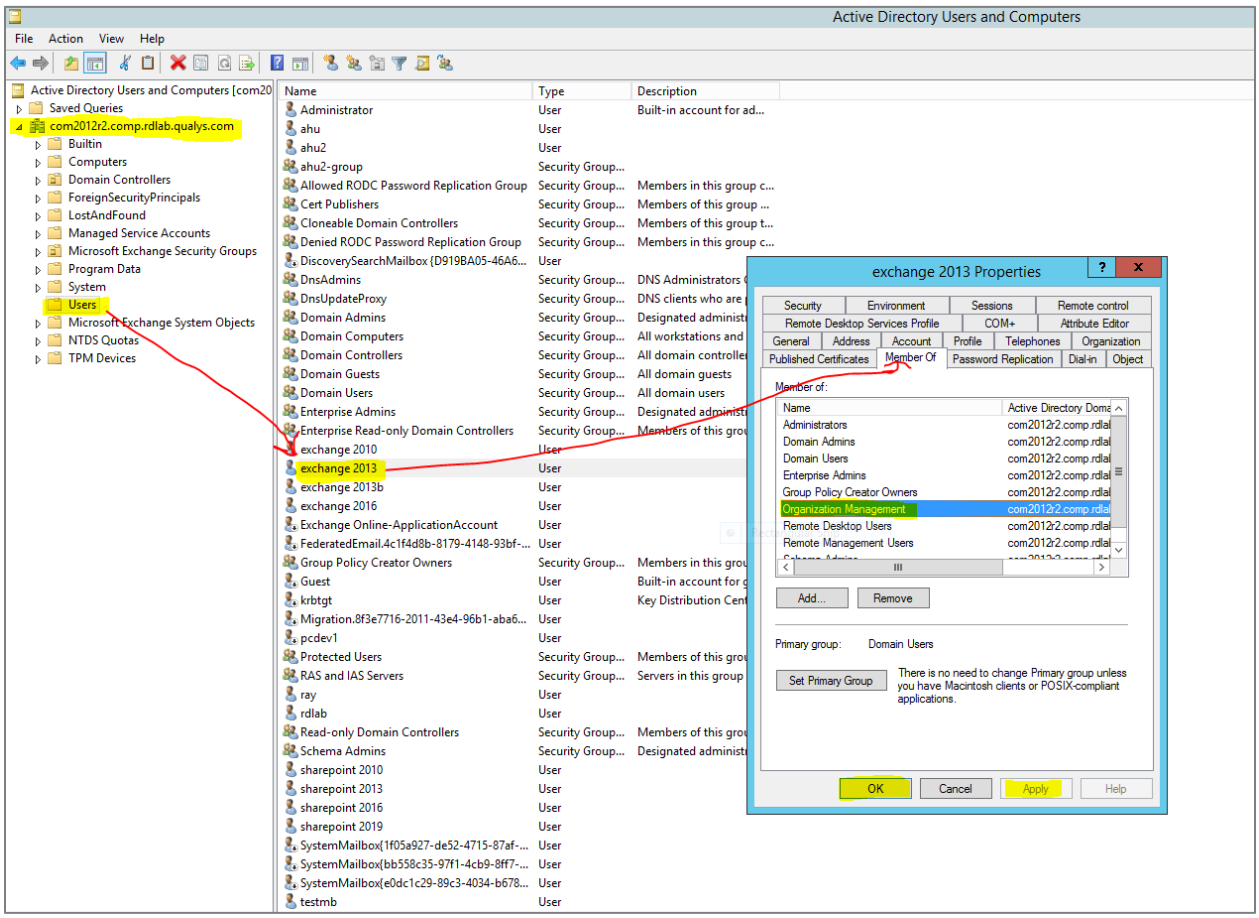
1) To assign a specific role to the user, go to **Active Directory Users and Computers** (dsa.msc). Under **Microsoft Exchange Security Groups**, right click the required group and add the **Exchange user** to **Exchange Role Group** as per the requirements listed below:

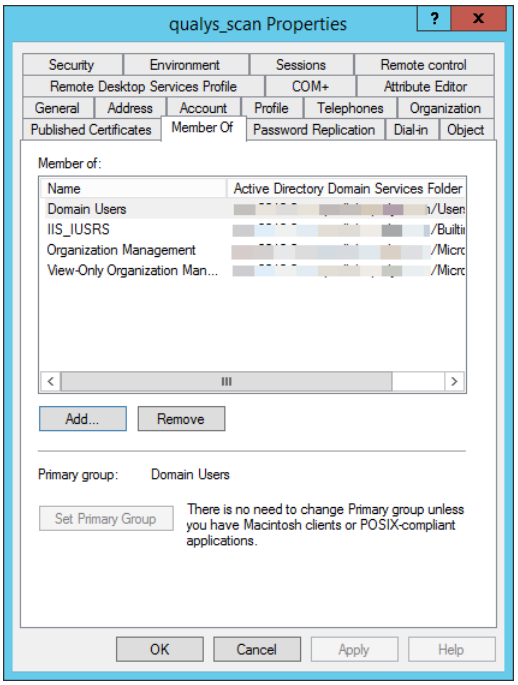
- IIS_IUSRS
- Organization Management
- Domain Users
- View-Only Audit Logs management

See the table below for requirements.

Feature/Exchange Cmdlets Category	Exchange Role/Security Group membership required
Administrator audit logging	Organization Management Records Management
Exchange admin center configuration settings	View-Only Organization Management
Exchange admin center connectivity	Organization Management Server Management
Exchange server configuration settings	Organization Management Server Management
Exchange Help settings	Organization Management
Message categories	Organization Management Hygiene Management Recipient Management Help Desk
Product key	Organization Management
Test system health	Organization Management Server Management
View-only administrator audit logging	Organization Management Records Management Note: You can also manually assign the View-Only Audit Logs management role to a management role group. For more information, see View-Only Audit Logs.

Feature/Exchange Cmdlets Category	Exchange Role/Security Group membership required
Write to audit log	Users that are members of any role group or assigned any management role can write to the administrator audit log.
Active Directory Domain Services server settings	Organization Management Server Management Recipient Management UM Management
Cmdlet extension agents	Organization Management
PowerShell virtual directories	Organization Management Server Management
PowerShell and WinRM installation	Local Server Administrator
Remote PowerShell	Organization Management

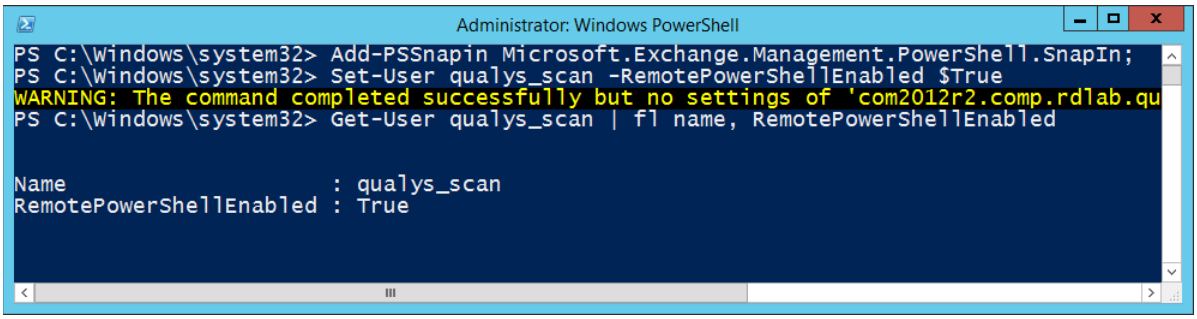




Enable Remote PowerShell for Newly Created User Account

Open a **Windows PowerShell** window (by selecting **Run as administrator**) and run the following command:

```
Set-User "qualys_scan" -RemotePowerShellEnabled $True
```



Verify Scan User Membership and Test Connection by PowerShell Script (when using a Scanner)

You'll need to complete these steps:

- Verify the membership of groups assigned to users
- Test connect to MS Exchange Server via Remote PowerShell

Verify the Membership of Groups Assigned to Users

Using the PowerShell commands below we can verify the above membership of groups assigned to users in AD. Note: Your user must be assigned the Role Management management role to run the `Get-ManagementRoleAssignment` cmdlet.

Below is the PowerShell command:

```
Get-ManagementRoleAssignment -RoleAssignee <Scan User Name>
```

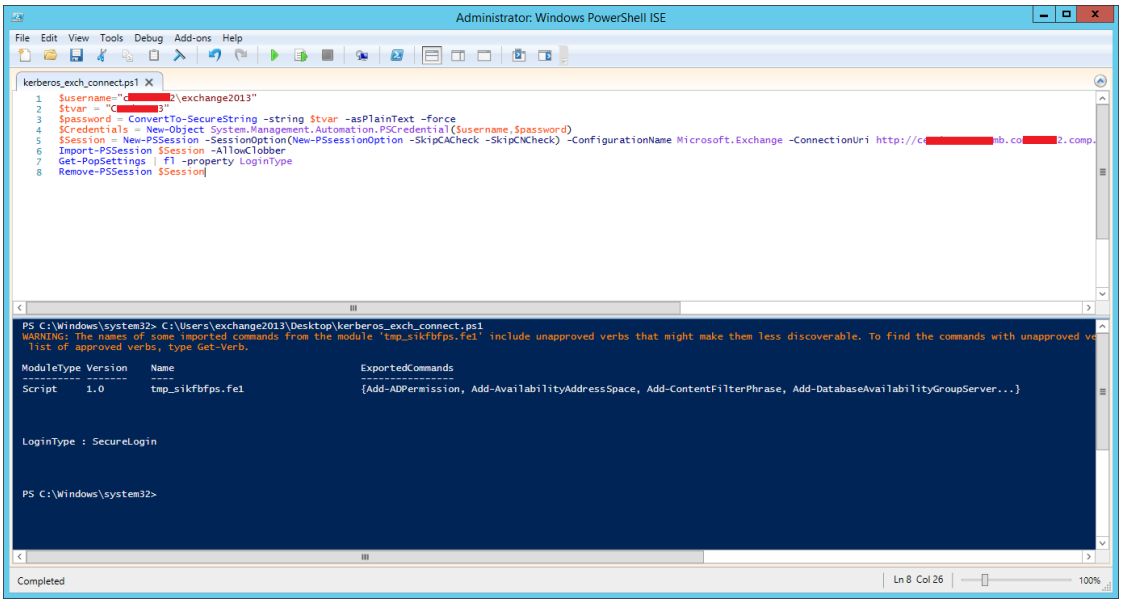
Test Connection to MS Exchange Server via Remote PowerShell

Here are the steps required to connect to PowerShell Virtual Directory using PS Script:

1) Open **PowerShell** or **PowerShell ISE** with **Run as Administrator** and insert below code:

```
$username="<DomainName>\<ScanUserName>"
$tvar = "<Password_Of_Scan_User>"
$password = ConvertTo-SecureString -string $tvar -asPlainText -force
$Credentials = New-Object
System.Management.Automation.PSCredential($username,$password)
$Session = New-PSSession -SessionOption(New-PSsessionOption -SkipCACheck -
SkipCNCheck) -ConfigurationName Microsoft.Exchange -ConnectionUri
http://<FQDN_of_Exchange_Server_Host>:80/powershell -authentication Kerberos
-Credential $Credentials
Import-PSSession $Session -AllowClobber
#You Can test any Exchange PowerShell Command as shown in below line:
Get-PopSettings | fl -property LoginType
Remove-PSSession $Session
```

2) Run the above code with correct input details as per your host setup and you should be able to see the connection result. An example is shown below. This ensures you are able to connect the PowerShell Virtual Directory using Remote PowerShell with the Scan User specified.



Manage Authentication Records (when using a Scanner)

Create an MS Exchange Server record in order to authenticate to a Microsoft Exchange Server running on a Windows host and scan it for compliance. Windows authentication is required so you will also need to create a Windows record for the host running the web server.

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

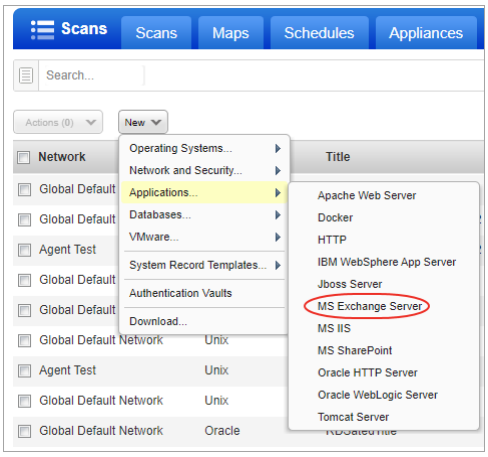
How to Create Authentication Records

Follow these steps to create authentication records.

1) Go to **Scans** > **Authentication**.

2) Check that you have a Windows record already defined for the host running the web server. If you don't, go to **New** > **Operating Systems** > **Windows** to create one.

3) Create an MS Exchange Server record for the same host. Go to **New** > **Applications** > **MS Exchange Server**.



Which users have permission to create records?

Managers can add authentication records. Unit Managers must be granted these permissions:

- Manage PC module

- Create/edit authentication records/vaults

How does it work?

We'll authenticate to each target host using the credentials provided in the Windows record. If the host is running an MS Exchange Server, then we'll check to see if an MS Exchange Server record exists. If yes, we'll use credentials from the Windows record to authenticate to the Windows system, access the web server configuration, and scan it for compliance.

Last updated: November 8, 2022