

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)	2
System Configuration Requirements (when using a Scanner)	2
Scan User Privileges Required (when using a Scanner)	7
Create New User Account as MS Exchange Scan User in Active Directory	7
Add Roles/Group Membership for Newly Created User Account	9
Enable Remote PowerShell for Newly Created User Account	
Verify Scan User Membership and Test Connection by PowerShell Script (when us Scanner)	sing a 11
· Verify the Membership of Groups Assigned to Users	
Test Connection to MS Exchange Server via Remote PowerShell	12
Manage Authentication Records (when using a Scanner)	13
Which technologies are supported?	
How to Create Authentication Records	
How does it work?	

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.

Add Roles and Features Wizard		- 0
Select features		DESTINATION SERVER SVR1.winadmins.loca
Before You Begin Installation Type	Select one or more features to install on the selected server. Features	Description
Server Selection Server Roles	Telnet Client TFIP Client VM Shielding Tools for Fabric Management	Windows Remote Management (WinRM) IIS Extension enables a server to receive a management
Features Confirmation Results	Windows Biometric Framework Image: Windows Defender Features (Installed) Windows Identity Foundation 3.5 Windows Internal Database Image: Windows PowerShell (2 of 5 installed) Image: Windows Server Backup Image: Windows Server Image: Windows Se	request from a client by using WS- Management. WinRM is the Microsoft implementation of the WS-Management protocol which provides a secure way to communicate with local and remote computers by using Web services.
	XPS Viewer	

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**.

Add Roles and Features Wiza	rd	– 🗆 X
Installation prog	ress	DESTINATION SERVER SVR1.winadmins.local
	View installation progress	
	Feature installation	
	Installation succeeded on SVR1.winadmins.local.	
	WinRM IIS Extension	
Results		
	You can close this wizard without interrupting run	nning tasks. View task progress or open this
	Export configuration settings	
	< Previous	Next > Close Cancel

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**.

V 3		Internet Information Services (IIS) Manager	_ 0 X
CEXCHANGE2013MB > Sites > Default Web S	ite + PowerShell +		□ ≈ ☆ @ •
File View Help			
Connections C C C C C C C C C C C C C	Authentication Group by: No Geoging Name Anonymous Authentication ASPAET Impersonation Basic Authentication Digit Authentication Windows Authentication	Status Reportse Type Diabled Diabled Diabled HTTP 401 Challenge Diabled HTTP 301 Challenge Diabled HTTP 301 Challenge Diabled HTTP 301 Challenge Pashed HTTP 301 Challenge	Alerts ▲ Click here blenn hon to Protrioure Estended Protrioure Advanced Setting Provider ₩ Help
Configuration: localnost applicationHost.config. < location pather Deta	uit web site/Powersnell >	II I I I I I I I I I I I I I I I I I I	
	Administrator	Window Since interimentation -	11:22 PM

Negotiate	Move Up
	Move Down
	Remove
Select a provider from	the list of available providers and click Add
Select a provider from to add it to the enable Available Providers:	the list of available providers and click Add d providers.

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:

Internet Information Services (IIS) Manager	- 0 X
د کرد کرد کرد کرد کرد کرد کرد کرد کرد کر	🚥 🖂 🏠 🔞 •
File View Help	
Connections	Actions
Q. El 2 19. Proversnei Home	Open Festure
- Start Page - B - concurrent till & COLUME TO BE	🔉 Explore
Application Pools	Edit Permissions
	Basic Settings
A top detautive Site	View Virtual Directories
Autodiscover Autonizat Compilation Globalization Settings Strings Controls	Manage Application
bin Health and Disgnostics	Browse Application
EVS EVS	Browse *:88 (http)
> Transfer Antipolity Failed Logging	Browse *:443 (https)
k-g 0.AB Request is a function of the contract of the contrac	Browse *:80 (http)
HTTP:Fettures	Advanced Settings
	😻 Help
b Schunge Back End NIET From Default Directory Error Pages HTTP MIME Types Request Directory Error Pages HTTP AMME Types Request	
Pages outwinds providing induction negative reading	
A He	
Compression Ustput	
Security W Window Step	
NT Take Arthur Arthur Arthur State Contact	
Levels Permissions	
Server Components	
Configurat. Handler Modules	
Editor Mappings	
C features View WC Content View	
Configuration: Tocathost applicationHost.config., <location path="Datault Web Site/PowerShill"></location>	•]

Default Web Site:

v 3	Internet Information Services (IIS) Manager	- 0 ×
🕞 🔞 + CEXCHANGE2013MB + Sites + Default Web Sit		📅 🖂 🔂 🛞 •
File View Help		
Connections	C Defendbulleb Cite United	Actions
Q, · 🔡 💋 😣	Default web site Home	Open Feature
Start Page	Filter: • 🐺 Go - 😡 Show All Group by: Category • 🔝 •	🔉 Explore
- J Application Pools	Application Development	Edit Permissions
A B Default Web Ste		Edit Site Bindings
	NET .NET .NET NETProfile Application Connection Machine Key Pages and Providers Session State SMTP E-mail	Basic Settings
	Authorizzt Compilation Olobalization Settings Strings Controls	View Applications
5-39 ecp	Heath and Usegnotics	View Virtual Directories
b ⊕ EWS b ⊕ mapi		Manage Website
Microsoft-Server-ActiveSync	Failed Logging Request Tra-	 Nestart Start
b OAB	HTTP/features A	Stop
- @ PowerShell		Browse Website
b-gr KpC b Exchange Back End	NECTION Default Default Protocols HTTP HTTP MIME Types Request	Browse 127.0.0.1:443 (https) Browse *30 (https)
	Page Document Browsing Redirect Respon Filtering	Browse *>443 (https)
	Performance	Browse *:80 (http)
	에 좋~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Advanced Settings
	Compression Output	Configure Failed Request Tracing
	Country Country	Limits
		🕜 Help
	instructes asterios instructes instructes de la manager (asterios de la manager) Levels Permisions	
	Server Components	
	i 🗊 🛋 🍯 付	
	Configurat Handler ISAPI filters Modules	
	Editor Meppings	
		-
	Content View	
Ready		4

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.

			Active Directory Users and Computers
File Action View Help			
🗢 🏟 🖄 📰 🤞 🖬 🚺 🗶 🖾 🎯 🕞 🚺	l 🗊 🗏 🔌 🛍 🍸 🚨 🖗		
Active Directory Users and Computers [com20 Saved Queries com2012r2.comp.rdlab.qualys.com b Builtin b Computers b Domain Controllers b Domain Controllers b Domain Controllers b Domain Controllers b Microsoft Exchange Security Groups b Program Data b Nicrosoft Exchange Security Groups b Program Data b N Find b N Find b TT New All Tasks View All Tasks View Refresh Export List Properties Help	Name Administrator ahu ahu2-group Allowed RODC Password Replication Group Cert Publishers Coneable Domain Controllers Denied RODC Password Replication Group DiscoverySearchMailbox (D919BA05-46A6 DnsAdmins DnsJpdateProxy Domain Admins Domain Computers Computer Computer Contact Group InetOrgBerson msDS-ResourcePropertyList msExchDynamicDistributionList msImaging-PSPs MSMQ Queue Alias	Type User User Security Group Security Group.	Description Built-in account for ad Members in this group c Members of this group t Members of this group c DNS Administrators Gro All domain controllers i All domain users Designated administrato Members of this group
	Printer F User	User Security Group	Members in this group c
	Shared Folder	User User	Built-in account for gue Key Distribution Center

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

	New Object - User
🧏 Create	in: /Users
First name:	qualys_scan Initials:
Last name:	
Full name:	qualys_scan
User logon name:	
qualys_scan	@
User logon name (p	pre-Windows 2000):
(qualys_scan
	< Back Next > Cancel

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

New Object - User
Create in:
Password: Confirm password:
User must change password at next logon User cannot change password Password never expires Account is disabled
< Back Next > Cancel

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

New Object - User	¢		
Create in:			
When you click Finish, the following object will be created:			
Full name: qualys_scan			
User logon name:			
The password never expires.	The password never expires.		
×			
	-		
< Back Finish Cancel]		

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	<u>Organization Management</u> <u>Records Management</u>
Exchange admin center configuration settings	View-Only Organization Management
Exchange admin center connectivity	<u>Organization Management</u> <u>Server Management</u>
Exchange server configuration settings	<u>Organization Management</u> <u>Server Management</u>
Exchange Help settings	Organization Management
Message categories	Organization Management Hygiene Management Recipient Management Help Desk
Product key	Organization Management
Test system health	<u>Organization Management</u> <u>Server Management</u>
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 <u>View-Only Audit</u> 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	<u>Organization Management</u> <u>Server Management</u>
PowerShell and WinRM installation	Local Server Administrator
Remote PowerShell	Organization Management



		qualys_s	can	Prop	erties		?	X
Security Environme		vironment	Sessions		Remote control		ontrol	
Remote	Remote Desktop Services Profile		•	COM+ /		A	Attribute Editor	
General	eneral Address Account		P	rofile	ofile Telephones		Organization	
Published Certificates		Member Of		Password Replication		tion	on Dial-in Obje	
Member of	:							
Name			Activ	e Direc	tory Doma	ain Ser	vices Fo	lder
Domain I	Jsers						1/	Usen
IIS_IUSF	RS	1					/	Builtir
Organiza	tion Manag	ement					/	Micro
Add Remove								
Primary group: Domain Users Set Primary Group you have Macintosh clients or POSIX-compliant applications.								
OK Cancel Apply Help								

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
```

	Administrator: Windows PowerShell		x
PS C:\Windows\system32>	Add-PSSnapin Microsoft.Exchange	.Management.PowerShell.SnapIn;	^
WARNING: The command co PS C:\Windows\system32>	mpleted successfully but no sett Get-User qualys_scan fl name,	ings of 'com2012r2.comp.rdlab.qu RemotePowerShellEnabled	
Name RemotePowerShellEnabled	: qualys_scan : 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.

50 5 0 M T 1			
File Edit View Tools	Debug Add-ons Help		
1 🗀 🔒 🤾 🧣	🗈 ≽ 🔊 (° 🕨 🚯		
kerberos exch connect.p	s1 X		
1 \$username="d	2\exchange2013"		^
2 \$tvar = "C 3 \$password = 0	3" ConvertTo-SecureString -string 1	Stvar -asPlainText -force	
4 \$Credentials 5 \$Session = N	 New-Object System.Management. ew-PSSession -SessionOption(New- 	.Automation.PSCredential(Susername,Spassword) -PSsessionOption -SkipCACheck -SkipCNCheck) -ConfigurationName Microsoft.Exchange -ConnectionUri http://ce uincomm ub.co	2.comp.
6 Import-PSSes 7 Get-PopSetti	sion SSession -AllowClobber ngs fl -property LoginType		
8 Remove-PSSes	sion \$Session		=
		84	~
RE C () Windows) syste		11	/
PD C. (WITHOWS (System	m22x CiVUconcVoychango2012\Dock	stop) konhonos oveh connost psi	
WARNING: The names list of approved of	m32> C:\Users\exchange2013\Desk of some imported commands from verbs, type Get-Verb.	<pre>ctopikerberos_exch_connect.ps1 the module 'tmp_sikfbfps.fc1' include unapproved verbs that might make them less discoverable. To find the commands with the module 'tmp_sikfbfps.fc1'</pre>	unapproved ve
WARNING: The names list of approved of ModuleType Version	m32> C:\Users\exchange2013\Desk of some imported commands from verbs, type Get-Verb. Name	<pre>ctop\kerberos_exch_connect.p1 the module 'tmp_sikfbfps.fe1' include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands</pre>	unapproved ve
WARNING: The names list of approved of ModuleType Version Script 1.0	<pre>m32> C:\Users\exchange2013\Desk of some imported commands from verbs, type Get-Verb. Name tmp_sikfbfps.fe1</pre>	<pre>ctop\kerberos_exch_connect.psi the module 'trap_sitfifps.fel' include unapproved verbs that might make them less discoverable. To find the commands with</pre>	unapproved ve
WARNING: The names list of approved of ModuleType Version Script 1.0	m32> C:\Users\exchange2013\Desk of some imported commands from verbs, type Get-Verb. Name tmp_sikfbfps.fe1	<pre>ctop\tepros_exch_connect.ps1 the module 'trap.istfifps.fe1' include unapproved verbs that might make them less discoverable. To find the commands with</pre>	unapproved ve
WARNING: The names list of approved y ModuleType Version Script 1.0	m32> C:\Users\exchange2013\Desk of some imported commands from erbs, type Get-Verb. Name tmp_sikfbfps.fe1	<pre>ctop\kerberos_exch_connect.ps1 the module 'txp_sikfifps.fc1' include unapproved verbs that might make them less discoverable. To find the commands with</pre>	unapproved ve
WARNING: The names list of approved of ModuleType Version Script 1.0 LoginType : Secured	m32> C:Vlser3/exchange2013/Desk of some imperied commands from erbs, type Get-Verb. Name tmp_sikfbfps.fel	<pre>ctop\theros_exch_connect.ps1 the module trap_intrifus_rel1 include unapproved verbs that might make them less discoverable. To find the commands with the module trap_intrifus_rel1 include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands (Add-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer)</pre>	unapproved ve
WARNING: The names list of approved v ModuleType Version Script 1.0 LoginType : Secure	mB2> C:Vusers/exchange2013/Desk of some: reported commands from erbs; type Get-Verb. Name tmp_sikfbfps:fe1 ogin	<pre>ctop\Leberos_exch_connect.ps1 the module 'trap_sitrfFast_include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands [Add-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer}</pre>	unapproved ve
WARNING: The names list of approved / ModuleType Version Script 1.0 LoginType : Secured PS C:\Windows\syst	mB2> C:VUsers/vexchange2013/Desk of some mported commands from erbs; type Get-Verb. Name tmp_sikfbfps.fel	<pre>ctop\Leberos_exch_connect.ps1 the nodule 'trap_sitfips.fe1' include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands</pre>	unapproved ve
WARING: The names list of approved ModuleType Version Script 1.0 LoginType : Secured PS C:\Windows\syste	mB2> C:VUsers/vexchange2013/Desk of some :mported commands from erbs; type Get-Verb. Name tmp_sikfbfps.fel	<pre>ctop\teperos_exch_connect.ps1 the module 'tep_siftifps.fe1' include unapproved verbs that might make them less discoverable. To find the commands with</pre>	unapproved ve
WARKING: The names list of approved 1 ModuleType Version Script 1.0 LoginType : Securel PS C:\Windows\syste	<pre>mB2> C:\User3vexchange2013\Deek of some :mpo:cel commands from erbs; type Get=Verb; name tmp_sikfbfps.fel ogin</pre>	<pre>ctop\kreperos_exch_connect.ps1 the module trap_intfigure_set1 include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands {Add-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer}</pre>	unapproved ve
WARKING: The nomes list of approved ModuleType Version Script 1.0 LoginType : Securet PS C:\Windows\syste	m32> C:VUser3vexchange2013/Desk of some: mpored commands from erbs, type Get-Verb. Name tmp_sikfbfps.fel	<pre>ctop\LevBeros_exch_connect.psi the module trap_liftFigs.fcl' include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands {Add-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer}</pre>	unapproved ve
WARKING: The names list of approved ModuleType Version Script 1.0 LoginType : Secured PS C:\Windows\syste	m32> C:Vuser3vexchange2013/Desk of some: reported commands from erbs; type Get-Verb. Name tmp_sikfbfps;fe1 ogin	<pre>ctop\LepParse_exch_connect.ps1 the module 'trap_sitrifps:fe1' include unapproved verbs that might make them less discoverable. To find the commands with ExportedCommands {/dd-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer} {/dd-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-DatabaseAvailabilityGroupServer} </pre>	unapproved ve

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**.

E Scans	Scans	Maps		Schedules	Appliances
Search					
Actions (0) 🔻	New 🕶				
Network	Operating Syste Network and Se	ms curity	•	Title	
Global Default	Applications		•	Apache We	b Server
Global Default	Databases		Þ	Docker	
Agent Test	VMware		Þ	HTTP	
Global Default	System Record	Templates	Þ	IBM WebSp	ohere App Server
Global Default	Authentication V	/aults		MS Exchan	ge Server)
Clobal Default	Download			MSIIS	
Giobal Default I	Network	Unix		MS ShareP	oint
Agent Test		Unix		Oracle HTT	P Server
Global Default Network		Unix		Oracle Web	Logic Server
Global Default Network		Oracle	1	Tomcat Ser	nue

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