



Hardening Guide

Netsurion Open XDR 9.4 Server

Publication Date

April 05, 2024

Abstract

This guide describes the procedure to create and maintain a secure environment for the server that runs the Netsurion Open XDR 9.4 Manager.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.4.

Audience

This guide is for the Netsurion Open XDR users responsible for monitoring and managing network security.

Table of Contents

1	Overview	5
1.1	Applying Group Policies on Windows Server 2019	5
1.2	Securing IIS Web Server	5
1.3	Securing SQL Server	5
1.4	Adding Windows Firewall Exceptions	6
1.5	Allowing Outbound Access to Public URL's	8
1.6	Checking for Vulnerability Scanner	9
1.7	Restricting Email/File-Sharing Website Access	9
1.8	Netsurion Open XDR Endpoint Security	10
2	Harden Windows Server – Detailed View	10
2.1	Applying Group Policies in a Member Server on Windows Server 2019	10
2.2	Applying Group Policies in a Workgroup on Windows Server 2019	17
3	Securing IIS Web Server (10 and 11)	19
3.1	Mandatory Requirements	19
3.2	IIS setup on Windows	19
3.3	Restricting Netsurion Open XDR Web Console Access	39
3.4	Installing IP and Domain Restriction in Windows	39
3.5	Configuring IP Address and Domain Restrictions in Windows	41
3.6	Request Filtering in IIS 10 and 11	42
3.6.1	Installing Request Filtering in Windows	42
3.6.2	Installing Request Filtering in Windows	43
3.6.3	Allowing/Denying Access to a Specific File Name Extension	44
4	Securing SQL Database Server	46
4.1	Reducing the Surface Area for SQL Server Components	46
4.2	Reducing the Surface Area for SQL Server Services	47
4.2.1	SQL Server SA Account	51
5	Netsurion Open XDR Settings	51
5.1	Securing Agent Configuration and Saving it as a Template	51
5.2	Protecting the Current Configuration Settings for Local System	51
5.2.1	Applying Configuration to Agent System(s)	53
5.3	Securing EventVault Storage	55
5.3.1	Changing the Service Account	56

6	Enabling Two-Factor Authentication in Netsurion Open XDR Web Console	58
6.1	Adding New Users.....	60
6.2	Enabling 2FA Option for Existing Users	61
6.3	Disabling 2FA.....	62
7	Checking for Vulnerability Scanner.....	63

1 Overview

Apply the Microsoft security policies (SSLF- Specialized Security Limited Functionality) to harden the Windows server. Considered the following policies for the hardening process.

1.1 Applying Group Policies on Windows Server 2019

Harden Windows Server 2019 according to the standard policy. Click the following link to download the GPO.

[Download WS2019-GPO.zip](#)

Apply the following policies:

- WS2019-Domain Security
- WS2019-Member Server
- WS2019-Defender Antivirus
- WS2019-Member Server Credential Guard
- WS2019-Internet Explorer 11 - User
- WS2019-Internet Explorer 11 – Computer

1.2 Securing IIS Web Server

In the IIS Manager, create a **Certificate request**. After receiving, install the certificate.

For IIS 7 Web Server,

- Do not place the Netsurion Open XDR Manager in the DMZ network.
- Give administrative access only to Authorized users or administrators.
- Disable Directory Browsing in IIS.
- Do not install Internet printing Extension on the Netsurion Open XDR Manager.

1.3 Securing SQL Server

- While installing the SQL server, install only 'Database Engine Services'. Other services are not required.
- Disable (or leave disabled) the following SQL services:
 - **SQL Server VSS Writer** service
 - **SQL Server Browser** service
 - **SQL Active Directory Helper** service
- Assign the **Sysadmin** role only to the authorized administrators and users.
- Install the recent service packs and critical fixes for the SQL Server and Windows.
- Remove the BUILTIN\Administrators group from the SQL Server Logins.

Note

Assign **sysadmin** privileges to other users before removing the built-in administrators.

1.4 Adding Windows Firewall Exceptions

Add the ports/.exe in use to the firewall exception list. Any number of VCPs can be added based on the system capacity. For Netsurion Open XDR, add the following port numbers/.exe to the firewall exception list:

Port Number	Used For
14505 (TCP/UDP)	Windows Receiver, Multiple VCPs can be configured
14502, 14508 (TCP)	Change Audit
14503 (TCP)	Netsurion Open XDR Certificate server
14506 (TCP)	Netsurion Open XDR Agent
14507 (TCP)	Collection Master
443 (TCP)	Netsurion Open XDR securely access (HTTPS), Netsurion Open XDR Endpoint Security
514 (UDP/TCP)	Syslog Receiver, Multiple VCP's can be configured
14504	Netsurion Open XDR Active Watchlist
9200	Elasticsearch-service-x64, Elastic Cross Cluster
9300	Elastic Cross Cluster Note: Applicable for Netsurion Open XDR 9.4 version.
6514	Netsurion Open XDR Endpoint Security Note: This port is configurable. In case of a change in port number, the Netsurion Open XDR team will notify. Note: Applicable for Netsurion Open XDR 9.4 version.

Netsurion Open XDR Web console by default uses few ports for communication. These ports must be added to the firewall exception on the Netsurion Open XDR Manager.

Protocol	Local Port	Remote Port	Source (Session Initiator)	Target (Listener)	Usage/Purpose
TCP	14506	All	Netsurion Open XDR Agent Service	Netsurion Open XDR Agent Service running on Netsurion Open XDR Console	Configuration synchronization request
TCP	14503	All	Netsurion Open XDR Agent Service	License Server running on Netsurion Open XDR Console	License details and verification request
TCP/UDP	14505	All	Netsurion Open XDR Agent Service	Netsurion Open XDR Receiver running on Netsurion Open XDR Console	Default port used for receiving events
TCP	14502	All	Change Audit Service	Change Audit Service running on Netsurion Open XDR Console	Receiving snapshot files
TCP	14509	All	Event Correlator	Correlator	Event Correlator component
TCP/UDP	514	All	syslog devices	Netsurion Open XDR Syslog Receiver running on Netsurion Open XDR Console	Virtual Collection Point Syslog Port used for receiving Syslog
TCP	14507	All	Collection Point	Collection Master	Data transfer between Collection Point and Collection Master [Default port]
TCP/UDP	162	All	SNMP devices	Trap Tracker Receiver running on Netsurion Open XDR Console	Port used for receiving SNMP v1, v2c and v3 Traps/Informs
TCP	14504	All	Netsurion Open XDR modules requesting Active watch list lookups	Netsurion Open XDR Watch list server running on Netsurion Open XDR Console	Serves the Active watch list lookup requests.
TCP	9200,9300	Any	Collection Master	Collection Point	Cross-Cluster Elastic Search Collection.
TCP	All	14503	Netsurion Open XDR Agent Service	License Server running on Netsurion Open XDR Console	License update request
TCP	All	14506	Netsurion Open XDR Agent Service	Netsurion Open XDR Agent Service running on Netsurion Open XDR Console	Configuration synchronization request
TCP/UDP	All	14505	Netsurion Open XDR Agent Service	Netsurion Open XDR Manager	Sending the logs
TCP	All	14502	Change Audit Service on	Change Audit Service on Netsurion Open XDR	Configuration management

Protocol	Local Port	Remote Port	Source (Session Initiator)	Target (Listener)	Usage/Purpose
			ChangeAudit Agent	Console	
TCP	All	14508	Change Audit Service on ChangeAudit Agent	Change Audit Service on Netsurion Open XDR Console	On-demand policy comparison request
TCP	All	443	Netsurion Open XDR Endpoint Security Agent	IP address: 35.237.75.235	Applicable for EES sensor deployment only

1.5 Allowing Outbound Access to Public URL's

Netsurion Open XDR Manager/Sensor requires access to certain public URL/IP addresses to perform various functions like IOC validation/DNS lookup, etc. Below are the URLs that must be allowed in your gateway firewall/Proxy for Netsurion Open XDR to access these URLs.

URL/Domain	Port/Protocol/Direction	Purpose
*.eventtracker.com *.netsurion.com	443/TCP/Outbound	Download the XDR updates and DSI
threatcenter.netsurion.com threatcenter.eventtracker.com	443/TCP/Outbound	Netsurion Threat Center
nsrl.eventtracker.com	9120/TCP/Outbound	Netsurion NSRL server (Hash IOC Lookup)
certificates.eventtracker.com	443/TCP/Outbound	Netsurion Licensing server
ipinfo.io	443/TCP/Outbound	Load the map in Machine Learning Dashboard
geolite.maxmind.com	80/TCP/Outbound	Download the Geolocation details in the Attackers Dashboard
maps.google.com	443/TCP/Outbound	Load the map in the Attackers Dashboard
virustotal.com	443/TCP/Outbound	IOC lookup from Application Control
hybrid-analysis.com	443/TCP/Outbound	IOC lookup from Application Control
whois.domaintools.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
exchange.xforce.ibmcloud.com api.xforce.ibmcloud.com xforce-api.mybluemix.net	443/TCP/Outbound	IOC lookup from Threat Dashboard

URL/Domain	Port/Protocol/Direction	Purpose
rules.emergingthreats.net	443/TCP/Outbound	IOC lookup from Threat Dashboard
otx.alienvault.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
ipvoid.com	80/TCP/Outbound	IOC lookup from Threat Dashboard
senderbase.org talosintelligence.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
app.recordedfuture.com	443/TCP/Outbound	IOC lookup from Threat Dashboard

1.6 Checking for Vulnerability Scanner

Scan the hardened Netsurion Open XDR system for vulnerabilities. This is applicable only if the Vulnerable Scanner is used.

1.7 Restricting Email/File-Sharing Website Access

- Though Internet access is required for Netsurion Open XDR to perform certain functions such as Threat Intel Feeds etc., certain accesses need to be restricted to ensure security.
- Restrict access to personal emails/file sharing websites (**Gmail, Yahoo, Hotmail, FileZilla, Dropbox, External SharePoint, etc.**) under the category blocking of URL or Web content filtering service. This secures the system against Data Ex-filtration attempts of the logs stored in the Netsurion Open XDR instance.
- Apart from this, it is mandatory to block the below sites on the Netsurion Open XDR Manager. Popular categories to be blocked are shown below:

Abortion	Illegal / Questionable	Pornography
Adult / Mature Content	Illegal Drugs	Proxy Avoidance
Alcohol	Intimate Apparel / Swimsuit	Sex Education
Alternative Sexuality / Lifestyles	Nudity	Spyware / Malware Sources
Alternative Spirituality / Occult	Open Image / Media Search	Spyware Effects
Extreme	Peer-to-Peer (P2P)	Suspicious
Gambling	Personals / Dating	Tobacco
Hacking	Phishing	Violence / Hate / Racism

1.8 Netsurion Open XDR Endpoint Security

The logs from the EES endpoints are collected centrally and forwarded to the Netsurion Open XDR Web console. Hence to receive the logs, some configuration changes are needed on the Netsurion Open XDR console. As part of the standard configuration, the logs are received from prod080520.customers.deepinstinctweb.com (**35.237.75.235**) on port **6514**.

2 Harden Windows Server – Detailed View

Configure the following aspects to harden the Netsurion Open XDR Manager:

- Harden Windows Server
- Secure IIS Web Server
- Secure SQL Server
- Firewall Settings
- Netsurion Open XDR Settings
- Check with Vulnerability Scanner

2.1 Applying Group Policies in a Member Server on Windows Server 2019

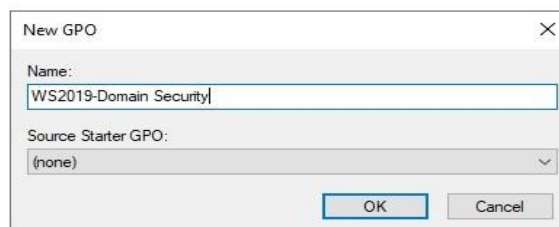
Step 1: Click the link below to download the GPO and extract the contents of the zip file to the system.

[Download WS2019-GPO.zip](#)

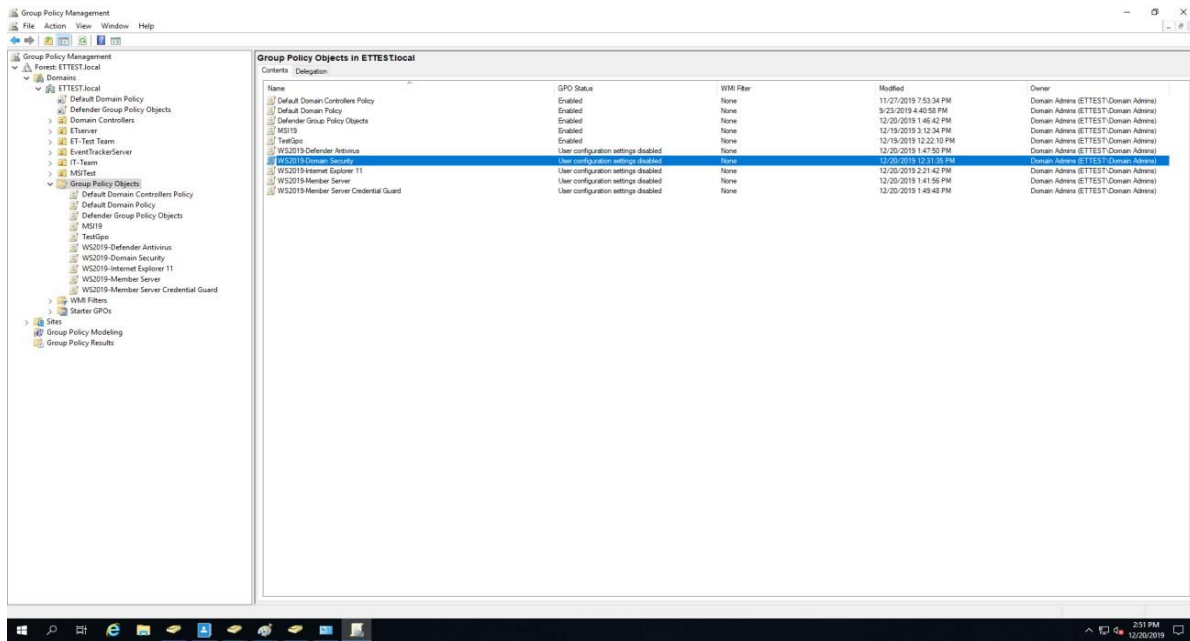
When creating a new 'Group Policy Objects', refer the GPO folder available in the extracted folder.

Step 2: Create new Group Policy Objects.

1. Click the **Start** button, select **Administrative Tools**, and then select **Group Policy Management**.
2. In the **Group Policy Management** pane, expand the **Domains** node, and then expand the 'local system' node.
3. Right-click **Group Policy Objects** and click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS2019-Domain Security** and click **OK**.

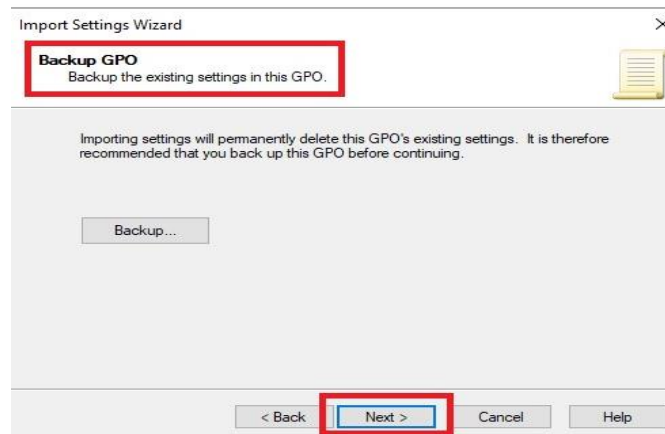


Similarly, create a new GPO for **WS2019-Member Server**, **WS2019-Defender Antivirus**, **WS2019-Member Server Credential Guard**, **WS2019-Internet Explorer 11 - User**, and **WS2019-Internet Explorer 11 - Computer** respectively.

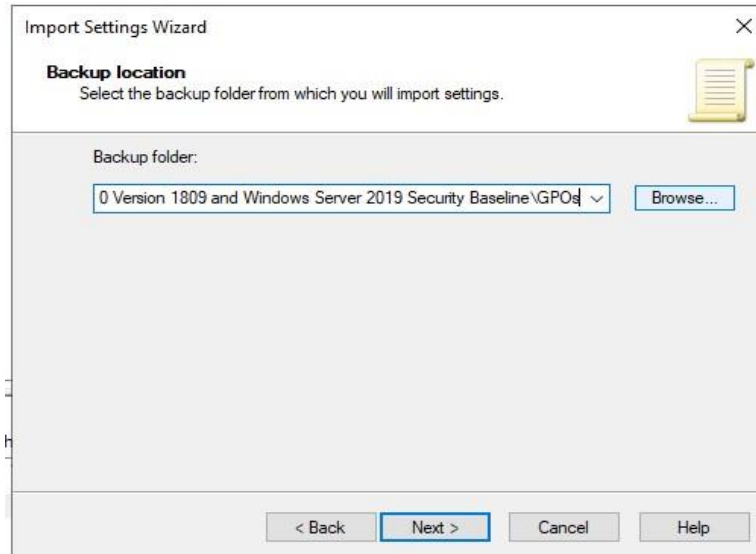


Step 3: Import Group Policy Settings.

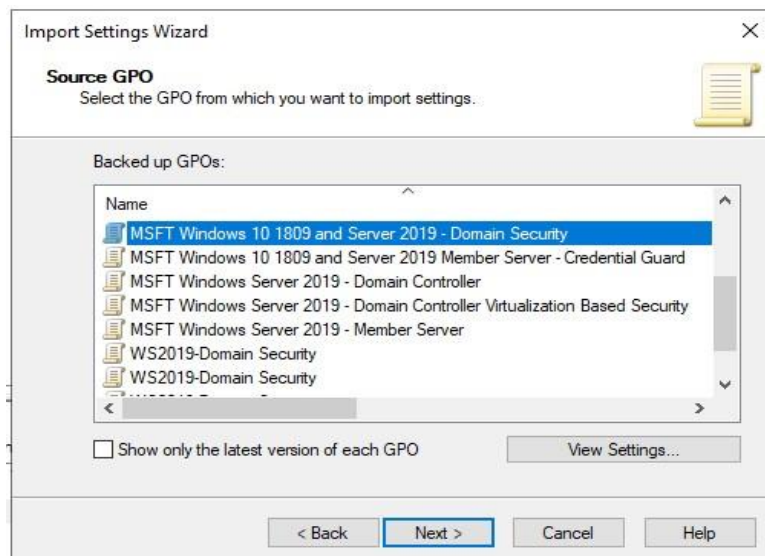
1. Right-click the newly created GPO (For example, **WS2019-Domain Security**), and click **Import settings**.
2. Click the **Next** button to start the importing process.
3. In **Backup GPO**, click the **Next >** button.



4. In the **Backup location**, browse the backup folder path where the settings are to be imported.
5. Click the **Next >** button.



6. Click the **Next** button.



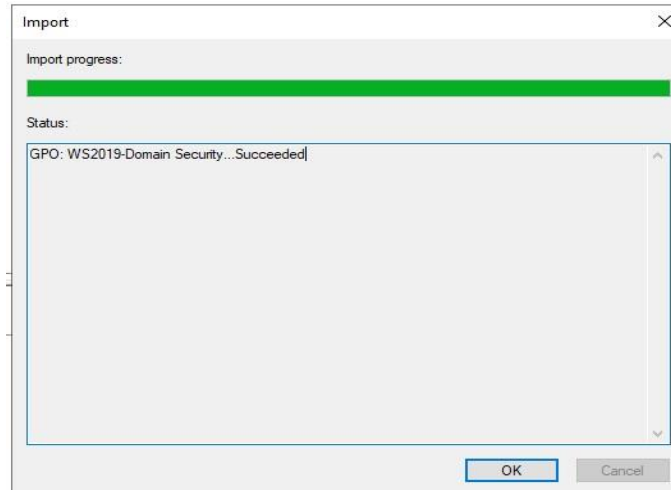
7. In **Source GPO**, select the **WS2019-Domain Security** GPO and click the **Next >** button.

8. In **Scanning Backup**, after scanning settings are complete, click the **Next >** button.

9. In **Migrating References**, click the **Next >** button.

10. Click **Finish**.

11. After successfully importing, click the **OK** button.

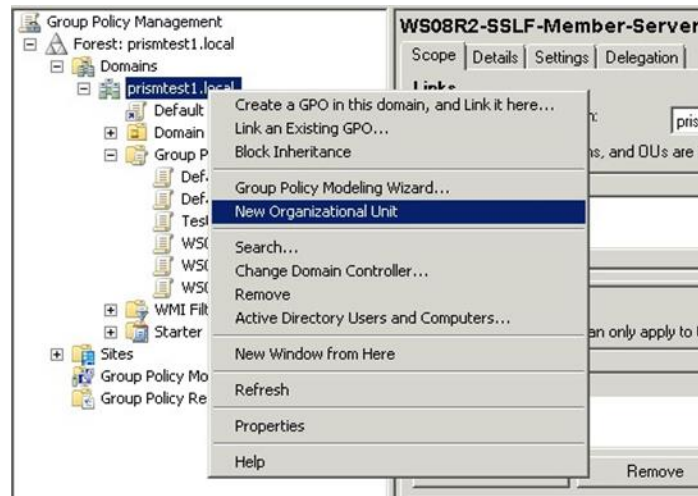


Group policy import is complete for **WS2019-Domain Security**.

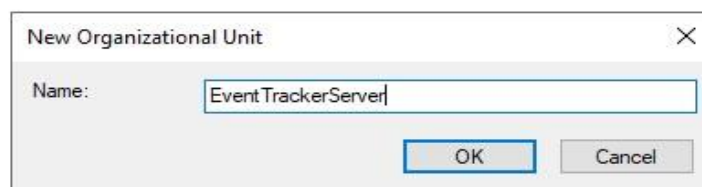
12. Repeat the steps from 1 to 11 to import Group Policy for **WS2019-Member Server, WS2019Defender Antivirus, WS2019-Member Server Credential Guard, and WS2019-Internet Explorer 11- User and Computer**.

Step 4: Create new 'Organizational Unit' (OU).

1. Right-click the server computer name and click **New Organizational Unit**.

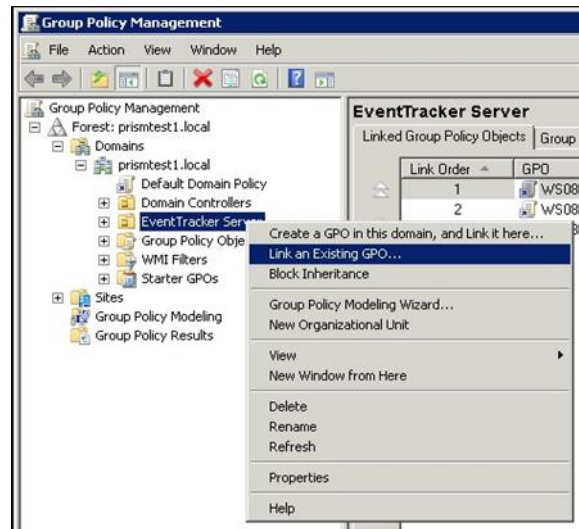


2. Enter the new organizational unit (OU) name and click **OK**. Example: Netsurion Open XDR Manager

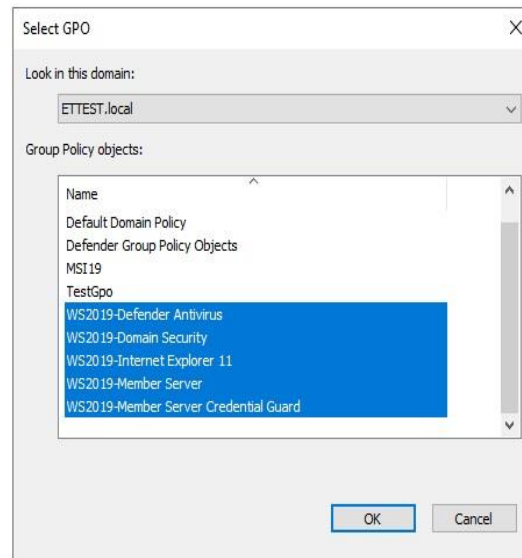


Step 5: Link the existing GPO to the newly created OU.

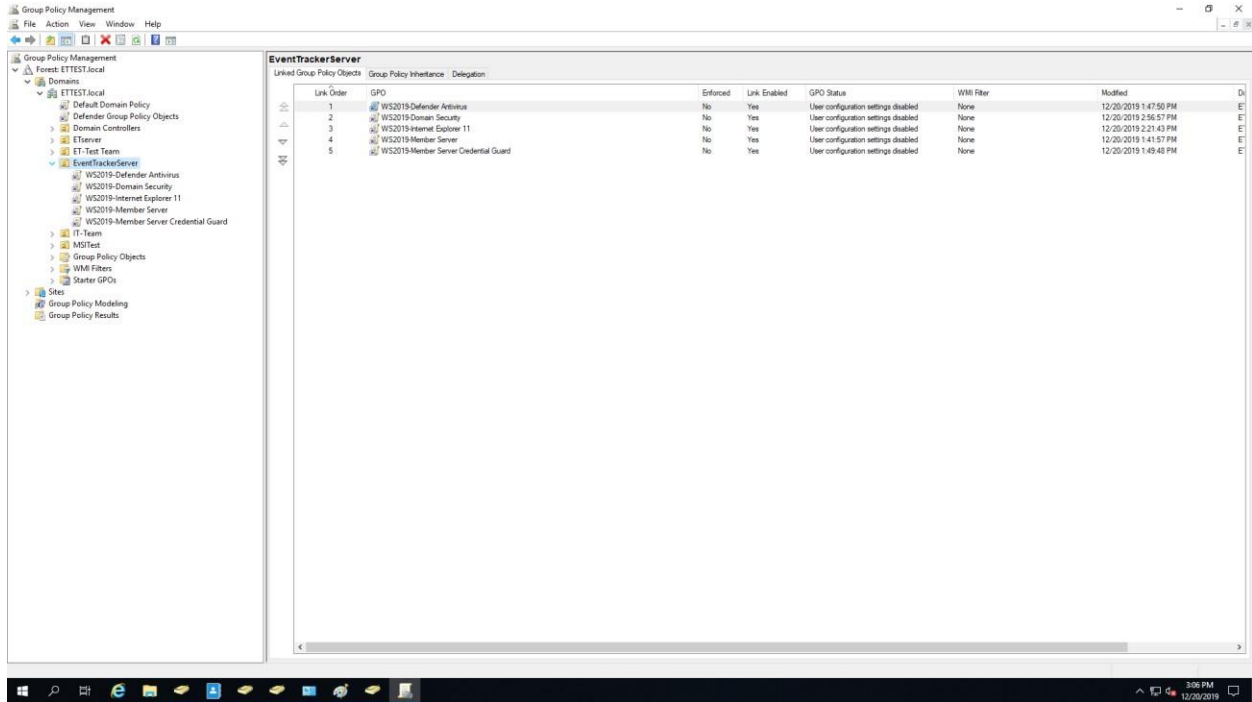
1. Right-click the newly created OU – Netsurion Open XDR Manager and click **Link an existing GPO**.



2. In the **Select GPO** dialog box, using the Control key, select all three newly created GPOs, and click **OK**.

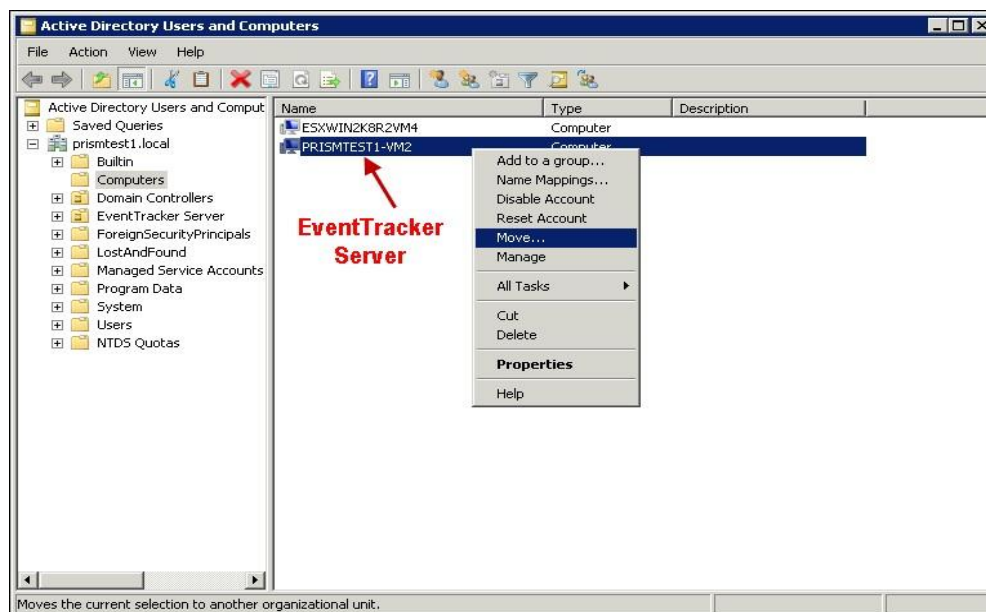


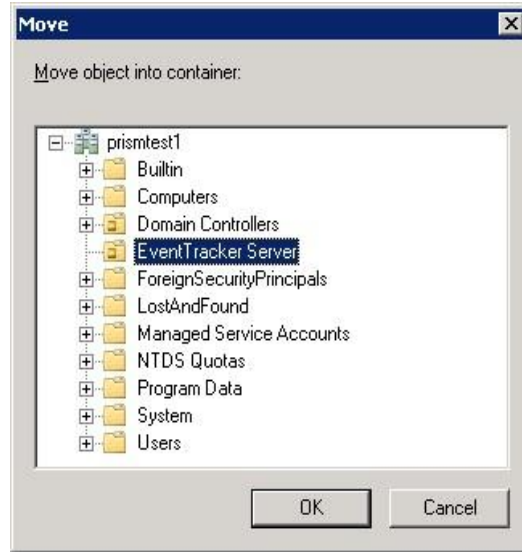
3. The Group Policy objects are now linked to the organizational unit.



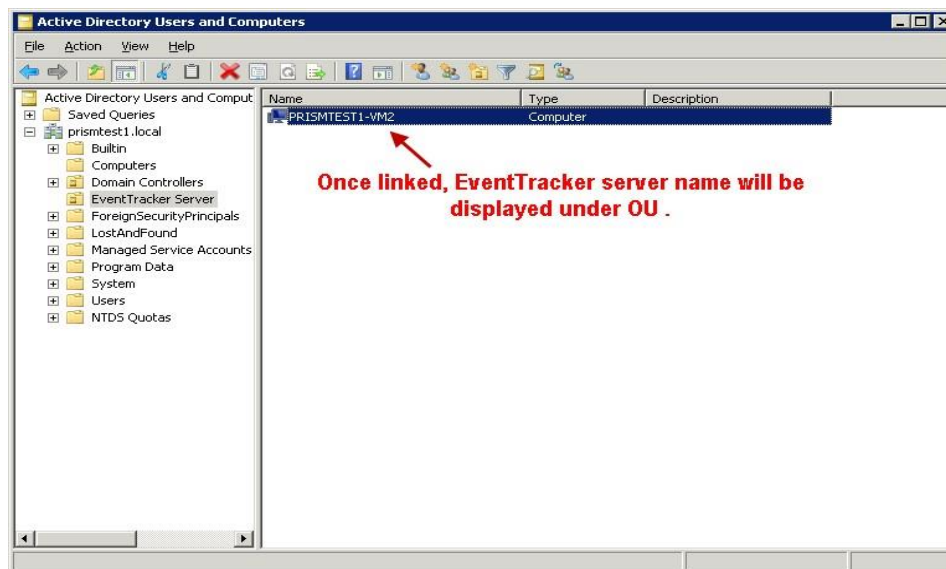
Step 6: Link Netsurion Open XDR Manager to the newly created OU and reboot the Netsurion Open XDR Manager system.

1. Click the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** pane, expand **Domain's** node, and then click the **Computers** node.
4. Right-click **Netsurion Open the XDR Manager system**, and then click **Move**.





5. Select the newly created OU (in this case, select **Netsurion Open XDR Manager**), and click **OK**.
6. In the **Active Directory Users and Computers** pane, click 'Organizational unit' (in this case, click **Netsurion Open XDR Manager**).

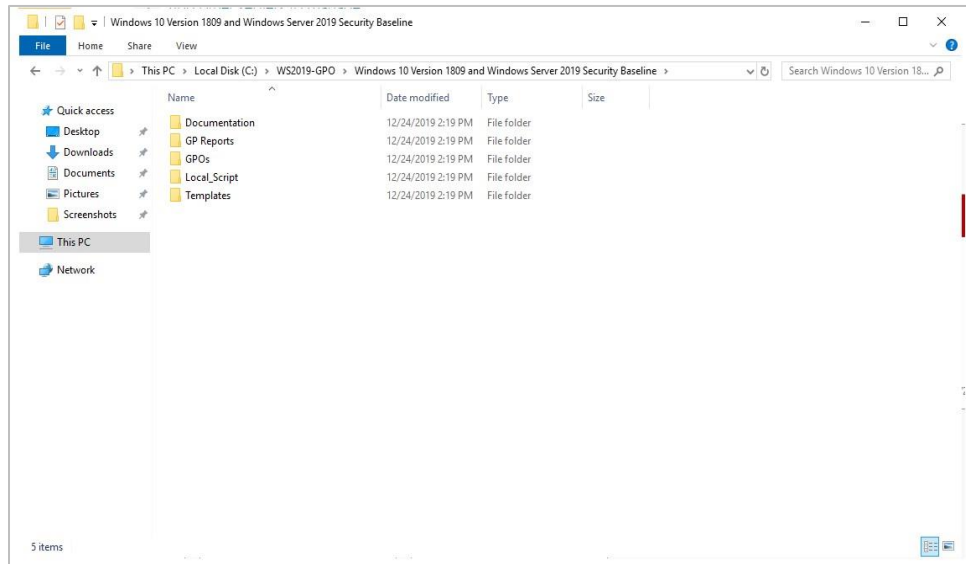


7. Reboot the Netsurion Open XDR Manager system linked to the OU.

2.2 Applying Group Policies in a Workgroup on Windows Server 2019

Step 1: On the workgroup system, download the Windows server 2019 local security policy backup file.

1. Click the link below to download the GPO and extract the contents of the zip file onto the system.
[Download WS2019-GPO.zip](#)
2. Extract the downloaded file to C:\WS2019-GPO.



Step 2: On the workgroup system, install GPO by running the PowerShell script which is available in the downloaded folder.

1. Launch PowerShell and run as administrator. The PowerShell script is available in the downloaded Local_Script folder.
2. Run the command as shown in the figure. Change the work directory to the folder where the file got extracted and run the below command.

`.\BaselineLocalInstall.ps1 -WS2019NonDomainJoined`

```

PS C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Sc
ript> .\BaselineLocalInstall.ps1 -WS2019NonDomainJoined
# Logging to C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\
Local_Script\BaselineInstall-20191219-1437-21.log ...
#-----
SG Windows Server 2019 - non-domain-joined
SG GPOs to be installed:
SG     MSFT Internet Explorer 11 - Computer
SG     MSFT Internet Explorer 11 - User
SG     MSFT Windows 10 1809 and Server 2019 - Defender Antivirus
SG     MSFT Windows 10 1809 and Server 2019 - Domain Security
SG     MSFT Windows 10 1809 and Server 2019 Member Server - Credential Guard
SG     MSFT Windows Server 2019 - Member Server
SG-----
SG Copy custom administrative templates...
SG Configuring Client Side Extensions...
Running LGPO.exe /v /e mitigation /e audit /e zone
Installing Exploit Protection settings...
Applying GPO "MSFT Internet Explorer 11 - Computer"...
Running LGPO.exe /v /g ..\GPOs\{ABFB52F2-1560-4100-9103-8C10F57DC9DE}
Applying GPO "MSFT Internet Explorer 11 - User"...
Running LGPO.exe /v /g ..\GPOs\{E913422C-4F06-4D37-A739-2CD2B701978E}
Applying GPO "MSFT Windows 10 1809 and Server 2019 - Defender Antivirus"...
Running LGPO.exe /v /g ..\GPOs\{FEE76283-957E-4B25-9380-2F737E13E972}
Applying GPO "MSFT Windows 10 1809 and Server 2019 - Domain Security"...
Running LGPO.exe /v /g ..\GPOs\{B9263530-926F-46F3-8382-832C31EC185}
Applying GPO "MSFT Windows 10 1809 and Server 2019 Member Server - Credential Guard"...
Running LGPO.exe /v /g ..\GPOs\{7D41EEC9-3F30-4473-9447-E77D6EEF0E17}
Applying GPO "MSFT Windows Server 2019 - Member Server"...
Running LGPO.exe /v /g ..\GPOs\{C92CC433-A4EA-47B1-8B24-6FF732940E0E}
Non-domain-joined: back out the local-account restrictions...
Running LGPO.exe /v /s ConfigFiles\DeltaForNonDomainJoined.inf /t ConfigFiles\DeltaForNonDomainJoined.txt
#-----
#-----
To test properly, create a new non-administrative user account and reboot.

Detailed logs are in this file: C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Script\BaselineInstall-20191219-1437-21.log

Please post feedback to the Security Guidance blog:

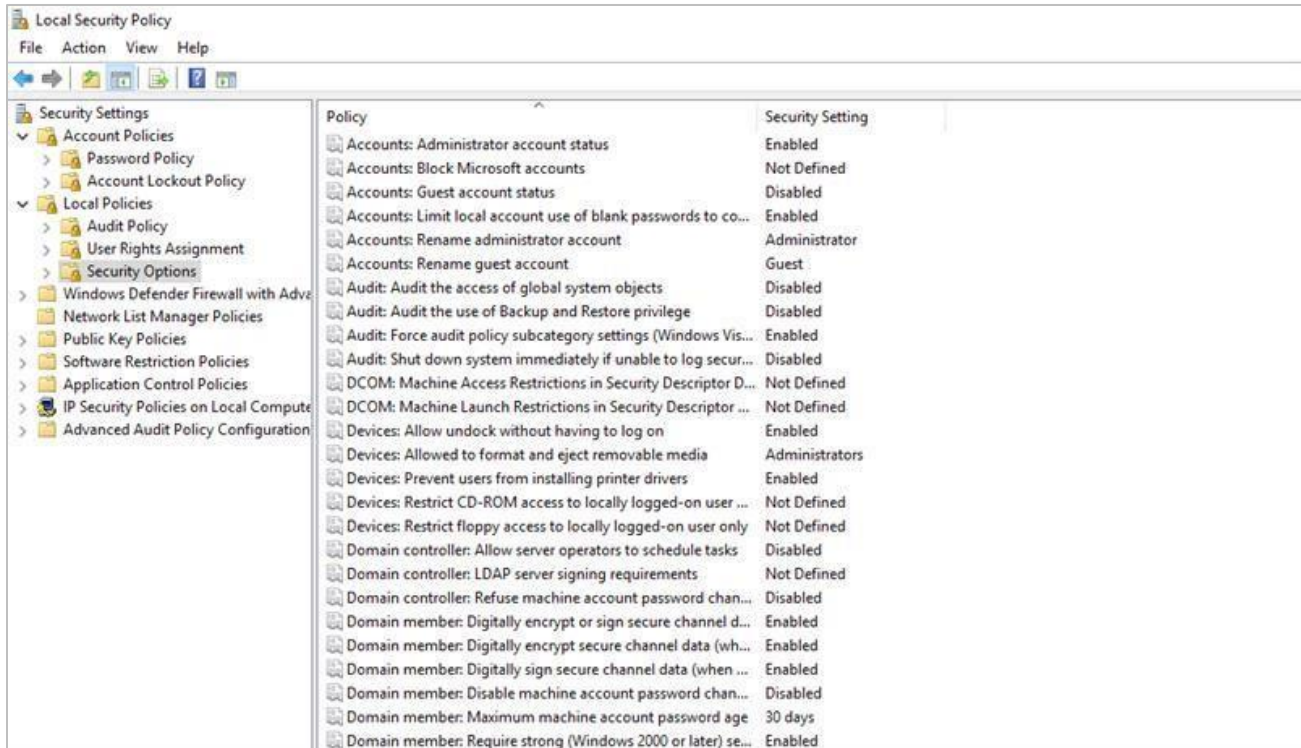
```

Step 3: Verify the applied Security Policy.

In the Workgroup System

1. Select the **Start** button, select **All Programs**, and then select-> **Administrative Tools**.
2. Click **Local Security Policy** and expand **Account Policies**.
3. Click **Password Policy** and check the **Security Settings** as shown in the below screen.





3 Securing IIS Web Server (10 and 11)

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the internet.

3.1 Mandatory Requirements

This section describes the mandatory software and component requirements to create an SSL digital certificate and secure website hosted on the IIS server with an SSL digital certificate.

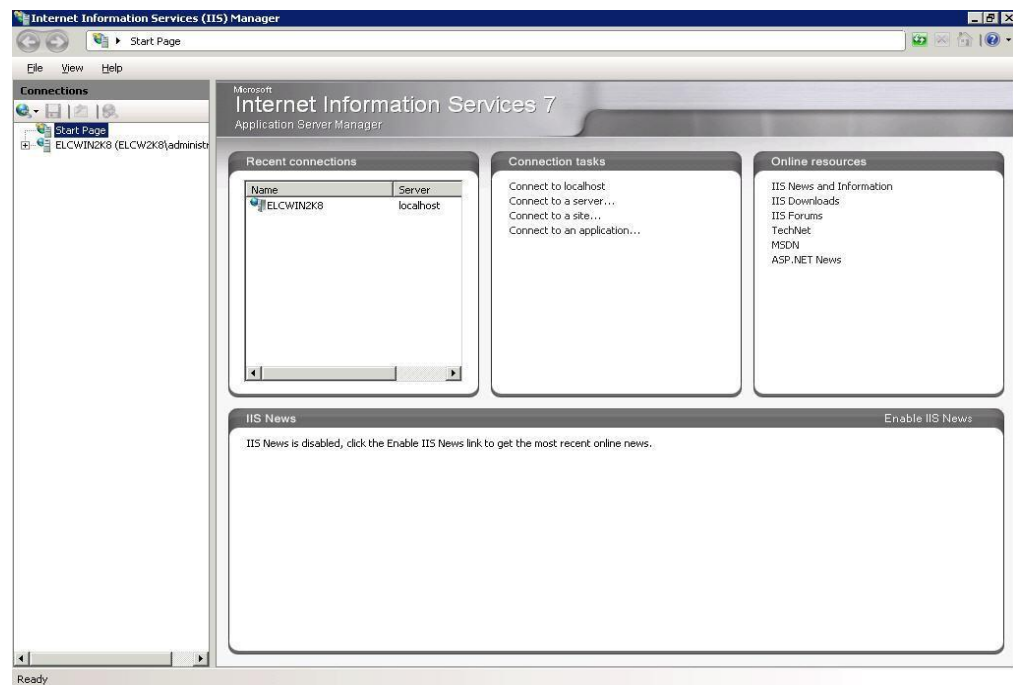
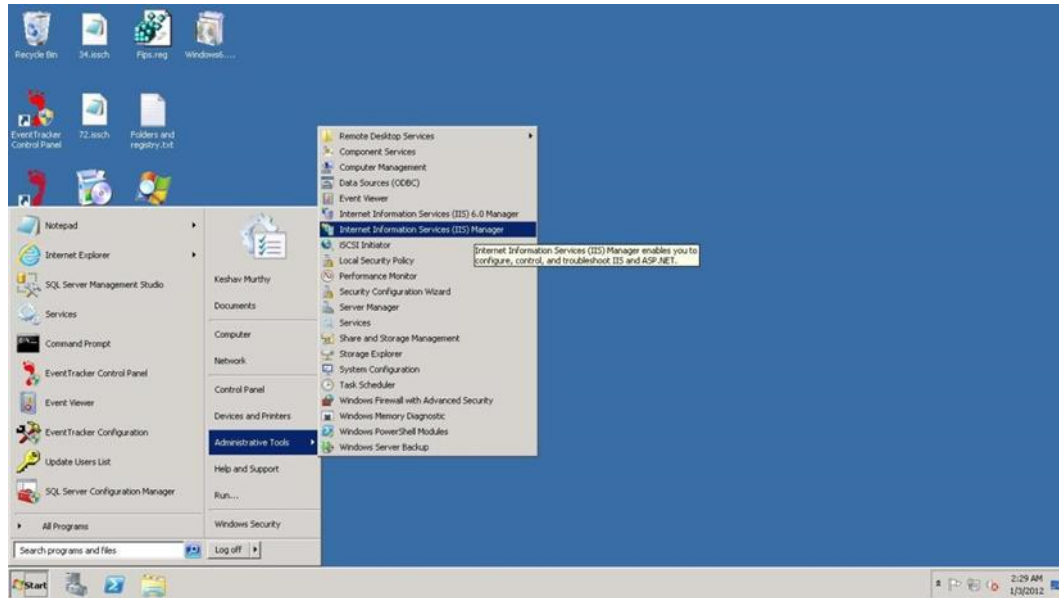
Operating System	Windows Server 2019
Software and Components	<ul style="list-style-type: none"> • Internet Information Server (IIS) 10 and 11. • Browser, which supports 128-bit encryption (IE 11 or above/ Firefox 3.5 or above).

3.2 IIS setup on Windows

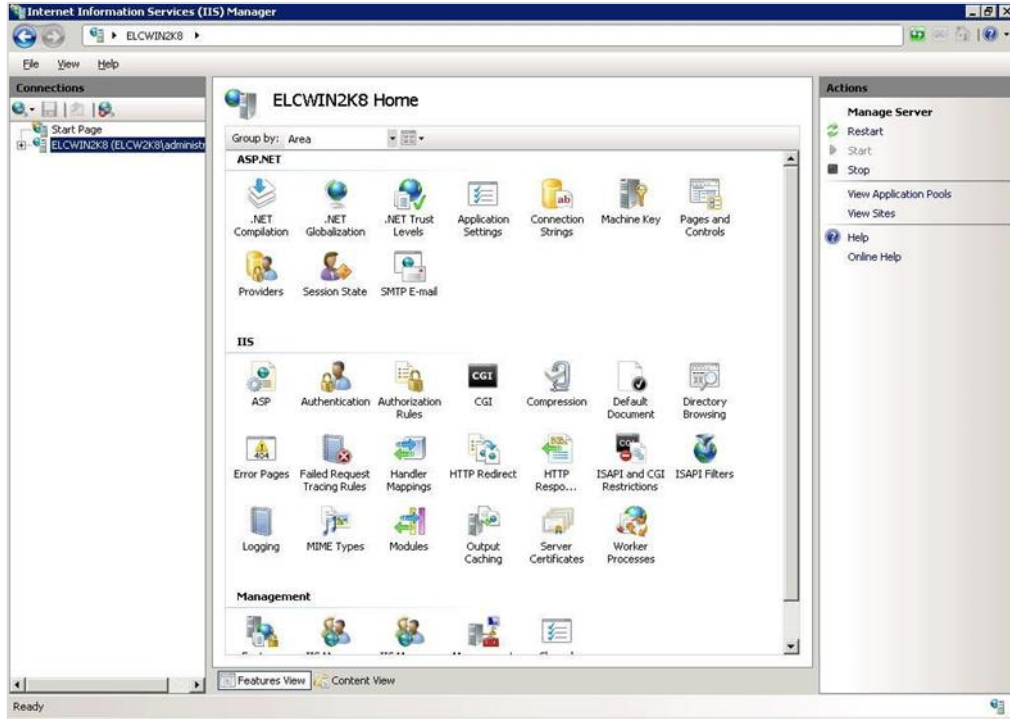
Step 1: Creating the 'Certificate Request'.

1. Click the **Start** button, select **All Programs**, and select **Administrative Tools**.

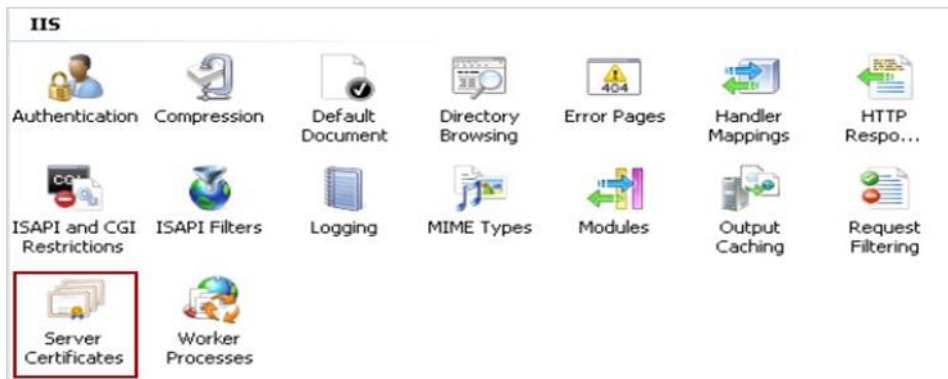
2. Select **Internet Information Services (IIS) Manager**.



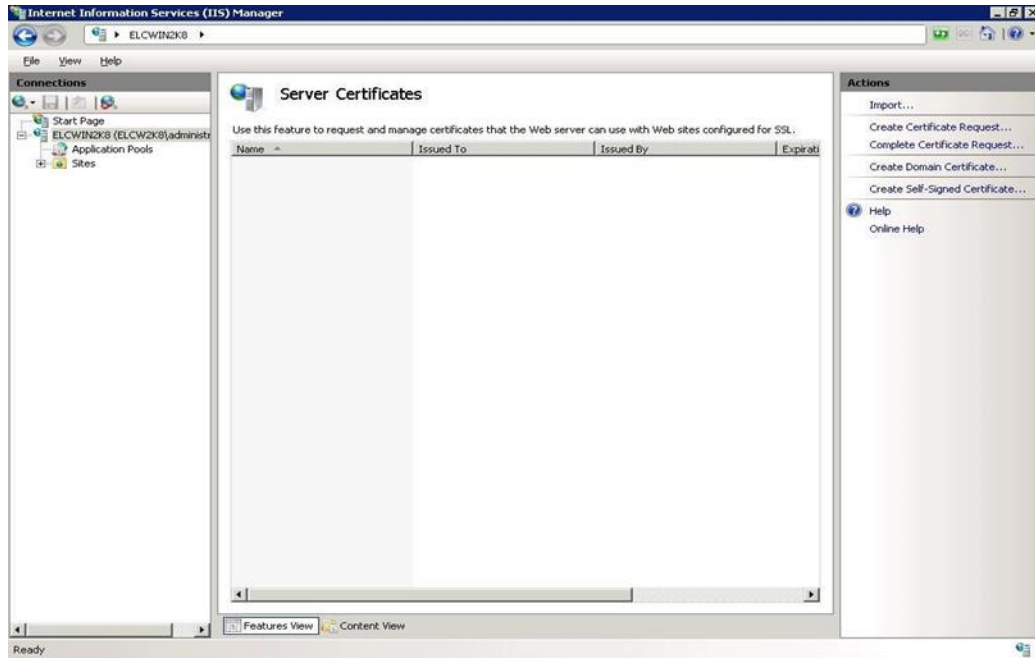
3. Click the server node.



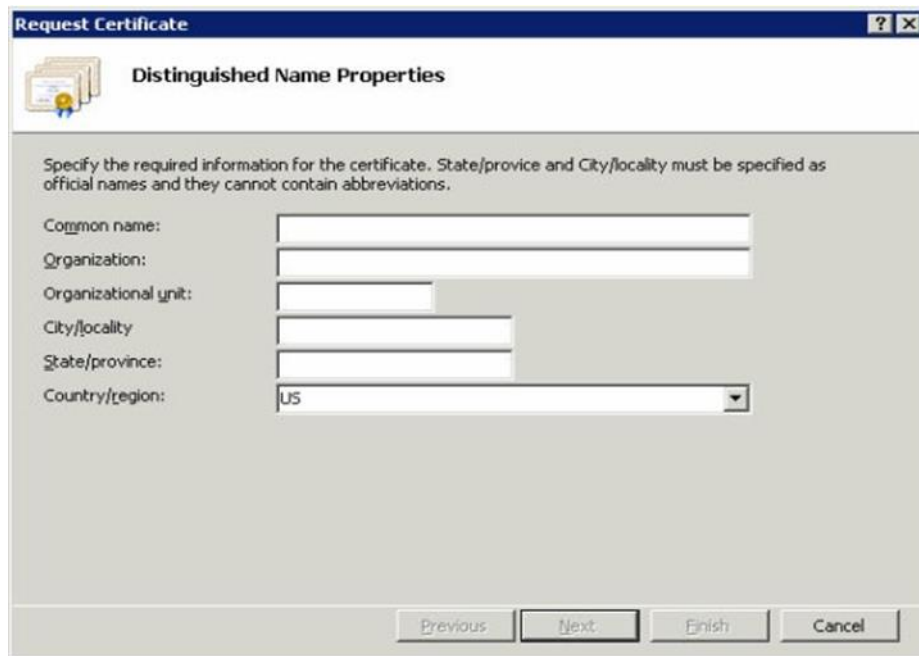
4. Double-click the **Server Certificates** icon in the IIS pane.



5. The Server Certificates panel will be displayed as shown below:

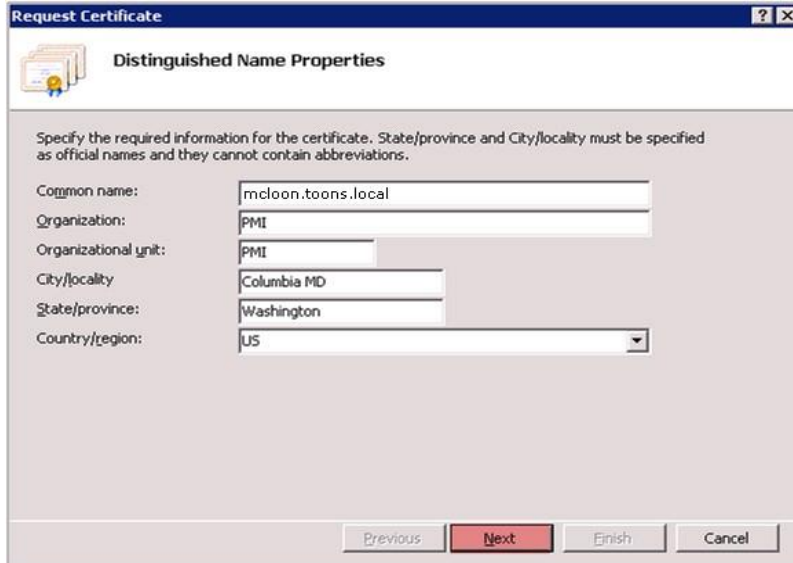


- In the **Actions** pane, click the **Create Certificate Request** link. The dialog box will be displayed as shown below:



- Type the system name (FQDN- Fully qualified domain name) as a common name in the **Common name** text box.

Example: mcloon.toons.local



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

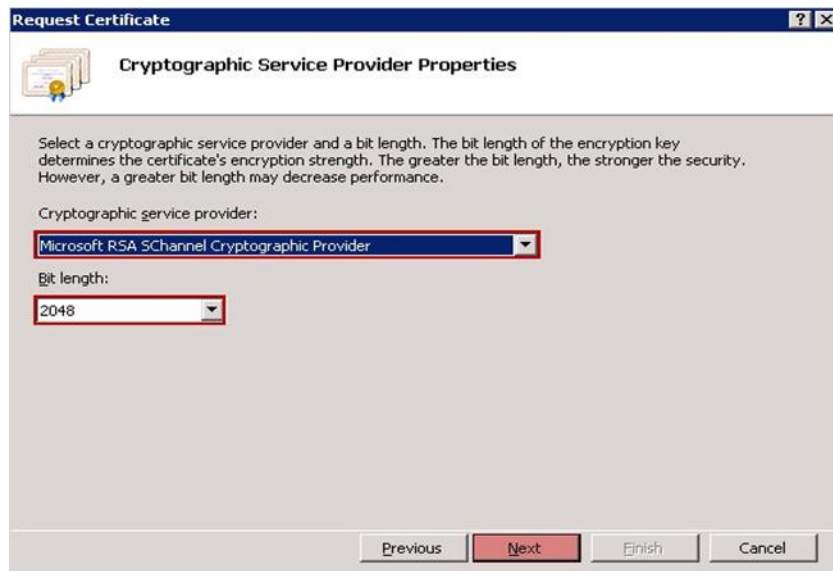
City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

8. Enter the organization and geographical details and click **Next**. Do not change the default selection in the **Cryptographic Service Provider Properties** pane.
9. Set the bit length to 2048 from the **Bit length** dropdown and click the **Next** button.



Request Certificate

Cryptographic Service Provider Properties

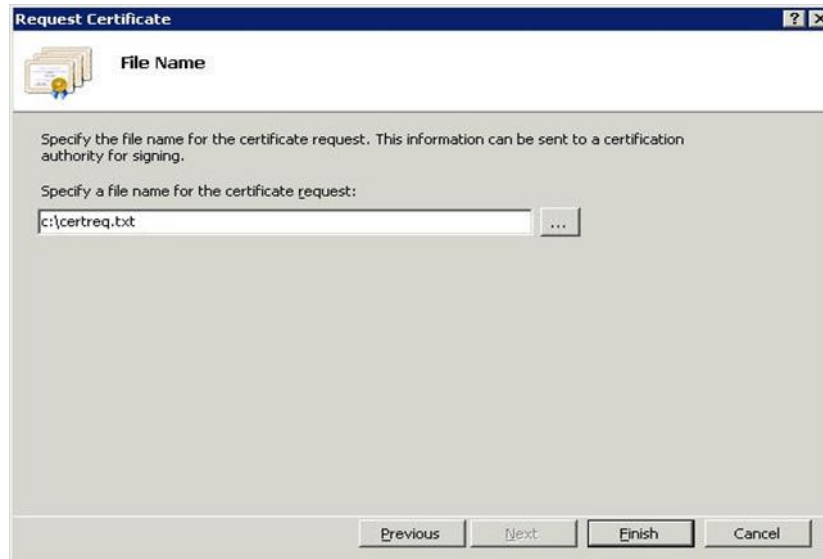
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

Previous Next Finish Cancel

10. Type the name and path of the file to save the CSR (Certificate Server Request).

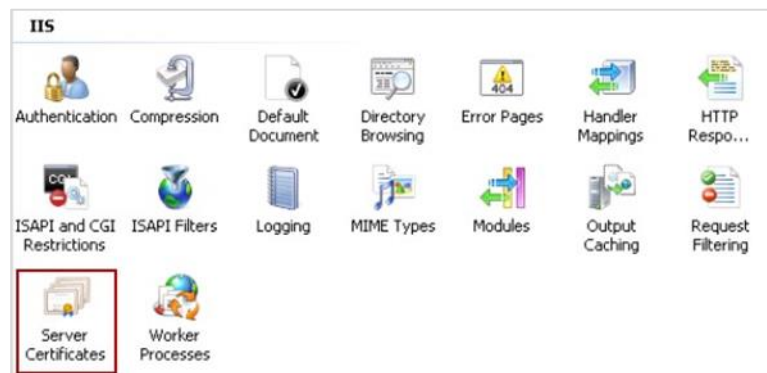


11. Click **Finish**.
12. Send this request file to the certificate vendor.

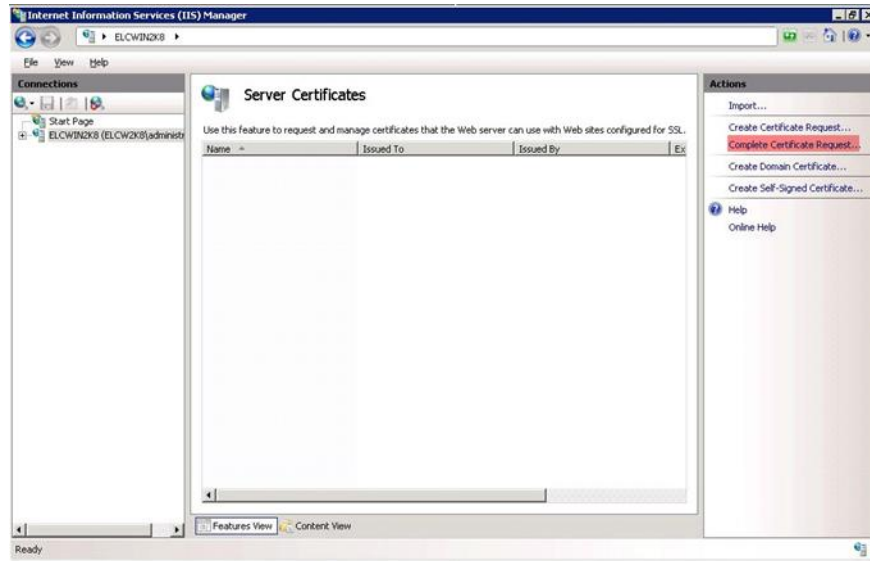
Step 2: Installing the Certificate.

The certificate received from the vendor needs to be copied to the system.

1. Click the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. Click the server node, and then double-click the **Server Certificates** icon in the IIS pane.



4. In the Actions pane, click the **Complete Certificate Request** hyperlink.

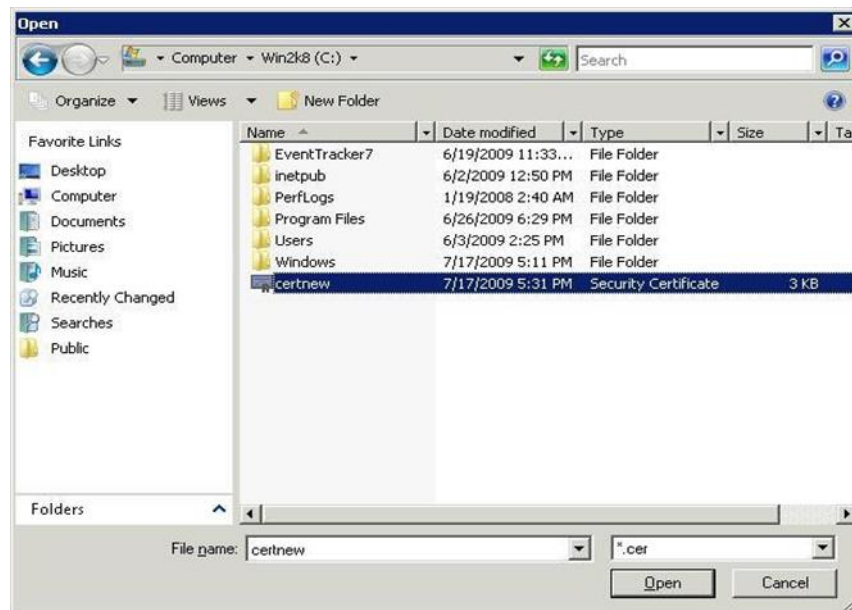


5. In the **Complete Certificate Request** dialog box, click the **browse** button.





6. Locate the server certificate received from the certificate authority.



7. Click **Open**.



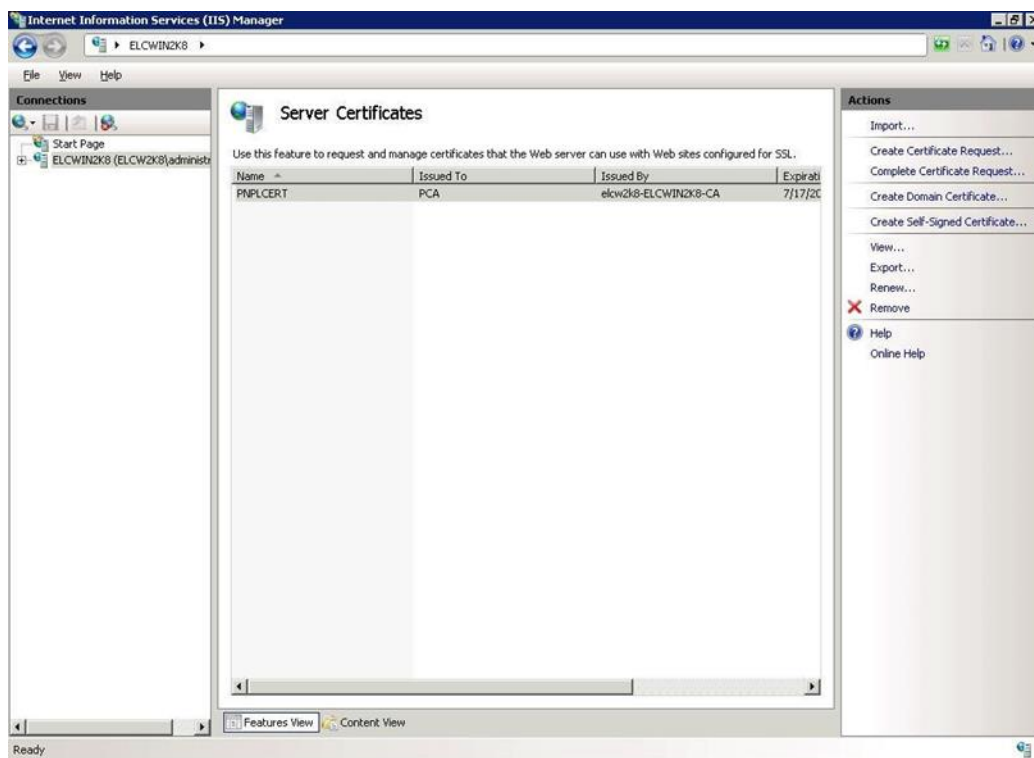
8. Type a relevant name in the **Friendly name** field to keep track of the certificate on this server.





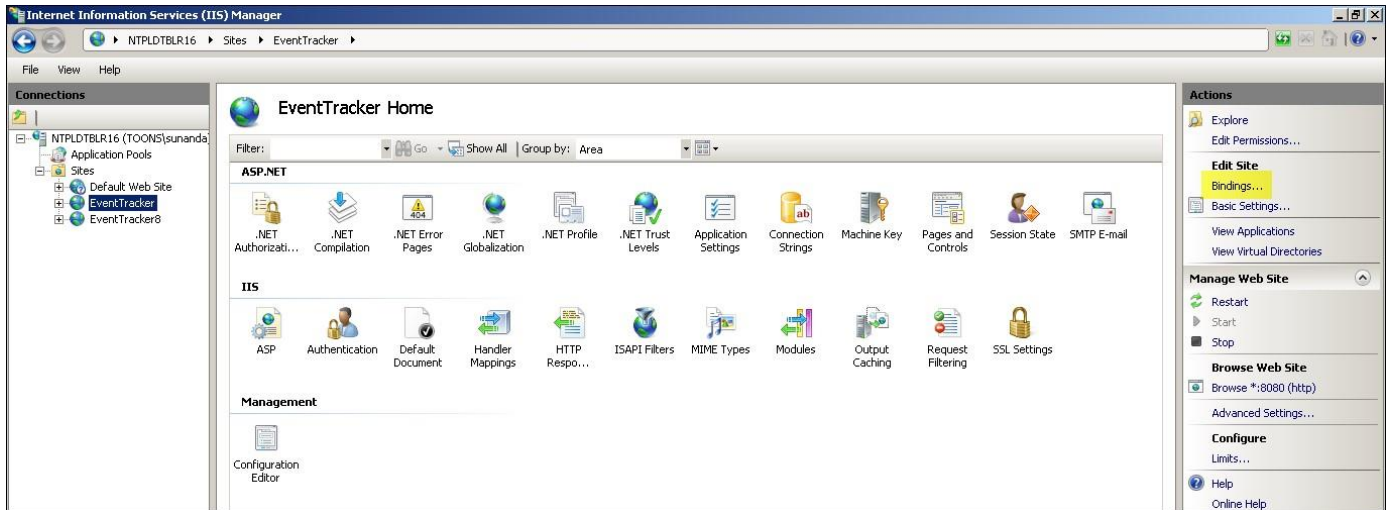
9. Click **OK**.

If successful, the newly installed certificate will be shown in the list. If the error 'the request or private key cannot be found' occurs, then ensure that the correct certificate is used and is installed on the same server where the CSR (Certificate Server Request) is generated. If these two things are in place, then proceed to create a new **Certificate Request** and reissue/replace the certificate.

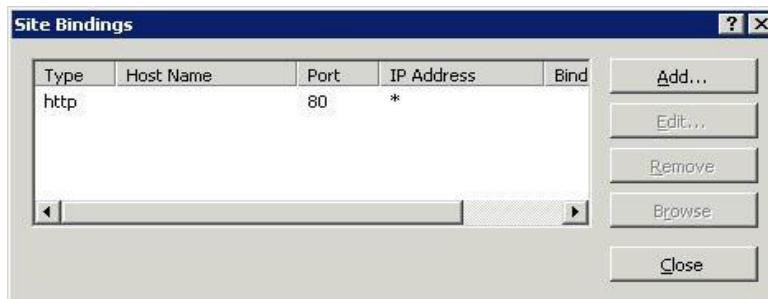


Step 3: Binding the certificate to Netsurion Open XDR.

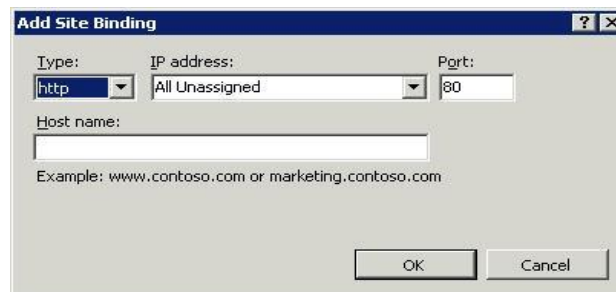
1. Expand the **Server** node.
2. Expand the **Sites** node.
3. Click **Netsurion Open XDR**.
4. In the **Actions** pane, click **Bindings**.



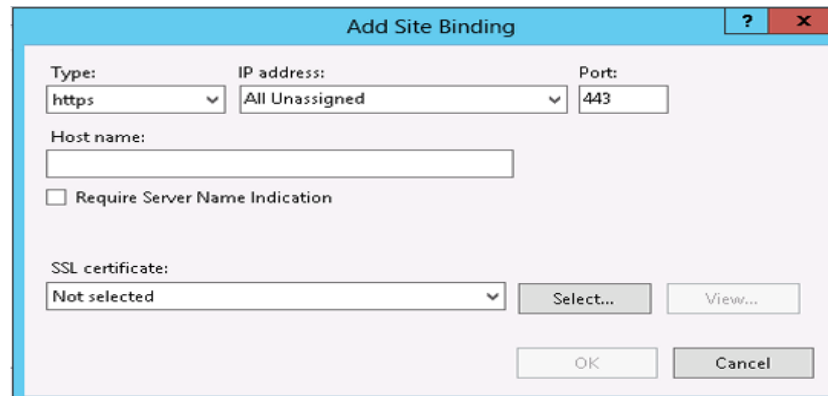
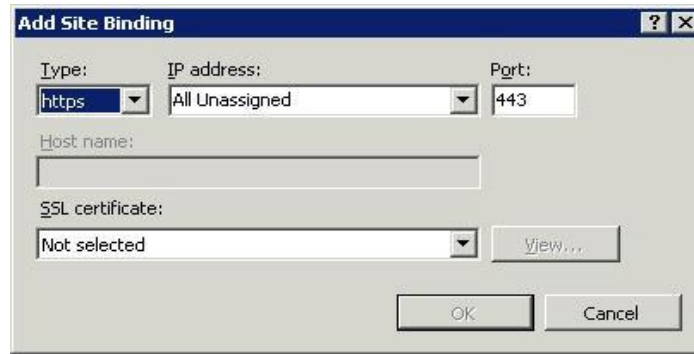
5. The **Site Bindings** dialog box appears as shown below:



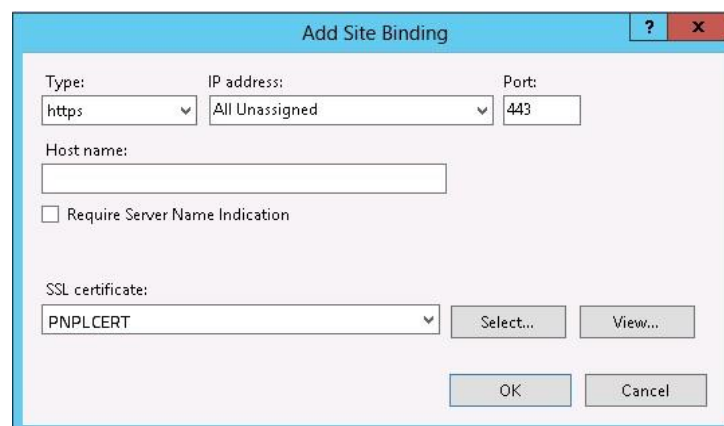
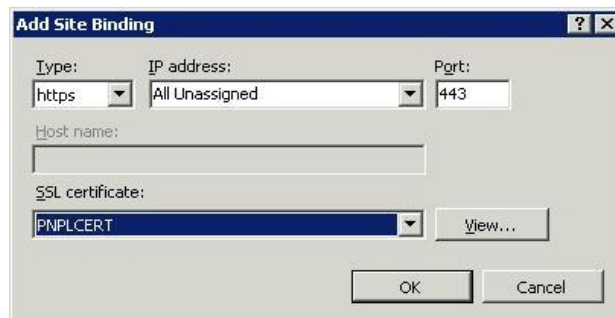
6. Click **Add**.



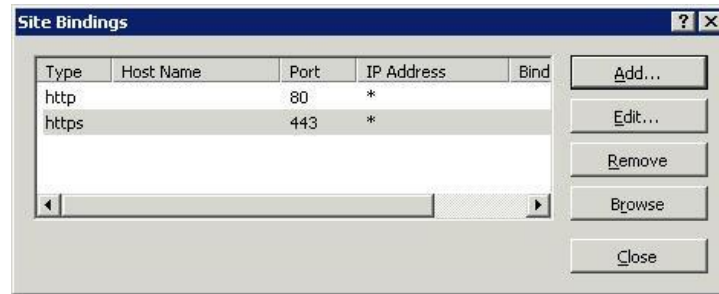
7. Change the **Type** to **https**. By default, the system will select the port number as 443. The default port number can be changed if required.



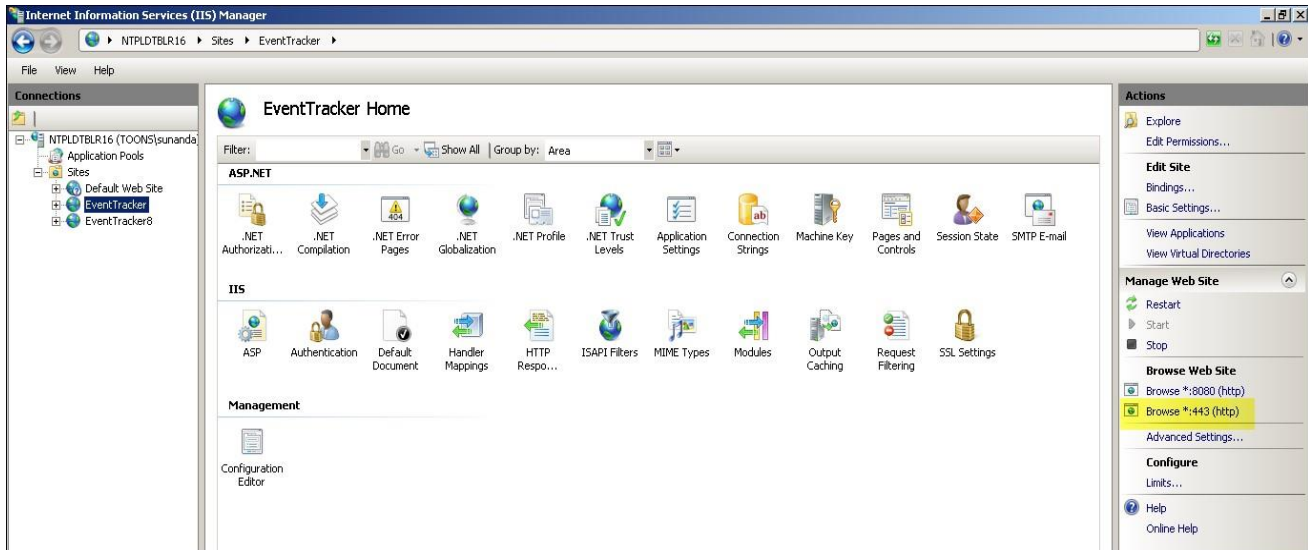
8. Select the recently installed **SSL certificate**.



9. Click **OK**. The binding for port 443 will be listed.



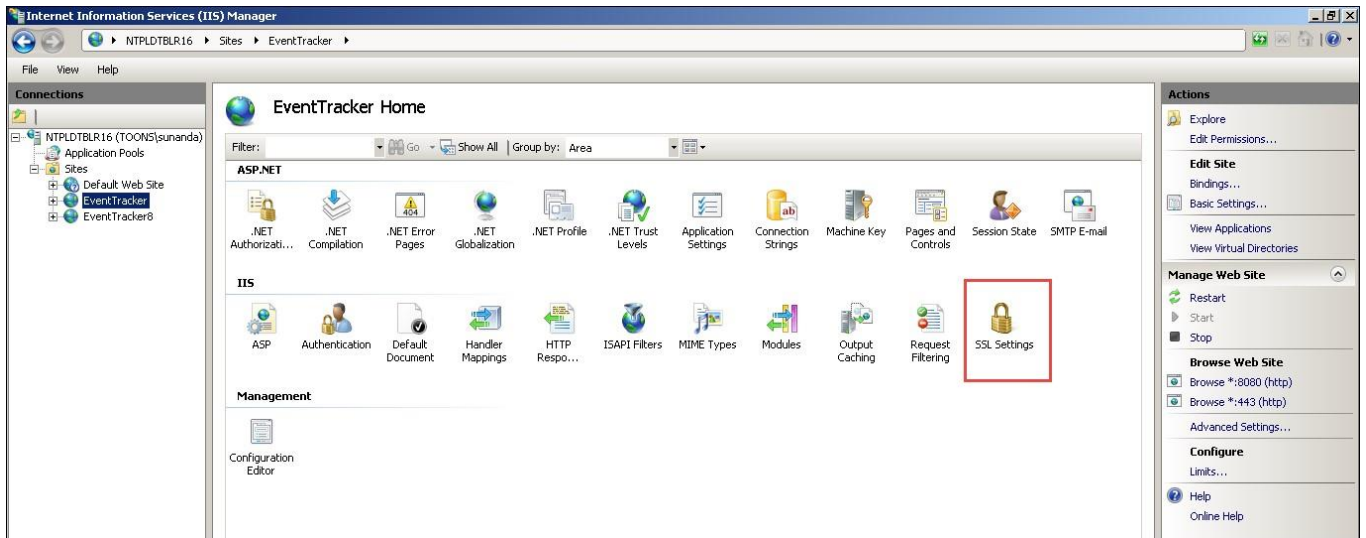
10. Click **Close**. The newly added https website will be listed under **Browse Web Site**.



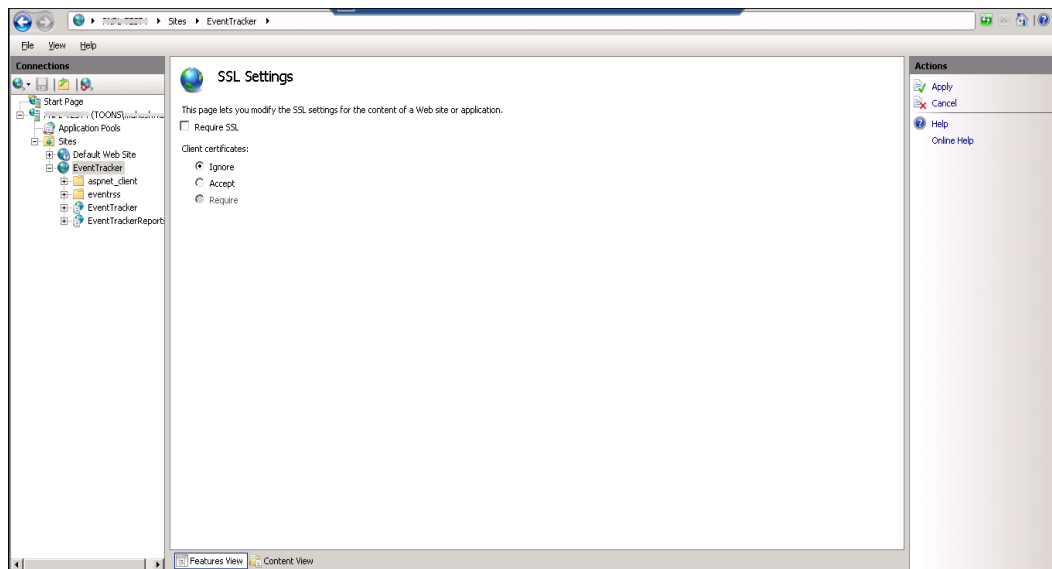
Step 4: Configure SSL Settings.

Configure **SSL Settings** to interact in a specific way with client certificates.

1. Expand the **Sites** node.
2. Click **Netsurion Open XDR**.
3. Double-click the **SSL Settings** icon.



4. The SSL Settings page will be displayed as shown below.



5. Select the **Require SSL** option.
6. In the **Actions** pane, click **Apply**. After successful SSL settings modification, a message will be displayed in the **Alerts** pane.



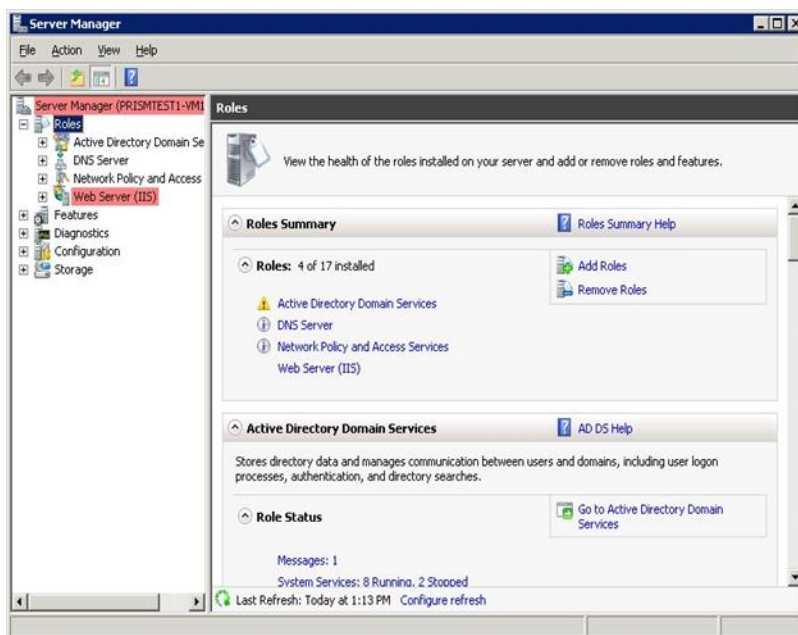
7. Close the IIS Manager.

Step 5: Create FTP Service.

Note

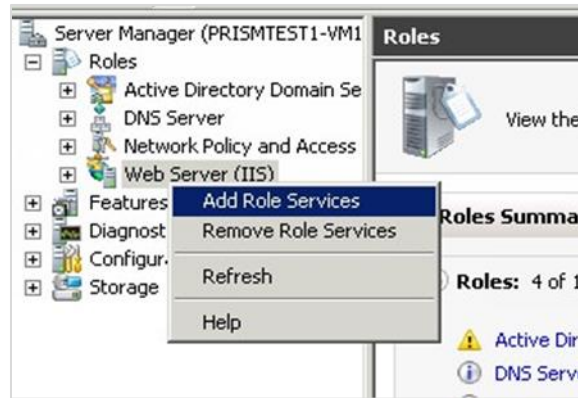
Follow steps 5 and step 6 only to transfer the custom logs from the remote server to the Netsurion Open XDR Manager.

1. Click the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Server Manager**.

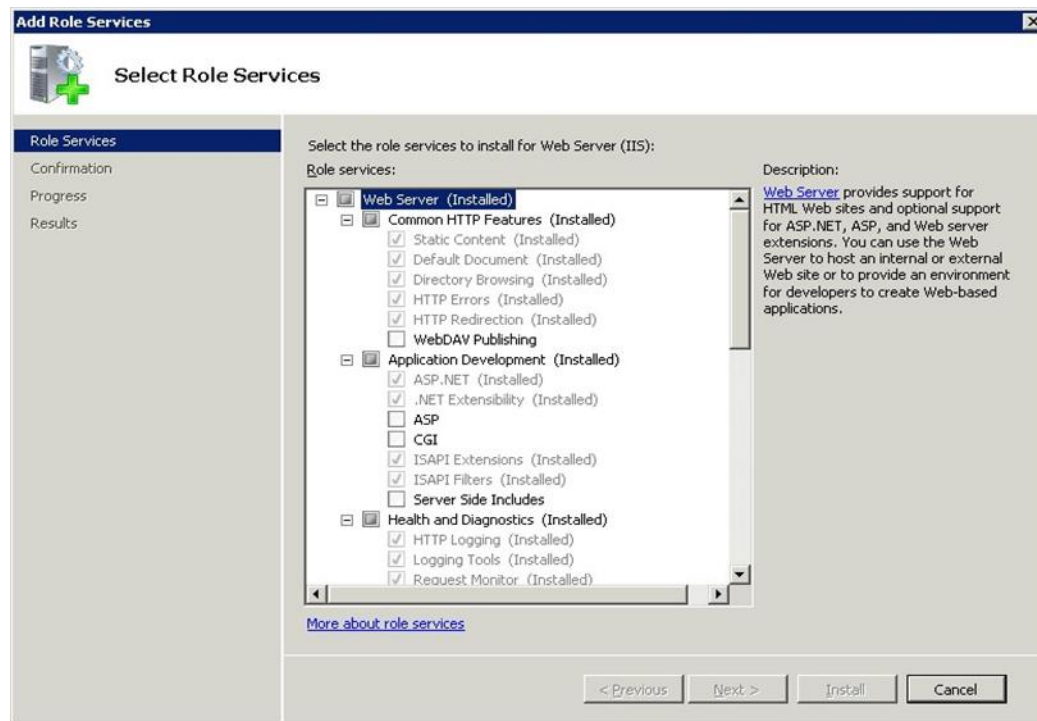


3. In the **Server Manager** pane, expand **Roles**.

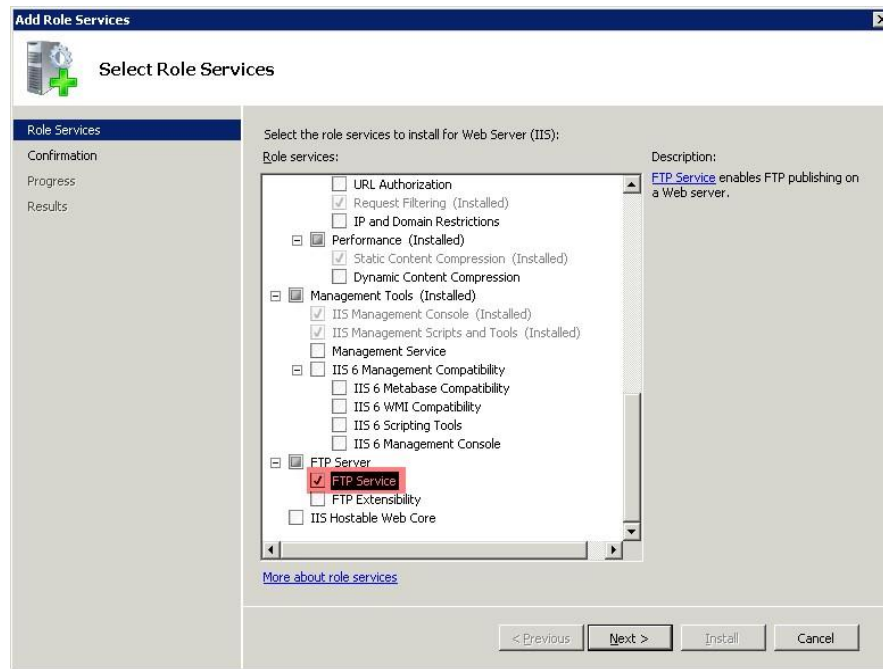
4. Right-click **Web Server (IIS)** and select **Add Role Services**.



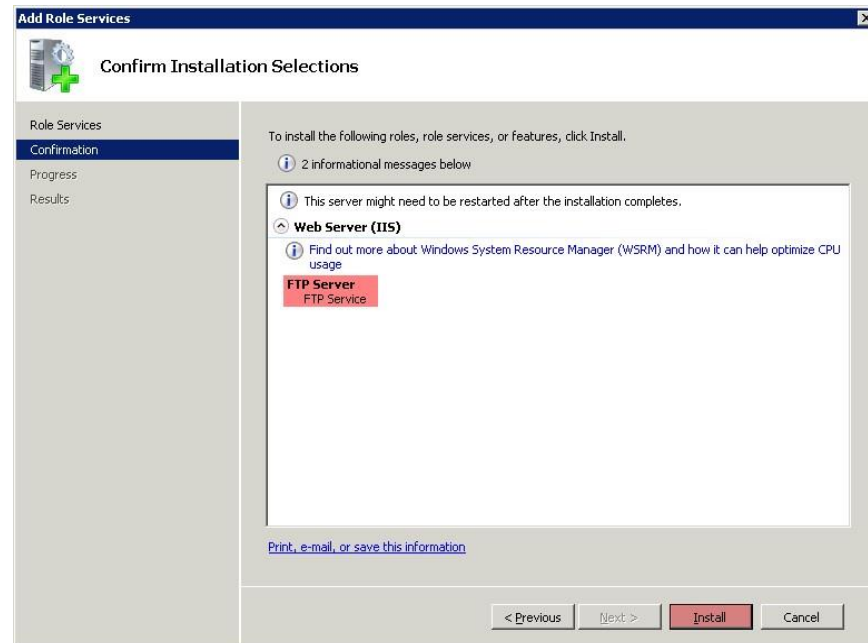
5. The **Server Manager** page displays the **Add Role Services** wizard.



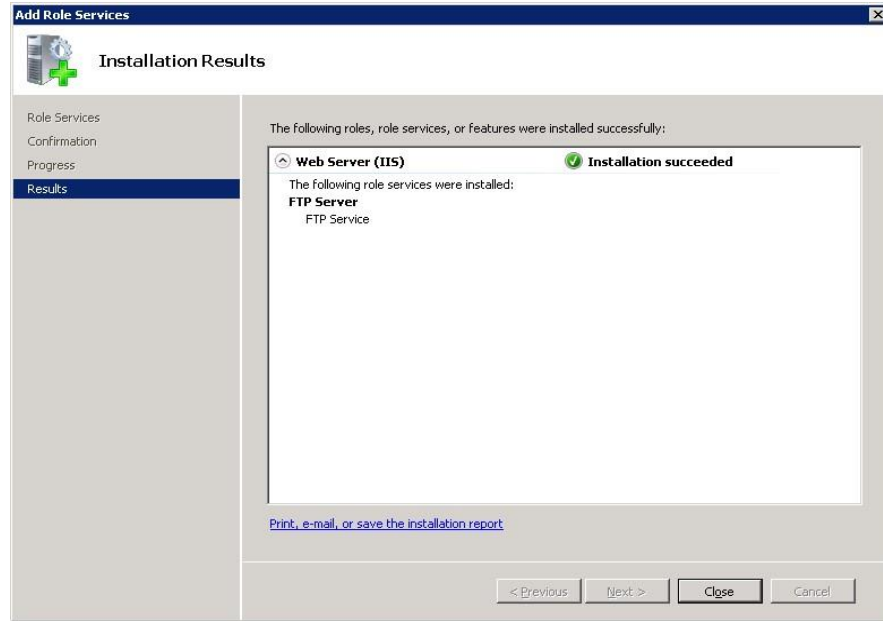
6. In the **Roles Services** pane, select the **FTP service** option, and then click **Next**.



7. In the **Confirmation** window, click the **Install** button.

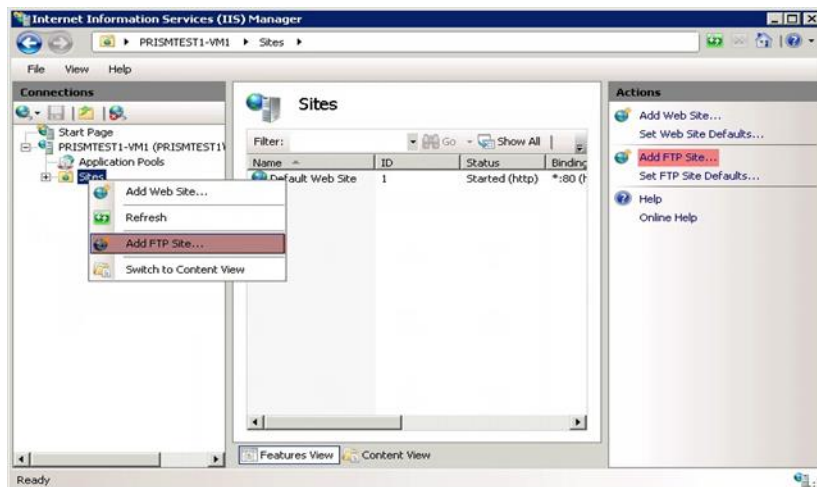


8. Click the **Close** button after the 'Installation Succeeded' message appears on the **Results** window.

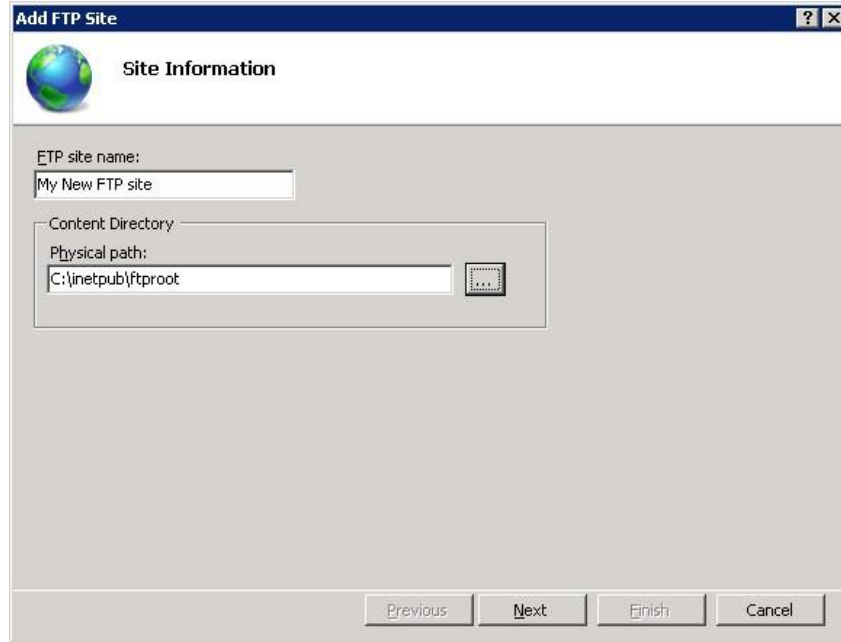


Step 6: Create an SSL-enabled FTP Site.

1. Click the **Start** button, select **Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. In the **Connections** pane, select **Sites** node.
4. Right-click the **Sites** node, and then click **Add FTP Site**.
(OR)
Click **Add FTP Site** in the **Actions** pane.

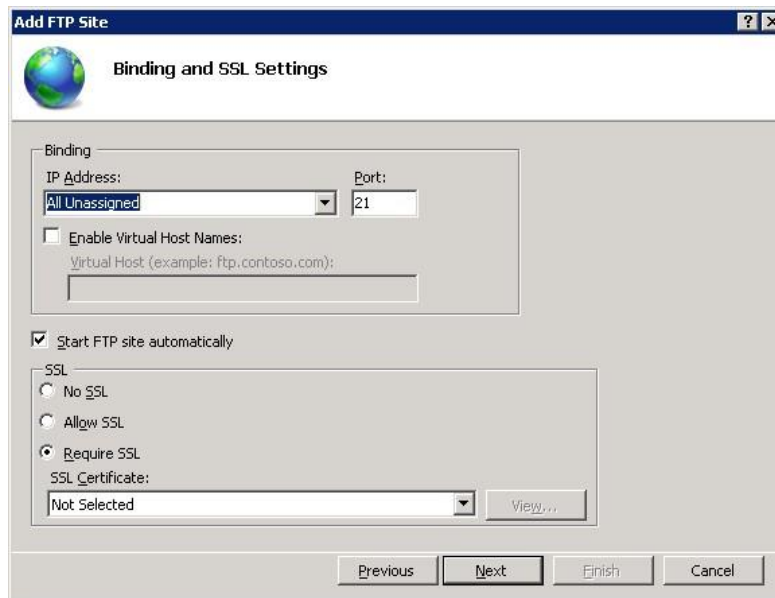


5. The **Add FTP Site** dialog box appears on the screen. In the **FTP site name**, type the site name as 'My New FTP Site', and then locate the physical path of the FTP root folder.



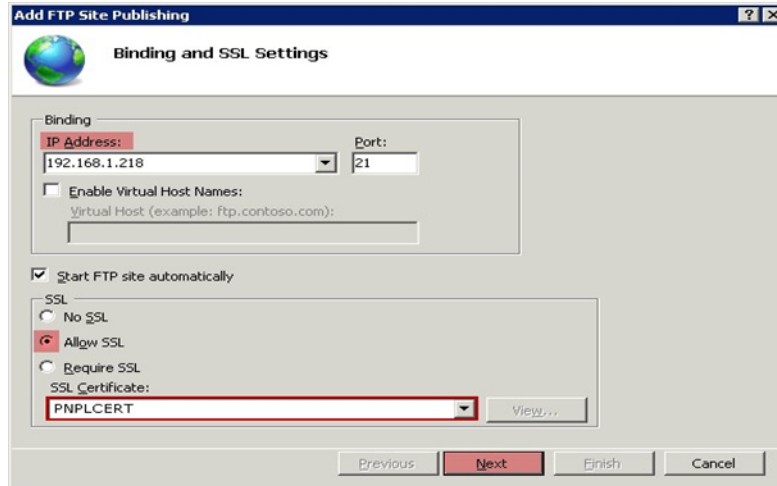
The screenshot shows the 'Add FTP Site' wizard in the 'Site Information' step. The title bar reads 'Add FTP Site'. Below the title bar is a globe icon and the text 'Site Information'. The main area contains two input fields: 'FTP site name:' with the text 'My New FTP site' and 'Content Directory' with the text 'Physical path:' and 'C:\inetpub\ftproot'. At the bottom, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

6. Click the **Next** button.

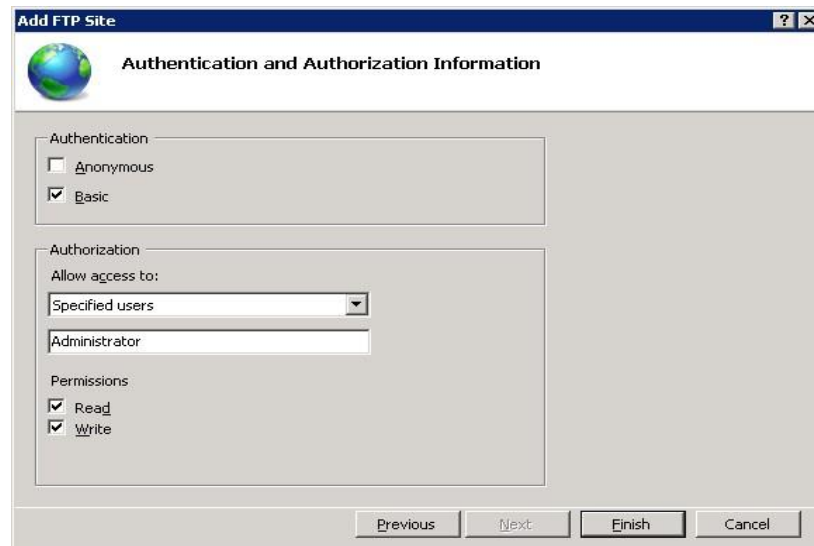


The screenshot shows the 'Add FTP Site' wizard in the 'Binding and SSL Settings' step. The title bar reads 'Add FTP Site'. Below the title bar is a globe icon and the text 'Binding and SSL Settings'. The main area is divided into two sections: 'Binding' and 'SSL'. The 'Binding' section has an 'IP Address:' dropdown menu set to 'All Unassigned', a 'Port:' text box with '21', and an unchecked checkbox for 'Enable Virtual Host Names:'. The 'SSL' section has a checked checkbox for 'Start FTP site automatically' and three radio button options: 'No SSL', 'Allow SSL', and 'Require SSL'. Below these is an 'SSL Certificate:' dropdown menu set to 'Not Selected' and a 'View...' button. At the bottom, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

7. Select the local IP address for the FTP site from the **IP Address** drop-down or type the local loopback IP address for the computer by typing "127.0.0.1" in the **IP Address** box.
8. Keep the default port selection as 21, or the port number can be changed if required.
9. In the SSL pane, select the **Allow SSL** option, and then click the **View** button to locate the SSL certificate received by the vendor.



10. Click the **Next** button. The **Authentication and Authorization Information** page appears.
11. In the **Authentication** pane, check the **Basic** option.
12. In the **Authorization** pane, select **Specified users** from the **Allow access to** drop-down.
13. Type the username that is authorized to do FTP access.
Example: Administrator.
14. Select the **Read** and **Write** as the **Permissions** option.



15. Click the **Finish** button.

3.3 Restricting Netsurion Open XDR Web Console Access

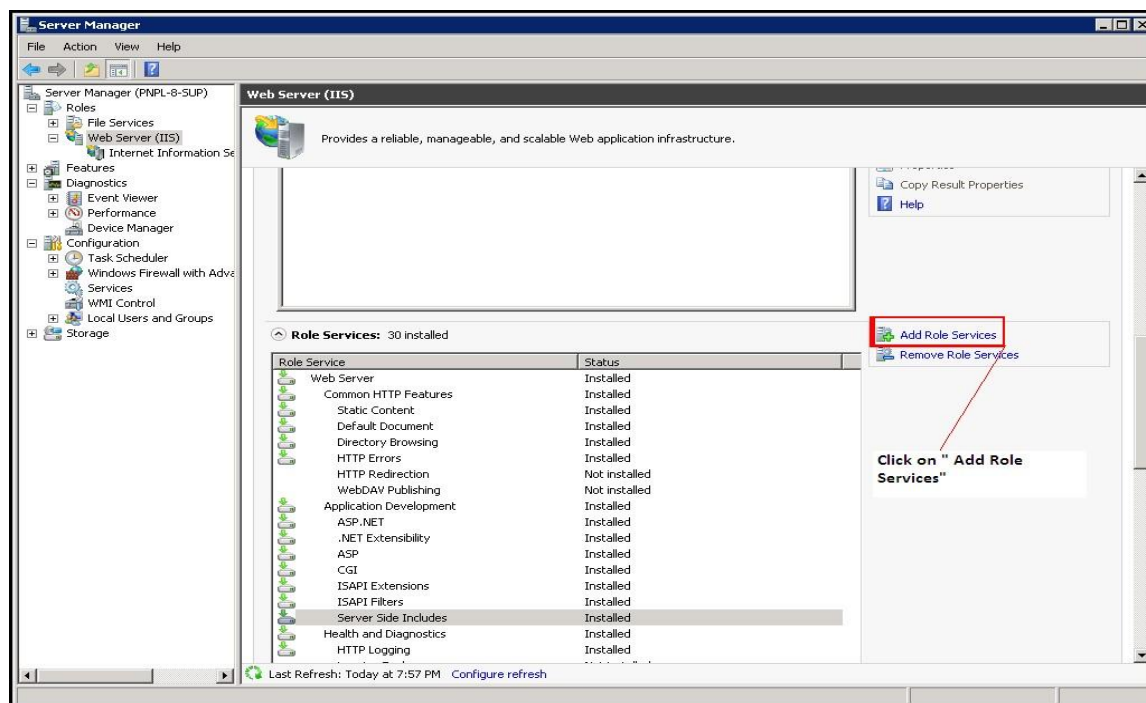
Configuring IP address and domain name restrictions in Internet Information Services (IIS) allows you to permit or deny access to the web server, websites, folders, or files. The rules can be configured for remote IP addresses or based on the Domain name.

When a remote client that is not permitted access requests a resource i.e. a 403.6 (“Forbidden: IP address of the client has been rejected”) or 403.8 (“DNS name of the client is rejected”), HTTP status will be logged by Internet Information Services (IIS).

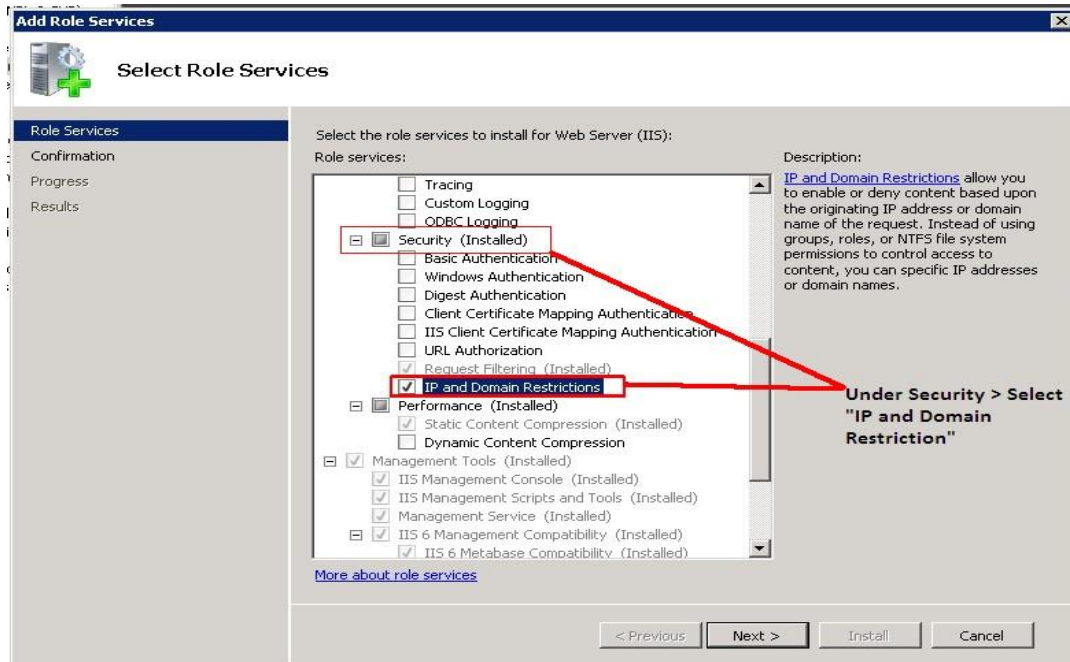
IP and Domain Restrictions option is not enabled by default when you install Internet Information Services (IIS). You can enable the IP and Domain Restrictions option by adding the above Role Service as mentioned below.

3.4 Installing IP and Domain Restriction in Windows

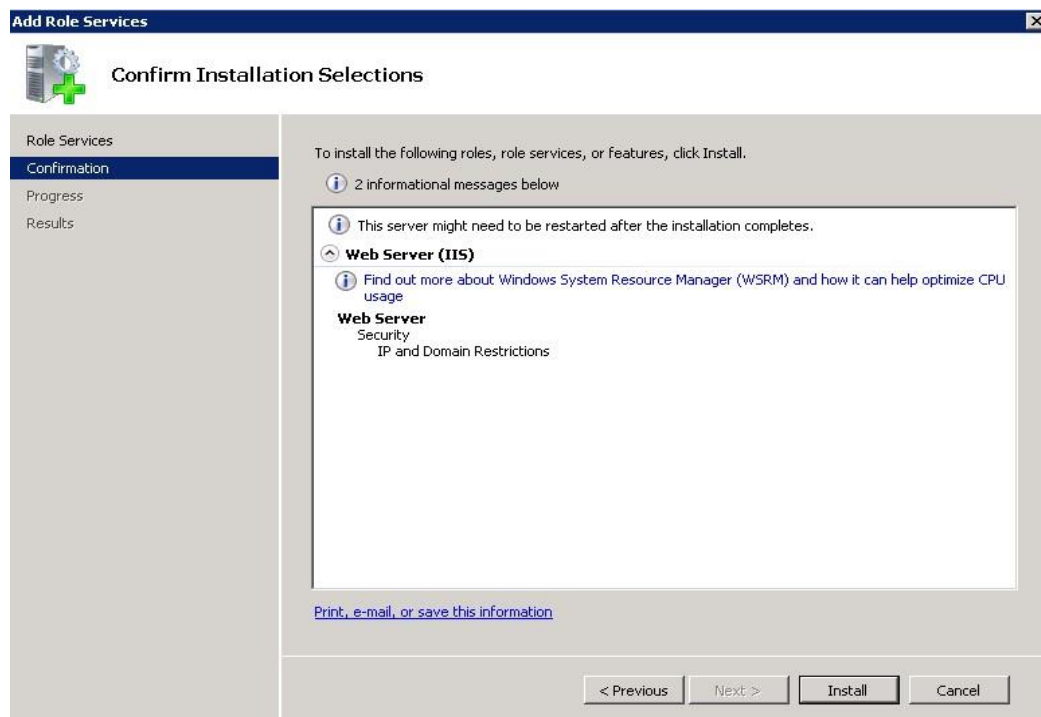
1. Click the **Start** button.
2. Select **Administrative Tools**, and then select **Server Manager**.
3. Select **Add Role Services**.



4. Under **Security**, select **IP and Domain Restrictions**, and then select **Next**.

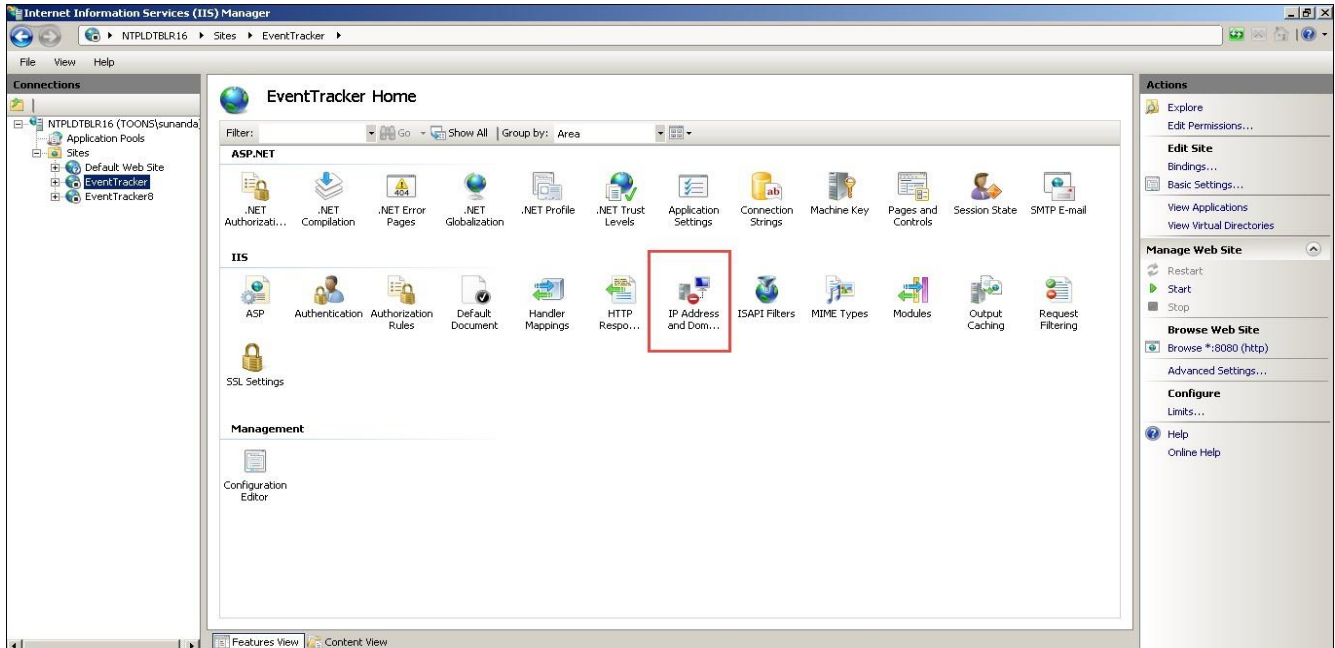


5. Click the **Install** button.

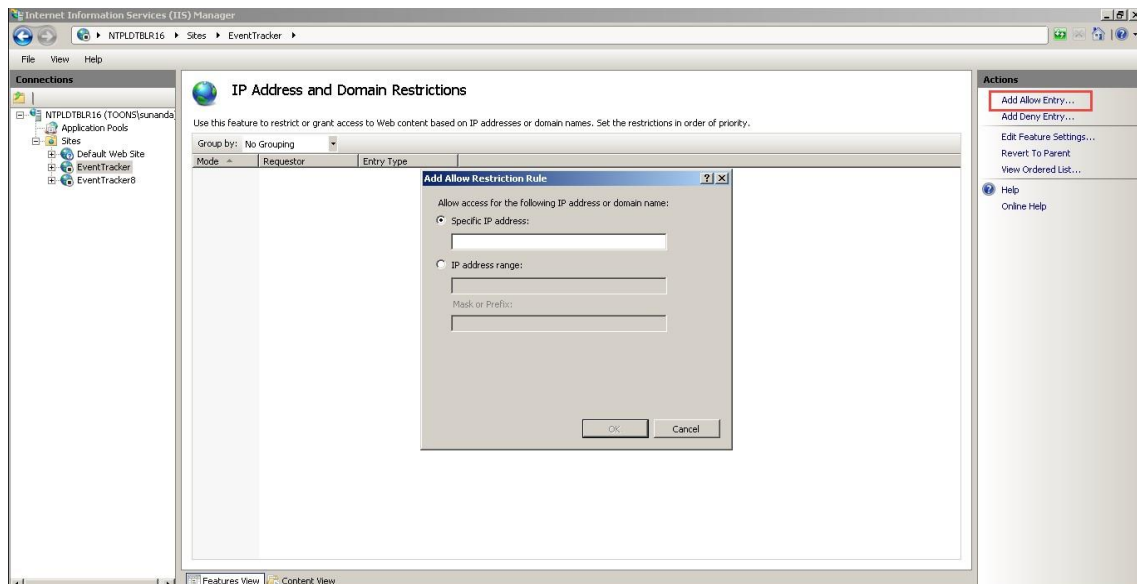


3.5 Configuring IP Address and Domain Restrictions in Windows

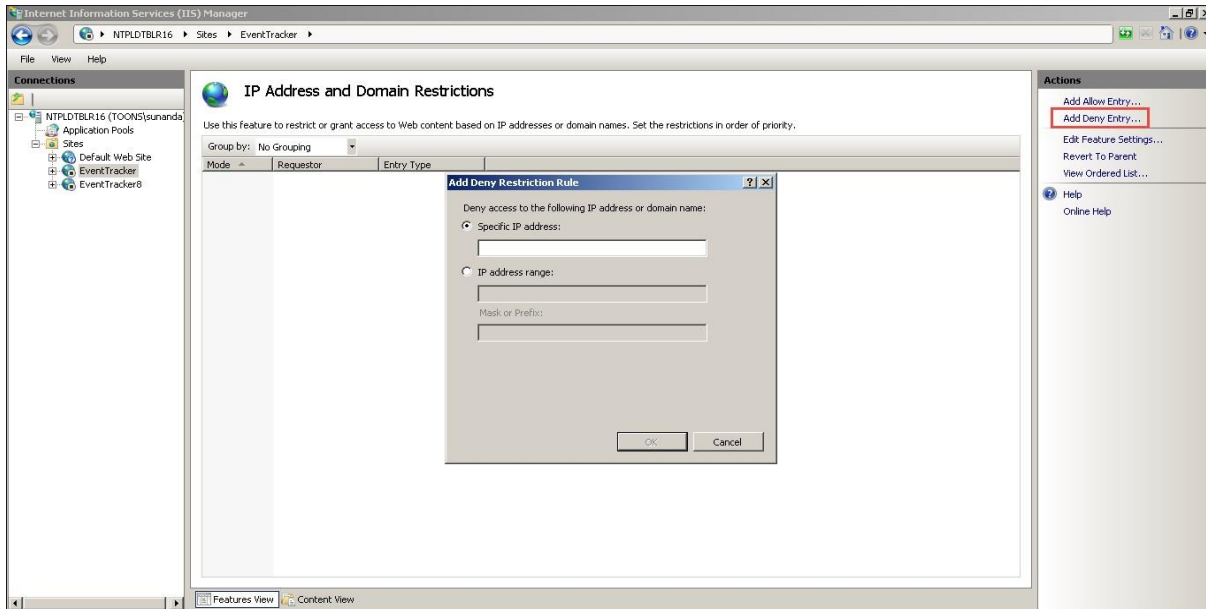
1. Open IIS Manager.
2. Select the **Netsurion Open XDR** site.



3. In **Features View**, double-click **IP Address and Domain Restrictions**.
4. In the **Actions** pane, select **Add Allow Entry** or **Add Deny Entry** to allow or deny entries.



(OR)

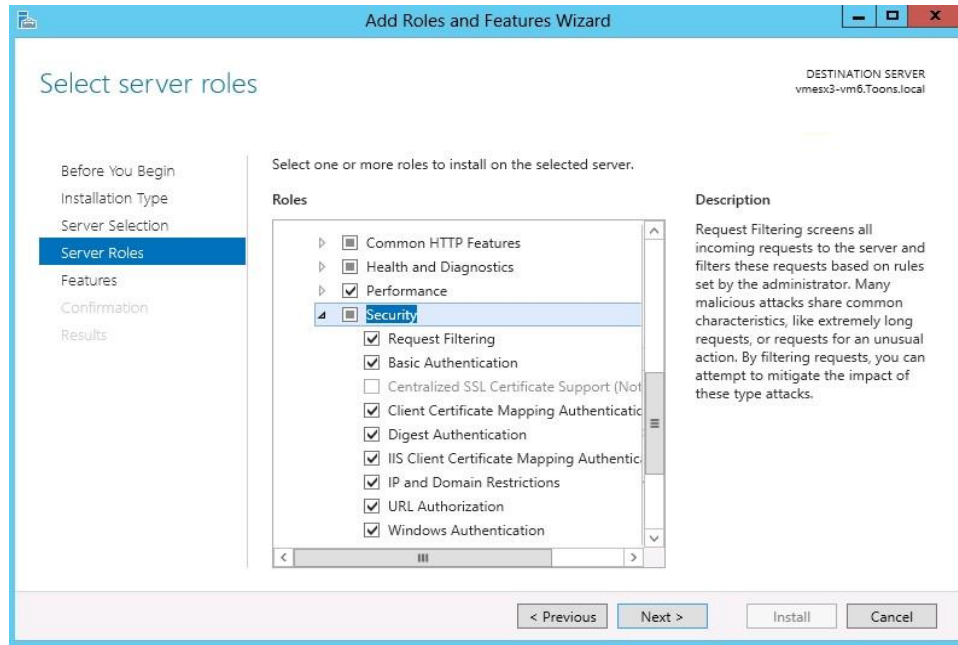


You can specify an IP address, an IP address range, or a Domain Name in the above dialog boxes. Configuring Allow or Deny restrictions using a Domain name requires reverse DNS look-up every time a request arrives from the server. Performing reverse DNS lookups is a potentially expensive operation that can severely degrade the performance of your IIS server.

3.6 Request Filtering in IIS 10 and 11

3.6.1 Installing Request Filtering in Windows

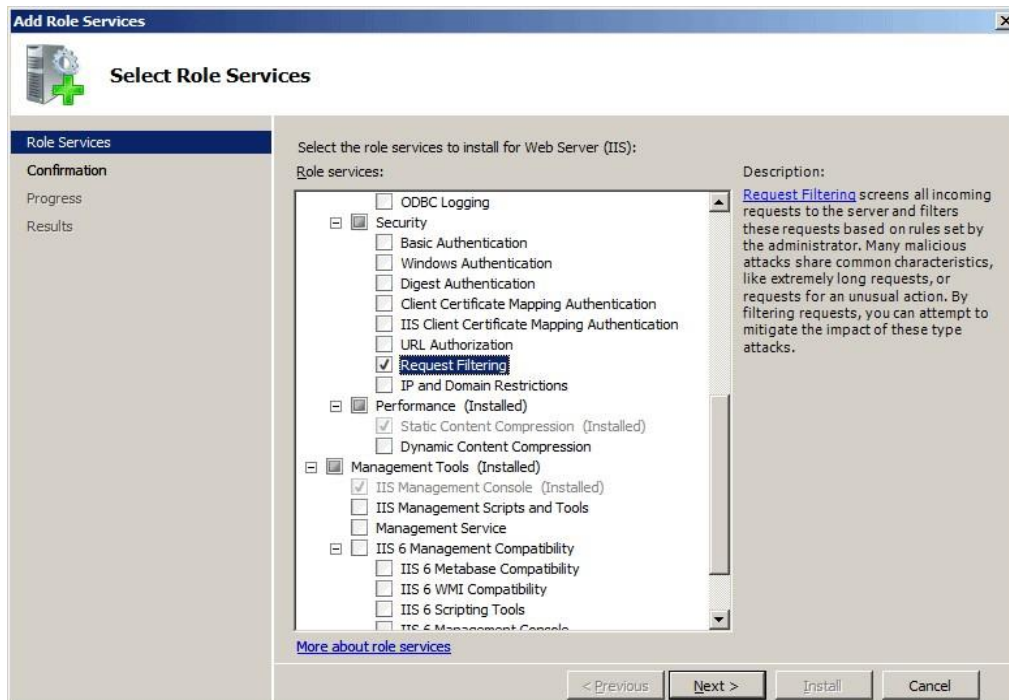
1. Click the **Start** button and select **Administrative Tools**.
2. Select **Server Manager**, select **Dashboard**, and select **Add Role and Features Wizard**. In the **Add Roles and Features** wizard, the **Before You Begin** page displays.
3. Click the **Next** button.
4. On the **Select Installation type** page, select **Role-based or Feature-based Installation**, and then click the **Next** button.
5. On the **Select Destination Server** page, choose **Select a server from the server pool**, select your server from the **Server Pool** list, and then choose the **Next** button.
6. In the **Select Server Roles** window, expand and select **Web Server**.
7. Expand and select **the Security** node, and then select **Request Filtering**, and then click **Next**.



8. On the **Confirm Installation Selections** page, click **Install**.
9. On the **Results** page, click **Close**.

3.6.2 Installing Request Filtering in Windows

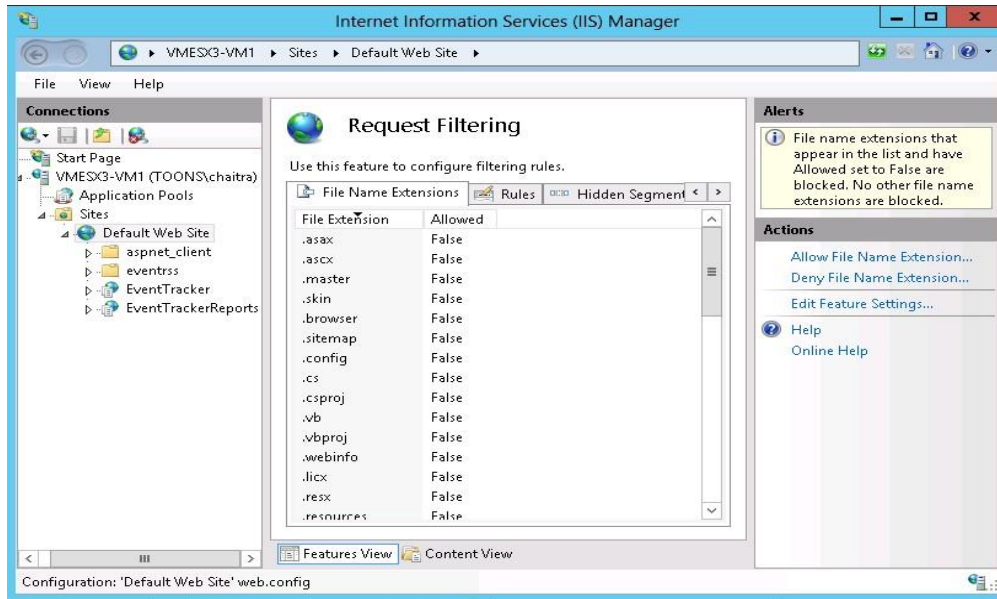
1. On the taskbar, click **Start**, point to **Administrative Tools**, and click **Server Manager**.
2. In the **Server Manager** hierarchy pane, expand **Roles**, and click **Web Server (IIS)**.
3. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and click **Add Role Services**.
4. On the **Select Role Services** page of the **Add Role Services Wizard**, select **Request Filtering**, and click **Next >**.



5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Results** page, click **Close**.

3.6.3 Allowing/Denying Access to a Specific File Name Extension

1. Open **Internet Information Services (IIS) Manager**. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, go to the connection, site, application, or directory for which you want to modify your request filtering settings.
3. In the **Home** pane, double-click **Request Filtering**.
4. In the **Request Filtering** pane, click the **File Name Extensions** tab.
5. To deny file name extensions in the **Actions** pane, click **Deny File Name Extension**.



- The **Deny File Name Extension** dialog box will be displayed as shown below. Enter the file name extension that you want to block and click **OK**.



For example, to prevent access to files with a file name extension of .inc, you would enter "inc" in the dialog box.

- To allow file name extensions in the **Actions** pane, click **Allow File Name Extension**.



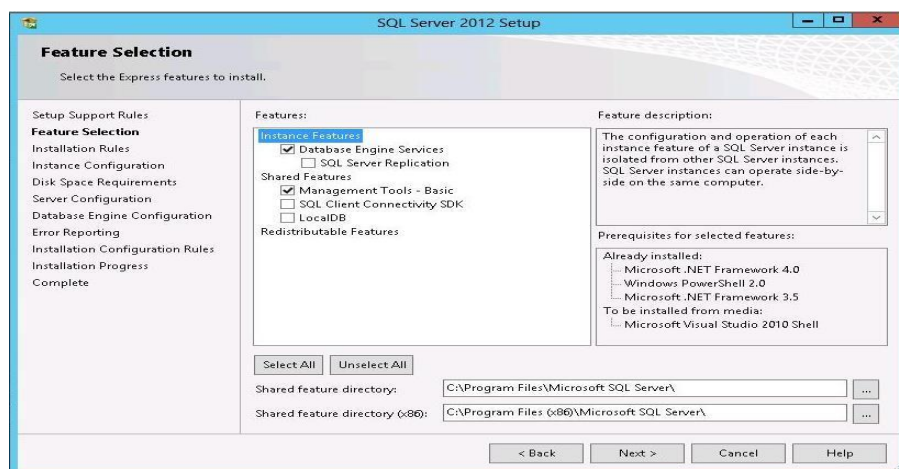
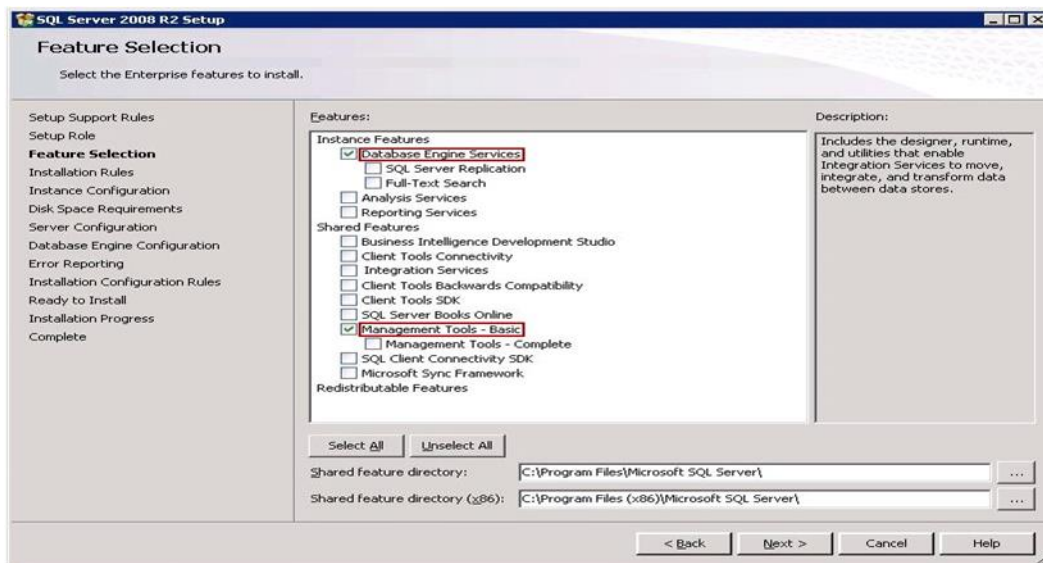
- Enter the file name extension that you want to allow and click **OK**.

4 Securing SQL Database Server

4.1 Reducing the Surface Area for SQL Server Components

To reduce the surface area of SQL Server components, apply the following best practices.

1. Install only the required SQL Server components.
2. While installing the SQL Server, do not include Analysis Services, Integration Services, and Full-Text engine.
3. Do not install SQL Server Reporting Services (SSRS) on the same server as the Database engine. Installing SSRS on the same server as the database engine, and web services opens a hole in the security layer.
4. Install only two features namely Database Engine Services and Management Tools – Basic.



5. Disable the following SQL Server services.
 - SQL Server VSS Writer service

- SQL Server Browser
 - SQL Active Directory Helper service
6. Ensure the latest antivirus version is configured correctly.
 7. Install the latest critical fixes and service packs for both Windows and SQL Server.

4.2 Reducing the Surface Area for SQL Server Services

To reduce the surface area of SQL Server services, apply the following best practices.

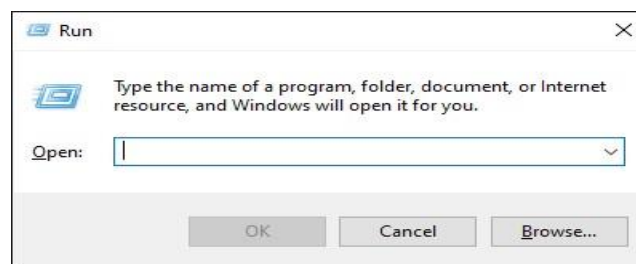
1. Install only Database Engine Services. Do not include **Analysis, Reporting, Notification, and Integration** services. Do not opt for **Workstation components, Books Online, and development tools** option.



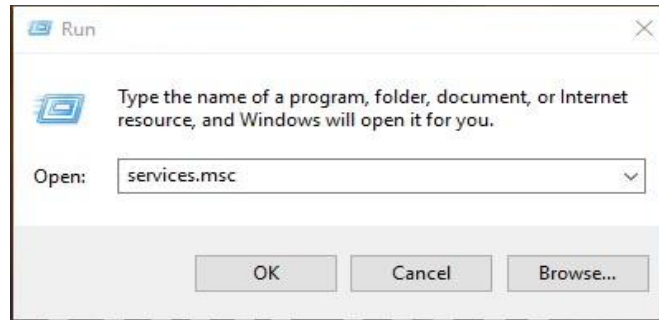
2. Disable the following SQL Server services.
 - SQL Server VSS Writer service
 - SQL Active Directory Helper service
 - SQL Server Browser service

Follow the steps given below to disable the services.

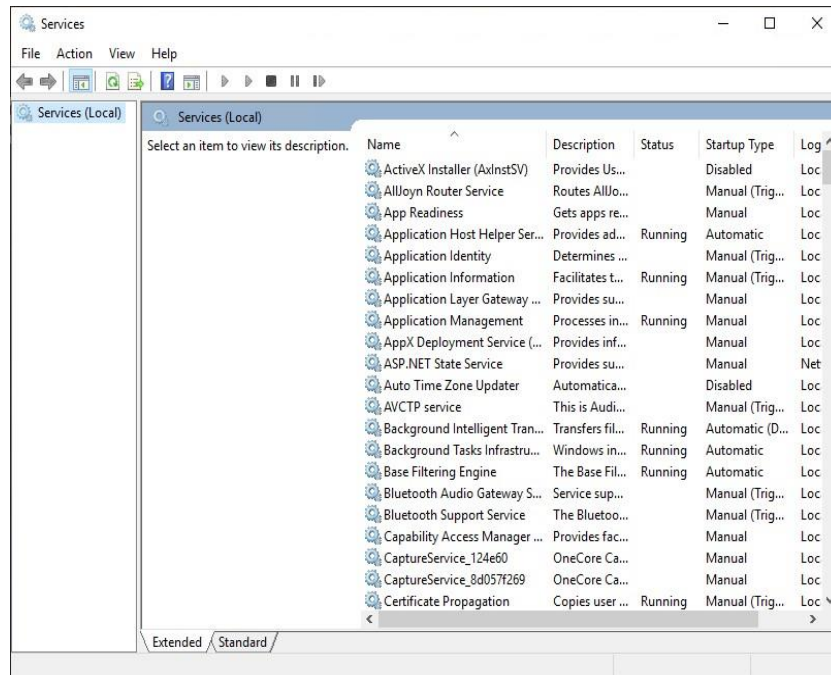
1. Click the **Start** button and click **Run**.



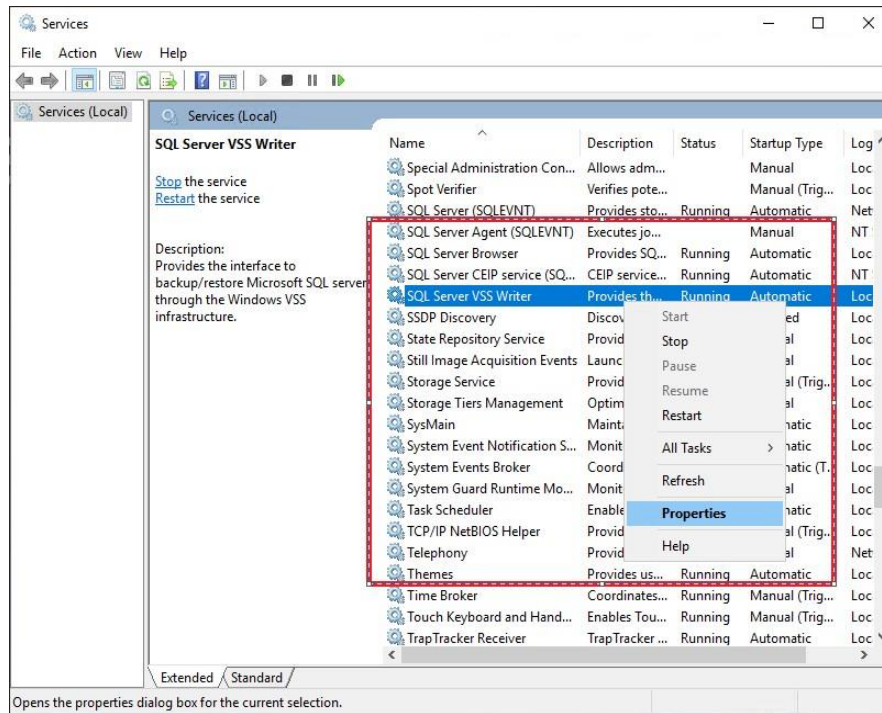
2. In the **Run** window, type '**Services.msc**', and click the **OK** button.



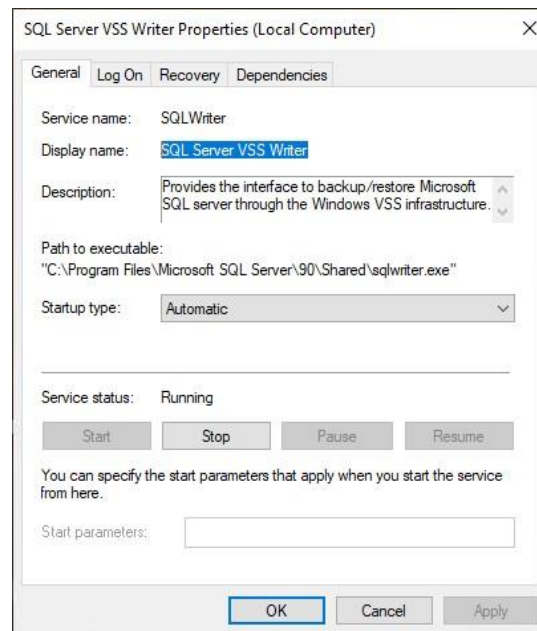
3. The **Services** window will be displayed as shown below:



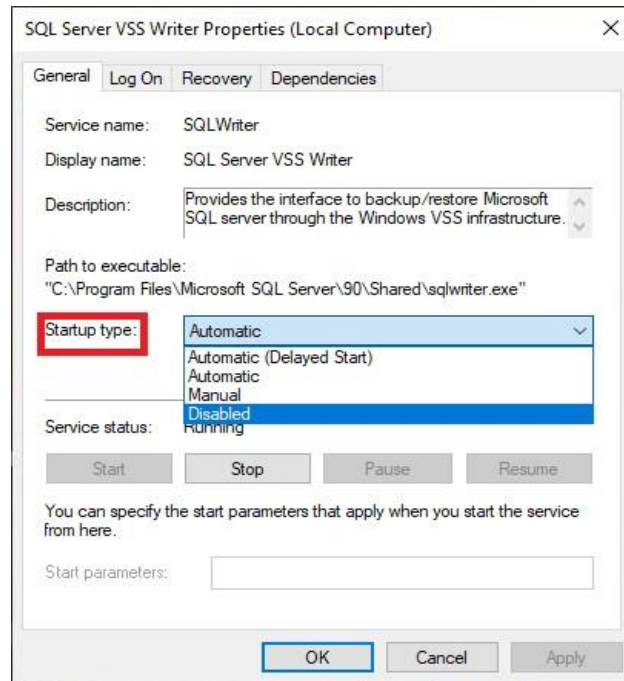
4. Locate the required service(s) name in the **Name** column.
Example: SQL Server VSS Writer service.
5. Right-click the service to be disabled and click **Properties**.



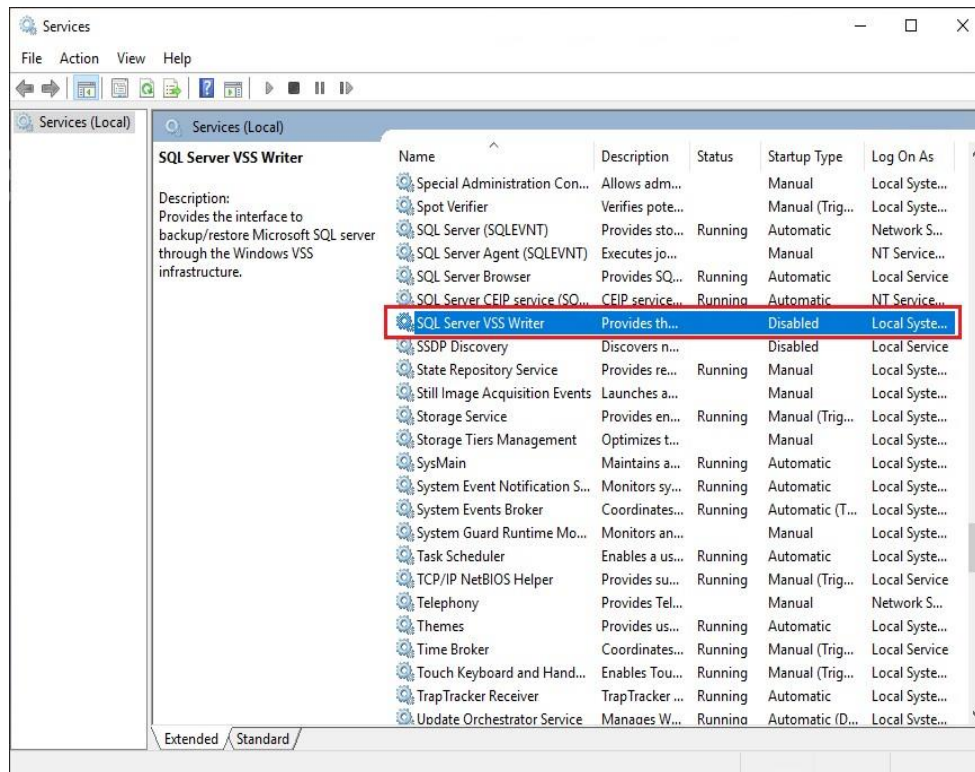
6. The **SQL Server VSS Writer Properties (Local Computer)** dialog box appears as shown below:



7. Click the **Startup type** dropdown and select **Disabled**.



8. Click the **Stop** button to stop the service.
9. Click **Apply**, and then **OK**.



Note

If the remote indexer is enabled in the Netsurion Open XDR Manager then,

- 'SQL server browser' service should be enabled.
- 'sqlbrowser.exe' and 'sqlservr.exe' must be added to the firewall exception list.

4.2.1 SQL Server SA Account

- The Windows Authentication mode is more secure than SQL Authentication. Hence, configure the SQL Server to use Windows authentication only.
- If the Windows Authentication mode is selected during installation, the SA login is disabled by default. If the authentication mode is switched to SQL Server mixed mode after the installation, the SA account is still disabled and must be manually enabled if required.
- Enabling mixed-mode authentication will
 - Disable or rename the SA Account. Do not use this account for SQL server management.
 - Enforce a strong password policy, while using SQL Authentication.

5 Netsurion Open XDR Settings

5.1 Securing Agent Configuration and Saving it as a Template

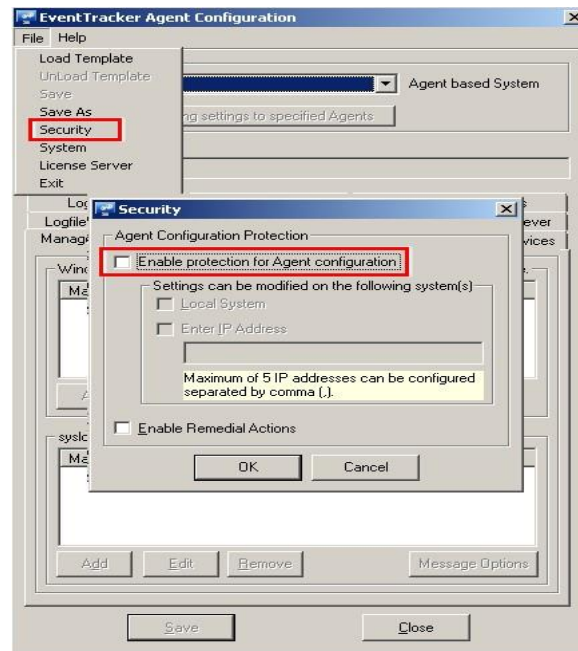
The current Agent configuration settings on the local system can be protected from being modified by any unauthorized remote system. This option allows only the local system to modify the agent settings or configure up to five IP addresses of remote systems where the modification of agent configuration is possible.

It is recommended to save the agent configuration settings as a **Template** and apply it to multiple agent systems at once instead of applying them individually.

To use the same configuration settings for agent systems, the agent configuration on the local system needs to be saved as a **Template** first. The template is saved as a **.ini** file in the default path, which would be ProgramFiles\PrismMicrosystems\EventTracker\RemoteInstaller.

5.2 Protecting the Current Configuration Settings for Local System

1. Go to the **Netsurion Open XDR** Control Panel.
2. Double-click the **Netsurion Open XDR Agent Configuration**, and then click the **File** dropdown.
3. Click the **Security** option.



Field	Description
Agent Configuration Protection	
Enable Protection for Agent Configuration	Select this option to protect the configuration settings from being modified by a remote agent system.
Settings can be modified on the following system(s)	
Local System	Select this checkbox to protect the current configuration settings of the local system. Other users cannot modify the settings from their machines.
Enter IP Address	Select this checkbox to allow the specified remote systems to do the configuration changes in the local system. Type the IP address in the IP Address field. Up to five IP addresses can be configured, separated by commas (,).
Remedial Action	Remedial actions are scripts or EXEs that can be launched at either the agent or Manager side, in response to events.

4. Select the **Enable Protection for Agent Configuration** option.
5. Click the **OK** button.

Note

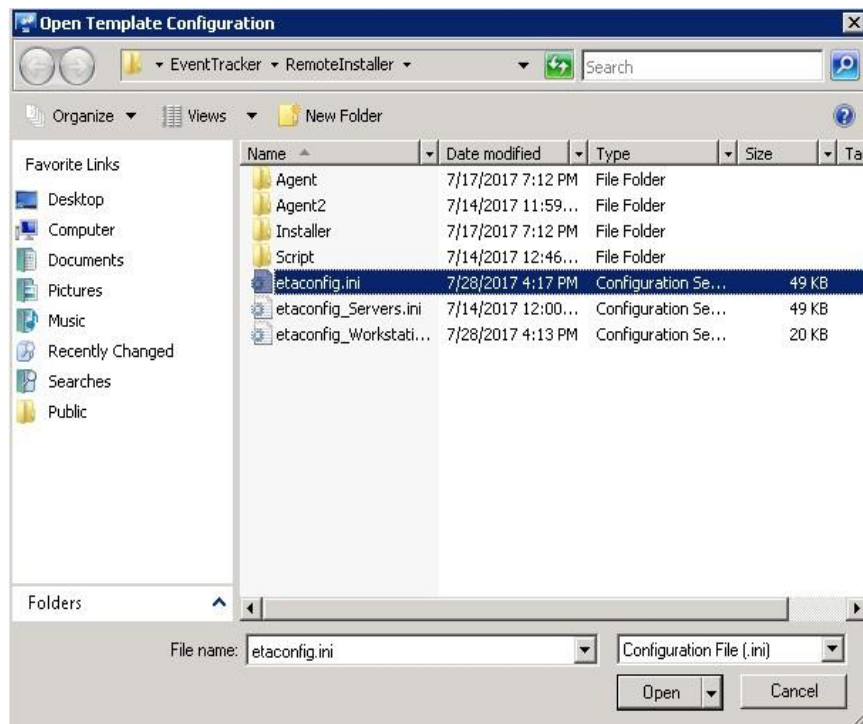
To apply this configuration to the agent systems in the enterprise, click the **Apply this configuration to agents** button.

5.2.1 Applying Configuration to Agent System(s)

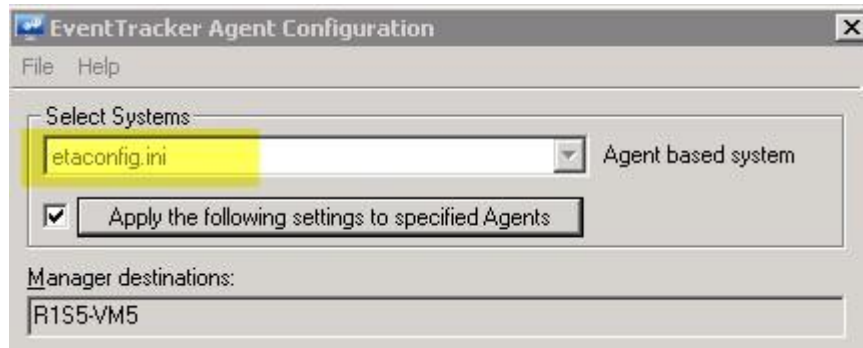
1. Go to the **Netsurion Open XDR Control Panel**.
2. Double-click the **Netsurion Open XDR Agent Configuration** and click the **File** dropdown.
3. Click the **Load Template** button.



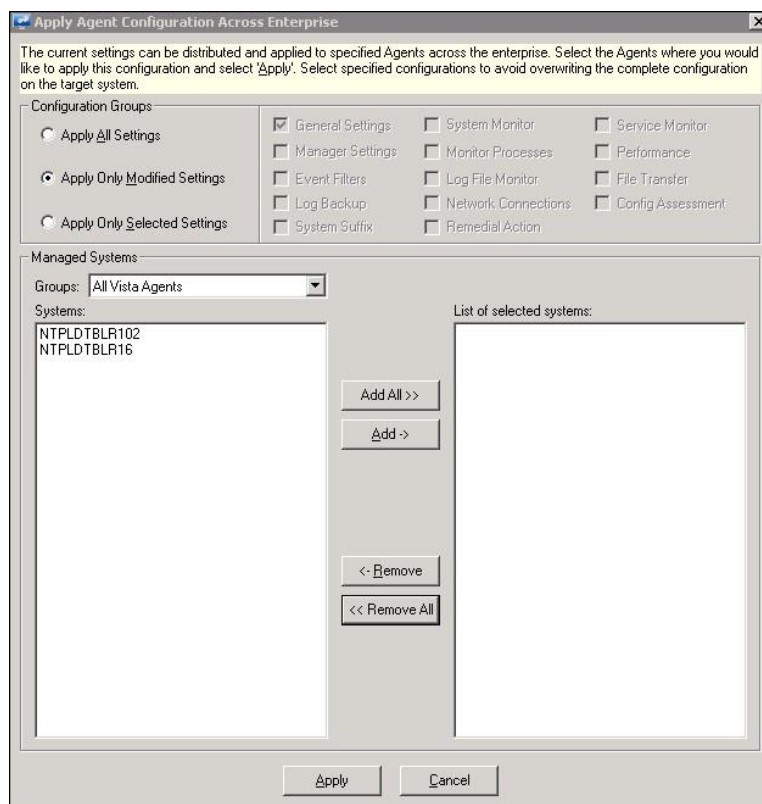
4. Select the **File name** from the file location and click the **open** button.



5. Netsurion Open XDR loads the selected template configuration.



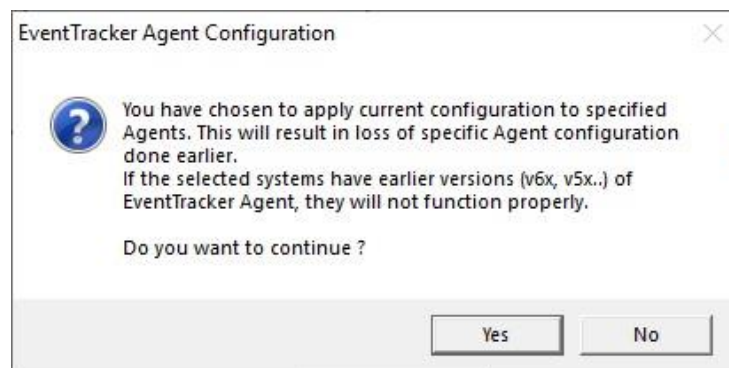
6. To apply this configuration to the agent systems in the enterprise, click the **Apply the following settings to specified Agents** button.
7. The **Apply client configuration across the enterprise** dialog box appears as shown below:



8. Select a system group from the **Select a group** dropdown. Netsurion Open XDR displays the managed systems associated with the selected group.
9. Check the required system options for which the configuration needs to be applied.
10. Select the **Configuration Groups** option as required.

Field	Description
Apply Only Modified Settings	Netsurion Open XDR selects this option by default. Leave the default selection to apply only modified settings.
Apply All Settings	Select this option to apply all the settings including the default and modified settings.
Apply Only Selected Settings	Select this option to apply only the selected settings made under respective tabs. Netsurion Open XDR enables the checkboxes. Select appropriately and then click Apply .

11. Click the **Apply** button. Netsurion Open XDR displays a warning message as shown below:



12. Click the **Yes** button. The template configuration is loaded successfully on the selected systems.

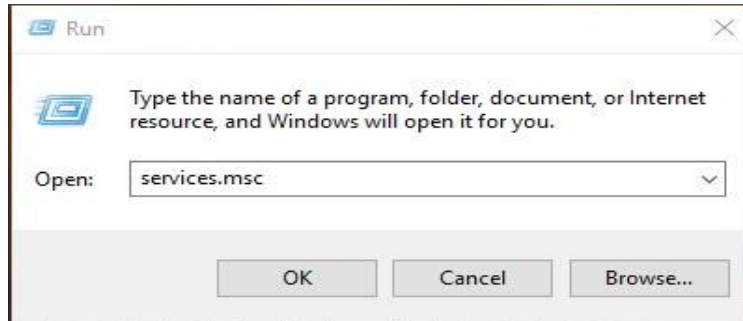
5.3 Securing EventVault Storage

Provide EventVault storage access only to the required Netsurion Open XDR administrators/users.

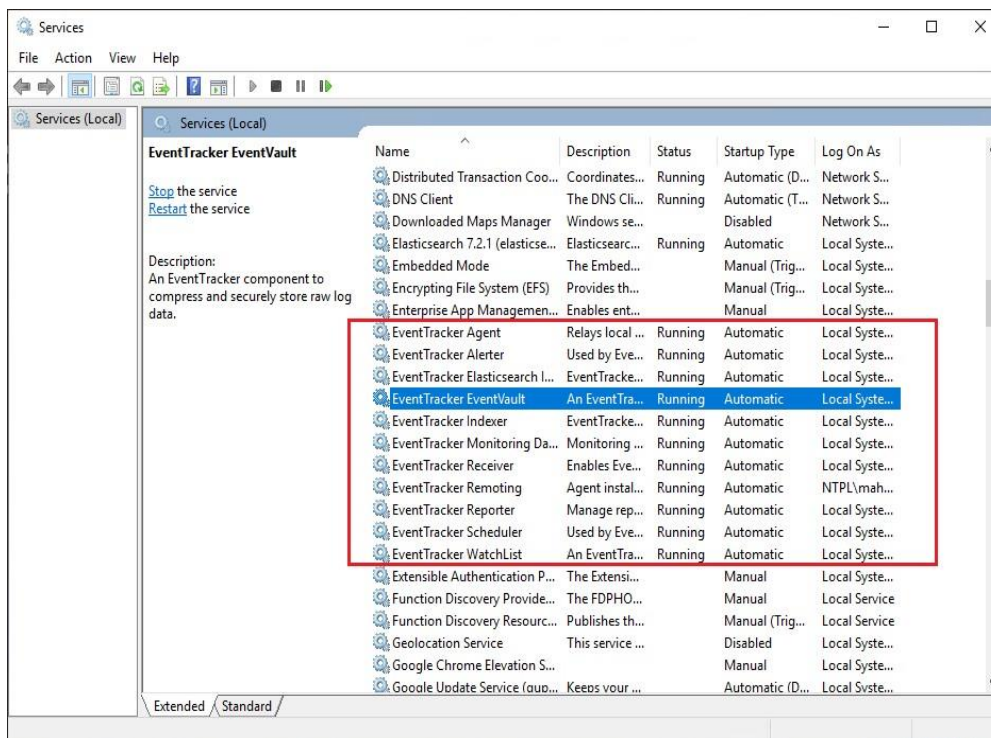
1. **Backup purpose:** Provide full permission to the user responsible to take periodic backup of the data.
2. **Archives stored in UNC (Uniform Naming Convention) path:**
 - a. Create a service account.
 - b. Provide full permission to the created service account.
 - c. Change the following services to run under the created service account.
 - Netsurion Open XDR Scheduler
 - Netsurion Open XDR EventVault
 - Netsurion Open XDR Reporter
 - Netsurion Open XDR Indexer
 - Event Correlator (if available)

5.3.1 Changing the Service Account

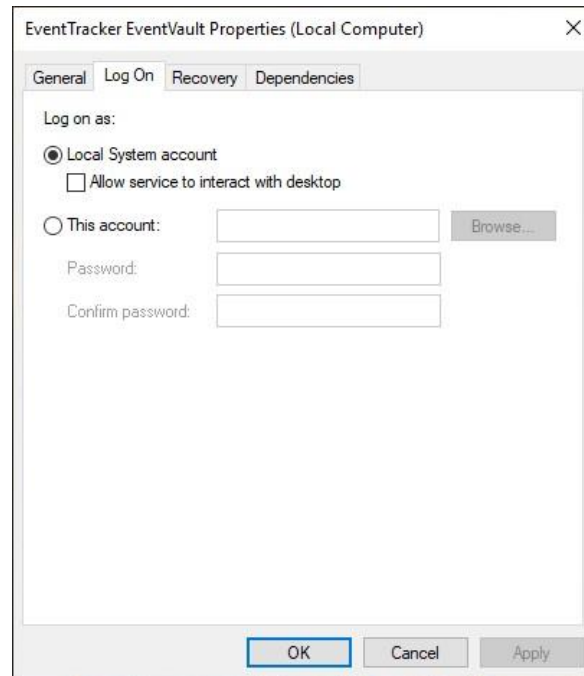
1. Click the **Start** button and select **Run**.
2. Type **services.msc**, and then click the **OK** button.



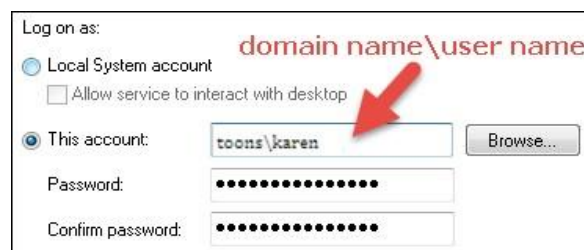
3. In the **Services** window, search for Netsurion Open XDR services.



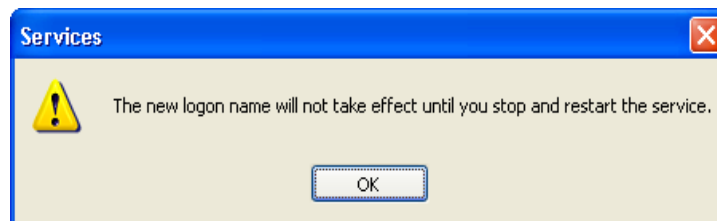
4. Right-click the service name and click **Properties**.
For example, right-click **Netsurion Open XDR EventVault** service
5. The Netsurion Open XDR EventVault Properties (Local Computer)' window will be displayed as shown below.



6. Click the **Log On** tab and select **This account** option.



7. Enter the user credentials and correct password. The username should be in the 'domain name\username' format.
8. Click the **Apply** button. An alert window will be displayed as shown below:



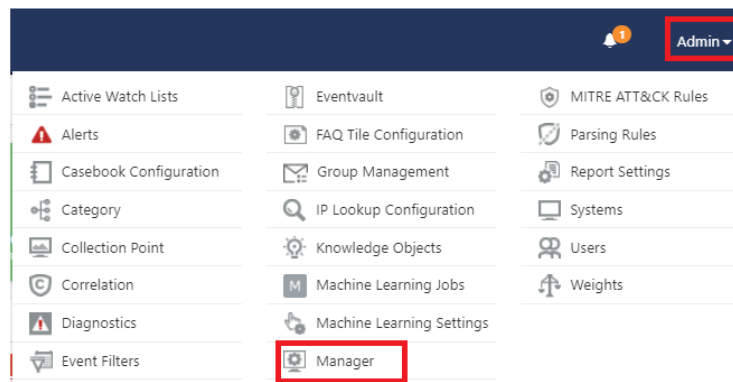
9. Click the **OK** button.
10. To run the service with a new login name, stop and start the service.
11. Likewise, for the rest of the services, repeat steps 4 to 10 to change the service account. The **Log On As** column will display the changed service account name.

Name	Description	Status	Startup Type	Log On As
Event Log	Enables ev...	Started	Automatic	Local System
EventTracker Agent	Relays loca...	Started	Automatic	Local System
EventTracker Alerter	Used by Ev...		Automatic	Local System
EventTracker EventVault	An EventTr...	Started	Automatic	toons\sonal
EventTracker Indexer	EventTrack...	Started	Automatic	toons\sonal
EventTracker Receiver	Enables Ev...	Started	Automatic	Local System
EventTracker Remoting	Agent inst...	Started	Automatic	Local System
EventTracker Reporter	Manage re...	Started	Automatic	toons\sonal
EventTracker Scheduler	Used by Ev...	Started	Automatic	Toons\sonal
Extensible Authentication Protocol Service	Provides wi...		Manual	Local System

6 Enabling Two-Factor Authentication in Netsurion Open XDR Web Console

To enable Two-Factor Authentication in Netsurion Open XDR Web Console, perform the following steps:

1. Log into the Netsurion Open XDR Web Console.
2. Click **Admin > Manager**.



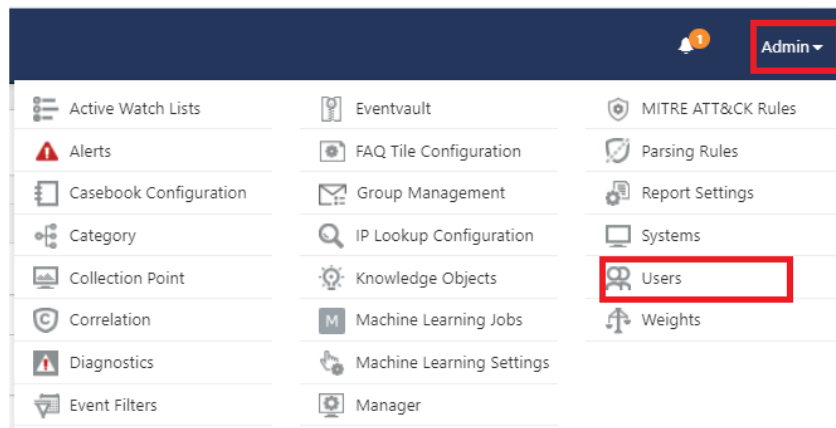
3. In the 2FA authentication section, select the **Enable 2FA** option, and click **Save**.

The screenshot shows the Netsurion Manager configuration interface. The 'Alert Events' section is active, displaying options to enable alert notifications, remedial actions, and email headers. Below this, the 'Configuration' section contains fields for KB website, News URL, Contact URL, EYVM URL, ntoping URL, Intrusion Detection System URL, Honeynet URL, and API Domain URL. The 'Reputation & Geolocation Configuration' section shows 'Netsurion Threat Center' as the IP Reputation provider and 'MaxMind GeoLite' as the IP Geolocation provider. The 'Keyword Indexer' section has 'Enable keyword indexing' checked. The 'Correlation Receiver' section has 'Send results of all correlation rules to port' set to 14509. The 'Logon Banner' section is empty. The 'PSA/RMM Integration' section is disabled. The 'Unknown Process Detection' section has 'Enable unknown process' and 'Look up in NSRL' checked. The 'Archiver' section has 'Archiver at Group level' checked. The 'Two-factor authentication(2FA)' section is highlighted with a red box, showing 'Enable 2FA' and 'Apply for all users' both checked. The 'Single Sign-On(SSO)' section is disabled. The footer shows the Netsurion logo, server time (Feb 29 11:00 PM), response time (0.270 secs), and copyright (© 2024 Netsurion).

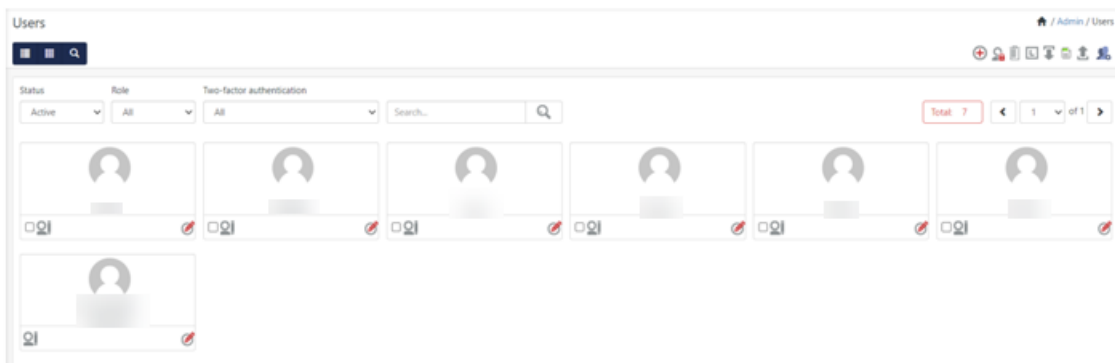
4. Now the 2FA option will be enabled by default while creating new users.

6.1 Adding New Users

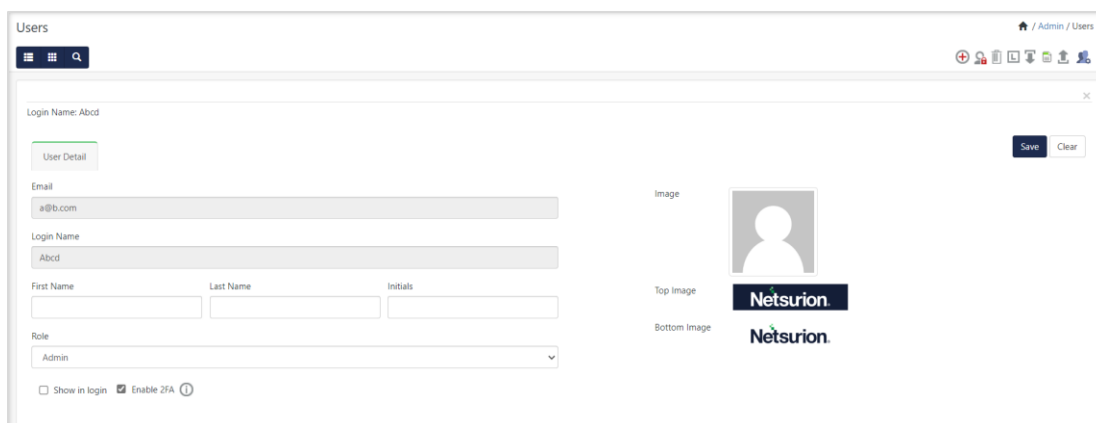
1. Click **Admin > Users**.



2. Click the + icon to add a new user.



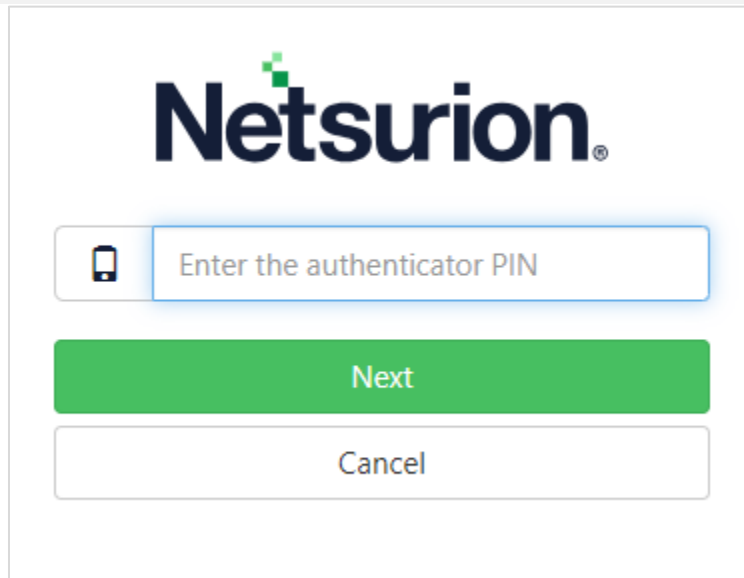
3. The **User Detail** page will be displayed as shown below. The 2FA option is enabled by default for the users.



4. Enter the required details and click **Save**. Next time, if the user logs into the Netsurion Open XDR Web console, the user will be asked to provide their authentication to log in.

Note

You may also choose to unselect the **Enable 2FA** option to disable the feature.

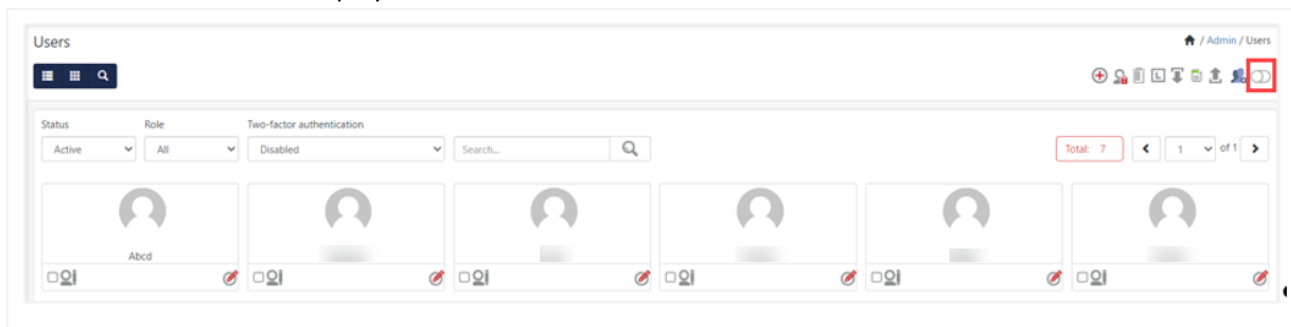


Refer to the following link to configure the Authenticator App.

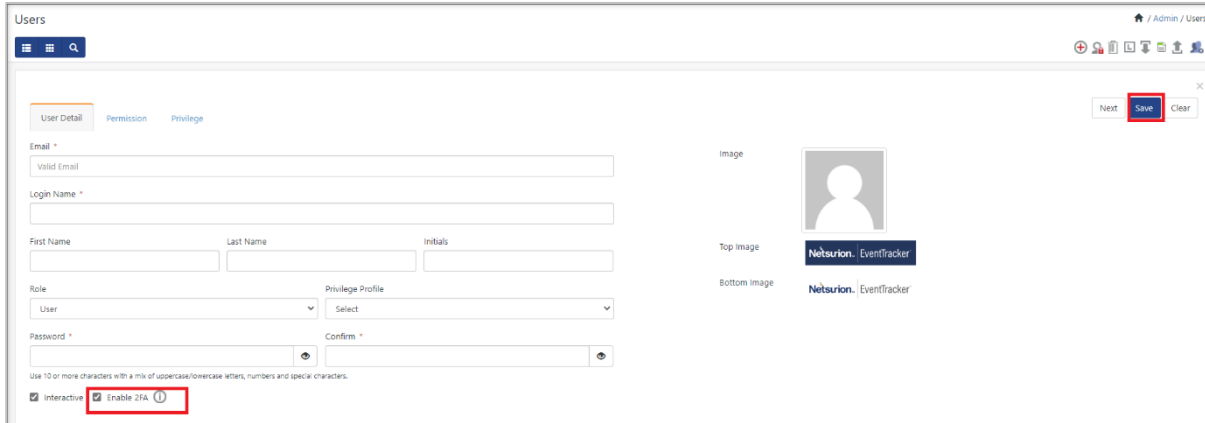
<https://www.netsurion.com/assets/content/uploads/files/support-docs/How-To-Configure-Two-Factor-Authentication-using-Authenticator-App-Netsurion.pdf>

6.2 Enabling 2FA Option for Existing Users

1. Click **Admin > Users**.
2. In the **Two-Factor Authentication** dropdown, select the **Disabled** option. All the user accounts with disabled 2FA will be displayed as shown below:

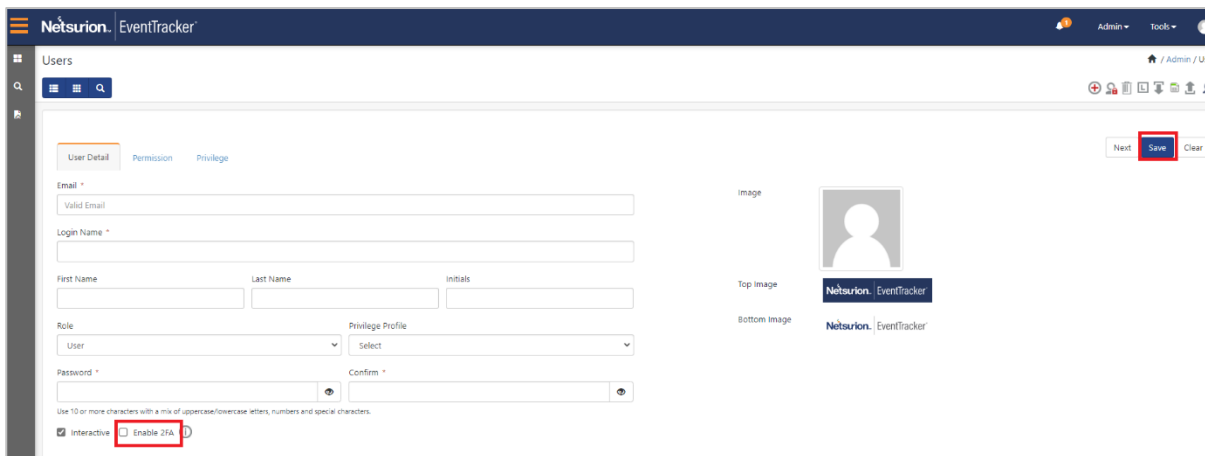


3. Click the **Edit** icon on the corresponding user account for which you want to enable 2FA and then click **Save**. Two-factor authentication will be enabled for the selected user.

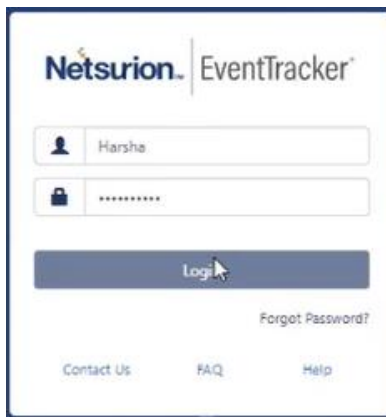


6.3 Disabling 2FA

1. Click **Admin > Users**.
2. Click **Add User**, and then unselect the 2FA option to disable the feature, and then click **Save**.



3. Next time, when the user logs into the Netsurion Open XDR Web console, the user will be prompted to reset the password.





7 Checking for Vulnerability Scanner

It is a standard practice to scan critical machines for vulnerabilities. Scan the hardened Netsurion Open XDR system for vulnerabilities. Some of the following vulnerabilities may be reported.

Note

The possibilities and their solutions/configuration changes are shown in the below table.

Vulnerability	Impact	Recommended actions
'rsh' Remote Shell Service Enabled (service-rsh) (CVE1999-0651)	This is a legacy service often configured to blindly trust some hosts and IPs. The protocol does not support encryption or any sort of strong authentication mechanism.	Netsurion Open XDR uses default port 514 for receiving syslog messages. Configure the firewall to allow incoming connections on port 514 from trusted hosts or use another port for receiving syslog in Netsurion Open XDR Manager Configuration.
The FTP server does not support the AUTH command (ftpgeneric-0007)	By default, FTP clients send user credentials (user ID and password) in clear text to the FTP server. This allows malicious users to intercept the credentials if they can eavesdrop on the connection.	FTP server is installed on the Netsurion Open XDR Manager to transfer custom logs from remote sources. In the case of IIS 6, FTP does not support the AUTH command. Use a third-party FTP that supports the AUTH command and configure FTP over SSL.
Untrusted TLS/SSL server X.509 certificate (tlsuntrusted-ca)	The server's TLS/SSL certificate is signed by a Certification Authority (CA) whose publisher is not known or a trusted one. It could indicate that a TLS/SSL man-in-the-middle is taking place and is eavesdropping on TLS/SSL connections.	Obtain a new certificate signed by trusted certificate authorities, such as Thawte or Verisign.
Guest access allowed to Windows	Windows event logs have been configured to allow guest access.	For each event log listed, find the following registry key:

<p>event logs</p>	<p>They contain information about application, security, and system events taking place on the local machine. These logs can contain sensitive information, therefore only administrators should be allowed to access/read them.</p>	<p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\[logname]</p> <p>Under this key, add a DWORD value named "RestrictGuestAccess" and set it to 1.</p>
<p>Microsoft IIS default installation/welcome page installed (http-iis-defaultinstall-page)</p>	<p>The IIS default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server that has not yet been configured properly and is not known about.</p>	<p>Replace the default page with a relevant content page.</p>
<p>TCP timestamp response (generictcp-timestamp)</p>	<p>The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.</p>	<p>Disable the TCP timestamp responses on Windows.</p> <p>For each event log listed, find the following registry key:</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters</p> <p>Under this key, add a DWORD value named "Tcp1323Opts " and set it to 1.</p>
<p>General Security Issue Clear text authentication</p>	<p>FTP specification primarily provides a means for authenticating User IDs and passwords stored in clear text, though there are secure mechanisms to authenticate. User IDs and passwords can be stolen by a malicious user if he can monitor FTP traffic.</p>	<p>FTP server is installed on the Netsurion Open XDR Manager to transfer custom logs from remote sources.</p> <p>In case of IIS 6, FTP does not support the AUTH command. Either use a third-party FTP that supports the AUTH command and configure FTP over SSL or configure the FTP server to allow connection from a trusted host.</p>

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

<https://www.netsurion.com/support>