Hardening Guide

Hardening Guide for EventTracker Server

EventTracker v9.x

Publication Date:

September 8, 2021

Abstract

The EventTracker solution includes a console component installed on a Windows Server 2008/ 2008 R2 / 2012/ 2016/ 2019.

It is important to harden and protect this server from disrupting the service delivery and unauthorized access.

This guide describes how to create and maintain a secure environment for the server that runs EventTracker v9.x console.

Audience

This guide is intended for use by all EventTracker users responsible for investigating and managing network security. This guide assumes that you have EventTracker access and understanding of networking technologies.

Table of Contents

1. Harden Windows Server – Quick View

Apply 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.

https://downloads.eventtracker.com/support/utils/WS2019-GPO.zip

And 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

Click here for the detailed steps to apply the policies.

1.2 Applying Group Policies on Windows Server 2012

Harden Windows Server 2012/2016 according to the standard policy. Click the following link to download the GPO.

Download WS201`2-GPO.zip

And apply the following policies:

- WS2012-Domain
- WS2012-Member-Server
- WS2012-Web-Server
  - WS2012-Remote Desktop Services

Click here for the detailed steps to apply the policies.

1.3 Applying Group Policies on Windows 2K8 / 2K8 R2 Enterprise SP1

Harden Windows Server 2008 R2 Enterprise SP1 according to the standard policy. Click the following link to download the GPO.

Download WS08R2-SSLF-GPO.zip

And apply the following policies:

- WS08R2-SSLF-Domain

- WS08R2-SSLF-Member-Server
- WS08R2-Web-Server Group Policy

Click here for the detailed steps to apply the policies.

1.4 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 EventTracker server in DMZ network.
- Give administrative access only to Authorized users or administrators.
- Disable directory Browsing in IIS.
- Do not install Internet printing Extension on EventTracker server.

1.5 Securing SQL Server

- While installing 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 Sysadmin role only to Authorized Administrators and users.
- Install Recent service packs and critical fixes for SQL Server and Windows.
- Remove BUILTIN\Administrators group from the SQL Server Logins.

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

1.6 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 EventTracker, 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)	EventTracker Certificate server
14506 (TCP)	EventTracker Agent
14507 (TCP)	Collection Master
443 (TCP)	EventTracker securely access(HTTPS), EventTracker Endpoint Security
514 (UDP/TCP)	Syslog Receiver, Multiple VCP's can be configured
14504	EventTracker Active Watchlist
9200	Elasticsearch-service-x64, Elastic Cross Cluster
9300	Elastic Cross Cluster **Note**: Applicable for EventTracker 9.3 version.
6514	EventTracker Endpoint Security **Note**: This port is configurable. In case of change in port number the EventTracker team will notify. **Note**: Applicable for EventTracker 9.3 version.

EventTracker Application by default uses few ports for communication. These ports must be added to the firewall exception on EventTracker Server.

Rules	Protocol	Local Port	Remote Port	Source (Session Initiator)	Target (Listener)	Usage/Purpose
Inbound (EventTracker Consoles)						
	TCP	14506	All	EventTracker Agent Service	EventTracker Agent Service running on EventTracker Console	Configuration synchronization request
	TCP	14503	All	EventTracker Agent Service	License Server running on EventTracker Console	License details and verification request
	TCP/UDP	14505	All	EventTracker Agent Service	EventTracker Receiver running on EventTracker Console	Default port used for receiving events
	TCP	14502	All	Change Audit Service	Change Audit Service running on EventTracker Console	Receiving snapshot files
	TCP	14509	All	Event Correlator	Correlator	Event Correlator component
	TCP/UDP	514	All	syslog devices	EventTracker syslog Receiver running on EventTracker 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 EventTracker Console	Port used for receiving SNMP v1, v2c and v3 Traps/Informs
	TCP	14504	All	EventTracker modules requesting Active watch list lookups	EventTracker Watch list server running on EventTracker Console	Serves the Active watch list lookup requests.
	TCP	9200,9300	Any	Collection Master	Collection Point	Cross-Cluster Elastic search Collection.

Rules	Protocol	Local Port	Remote Port	Source (Session Initiator)	Target (Listener)	Usage/Purpose
Outbound (EventTracker Sensor)						
	TCP	All	14503	EventTracker Agent Service	License Server running on EventTracker Console	License update request
	TCP	All	14506	EventTracker Agent Service	EventTracker Agent Service running on EventTracker Console	Configuration synchronization request
	TCP/UDP	All	14505	EventTracker Agent Service	EventTracker Manager	Sending the logs
	TCP	All	14502	Change Audit Service on ChangeAudit Agent	Change Audit Service on EventTracker Console	Configuration management
	TCP	All	14508	Change Audit Service on ChangeAudit Agent	Change Audit Service on EventTracker Console	On demand policy comparison request
	TCP	All	443	EventTracker Endpoint security Agent	IP address: 35.237.75.235	Applicable for EES sensor deployment only

1.7 Allowing Outbound Access to Public URL’s

EventTracker Server/Sensor requires access to certain public URL/IP address to perform various functions like IOC validation/DNS lookup who is etc. Below are the URL’s that must be allowed in your gateway firewall/Proxy for EventTracker to access these URL.

URL	Usage In EventTracker	Ports Requirement
threatcenter.eventtracker.com	Used as default reputation provider in EventTracker.	TCP-443-Outbound
reputationauthority.org	Used as a reputation provider in EventTracker.	TCP-443-Outbound
ipvoid.com	Used as a reputation provider in EventTracker.	TCP-443-Outbound
exchange.xforce.ibmcloud.com **api.xforce.ibmcloud.com**	Used as a reputation provider in EventTracker.	TCP-443-Outbound
borderware.com	Lookup used in threats dashboard.	TCP-443-Outbound

URL	Usage In EventTracker	Ports Requirement
nsrl.eventtracker.com	Used for unknown process detection to identify the process is safe/unknown.	TCP-9120-Outbound
***.virustotal.com**	Reputation provider and lookup for IP and process hash.	TCP-443-Outbound
***.Ipinfo.io**	Used to get the IP address info to populate the behavior dashboard.	TCP-443-Outbound
***.EventTracker.com**	To download the EventTracker updates and knowledge packs.	TCP-443-Outbound
hybrid-analysis.com	Used as a reputation provider in EventTracker.	TCP-443-Outbound
https://whois.domaintools.com/	Used for whois lookup.	TCP-443-Outbound
http://www.processlibrary.com/	Used for process lookup	TCP-443-Outbound
Netsurion.com	Used to access various info about Netsurion like news etc.	TCP-443-Outbound

1.8 Checking for Vulnerability Scanner

Scan the hardened EventTracker system for vulnerabilities. Click here to read the possibilities and solutions/configuration changes.

Note: Applicable only if Vulnerability Scanner is used.

1.9 Security Recommendation for EventTracker v9.x

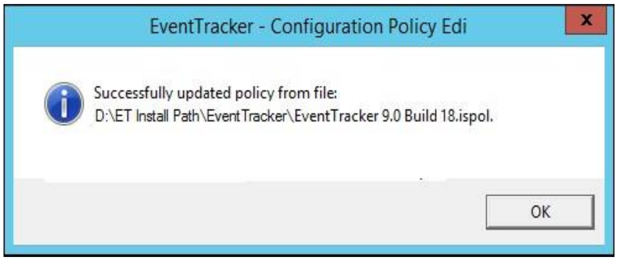
A golden snapshot of EventTracker v9.x is available (named Change Policy v9.0). After installing EventTracker in customer premises, take a snapshot of EventTracker v9.x and compare with the golden snapshot and accept the violations for the first time.

1. Download the Golden Baseline Policy file.
2. Open the content of this file in notepad and save the file in a desired location with extension '.ispol'.
3. Edit the '.ispol' file, enter the correct path of the folder where EventTracker is installed. i.e. the command [DefFolder] =C:\Program Files (x86)\Prism Microsystems\Common\has to be replaced with [DefFolder] = \\Installdir\Program Files\Prism Microsystems\Common in the entire file.
4. Select **Replace All** to update the path in the document.

To import the policies, follow the steps given below.

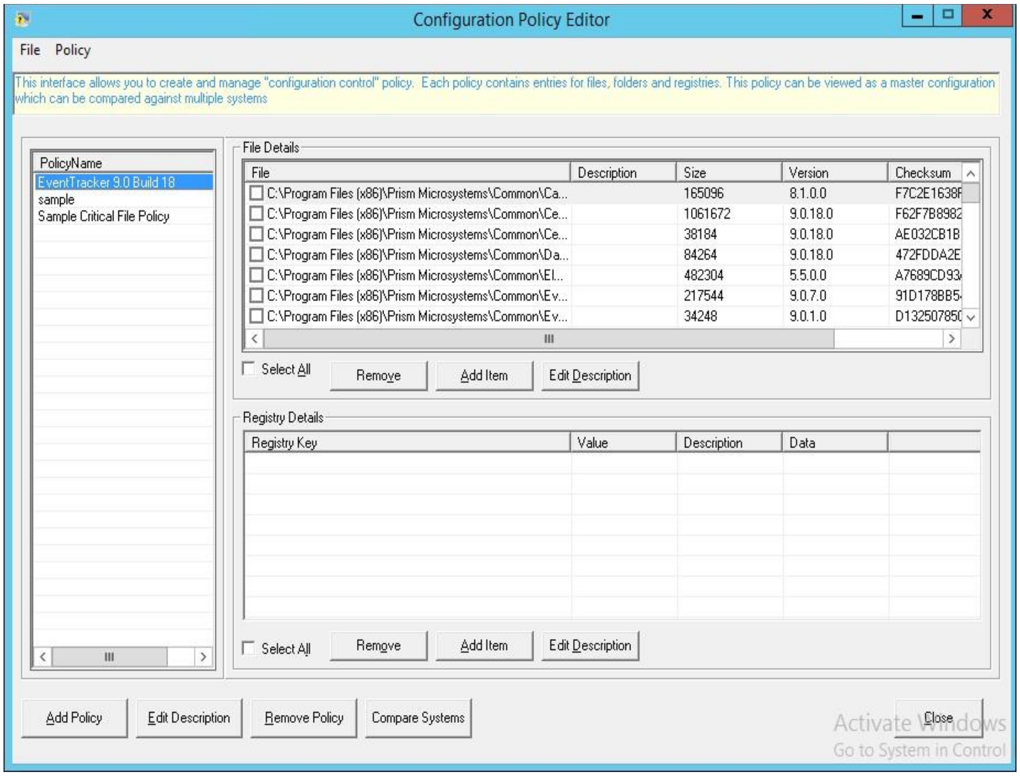
1. Click the **Start** button, select **Prism Microsystems**, and then select **EventTracker**.

2. Select **EventTracker Control Panel** and select **Change Audit**.
   Results Summary Console displays.
3. Select **Change Browser** on the toolbar.
   EventTracker - Change Browser displays.
4. Select the **Tools** menu and select **Configuration Policy Editor**.
5. Select the **Policy** menu and select **Import**.
6. Browse the file ***.ispol** and click **Open**.
   Successful updated message displays.



Successfully updated policy from file:
D:\ET Install Path\EventTracker\EventTracker 9.0 Build 18.ispol.

All the files, folders, registries related to the policy is displayed.



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
EventTracker 9.0 Build 18
sample
Sample Critical File Policy

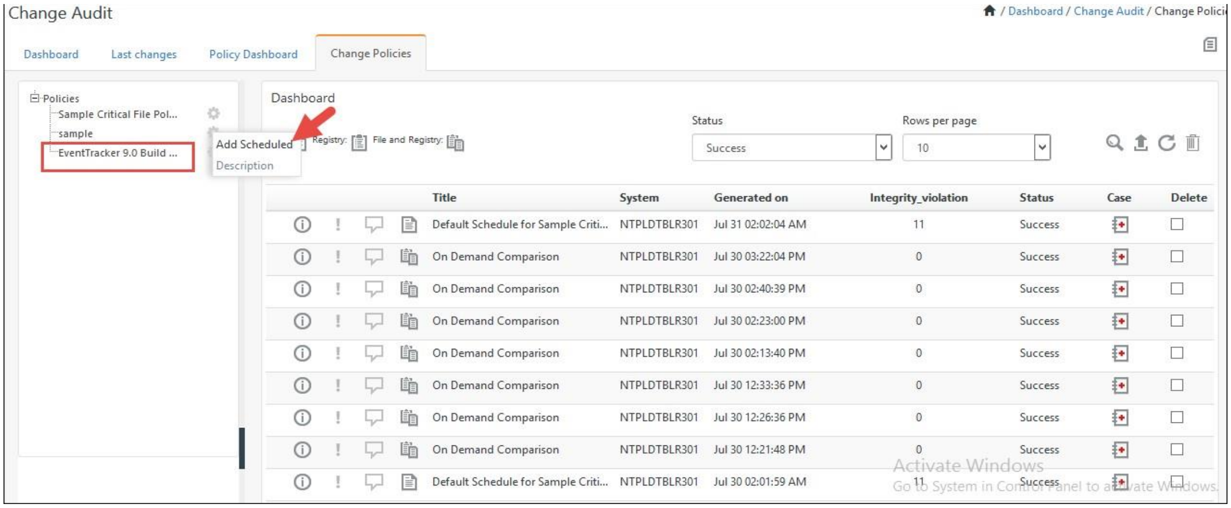
File	Description	Size	Version	Checksum
□ C:\Program Files (x86)\Prism Microsystems\Common\Ca...		165096	8.1.0.0	F7C2E1638F
□ C:\Program Files (x86)\Prism Microsystems\Common\Ce...		1061672	9.0.18.0	F62F7B8982
□ C:\Program Files (x86)\Prism Microsystems\Common\Ce...		38184	9.0.18.0	AE032CB1B
□ C:\Program Files (x86)\Prism Microsystems\Common\Da...		84264	9.0.18.0	472FDDA2E
□ C:\Program Files (x86)\Prism Microsystems\Common\El...		482304	5.5.0.0	A7689CD93
□ C:\Program Files (x86)\Prism Microsystems\Common\Ev...		217544	9.0.7.0	91D178BB5
□ C:\Program Files (x86)\Prism Microsystems\Common\Ev...		34248	9.0.1.0	D13250785C

Registry Key	Value	Description	Data

7. Click the **Close** button.
   These policies can be viewed and scheduled in EventTracker Web.

8. Login to **EventTracker**, select the **Change Audit** menu, and then select **Change Policies**.

9. Select the relevant policy to be scheduled.
10. Right-click policy and select **Add Scheduled**.



Change Audit

🏠 / Dashboard / Change Audit / Change Polici

Dashboard

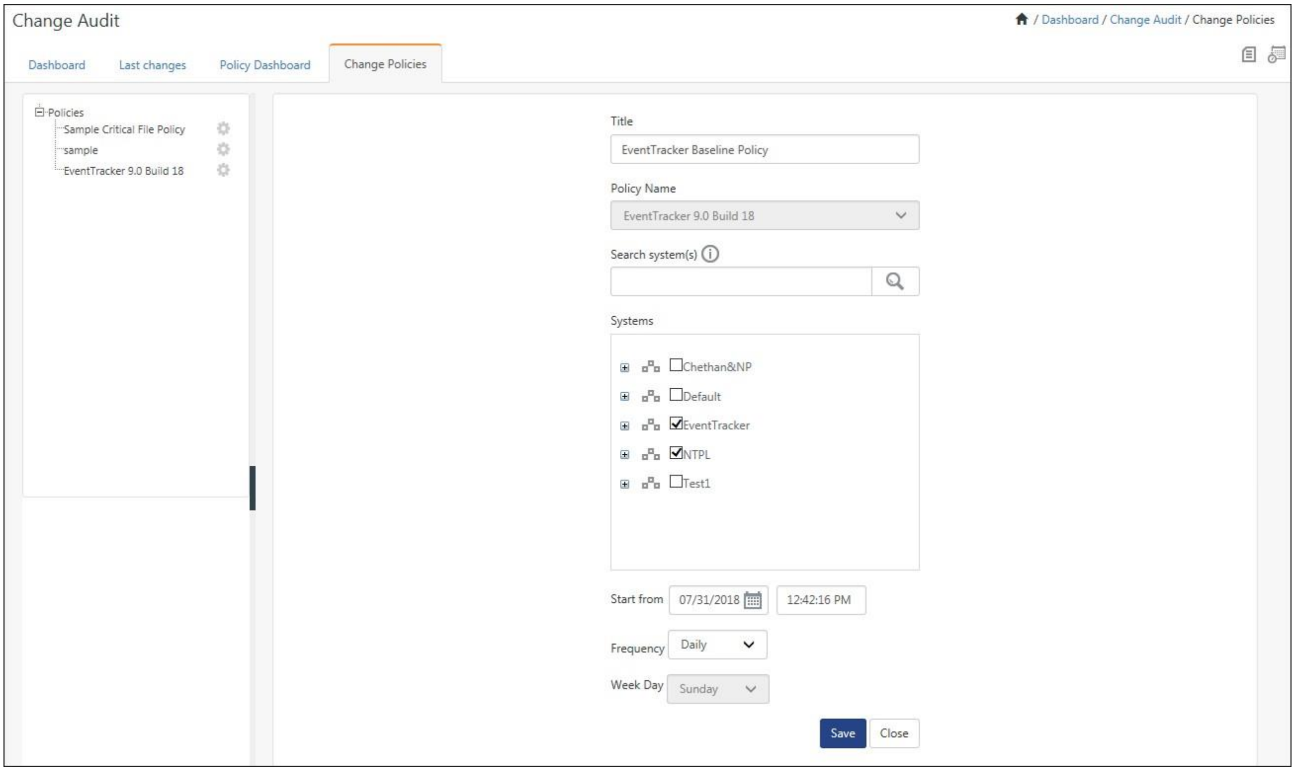
Status: Success

Rows per page: 10

Title	System	Generated on	Integrity_violation	Status	Case	Delete
Default Schedule for Sample Criti...	NTPLDTBLR301	Jul 31 02:02:04 AM	11	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 03:22:04 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 02:40:39 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 02:23:00 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 02:13:40 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 12:33:36 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 12:26:36 PM	0	Success		☐
On Demand Comparison	NTPLDTBLR301	Jul 30 12:21:48 PM	0	Success		☐
Default Schedule for Sample Criti...	NTPLDTBLR301	Jul 30 02:01:59 AM	11	Success		☐

Activate Windows
Go to System in Control Panel to activate Windows.

11. Enter the appropriate data and click **Save**.



Change Audit

🏠 / Dashboard / Change Audit / Change Policies

Title: EventTracker Baseline Policy

Policy Name: EventTracker 9.0 Build 18

Search system(s)

Systems

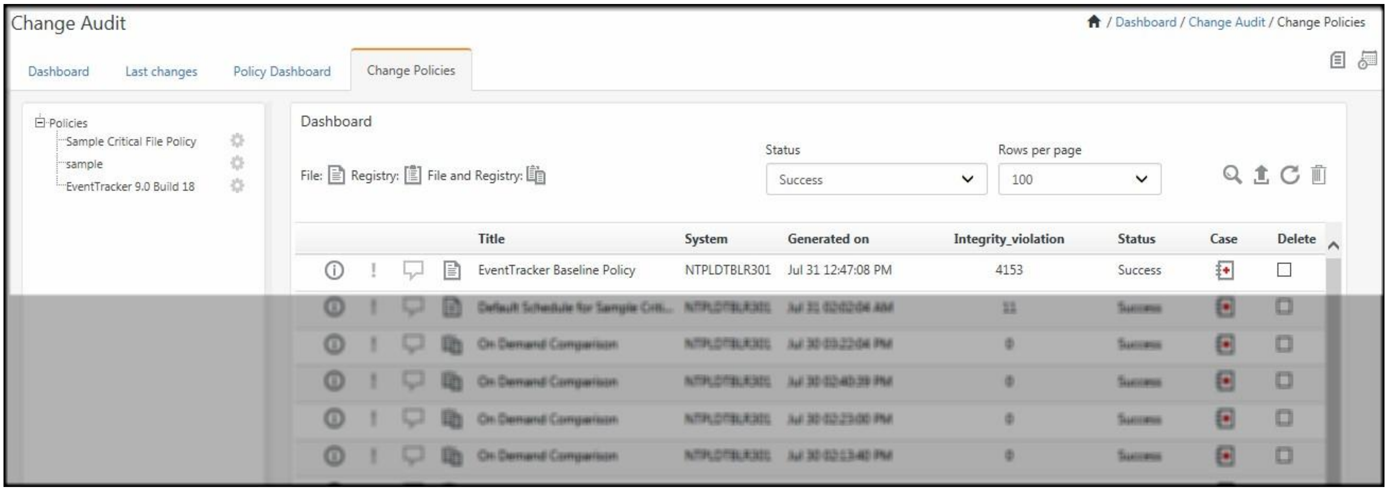
☐ Chethan&NP
☐ Default
☑ EventTracker
☑ NTPL
☐ Test1

Start from: 07/31/2018 12:42:16 PM

Frequency: Daily

Week Day: Sunday

12. Select the **Dashboard** icon 🗐 and then select the required policy.



Change Audit

🏠 / Dashboard / Change Audit / Change Policies

Policies
- Sample Critical File Policy
- sample
- EventTracker 9.0 Build 18

Dashboard

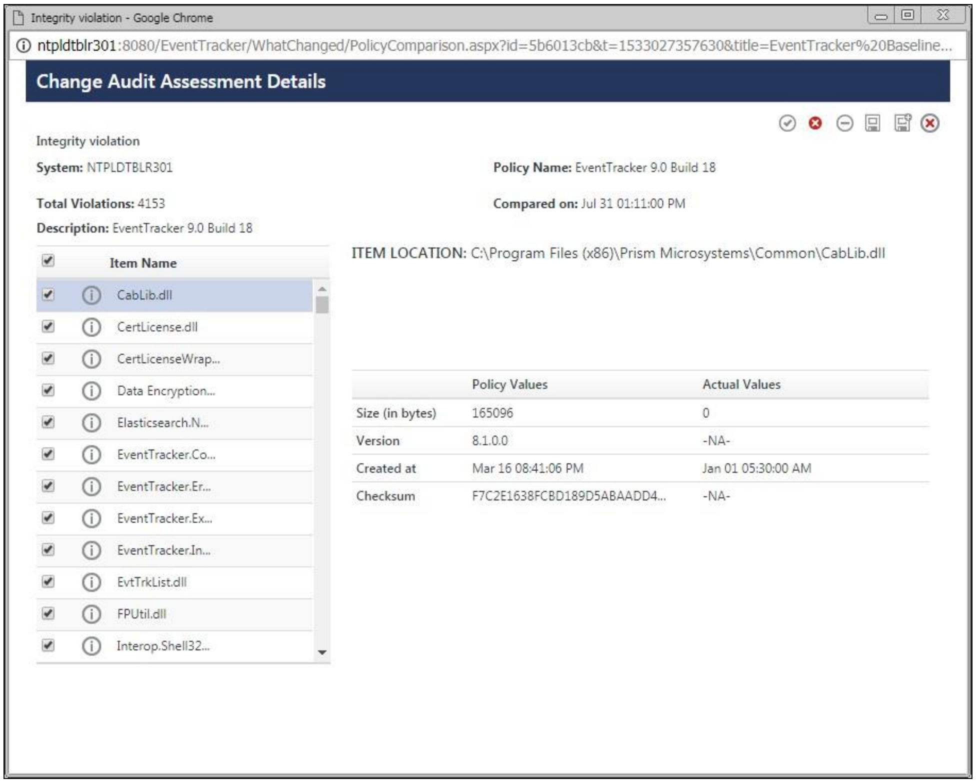
File: Registry: File and Registry:

Status: Success

Rows per page: 100

Title	System	Generated on	Integrity_violation	Status	Case	Delete
EventTracker Baseline Policy	NTPLDTBLR301	Jul 31 12:47:08 PM	4153	Success		□
Default Schedule for Sample Criti...	NTPLDTBLR301	Jul 31 02:02:04 AM	11	Success		□
On Demand Comparison	NTPLDTBLR301	Jul 30 03:22:04 PM	0	Success		□
On Demand Comparison	NTPLDTBLR301	Jul 30 02:40:39 PM	0	Success		□
On Demand Comparison	NTPLDTBLR301	Jul 30 02:23:00 PM	0	Success		□
On Demand Comparison	NTPLDTBLR301	Jul 30 02:13:40 PM	0	Success		□

13. To accept all the integrity violations for the first time, select the **Item Name** option.



Integrity violation - Google Chrome

ntpldtblr301:8080/EventTracker/WhatChanged/PolicyComparison.aspx?id=5b6013cb&t=1533027357630&title=EventTracker%20Baseline...

Change Audit Assessment Details

Integrity violation

System: NTPLDTBLR301

Policy Name: EventTracker 9.0 Build 18

Total Violations: 4153

Compared on: Jul 31 01:11:00 PM

Description: EventTracker 9.0 Build 18

ITEM LOCATION: C:\Program Files (x86)\Prism Microsystems\Common\CabLib.dll

☑	Item Name
☑	CabLib.dll
☑	CertLicense.dll
☑	CertLicenseWrap...
☑	Data Encryption...
☑	Elasticsearch.N...
☑	EventTracker.Co...
☑	EventTracker.Er...
☑	EventTracker.Ex...
☑	EventTracker.In...
☑	EvtTrkList.dll
☑	FPUtil.dll
☑	Interop.Shell32...

	Policy Values	Actual Values
Size (in bytes)	165096	0
Version	8.1.0.0	-NA-
Created at	Mar 16 08:41:06 PM	Jan 01 05:30:00 AM
Checksum	F7C2E1638FCBD189D5ABAADD4...	-NA-

14. Click **Accept icon** ✓, and then click **Save icon** 🖫.

To avoid flooding of events when auditing is enabled for a folder, grant only necessary permissions to the concerned users.

- For example: If users have **Read** permissions on a specific folder, they may read/download the files many times. As a result, the number of events increases. To avoid this, only relevant users should be granted permission.
- For detail information, refer EventTracker Change Audit User Guide.
  As a part of security best practice, server messages need to be parse d before it is passed on to the user. To avoid revealing the sensitive server information or private information, it is required to show a generic error messages when an error occurs. To do this, users need to follow the below mentioned steps after EventTracker is installed.

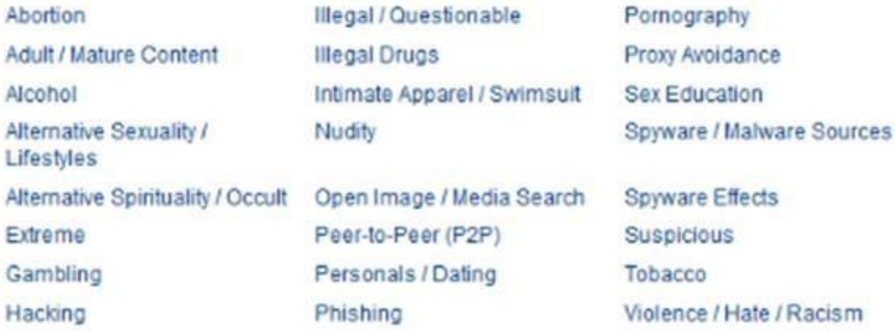
  Note: Applicable only if Change Audit is used.

1.10 Restricting Email/File Sharing Website access

- Though Internet access is required for EventTracker to perform certain functions such as Threat Intel Feeds etc., there are certain accesses that need to be restricted to ensure security.

- Restrict access to personal emails/file sharing website **(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 EventTracker instance.

- Apart from this, it is mandatory to block the below sites on the EventTracker Server. Popular categories to be blocked are shown below:



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

1.11 EventTracker Endpoint Security

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

2. Harden Windows Server – Detailed View

Configure the following aspects to harden the EventTracker server:

- Harden Windows Server
- Secure IIS Web Server
- Secure SQL Server
- Firewall Settings
- EventTracker Settings
- Check with Vulnerability Scanner

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

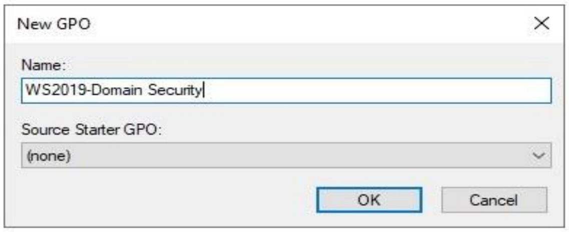
Step 1: Click the link below to download the GPO and extract the contents of zip file to the system.

https://downloads.eventtracker.com/support/utils/WS2019-GPO.zip

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

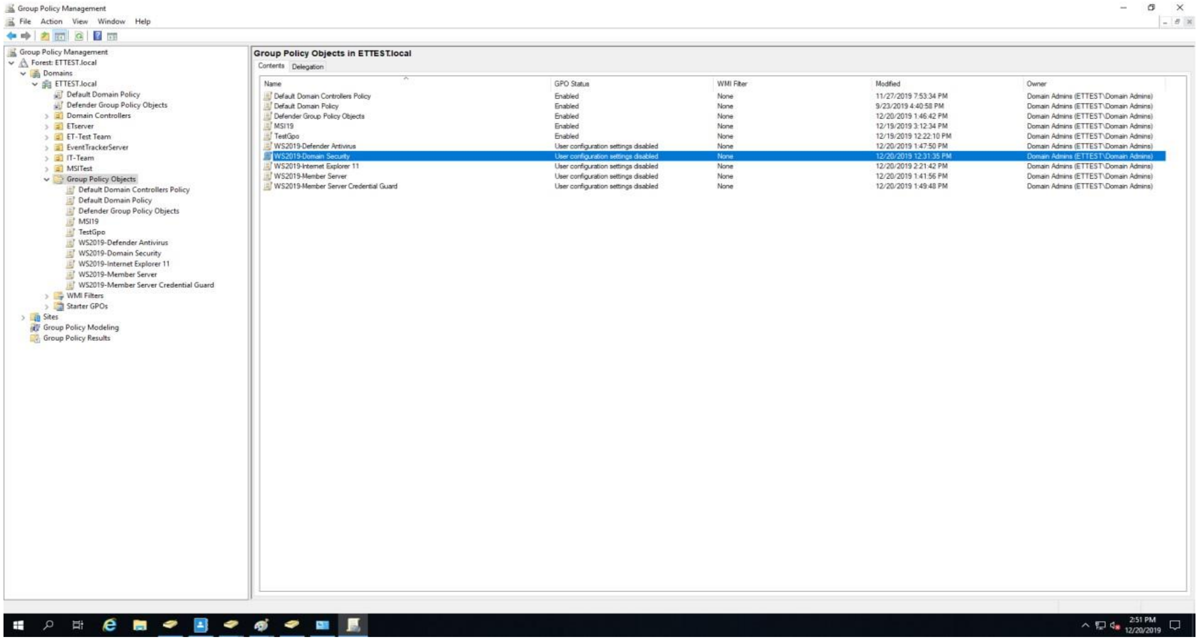
Step 2: Create new 'Group Policy Objects'

1. Click the **Start** button, select **Administrative Tools,** and then select **Group Policy Management**.
2. In the **Group Policy Management** pane, expand **Domains** node, and then expand '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**.



Name: WS2019-Domain Security
Source Starter GPO: (none)

Similarly, create 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.



Group Policy Objects in ETTEST.local

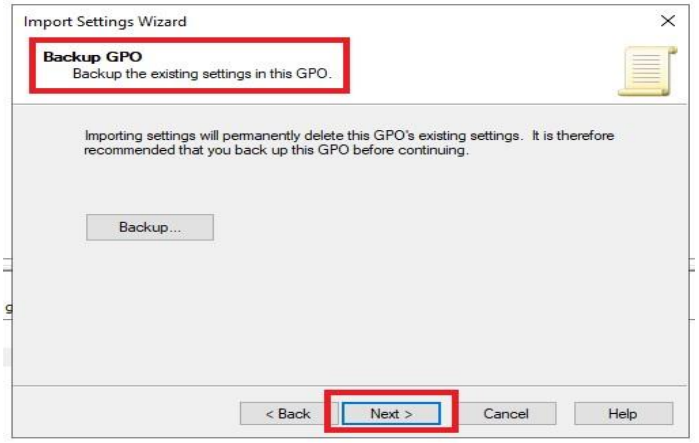
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	11/27/2019 7:53:34 PM	Domain Admins (ETTEST\Domain Admins)
Default Domain Policy	Enabled	None	9/23/2019 4:40:58 PM	Domain Admins (ETTEST\Domain Admins)
Defender Group Policy Objects	Enabled	None	12/20/2019 1:46:42 PM	Domain Admins (ETTEST\Domain Admins)
MSI19	Enabled	None	12/19/2019 3:12:34 PM	Domain Admins (ETTEST\Domain Admins)
TestGpo	Enabled	None	12/19/2019 12:22:10 PM	Domain Admins (ETTEST\Domain Admins)
WS2019-Defender Antivirus	User configuration settings disabled	None	12/20/2019 1:47:50 PM	Domain Admins (ETTEST\Domain Admins)
WS2019-Domain Security	User configuration settings disabled	None	12/20/2019 12:31:35 PM	Domain Admins (ETTEST\Domain Admins)
WS2019-Internet Explorer 11	User configuration settings disabled	None	12/20/2019 2:21:42 PM	Domain Admins (ETTEST\Domain Admins)
WS2019-Member Server	User configuration settings disabled	None	12/20/2019 1:41:56 PM	Domain Admins (ETTEST\Domain Admins)
WS2019-Member Server Credential Guard	User configuration settings disabled	None	12/20/2019 1:49:48 PM	Domain Admins (ETTEST\Domain Admins)

Step 3: Import Group Policy settings

1. Right click the newly created GPO (For example, **WS2019-Domain Security**), and click **Import settings**.

   Import Settings Wizard dialog box opens.

2. Click the **Next >** button to start the importing process.
3. In **Backup GPO**, click the **Next >** button.

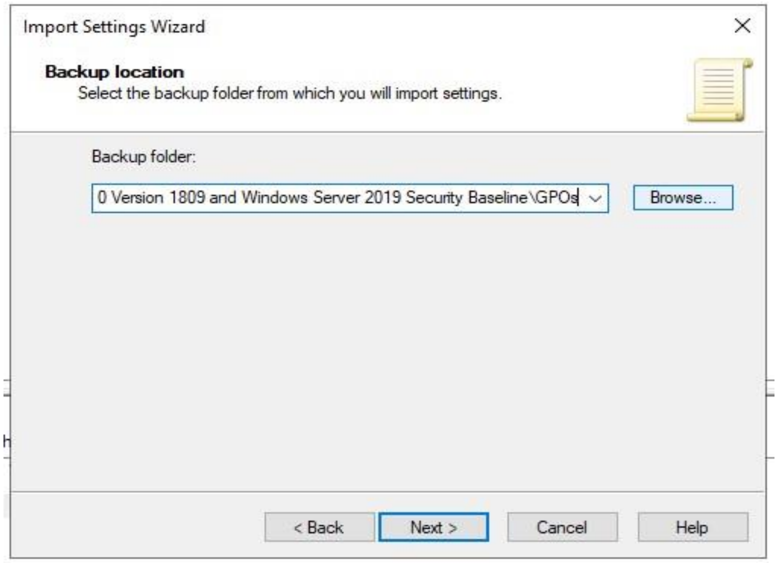


Import Settings Wizard

Backup GPO
Backup the existing settings in this GPO.

Importing settings will permanently delete this GPO's existing settings. It is therefore recommended that you back up this GPO before continuing.

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



Import Settings Wizard

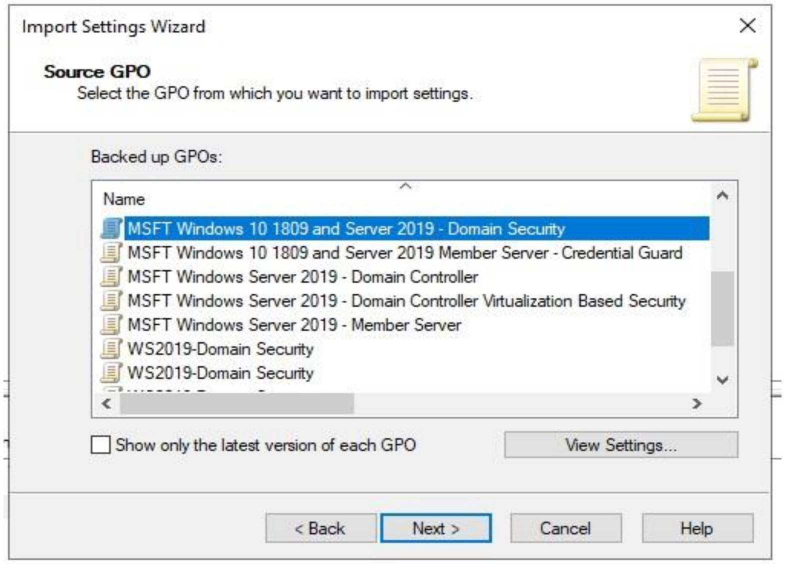
Backup location

Select the backup folder from which you will import settings.

Backup folder:

0 Version 1809 and Windows Server 2019 Security Baseline\GPOs

6. Click the **Next >** button.



Import Settings Wizard

Source GPO

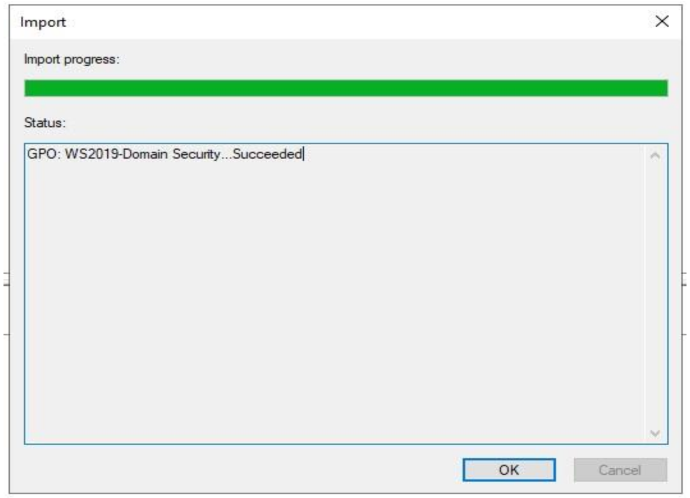
Select the GPO from which you want to import settings.

Backed up GPOs:

Name
MSFT Windows 10 1809 and Server 2019 - Domain Security
MSFT Windows 10 1809 and Server 2019 Member Server - Credential Guard
MSFT Windows Server 2019 - Domain Controller
MSFT Windows Server 2019 - Domain Controller Virtualization Based Security
MSFT Windows Server 2019 - Member Server
WS2019-Domain Security
WS2019-Domain Security

☐ Show only the latest version of each GPO

7. In **Source GPO**, select the **WS2019-Domain Security** GPO and click the **Next >** button.
8. In **Scanning Backup**, after scanning settings is complete, click the **Next >** button.
9. In **Migrating References**, click the **Next >** button.
10. Click **Finish.**
11. After successfully importing, click the **OK** button.



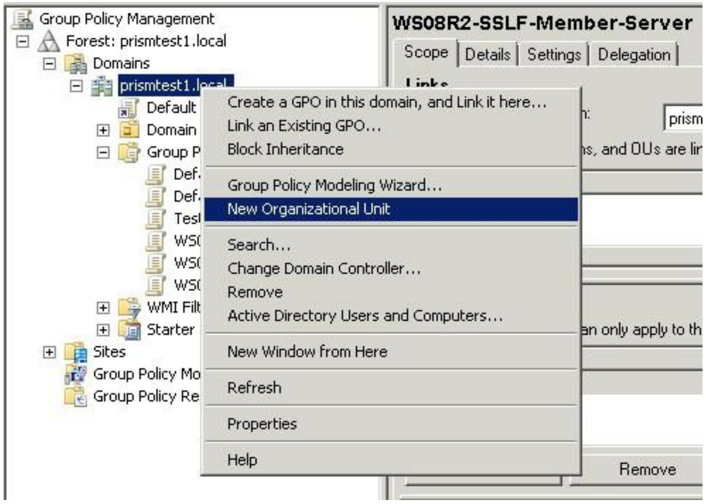
GPO: WS2019-Domain Security...Succeeded

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

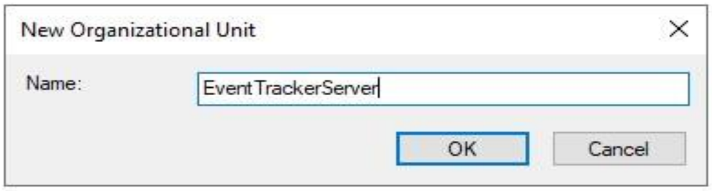
12. Repeat the steps from 1 to 11 to import Group Policy for **WS2019-Member Server, WS2019Defender Antivirus, WS2019-Member Server Credential Guard and WS2019-Internet Explorer 11- User and Computer.**

Step 4: Crete new 'Organizational Unit' (OU)

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



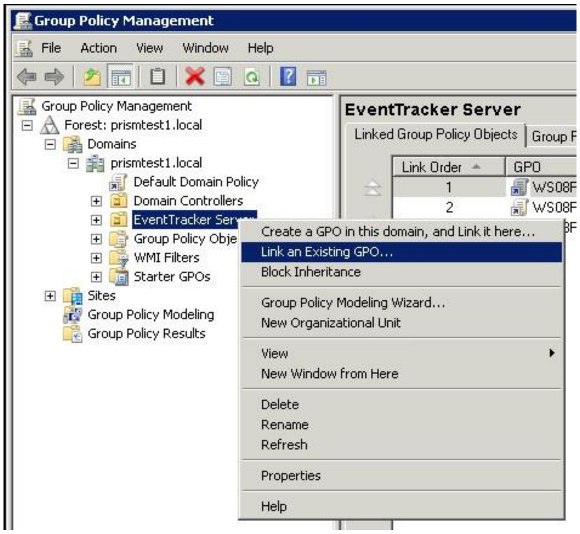
2. Enter the new organizational unit (OU) name and click **OK**.
   Example: EventTracker Server



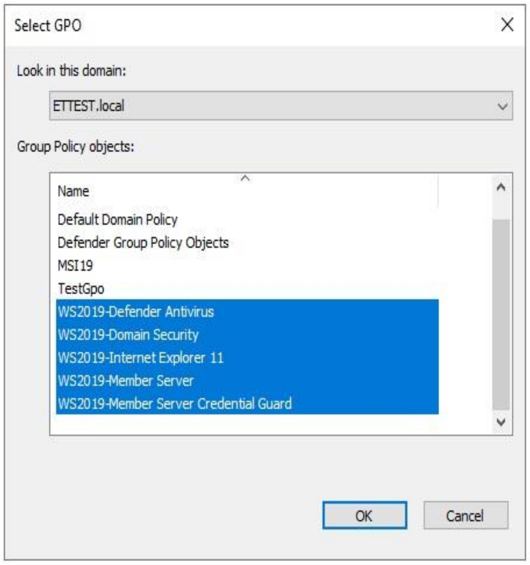
Name: EventTrackerServer

Step 5: Link the existing GPO to newly created OU

1. Right click the newly created OU – EventTracker Server and click **Link an existing GPO**.



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

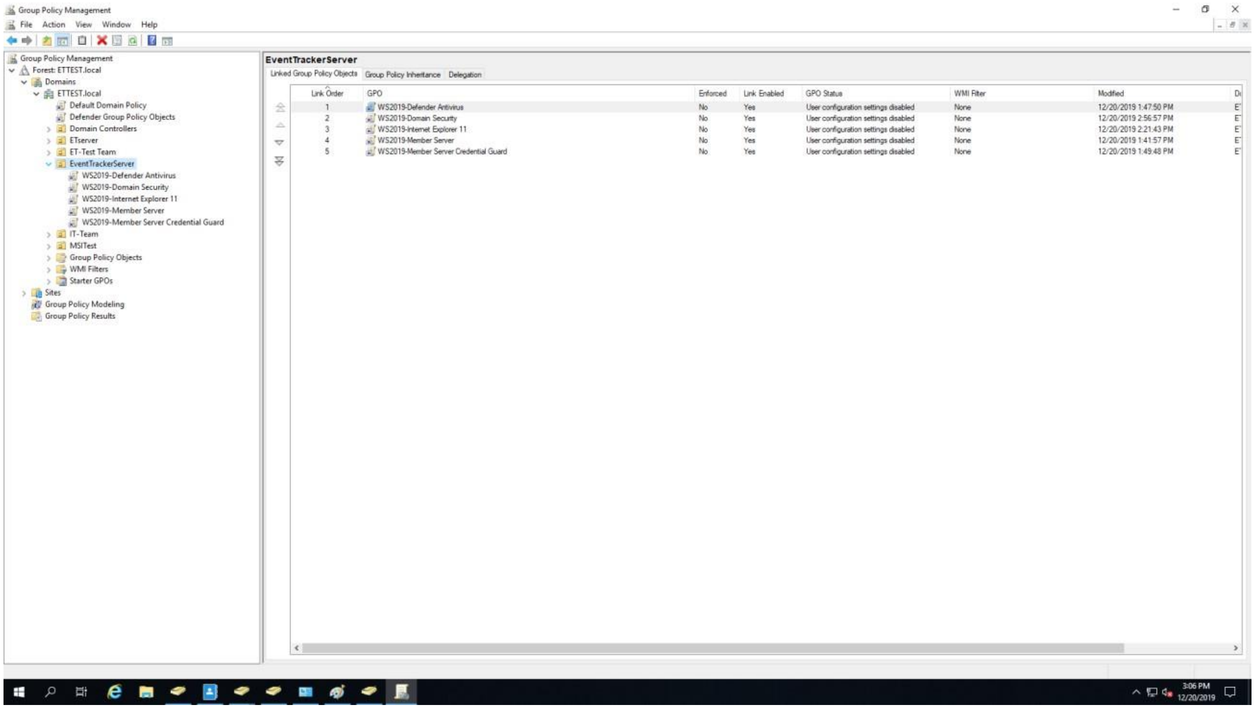


Look in this domain: ETTEST.local

Group Policy objects:

Name
Default Domain Policy
Defender Group Policy Objects
MSI19
TestGpo
WS2019-Defender Antivirus
WS2019-Domain Security
WS2019-Internet Explorer 11
WS2019-Member Server
WS2019-Member Server Credential Guard

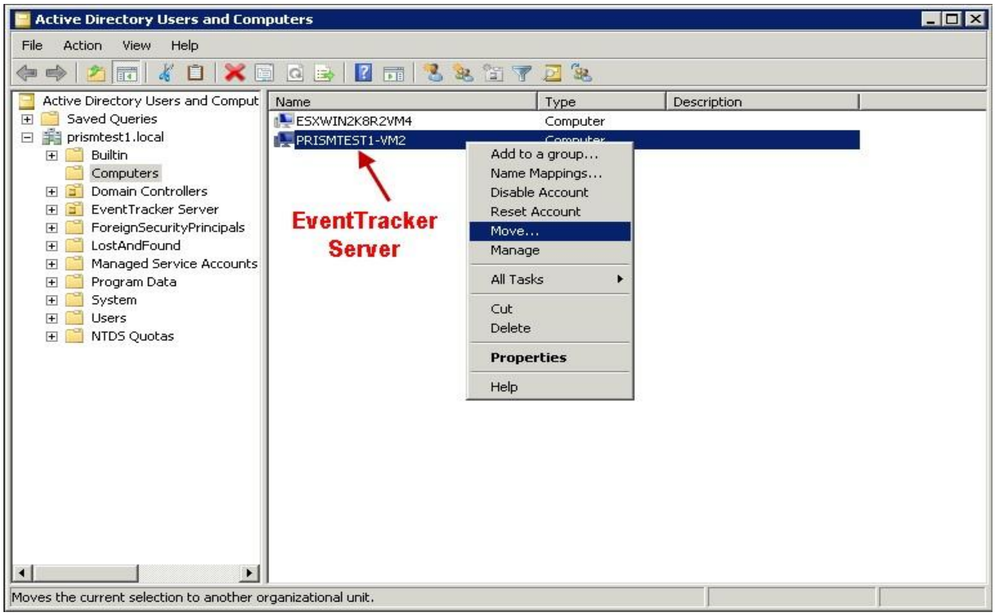
The Group Policy objects are now linked to the organizational unit.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Di
1	WS2019-Defender Antivirus	No	Yes	User configuration settings disabled	None	12/20/2019 1:47:50 PM	E'
2	WS2019-Domain Security	No	Yes	User configuration settings disabled	None	12/20/2019 2:56:57 PM	E'
3	WS2019-Internet Explorer 11	No	Yes	User configuration settings disabled	None	12/20/2019 2:21:43 PM	E'
4	WS2019-Member Server	No	Yes	User configuration settings disabled	None	12/20/2019 1:41:57 PM	E'
5	WS2019-Member Server Credential Guard	No	Yes	User configuration settings disabled	None	12/20/2019 1:49:48 PM	E'

Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system

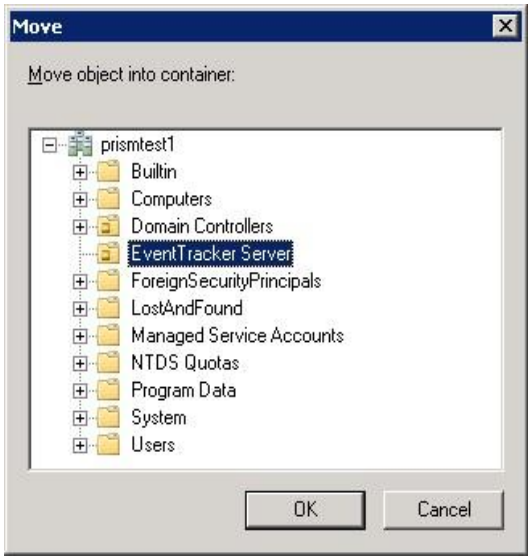
1. Click the **Start** button, select **All Programs,** and then select **Administrative Tools.**
2. Select **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** pane, expand **Domains** node, and then click **Computers** node.
4. Right click **EventTracker server system**, and then click **Move**.



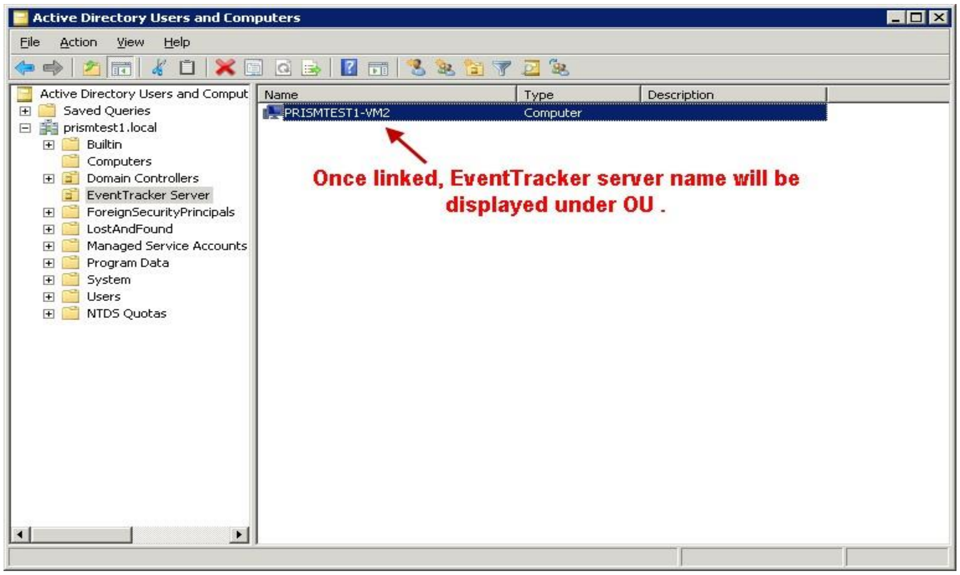
Name	Type	Description
ESXWIN2K8R2VM4	Computer	
PRISMTEST1-VM2	Computer	

Moves the current selection to another organizational unit.

Move dialog box opens.



5. Select the newly created OU (in this case, select **EventTracker Server**), and click **OK**.
6. In the **Active Directory Users and Computers** pane, click ‘organizational unit’ (in this case, click **EventTracker Server**).



Once linked, EventTracker server name will be displayed under OU .

7. Reboot the EventTracker server system linked to the OU.

Note: EventTracker application is accessible only through HTTPS protocol in IE browser.

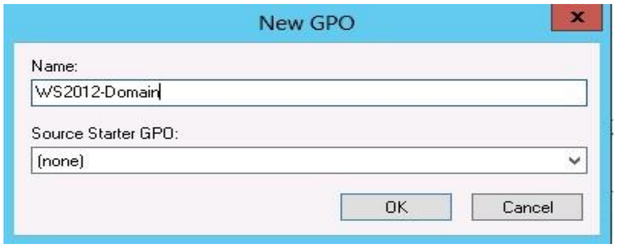
2.2 Applying Group Policies in a Member Server on Windows Server 2012

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

https://downloads.eventtracker.com/support/utils/WS2012-GPO.zip

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 **Domains** node, and expand 'local system' node.
3. Right click **Group Policy Objects** and click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS2012-Domain** and click **OK**.

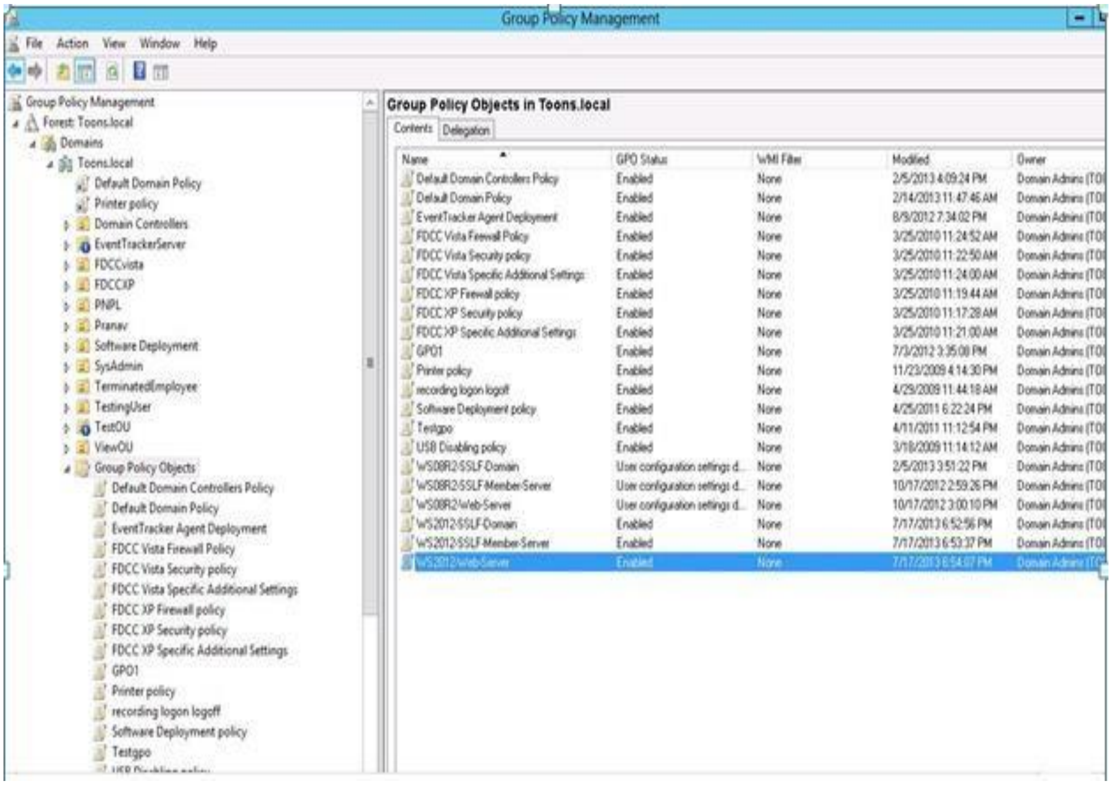


New GPO

Name: WS2012-Domain

Source Starter GPO: (none)

5. Create New GPO for member server, web server and Remote Desktop Services, and name them as WS2012-Member-Server, WS2012-Web-Server and WS2012-Remote Desktop Services respectively.



Group Policy Objects in Toons.local

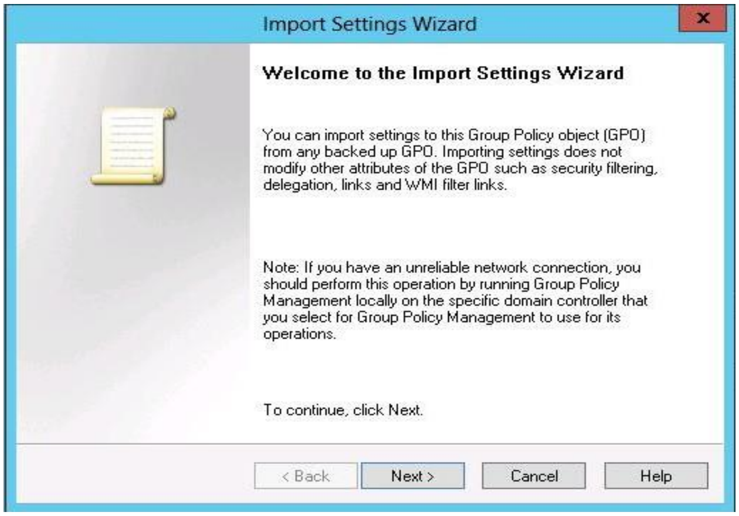
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	2/5/2013 4:09:24 PM	Domain Admins (TO
Default Domain Policy	Enabled	None	2/14/2013 11:47:46 AM	Domain Admins (TO
EventTracker Agent Deployment	Enabled	None	8/9/2012 7:34:02 PM	Domain Admins (TO
FDCC Vista Firewall Policy	Enabled	None	3/25/2010 11:24:52 AM	Domain Admins (TO
FDCC Vista Security policy	Enabled	None	3/25/2010 11:22:50 AM	Domain Admins (TO
FDCC Vista Specific Additional Settings	Enabled	None	3/25/2010 11:24:00 AM	Domain Admins (TO
FDCC XP Firewall policy	Enabled	None	3/25/2010 11:19:44 AM	Domain Admins (TO
FDCC XP Security policy	Enabled	None	3/25/2010 11:17:28 AM	Domain Admins (TO
FDCC XP Specific Additional Settings	Enabled	None	3/25/2010 11:21:00 AM	Domain Admins (TO
GPO1	Enabled	None	7/3/2012 3:35:08 PM	Domain Admins (TO
Printer policy	Enabled	None	11/23/2009 4:14:30 PM	Domain Admins (TO
recording logon logoff	Enabled	None	4/29/2009 11:44:18 AM	Domain Admins (TO
Software Deployment policy	Enabled	None	4/25/2011 6:22:24 PM	Domain Admins (TO
Testgpo	Enabled	None	4/11/2011 11:12:54 PM	Domain Admins (TO
USB Disabling policy	Enabled	None	3/18/2009 11:14:12 AM	Domain Admins (TO
WS08R2-SSLF-Domain	User configuration settings d...	None	2/5/2013 3:51:22 PM	Domain Admins (TO
WS08R2-SSLF-Member-Server	User configuration settings d...	None	10/17/2012 2:59:26 PM	Domain Admins (TO
WS08R2-Web-Server	User configuration settings d...	None	10/17/2012 3:00:10 PM	Domain Admins (TO
WS2012-SSLF-Domain	Enabled	None	7/17/2013 6:52:56 PM	Domain Admins (TO
WS2012-SSLF-Member-Server	Enabled	None	7/17/2013 6:53:37 PM	Domain Admins (TO
WS2012-Web-Server	Enabled	None	7/17/2013 6:54:07 PM	Domain Admins (TO

Step 3: Import Group Policy settings

1. Right click the newly created GPO (For example, **WS2012-Domain**), and click **Import settings**.

   Import Settings Wizard dialog box opens.
2. Click the **Next >** button to import.

3. In **Backup GPO**, click the **Next >** button.
4. In the **Backup location**, browse the backup folder path to import the settings.



Import Settings Wizard

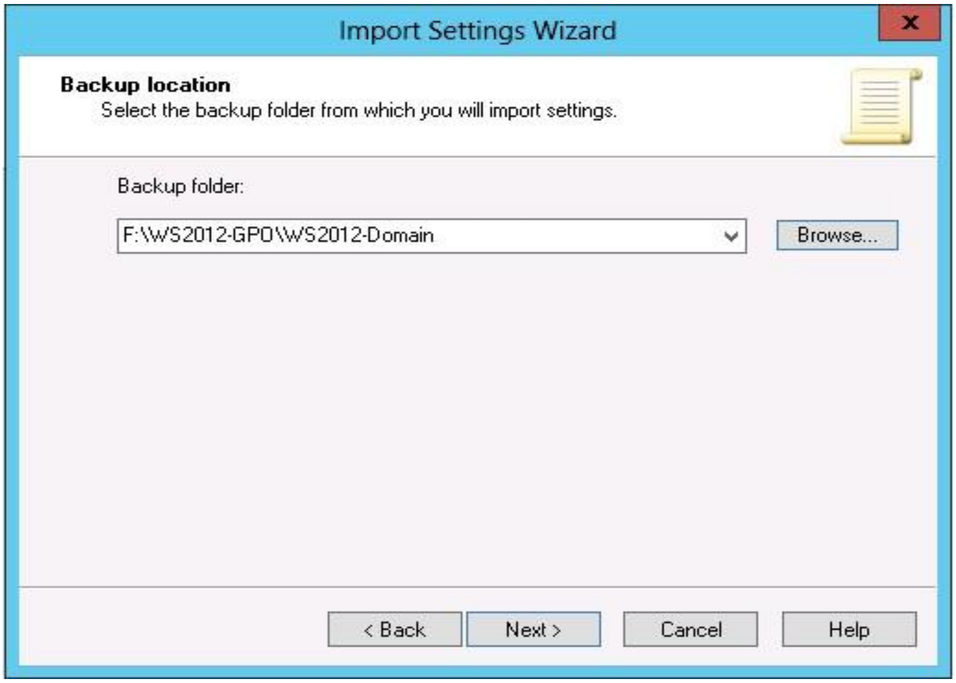
Welcome to the Import Settings Wizard

You can import settings to this Group Policy object (GPO) from any backed up GPO. Importing settings does not modify other attributes of the GPO such as security filtering, delegation, links and WMI filter links.

Note: If you have an unreliable network connection, you should perform this operation by running Group Policy Management locally on the specific domain controller that you select for Group Policy Management to use for its operations.

To continue, click Next.

5. Click the **Next >** button.



Import Settings Wizard

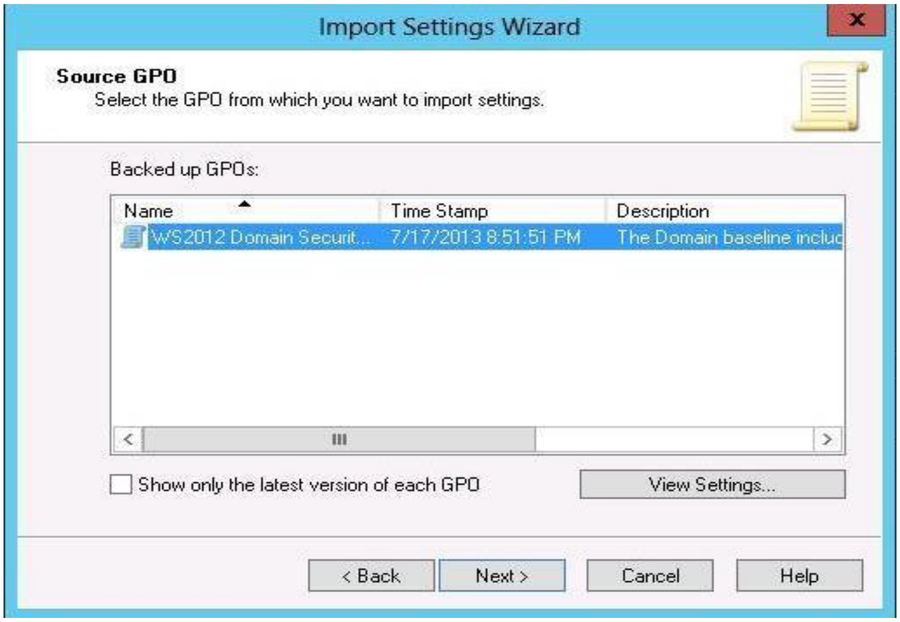
Backup location

Select the backup folder from which you will import settings.

Backup folder:

F:\WS2012-GPO\WS2012-Domain

6. Click the **Next >** button.



Import Settings Wizard

Source GPO

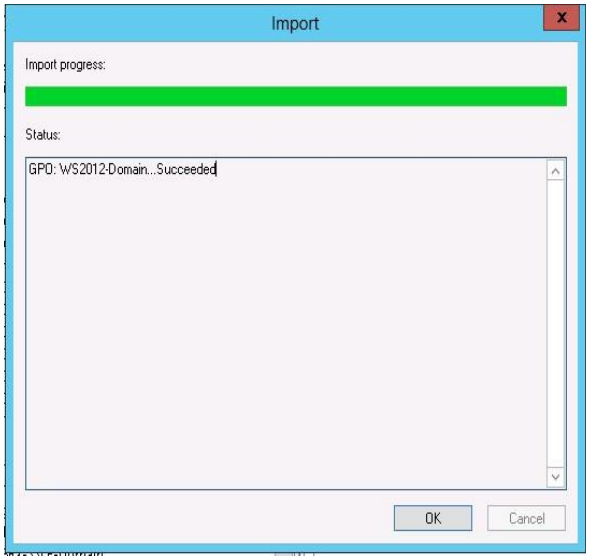
Select the GPO from which you want to import settings.

Backed up GPOs:

Name	Time Stamp	Description
WS2012 Domain Securit...	7/17/2013 8:51:51 PM	The Domain baseline incluc

□ Show only the latest version of each GPO

7. In **Source GPO**, select the backed-up GPO, and click the **Next >** button.
8. In **Scanning Backup**, after scanning settings is complete, click the **Next >** button.
9. In **Migrating References**, click the **Next >** button.
10. Click the **Finish** button.
11. After successfully importing click the **OK** button.



Import

Import progress:

Status:

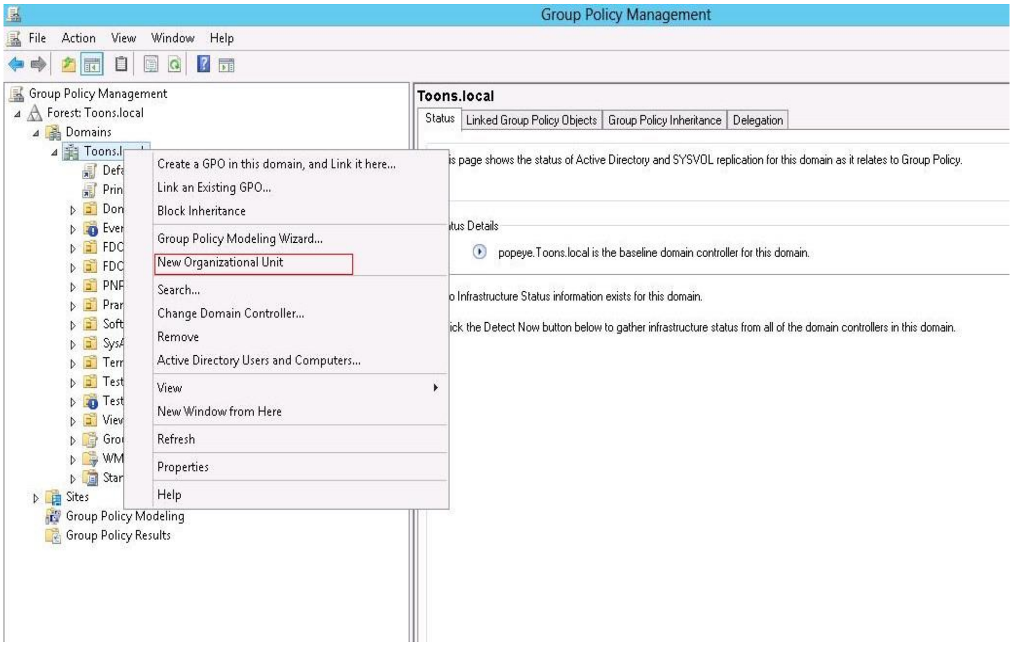
GPO: WS2012-Domain...Succeeded

Group policy import is complete for **WS2012-Domain.**

12. Repeat the steps from 1 to 10 to import Group Policy for **WS2012-Member-Server, WS2012-WebServer and WS2012-Remote Desktop Services**.

<u>Step 4: Crete new 'Organizational Unit'</u>

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



is page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

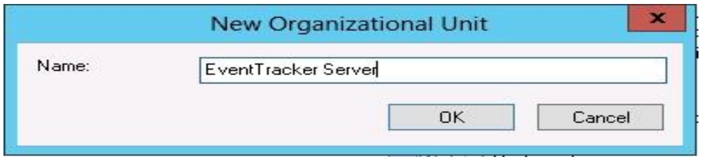
popeye.Toons.local is the baseline domain controller for this domain.

o Infrastructure Status information exists for this domain.

ick the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

2. Enter the new organizational unit (OU) name and click **OK**.

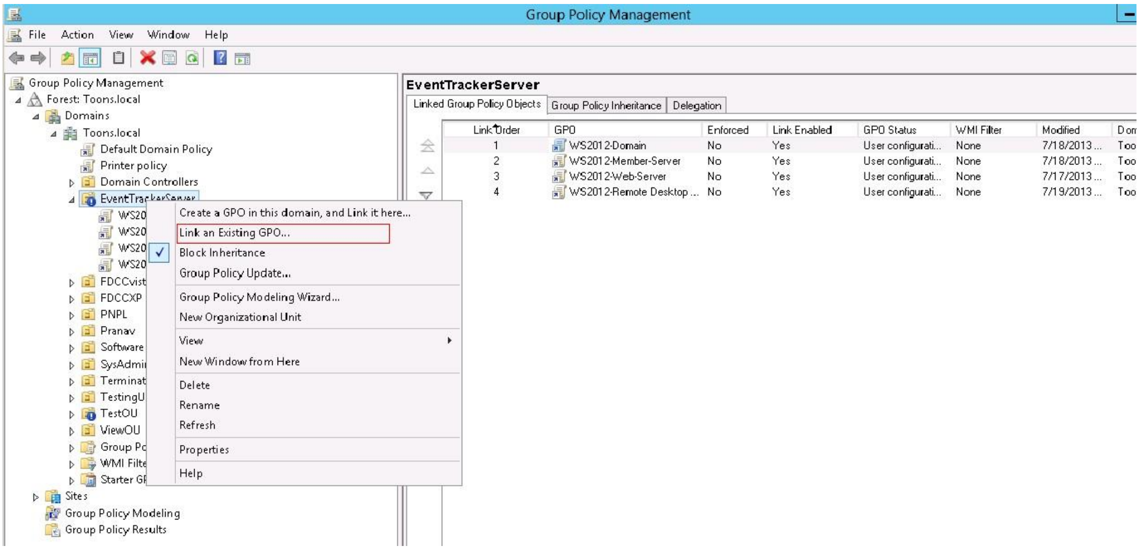
Example: EventTracker Server



Name: EventTracker Server

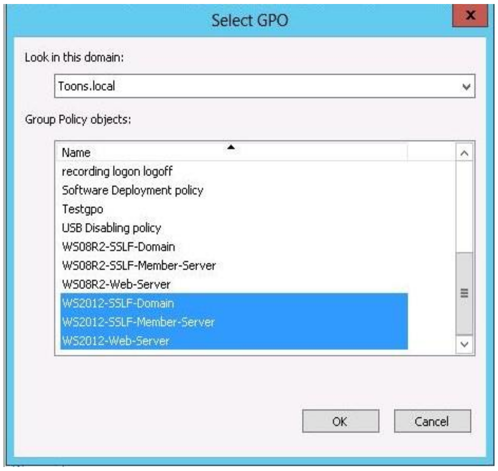
Step 5: Link the existing GPO to newly created OU

1. Right click the newly created OU – EventTracker Server and click **Link an existing GPO**.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Dom
1	WS2012-Domain	No	Yes	User configurati...	None	7/18/2013 ...	Too
2	WS2012-Member-Server	No	Yes	User configurati...	None	7/18/2013 ...	Too
3	WS2012-Web-Server	No	Yes	User configurati...	None	7/17/2013 ...	Too
4	WS2012-Remote Desktop ...	No	Yes	User configurati...	None	7/19/2013 ...	Too

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



Select GPO

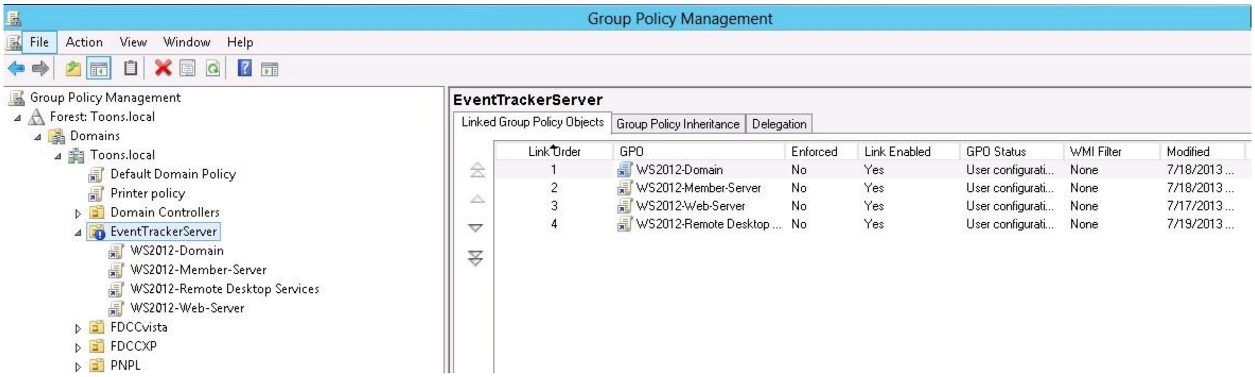
Look in this domain:

Toons.local

Group Policy objects:

Name
recording logon logoff
Software Deployment policy
Testgpo
USB Disabling policy
WS08R2-SSLF-Domain
WS08R2-SSLF-Member-Server
WS08R2-Web-Server
WS2012-SSLF-Domain
WS2012-SSLF-Member-Server
WS2012-Web-Server

The Group Policy objects are linked to the organizational unit.



Group Policy Management

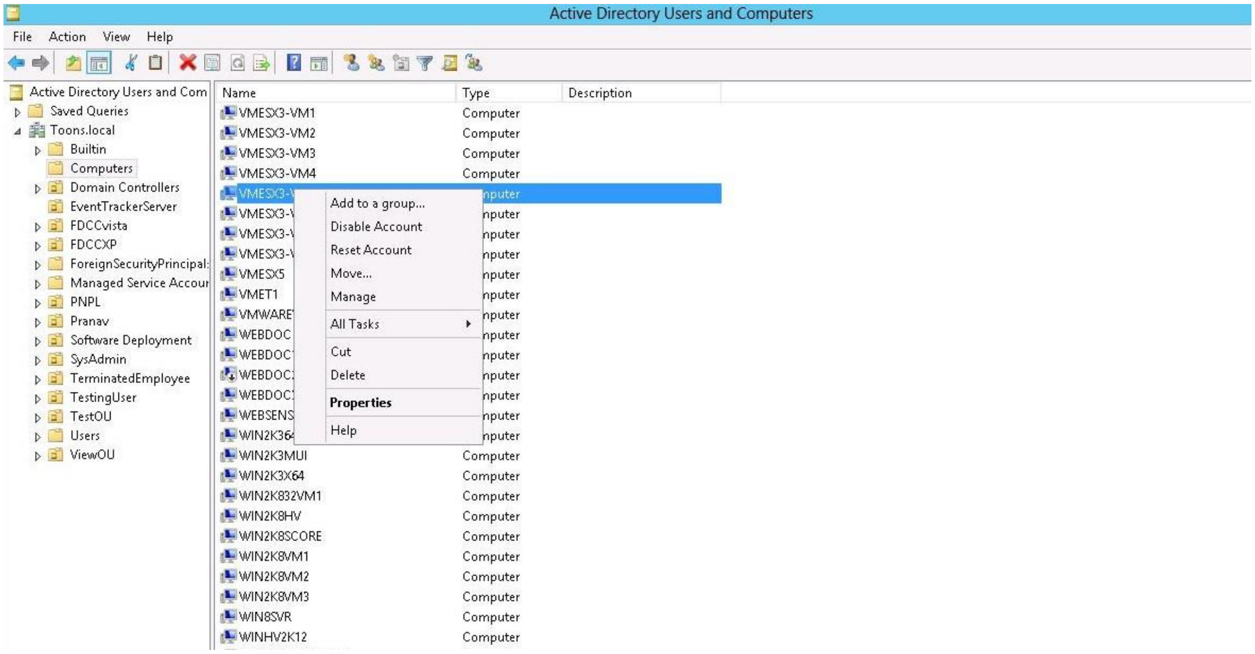
- Group Policy Management
  - Forest: Toons.local
    - Domains
      - Toons.local
        - Default Domain Policy
        - Printer policy
        - Domain Controllers
        - EventTrackerServer
          - WS2012-Domain
          - WS2012-Member-Server
          - WS2012-Remote Desktop Services
          - WS2012-Web-Server
        - FDCCvista
        - FDCCXP
        - PNPL

EventTrackerServer

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	WS2012-Domain	No	Yes	User configurati...	None	7/18/2013 ...
2	WS2012-Member-Server	No	Yes	User configurati...	None	7/18/2013 ...
3	WS2012-Web-Server	No	Yes	User configurati...	None	7/17/2013 ...
4	WS2012-Remote Desktop ...	No	Yes	User configurati...	None	7/19/2013 ...

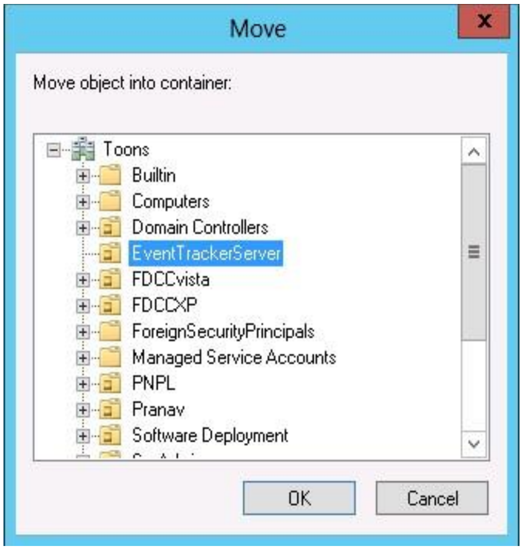
Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system

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 **Domains** node, and then click **Computers** node.
4. Right click any EventTracker server system, and then click **Move**.

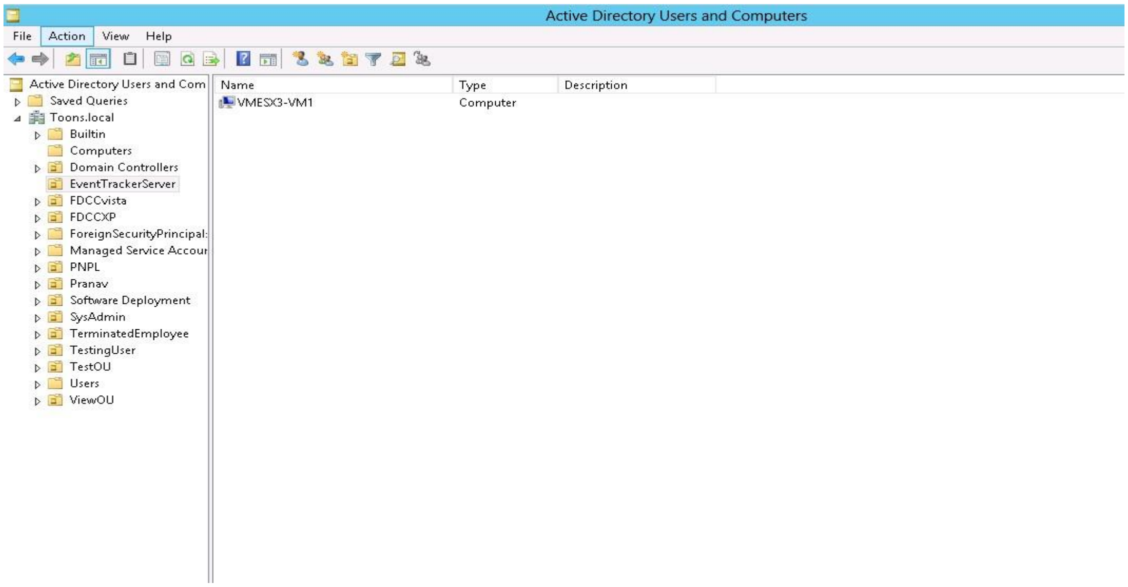


Name	Type	Description
VMESX3-VM1	Computer	
VMESX3-VM2	Computer	
VMESX3-VM3	Computer	
VMESX3-VM4	Computer	
VMESX3-\	nputer	
VMESX3-\	nputer	
VMESX3-\	nputer	
VMESX3-\	nputer	
VMESX5	nputer	
VMET1	nputer	
VMWARE	nputer	
WEBDOC	nputer	
WEBDOC	nputer	
WEBDOC	nputer	
WEBDOC	nputer	
WEBSENS	nputer	
WIN2K364	nputer	
WIN2K3MUI	Computer	
WIN2K3X64	Computer	
WIN2K832VM1	Computer	
WIN2K8HV	Computer	
WIN2K8SCORE	Computer	
WIN2K8VM1	Computer	
WIN2K8VM2	Computer	
WIN2K8VM3	Computer	
WIN8SVR	Computer	
WINHV2K12	Computer	

Move dialog box opens.



5. Select the newly created OU (in this case, select **EventTracker Server**), and then click **OK**.
6. In the **Active Directory Users and Computers** pane, click '**Organizational Unit'** (in this case, click **EventTracker Server**).



7. Reboot the EventTracker server system linked to the OU.

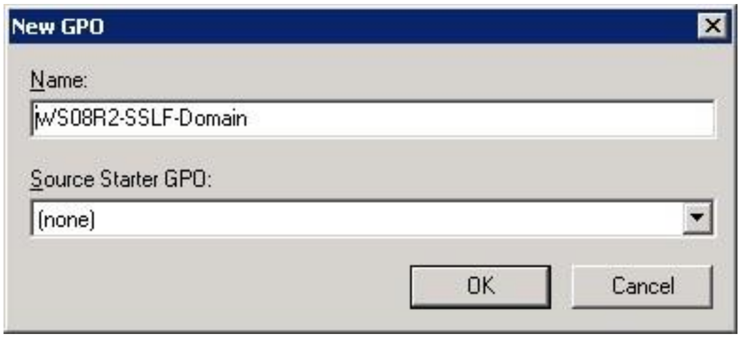
2.3 Applying Group Policies in a Member Server on Windows 2K8 / 2K8 R2 Enterprise SP1 (Active Directory)

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

https://downloads.eventtracker.com/support/utils/WS08R2-SSLF-GPO.zip

Step 2: Create new 'Group Policy Objects'

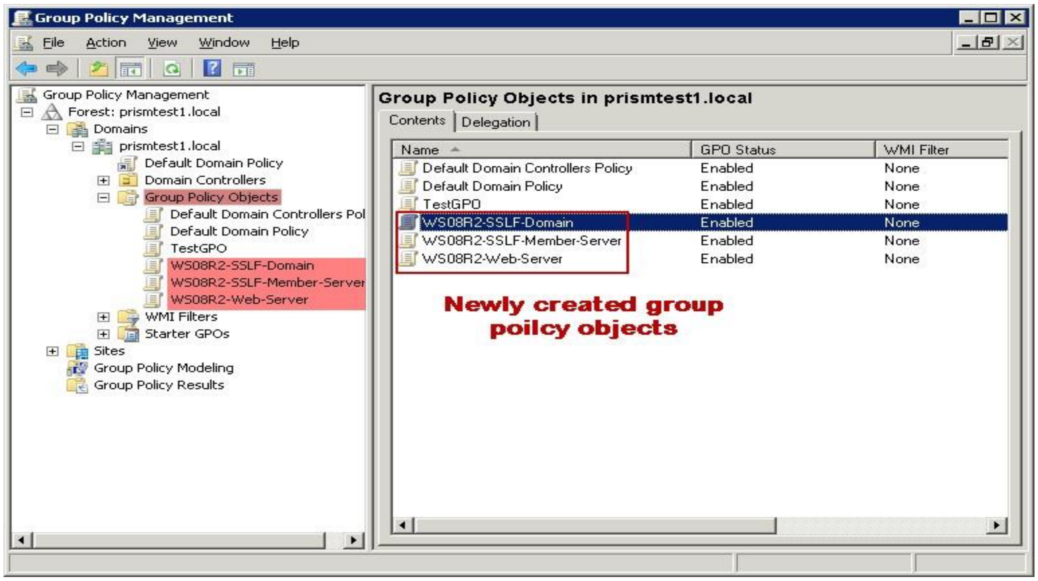
1. Select the **Start** button, select **All Programs,** and then select **Administrative Tools**.
2. Select **Group Policy Management,** expand **Domains** node, and expand 'local system' node.
3. Right click **Group Policy Objects** and click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS08R2-SSLF-Domain** and click **OK**.



Name: WS08R2-SSLF-Domain

Source Starter GPO: (none)

5. Similarly create **New GPO** for member server and web server, and name them as **WS08R2-SSLFMember-Server** and **WS08R2-Web-Server** respectively.



Group Policy Objects in prismtest1.local

Name	GPO Status	WMI Filter
Default Domain Controllers Policy	Enabled	None
Default Domain Policy	Enabled	None
TestGPO	Enabled	None
WS08R2-SSLF-Domain	Enabled	None
WS08R2-SSLF-Member-Server	Enabled	None
WS08R2-Web-Server	Enabled	None

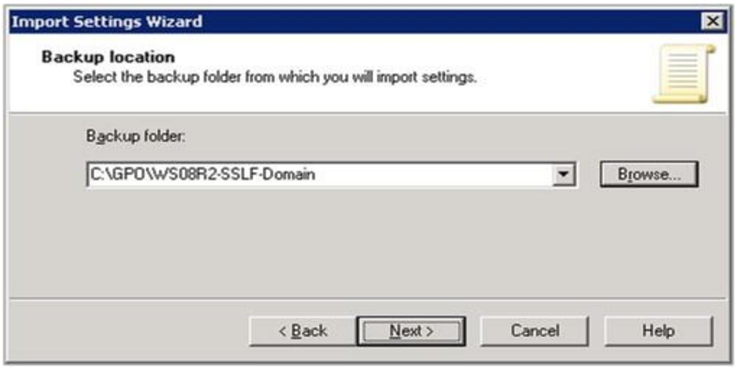
Newly created group poilcy objects

Step 3: Import Group Policy settings

1. Right click the newly created GPO (For example, **WS08R2-SSLF-Domain**), and click **Import settings**.

   Import Settings Wizard dialog box appears.

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.

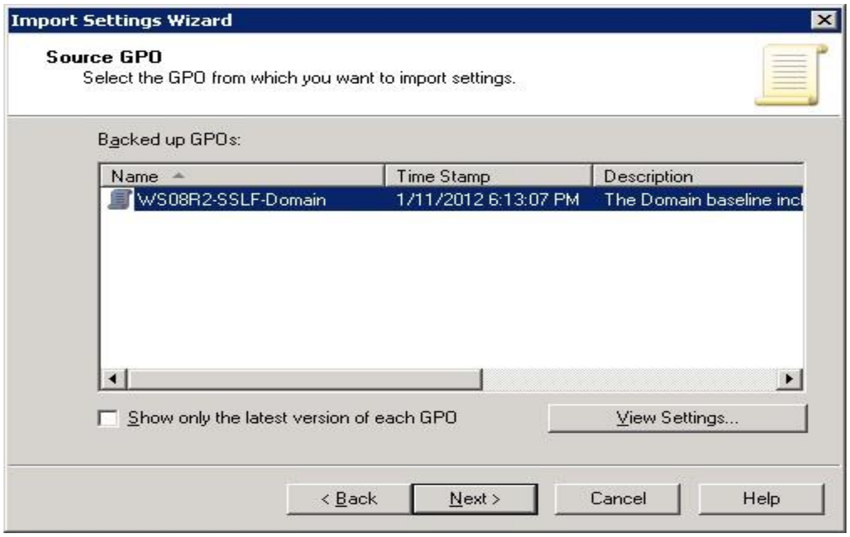


Backup location

Select the backup folder from which you will import settings.

Backup folder: C:\GPO\WS08R2-SSLF-Domain

5. Click the **Next >** button.



Import Settings Wizard

Source GPO

Select the GPO from which you want to import settings.

Backed up GPOs:

Name	Time Stamp	Description
WS08R2-SSLF-Domain	1/11/2012 6:13:07 PM	The Domain baseline incl

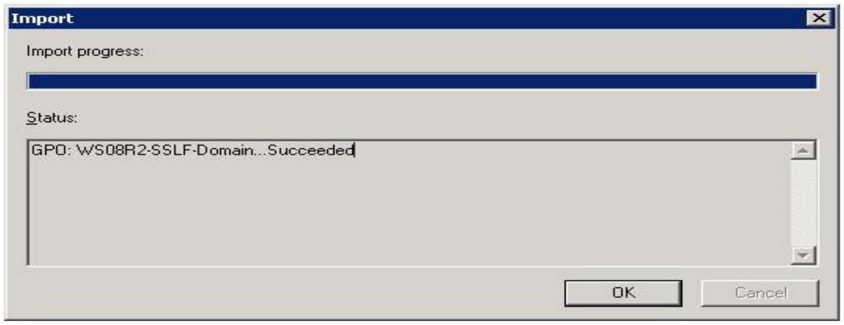
☐ Show only the latest version of each GPO

6. In **Source GPO**, select the backed-up GPO, and click the **Next >** button.

7. In **Scanning Backup** After settings scanning is complete, click the **Next >** button.
8. In **Migrating References**, click the **Next >** button.

9. Click the **Finish** button.

10. After successfully importing click the **OK** button.



Import

Import progress:

Status:

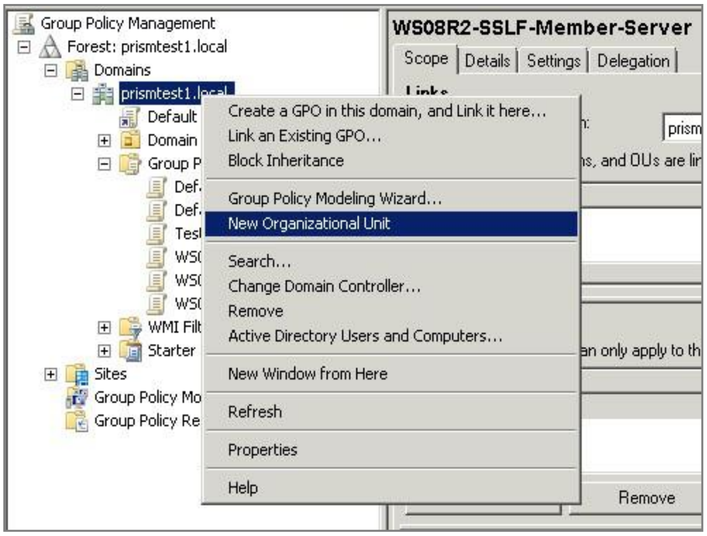
GPO: WS08R2-SSLF-Domain...Succeeded

Group policy import is complete for **WS08R2-SSLF-Domain.**

11. Repeat the steps from 1 to 10 to import Group Policy for **WS08R2-SSLF-Member-Server** and **WS08R2-Web-Server**.

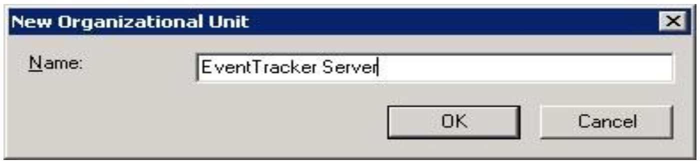
Step 4: Crete new 'Organizational Unit'

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



2. Enter the new organizational unit (OU) name and click **OK**.

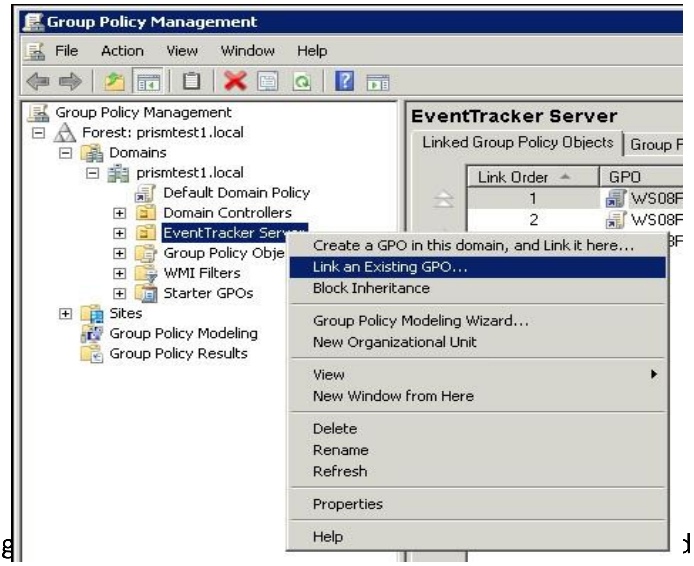
For example: EventTracker Server



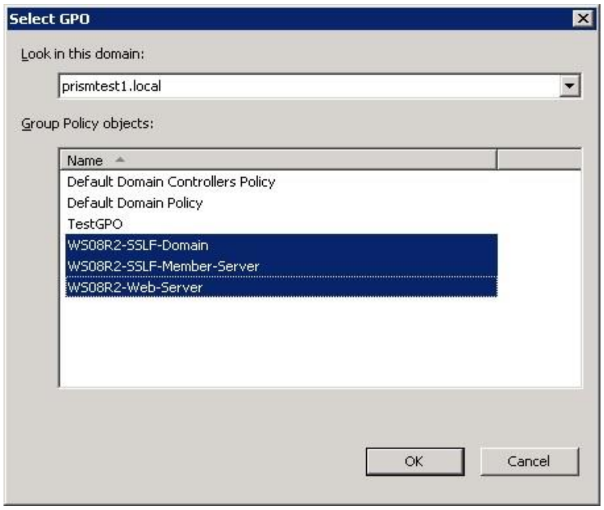
Name: EventTracker Server

Step 5: Link the existing GPO to newly created OU

1. Right click newly created OU – EventTracker Server and click **Link an existing GPO**.



2. In the **Select GPO** dialog d GPO, and click **OK**.



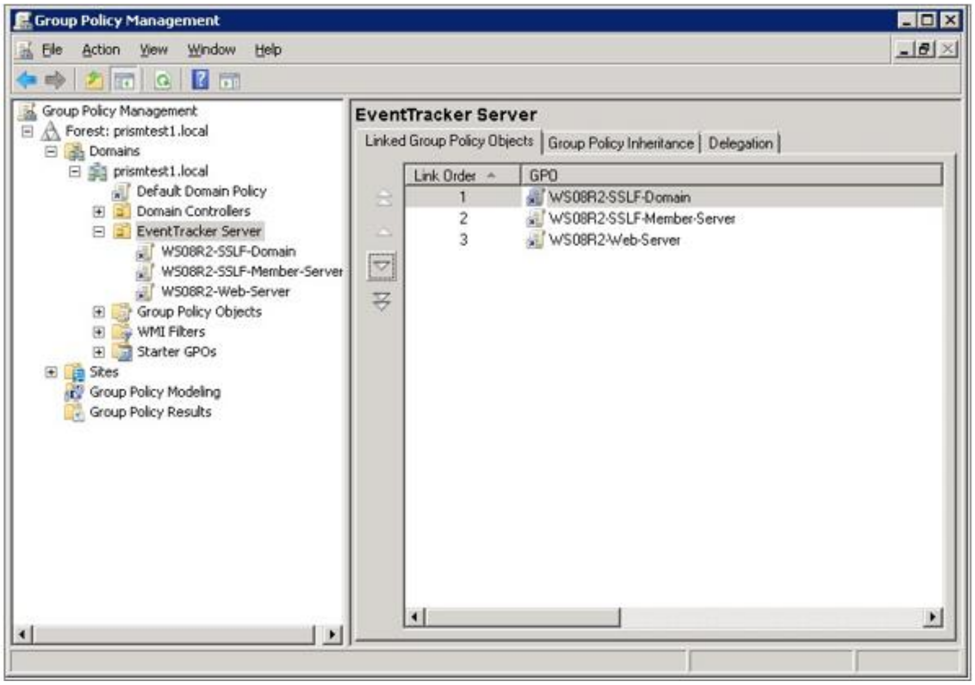
Look in this domain:

prismtest1.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
TestGPO
WS08R2-SSLF-Domain
WS08R2-SSLF-Member-Server
WS08R2-Web-Server

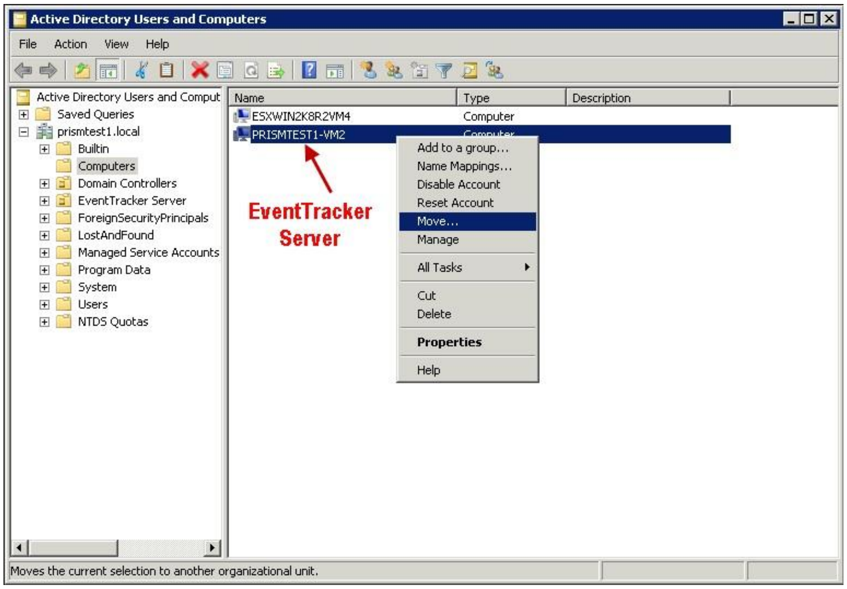
The Group Policy objects are now linked to the organizational unit.



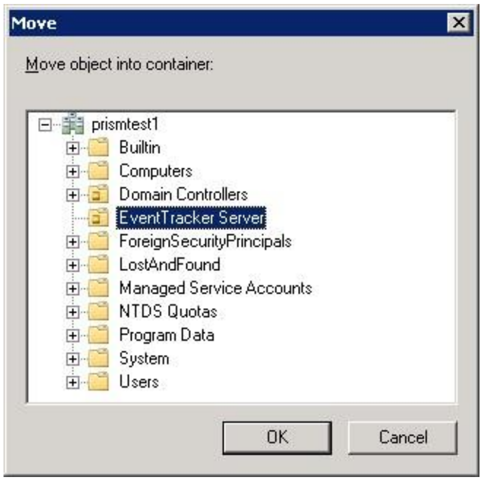
Link Order	GPO
1	WS08R2-SSLF-Domain
2	WS08R2-SSLF-Member-Server
3	WS08R2-Web-Server

Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system

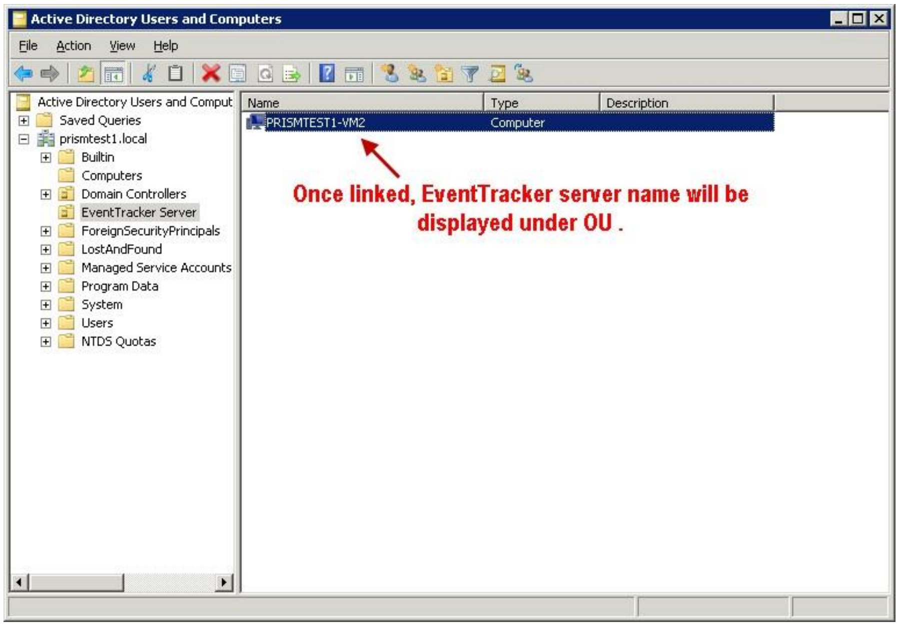
1. Select the **Start** button, select **All Programs,** and then select **Administrative Tools.**
2. Select **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** pane, expand **Domains** node, and click **Computers** node.
4. Right click **EventTracker server system** and click **Move**.



Move dialog box appears.



5. Select the newly created OU (in this case, select **EventTracker Server**), and click **OK**.
6. In the **Active Directory Users and Computers** pane, click ‘organizational unit’ (in this case, click **EventTracker Server**).



Once linked, EventTracker server name will be displayed under OU .

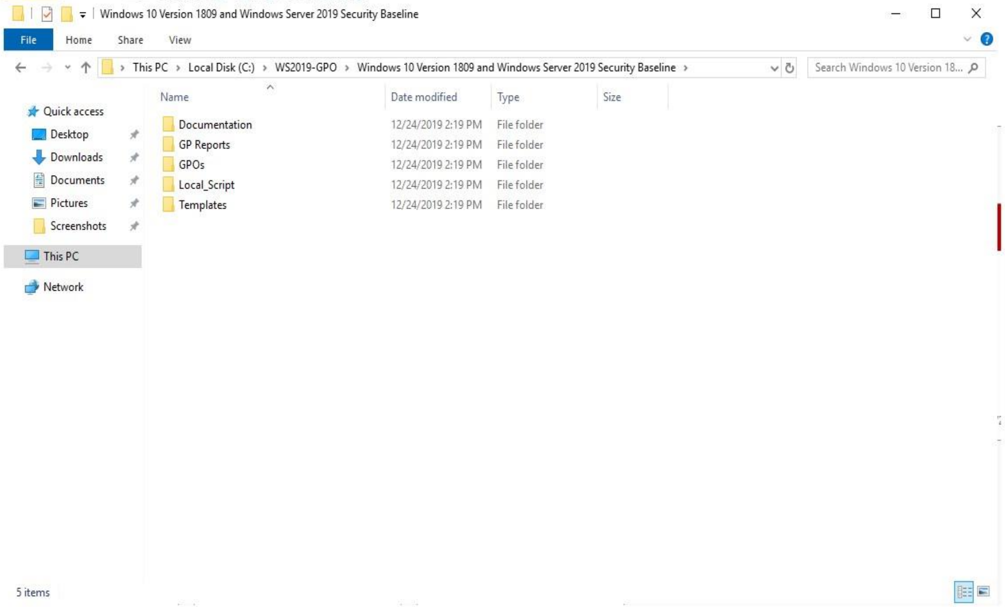
7. Reboot the EventTracker server system linked to the OU.

2.4 Applying Group Policies in a Workgroup on Windows Server 2019

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

1. Click the link below to download the GPO and extract the contents of zip file onto the system.
   https://downloads.eventtracker.com/support/utils/WS2019-GPO.zip

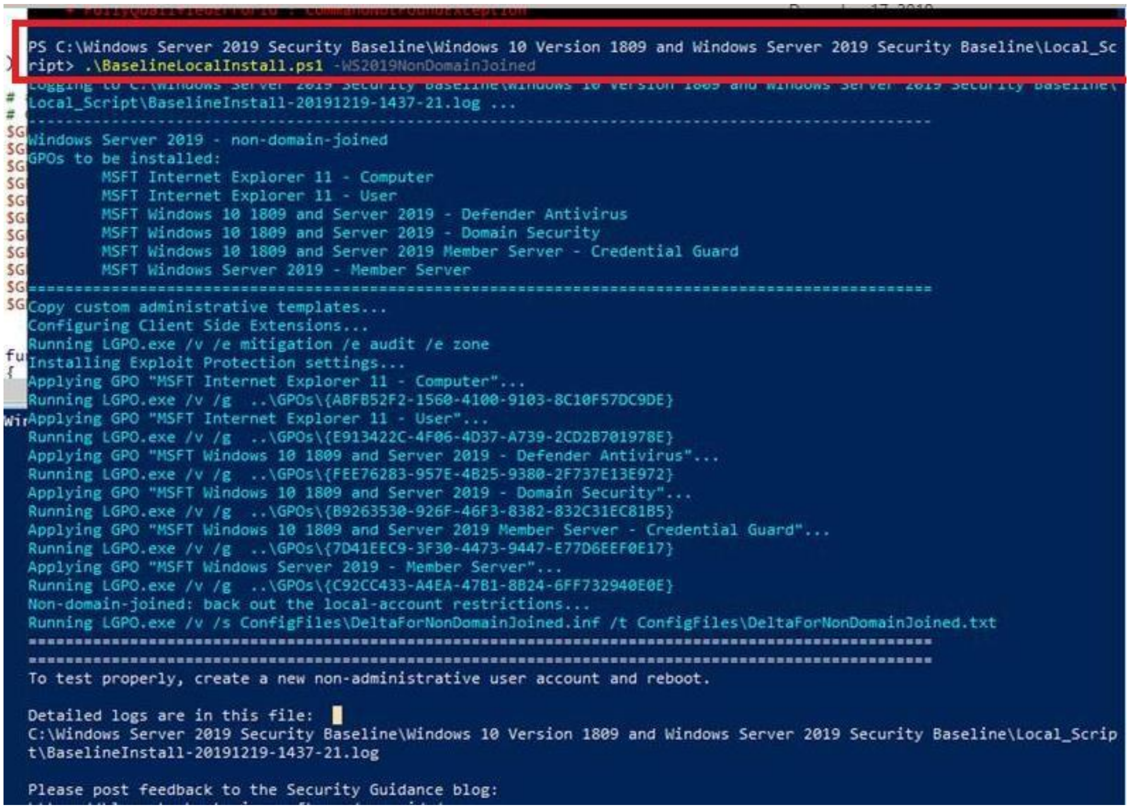
2. Extract the downloaded file to C:\WS2019-GPO


Windows 10 Version 1809 and Windows Server 2019 Security Baseline
File
Home
Share
View
This PC › Local Disk (C:) › WS2019-GPO › Windows 10 Version 1809 and Windows Server 2019 Security Baseline ›
Search Windows 10 Version 18...
Quick access
Desktop
Downloads
Documents
Pictures
Screenshots
This PC
Network
5 items

Name	Date modified	Type	Size
Documentation	12/24/2019 2:19 PM	File folder	
GP Reports	12/24/2019 2:19 PM	File folder	
GPOs	12/24/2019 2:19 PM	File folder	
Local_Script	12/24/2019 2:19 PM	File folder	
Templates	12/24/2019 2:19 PM	File folder	

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

1. Launch PowerShell with run as administrator. The PowerShell script is available in 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

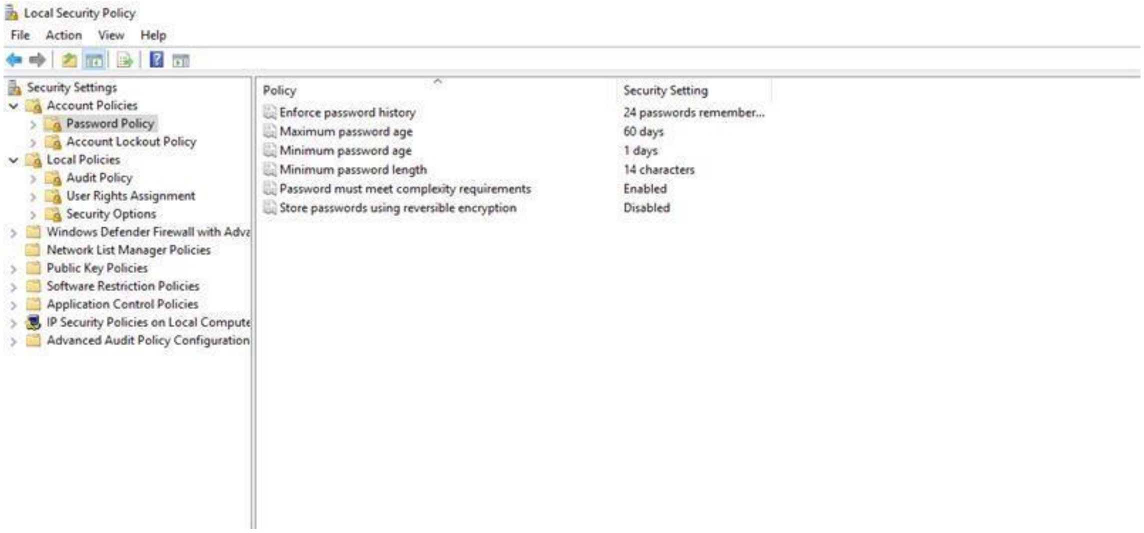


```
PS C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Sc
ript> .\BaselineLocalInstall.ps1 -WS2019NonDomainJoined
Logging to C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\
Local_Script\BaselineInstall-20191219-1437-21.log ...
-------------------------------------------------------------------------------------------------
Windows Server 2019 - non-domain-joined
GPOs to be installed:
        MSFT Internet Explorer 11 - Computer
        MSFT Internet Explorer 11 - User
        MSFT Windows 10 1809 and Server 2019 - Defender Antivirus
        MSFT Windows 10 1809 and Server 2019 - Domain Security
        MSFT Windows 10 1809 and Server 2019 Member Server - Credential Guard
        MSFT Windows Server 2019 - Member Server
=================================================================================================
Copy custom administrative templates...
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-46F3-8382-832C31EC81B5}
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_Scrip
t\BaselineInstall-20191219-1437-21.log

Please post feedback to the Security Guidance blog:
```

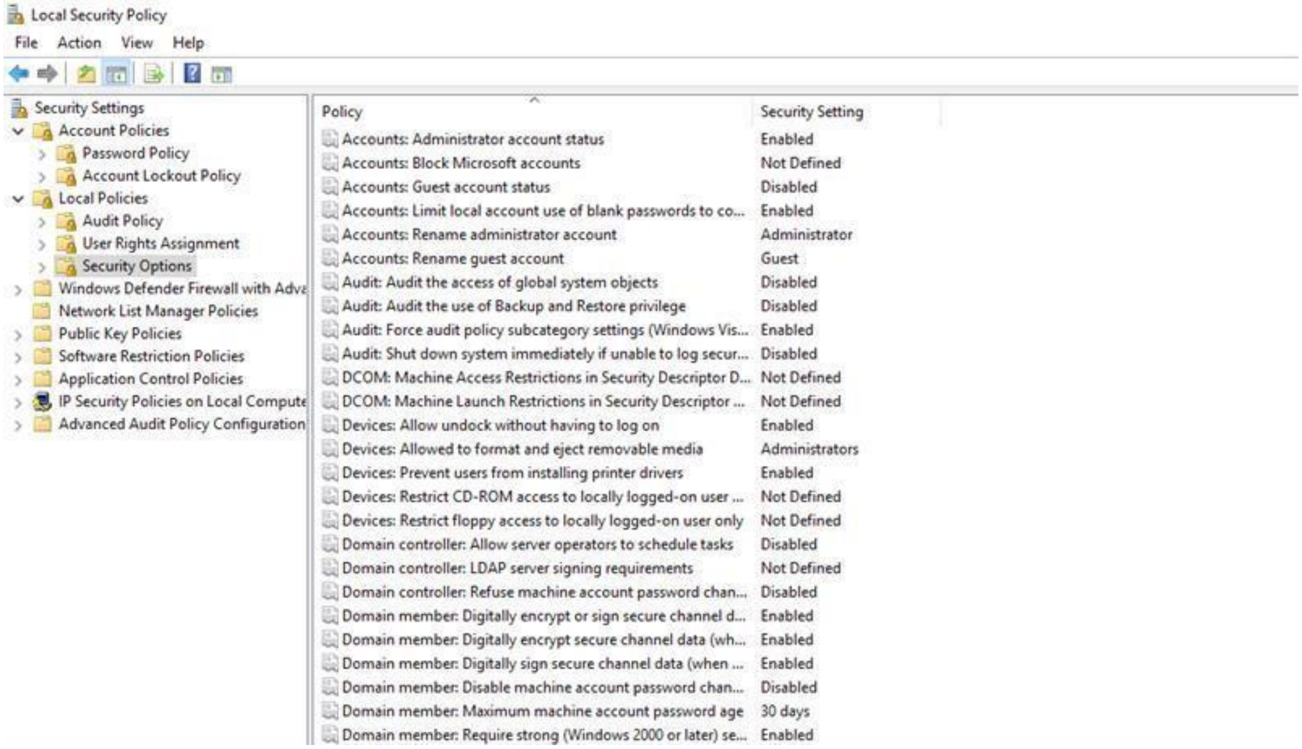
Step 3: Verify the applied Security Policy

In workgroup system:

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



Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Disabled
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Disabled
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled

2.5 Applying Group Policies in a Workgroup on Windows Server 2012

Step 1: On the workgroup system, download windows server 2012 local security policy backup file

1. Click the link below to download exported GPO backup.
   https://downloads.eventtracker.com/support/utils/WS2012-GPO.zip

2. Extract the downloaded file to \\<systemname>\2012GPOBackup.

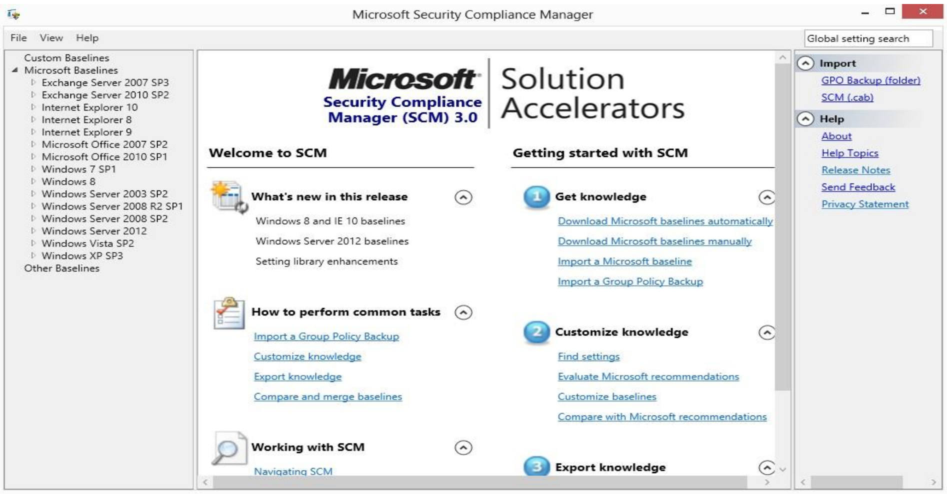
Step 2: On the workgroup system, install the MS Security Compliance Manager (MSCM)

1. Click the link below to download SCM 3

   http://technet.microsoft.com/en-in/solutionaccelerators/cc835245.aspx

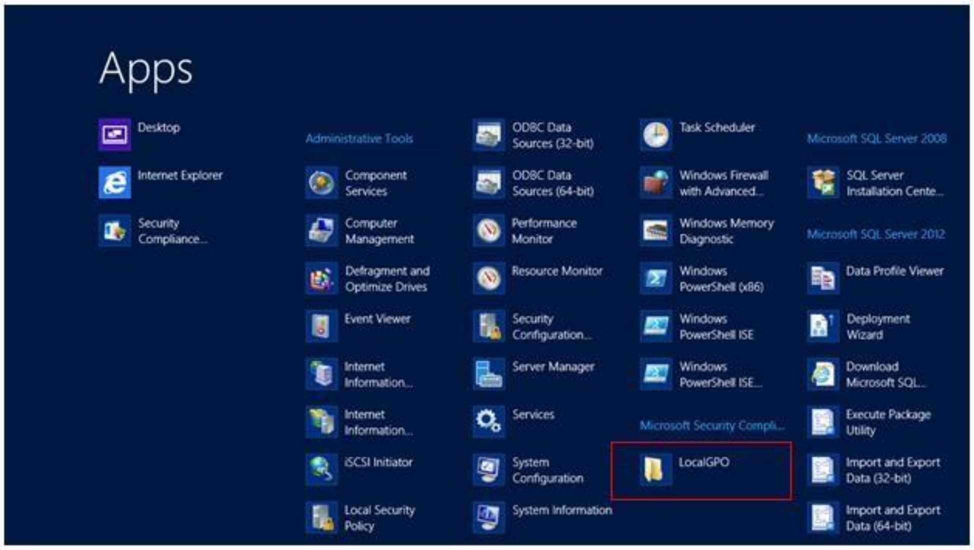
2. In the webpage, Download SCM 3.0 now! , click the link.
3. Download **'Security_Complaince_Manager_setup.exe'**, and then click **Run as Administrator**.
4. Click the Finish button once the installation is completed.

   NOTE: The installation will be interrupted if the prerequisites (Microsoft Visual C++ 2010 X86 Redistributable, .NET Framework 4, and SQL Express 2012) are not installed on the system.
   After successful MSCM Installation, **Microsoft Security Compliance Manager** window appears on the screen.



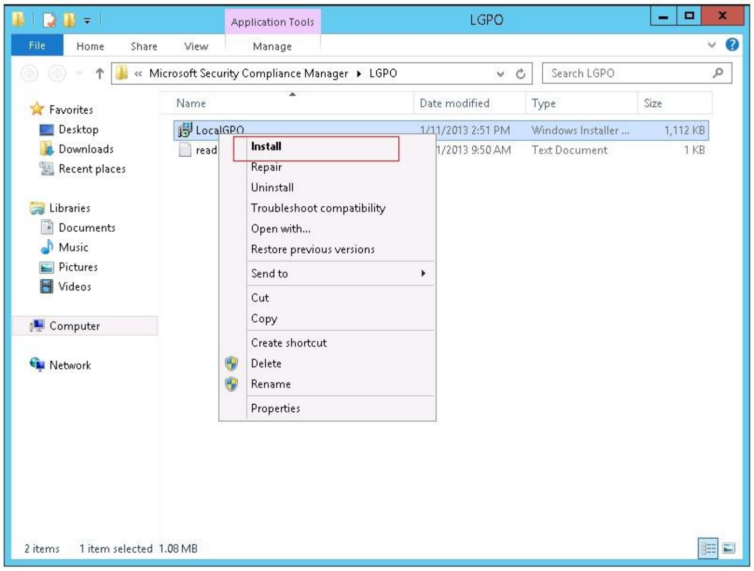
Step 3: On the workgroup system, install Local GPO

1. Select the **Search** button, select **Apps**, and then select **Microsoft Security Compliance Manager.**
2. Select **LocalGPO.**

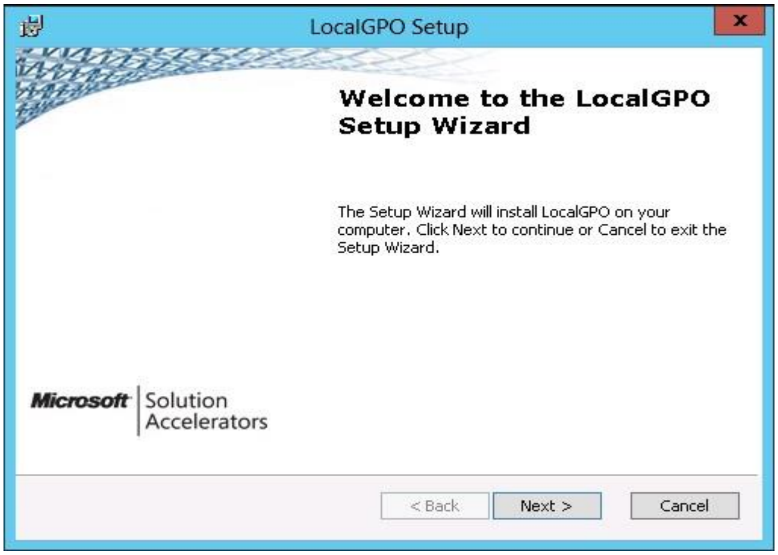


LGPO folder appears on the screen.

3. Right click **LocalGPO**, and then click **Install**.



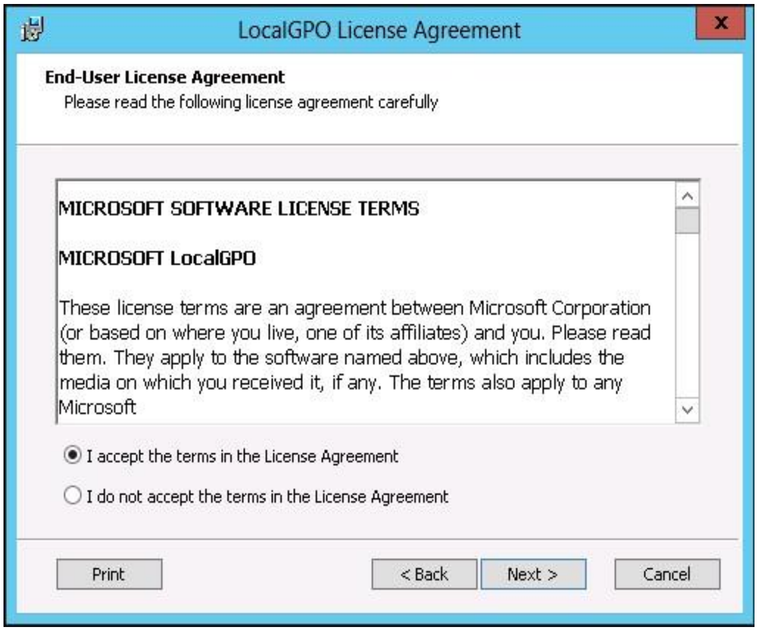
LocalGPO Setup wizard appears on the screen.



LocalGPO Setup
Welcome to the LocalGPO Setup Wizard
Microsoft | Solution Accelerators
< Back
Next >
Cancel

The Setup Wizard will install LocalGPO on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Click the **Next >** button.
5. Read the license agreement, select '**I accept the terms in the License Agreement**' and click **Next >**.



End-User License Agreement

Please read the following license agreement carefully

MICROSOFT SOFTWARE LICENSE TERMS

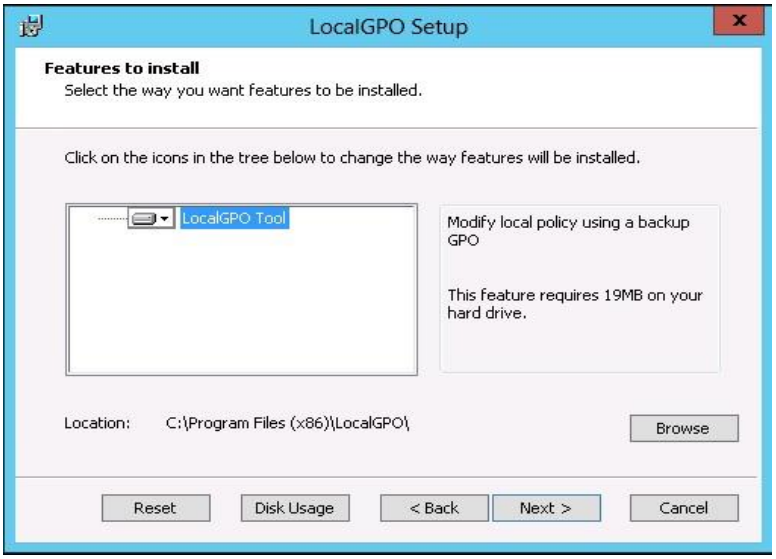
MICROSOFT LocalGPO

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

6. Click **LocalGPO** option, if not selected by default, click the **Next >** button.



LocalGPO Setup

Features to install

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

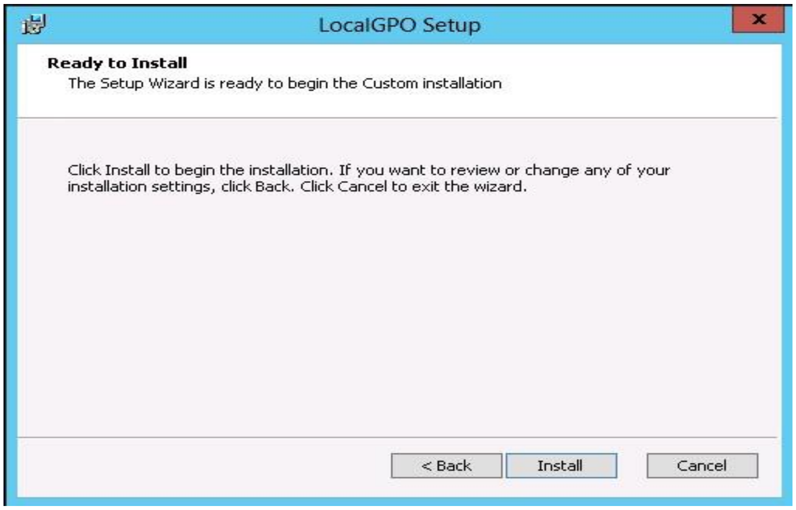
LocalGPO Tool

Modify local policy using a backup GPO

This feature requires 19MB on your hard drive.

Location: C:\Program Files (x86)\LocalGPO\

7. Click the **Install** button.



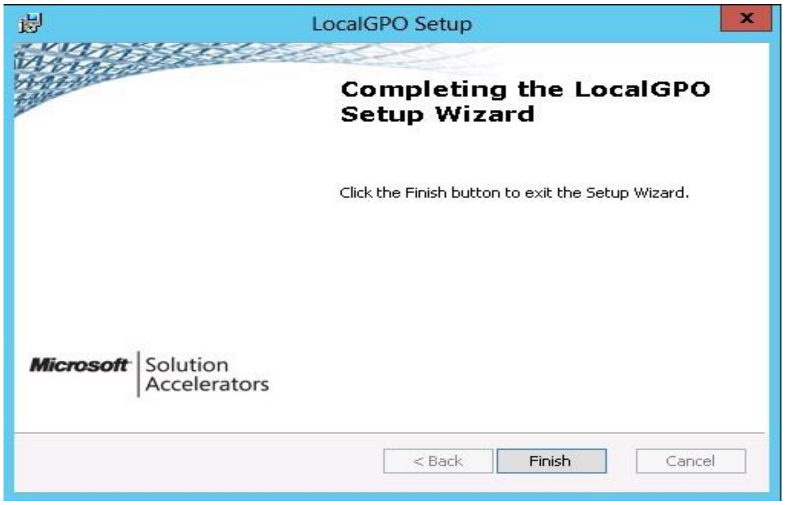
LocalGPO Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8. Click the **Finish** button.



LocalGPO Setup

Completing the LocalGPO Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 4: Restoring the Local Security Policy

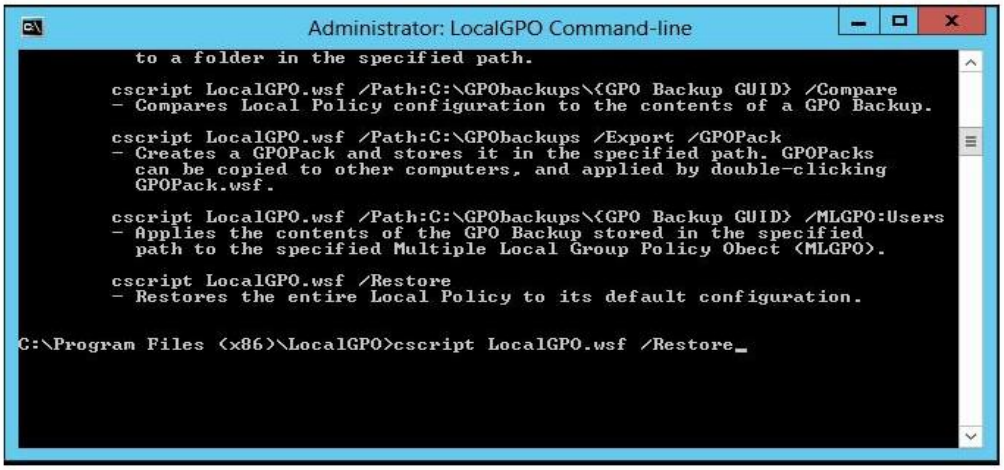
Before restoring the Local Group Policy, check the status of default Local Security Policy in the workgroup system.

1. Select the **Start** button**,** select **Administrative Tools,** and then select click **Local Security Policy**.
2. In **Local Security Policy** window, expand **Account Policies**.
3. Click **Password Policy** and check the **Security Settings**.
4. Click **Account Lockout Policy** and check the **Security Settings**.

Now restore the default Local Security Policy in the workgroup system.

1. Select the **Start** button**,** select **Administrative Tools,** and then select **LocalGPO.**
2. Right click **LocalGPO Command-line** and click **Run as administrator**.
3. In **Administrator: LocalGPO Command-line**, type the following command, and then press the **Enter** button.

   cscript LocalGPO.wsf /Restore



```
          to a folder in the specified path.

        cscript LocalGPO.wsf /Path:C:\GPObackups\{GPO Backup GUID} /Compare
        - Compares Local Policy configuration to the contents of a GPO Backup.

        cscript LocalGPO.wsf /Path:C:\GPObackups /Export /GPOPack
        - Creates a GPOPack and stores it in the specified path. GPOPacks
          can be copied to other computers, and applied by double-clicking
          GPOPack.wsf.

        cscript LocalGPO.wsf /Path:C:\GPObackups\{GPO Backup GUID} /MLGPO:Users
        - Applies the contents of the GPO Backup stored in the specified
          path to the specified Multiple Local Group Policy Obect (MLGPO).

        cscript LocalGPO.wsf /Restore
        - Restores the entire Local Policy to its default configuration.

C:\Program Files (x86)\LocalGPO>cscript LocalGPO.wsf /Restore_
```

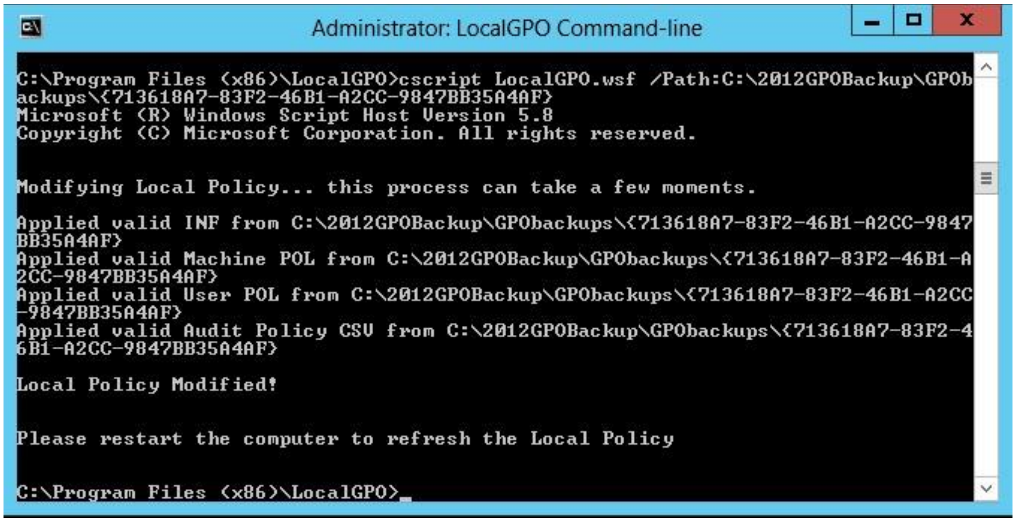
4. After the default Local Policy is restored, type **Exit** in command line.
5. Restart the workgroup system to refresh the Local Policy.

Step 5: Importing Security Policy downloaded in step 1

1. Select the **Start button,** select **Administrative Tools** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.
2. In **Administrator: LocalGPO Command-line**, type the following command, and then press the **Enter** button.
   cscript LocalGPO.wsf /<backup folder path>\{guid}

Here “guid’ is the folder name created under GPObackups.

Ex: \\<systemname>\2012GPOBackup\GPObackups\{713618A7-83F2-46B1-A2CC-9847BB35A4AF}

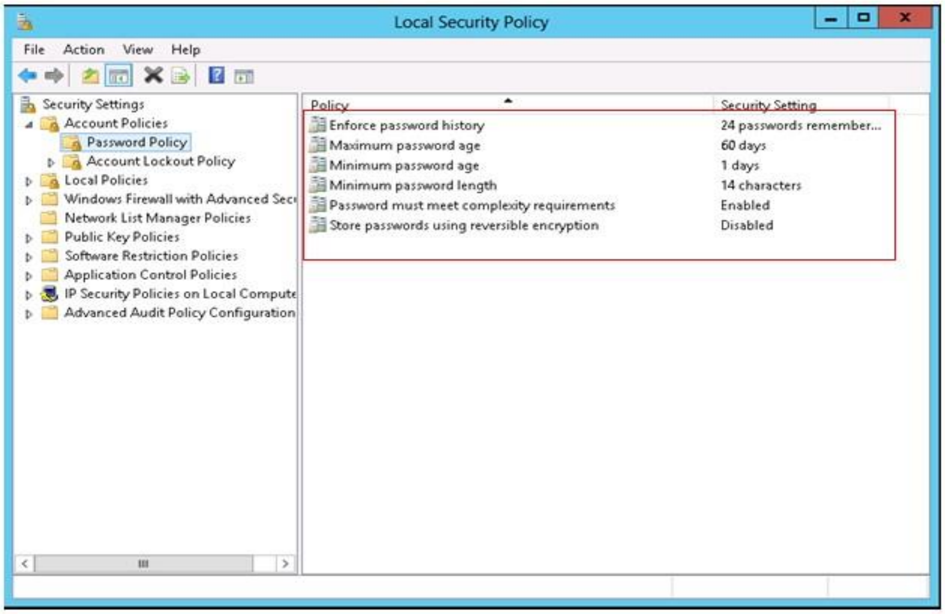


```
C:\Program Files (x86)\LocalGPO>cscript LocalGPO.wsf /Path:C:\2012GPOBackup\GPOb
ackups\{713618A7-83F2-46B1-A2CC-9847BB35A4AF}
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Modifying Local Policy... this process can take a few moments.

Applied valid INF from C:\2012GPOBackup\GPObackups\{713618A7-83F2-46B1-A2CC-9847
BB35A4AF}
Applied valid Machine POL from C:\2012GPOBackup\GPObackups\{713618A7-83F2-46B1-A
2CC-9847BB35A4AF}
Applied valid User POL from C:\2012GPOBackup\GPObackups\{713618A7-83F2-46B1-A2CC
-9847BB35A4AF}
Applied valid Audit Policy CSV from C:\2012GPOBackup\GPObackups\{713618A7-83F2-4
6B1-A2CC-9847BB35A4AF}

Local Policy Modified!

Please restart the computer to refresh the Local Policy

C:\Program Files (x86)\LocalGPO>_
```

3. Restart the computer to refresh the Local Policy.

Step 6: Verify the applied Security Policy In workgroup system:

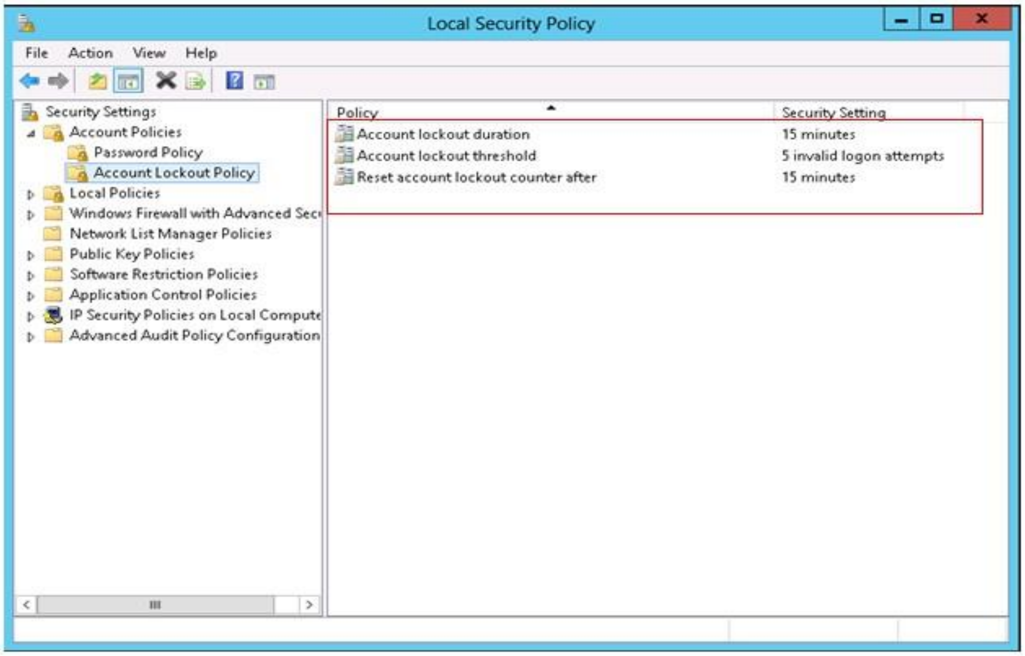
1. Select the **Start** button and select **Administrative Tools.**
2. Select **Local Security Policy**, expand **Account Policies**.
3. Click **Password Policy** and check the **Security Settings**.



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

4. Click **Account Lockout Policy** and check the **Security Settings**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

2.6 Applying Group Policies in a Workgroup on Windows 2K8 / 2K8 R2

Step 1: On the workgroup system, download windows server 2008 R2 / 2012 local security policy backup file

1. Click the link below to download exported GPO backup.

   https://downloads.eventtracker.com/support/utils/2008R2SSLFGPOBackup.zip

2. Extract the downloaded file to \\<systemname>\2008R2SSLFGPOBackup.

Step 2: On the workgroup system, install the MS Security Compliance Manager (MSCM)

1. Click the link below to download SCM 2.5.

   http://social.technet.microsoft.com/wiki/contents/articles/774.microsoft-security-compliancemanager-scm-en-us.aspx

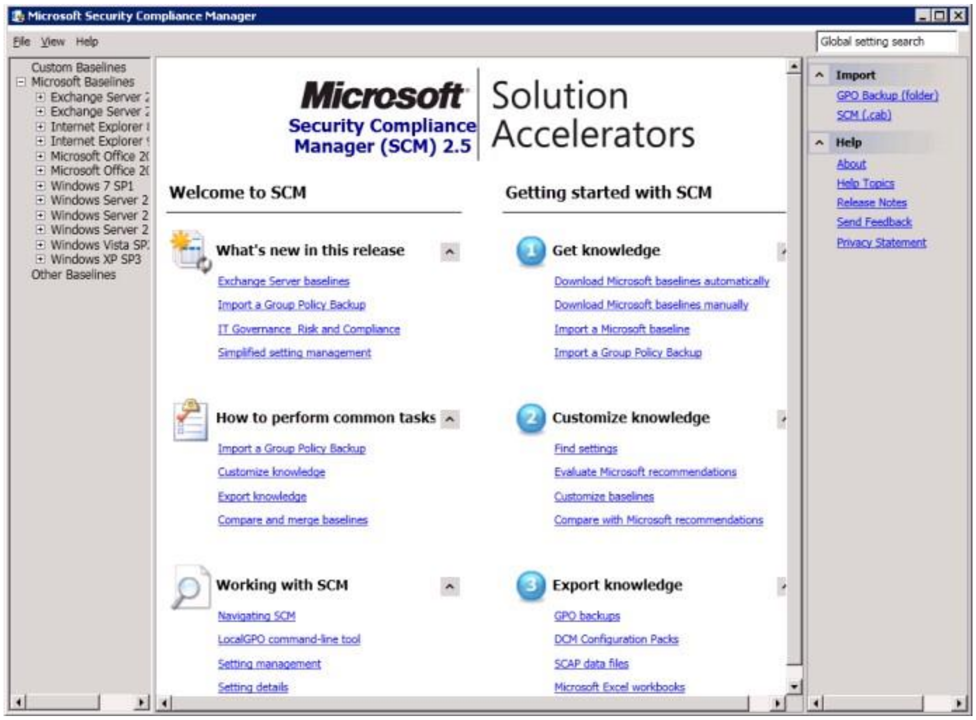
2. In the webpage, click the Download SCM 2.5 Now link.

3. Right click **Security_Complaince_Manager_setup.exe** and click **Run as Administrator**.

4. Click the **Finish** button after the installation is complete.

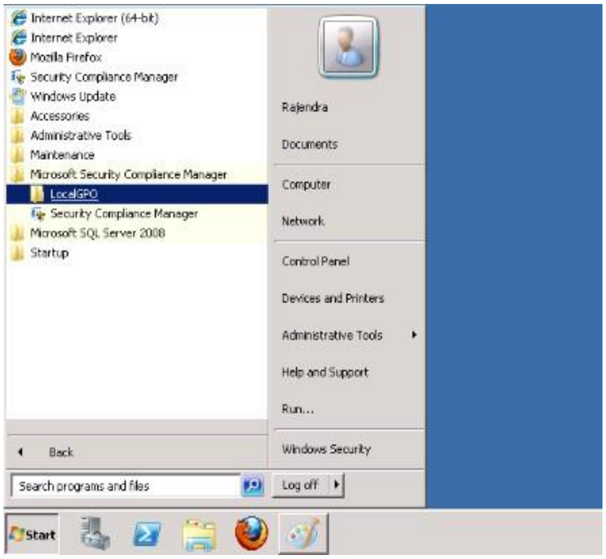
   NOTE: The installation will be interrupted if the prerequisites (Microsoft Visual C++ 2010 X86 Redistributable, .NET Framework 4, and SQL Express 2008) are not installed on the system.

   After successful MSCM Installation, **Microsoft Security Compliance Manager** window appears on the screen.



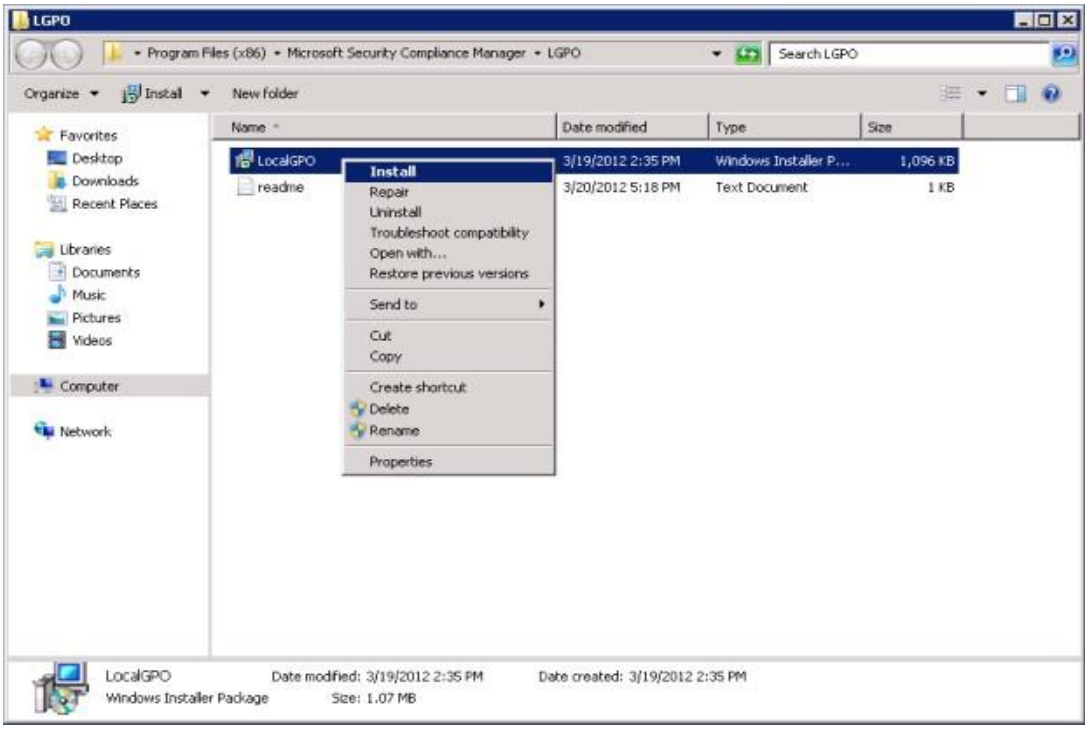
Step 3: On the workgroup system, install Local GPO

1. Select the **Start** button, select **All Programs,** and then select **Microsoft Security Compliance Manager.**
2. Select **LocalGPO**.



LGPO folder appears on the screen.

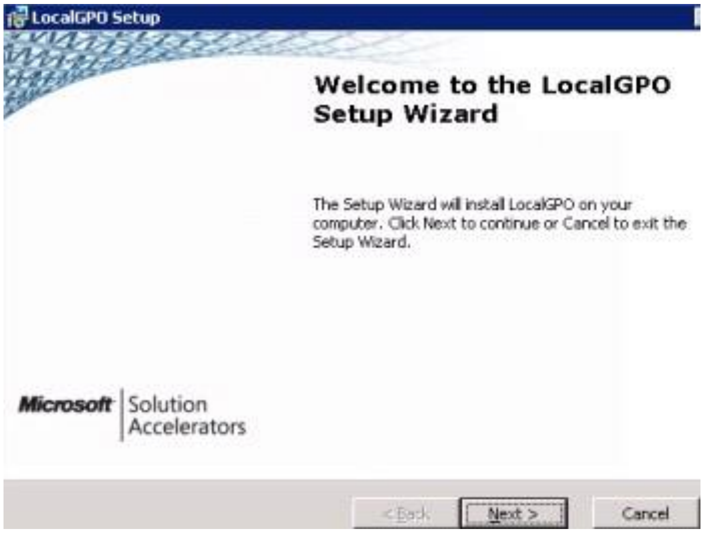
3. Right click **LocalGPO** and click **Install**.



Name	Date modified	Type	Size
LocalGPO	3/19/2012 2:35 PM	Windows Installer P...	1,096 KB
readme	3/20/2012 5:18 PM	Text Document	1 KB

LocalGPO Windows Installer Package Date modified: 3/19/2012 2:35 PM Size: 1.07 MB Date created: 3/19/2012 2:35 PM

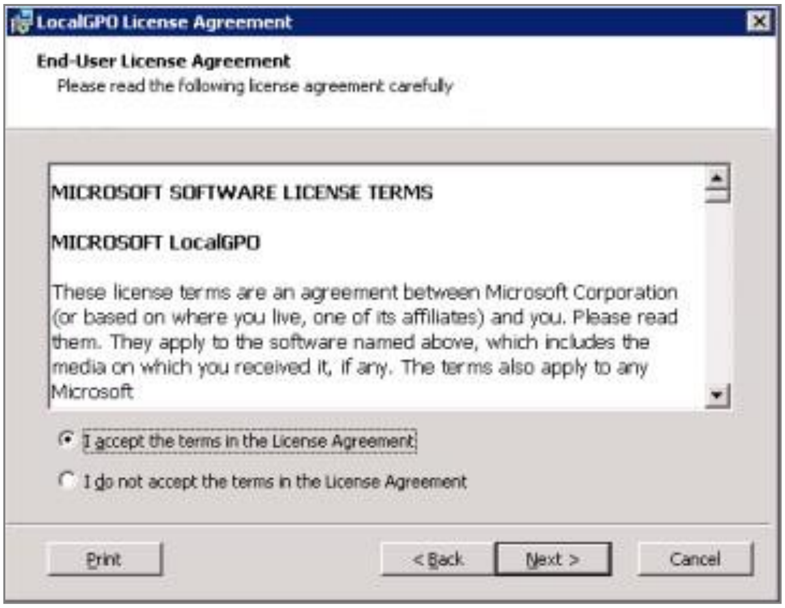
LocalGPO Setup wizard appears on the screen.



Welcome to the LocalGPO Setup Wizard

The Setup Wizard will install LocalGPO on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Click the **Next >** button.
5. Read the license agreement, select **I accept the terms in the License Agreement** & click **Next >**.



LocalGPO License Agreement

End-User License Agreement

Please read the following license agreement carefully

MICROSOFT SOFTWARE LICENSE TERMS

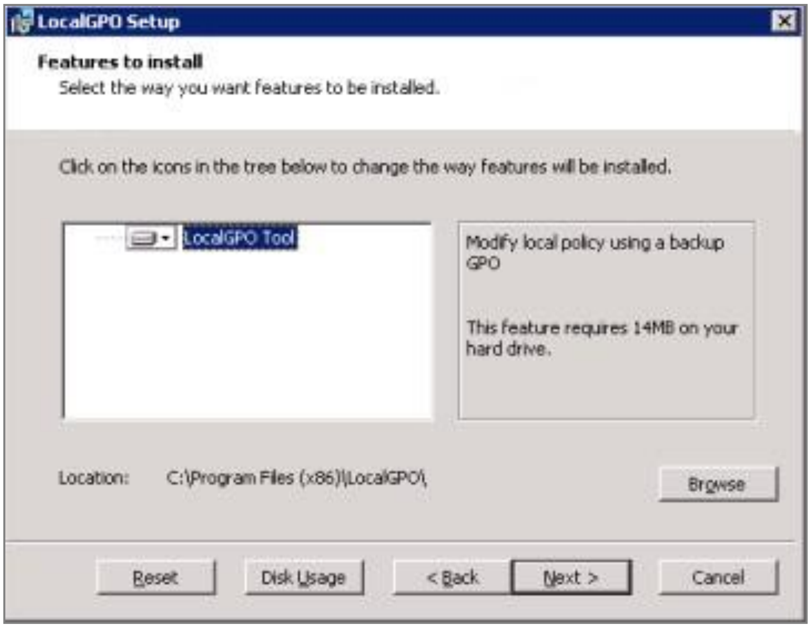
MICROSOFT LocalGPO

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

6. Click **LocalGPO** option, if not selected by default, click the **Next >** button.



LocalGPO Setup

Features to install

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

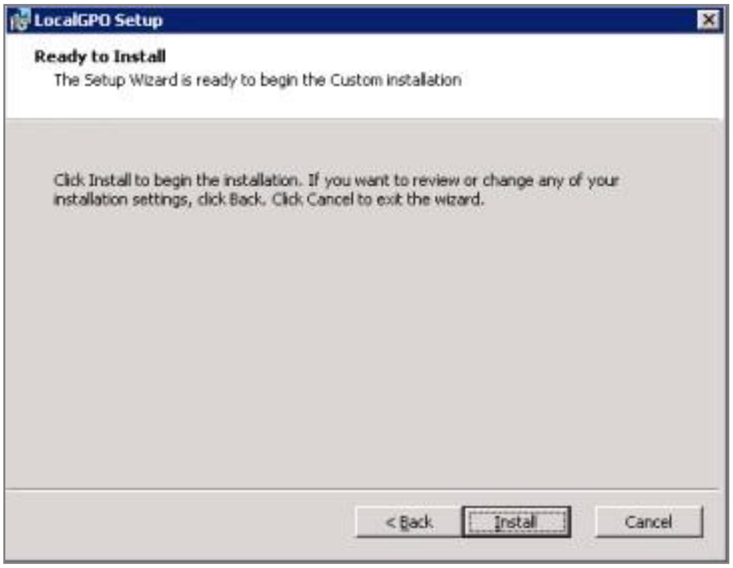
LocalGPO Tool

Modify local policy using a backup GPO

This feature requires 14MB on your hard drive.

Location: C:\Program Files (x86)\LocalGPO\

7. Click the **Install** button.

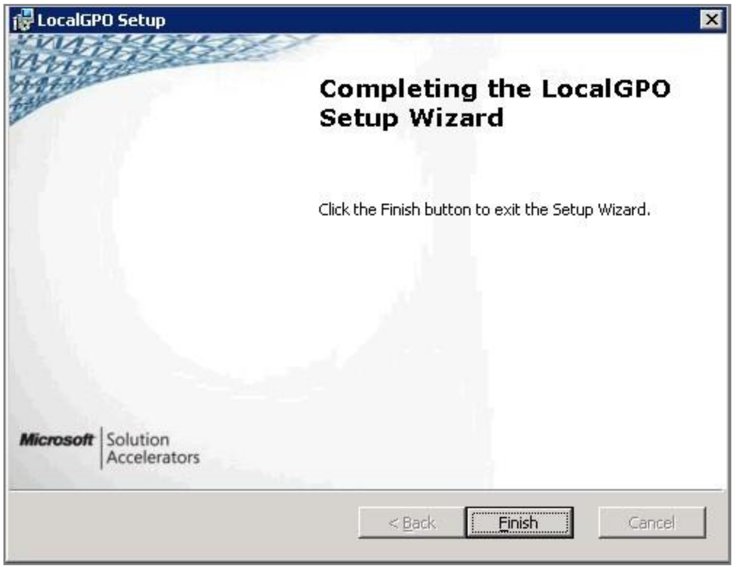


Ready to Install

The Setup Wizard is ready to begin the Custom installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8. Click the **Finish** button.



Completing the LocalGPO Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 4: Restoring the Local Security Policy

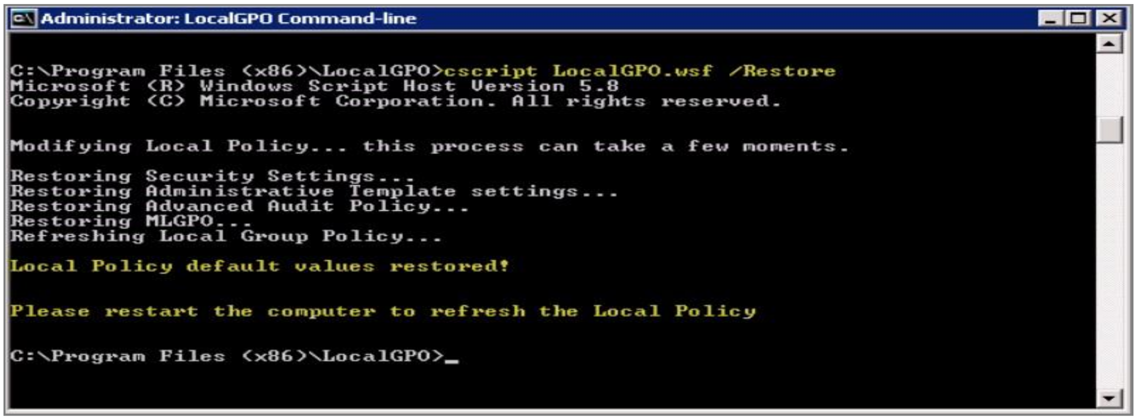
Before restoring the Local Group Policy, check the status of default Local Security Policy in the workgroup system.

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> click **Local Security Policy**.
2. In **Local Security Policy** window, expand **Account Policies**.
3. Click **Password Policy** and check the **Security Settings**.
4. Click **Account Lockout Policy** and check the **Security Settings**.

Now restore the default Local Security Policy in the workgroup system.

1. Click **Start** -> **All Programs** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.
2. In **Administrator: LocalGPO Command-line**, type the following command, and press the **Enter** button.

   cscript LocalGPO.wsf /Restore .



```
Administrator: LocalGPO Command-line

C:\Program Files (x86)\LocalGPO>cscript LocalGPO.wsf /Restore
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Modifying Local Policy... this process can take a few moments.

Restoring Security Settings...
Restoring Administrative Template settings...
Restoring Advanced Audit Policy...
Restoring MLGPO...
Refreshing Local Group Policy...

Local Policy default values restored!

Please restart the computer to refresh the Local Policy

C:\Program Files (x86)\LocalGPO>_
```

3. After the default Local Policy is restored, type **Exit** in command line.
4. Restart the workgroup system to refresh the Local Policy.

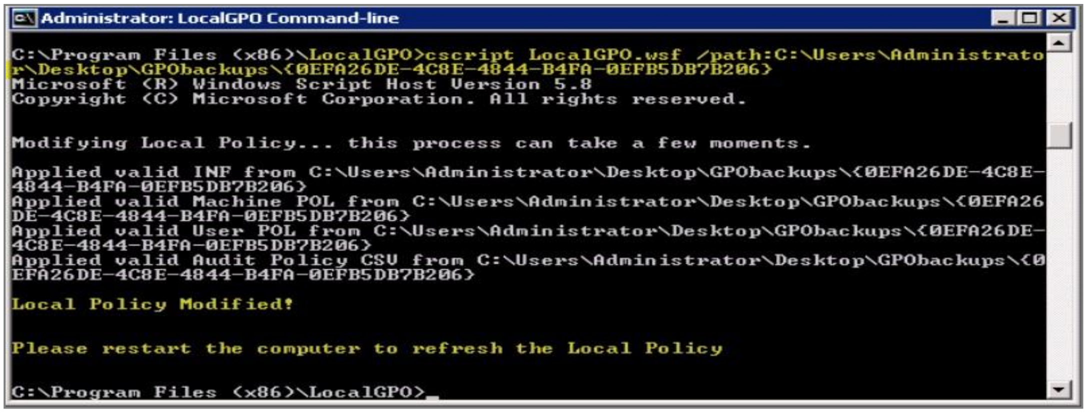
<u>Step 5: Importing Security Policy downloaded in step 1</u>

1. Click **Start** -> **All Programs** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.
2. In **Administrator: LocalGPO Command-line**, type the following command, and press the **Enter** button.

   cscript LocalGPO.wsf /<backup folder path>\{guid}

   Here “guid” is the folder name created under GPObackups.

   Ex**: C:\2008R2SSLFGPOBackup\{95881AD7-2BCD-4FBD-A299-8203899A2B2D}**

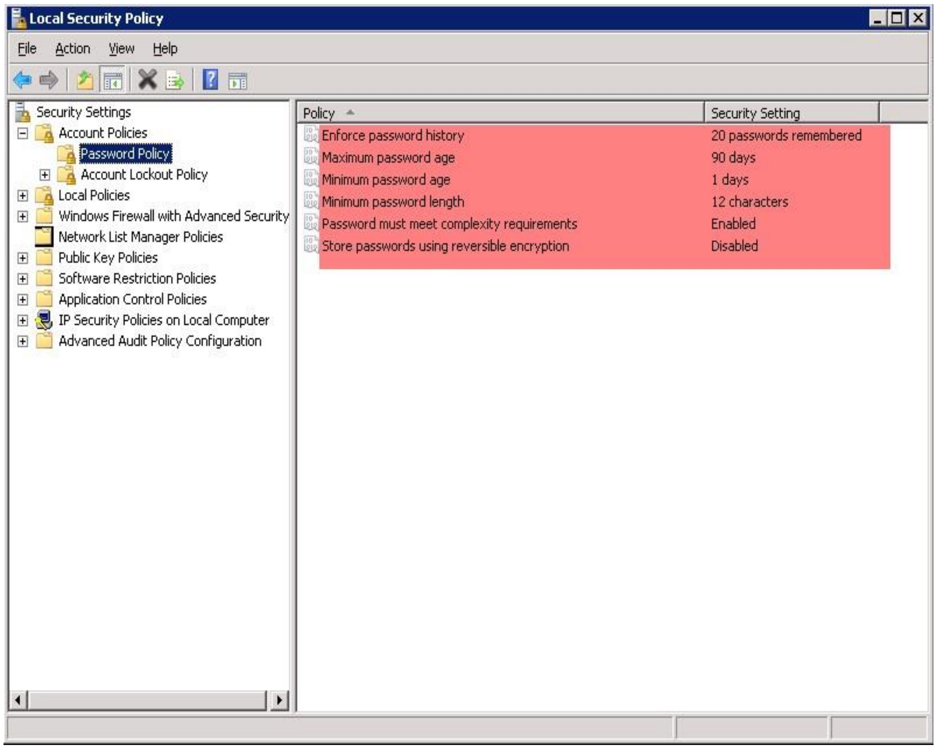


```
Administrator: LocalGPO Command-line

C:\Program Files (x86)\LocalGPO>cscript LocalGPO.wsf /path:C:\Users\Administrato
r\Desktop\GPObackups\{0EFA26DE-4C8E-4844-B4FA-0EFB5DB7B206}
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Modifying Local Policy... this process can take a few moments.

Applied valid INF from C:\Users\Administrator\Desktop\GPObackups\{0EFA26DE-4C8E-
4844-B4FA-0EFB5DB7B206}
Applied valid Machine POL from C:\Users\Administrator\Desktop\GPObackups\{0EFA26
DE-4C8E-4844-B4FA-0EFB5DB7B206}
Applied valid User POL from C:\Users\Administrator\Desktop\GPObackups\{0EFA26DE-
4C8E-4844-B4FA-0EFB5DB7B206}
Applied valid Audit Policy CSV from C:\Users\Administrator\Desktop\GPObackups\{0
EFA26DE-4C8E-4844-B4FA-0EFB5DB7B206}

Local Policy Modified!

Please restart the computer to refresh the Local Policy

C:\Program Files (x86)\LocalGPO>_
```

3. Restart the computer to refresh the Local Policy.

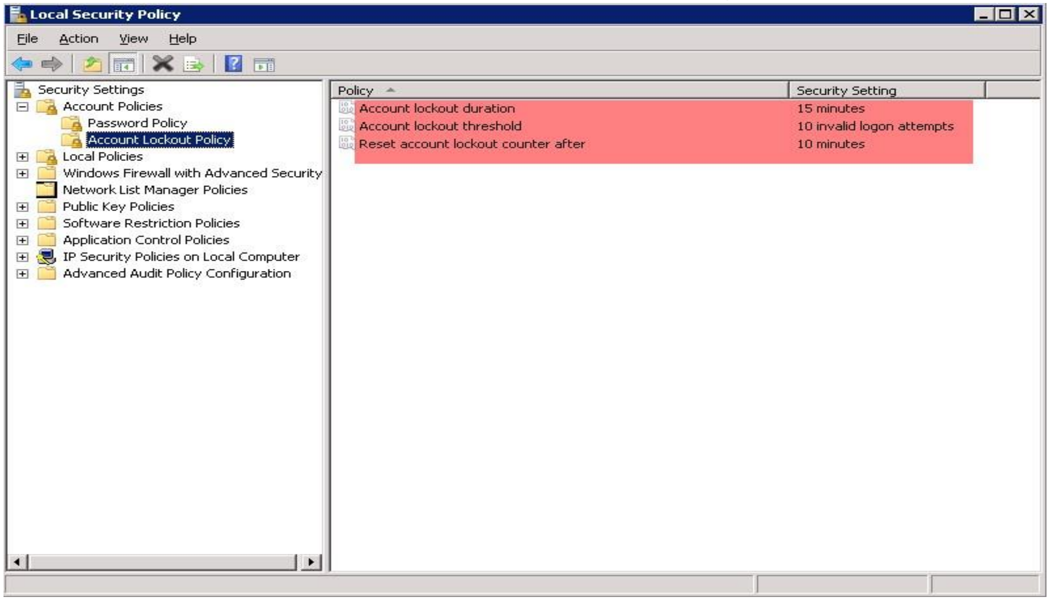
Step 6: Verify the applied Security Policy In workgroup system:

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


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	20 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

4. Click **Account Lockout Policy** and check the **Security Settings**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	10 minutes

3. Secure IIS Web Server (IIS 7, 7.5, 8, 8.5 and 10)

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

SSL is required to,

- Offer a login or sign in on the site
- Process sensitive data
- Comply with security requirements

3.1 Mandatory Requirements

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

Operating System	• Windows Server 2008, 2008 R2 Enterprise SP1/ 2012/ 2016/ 2019 ***OR***
Software and Component	• Internet Information Server (IIS) 7.0 and above. • Browser, which supports 128-bit encryption • (IE 11 or above/ Firefox 3.5 or above).

3.2 IIS setup on Windows 2K8 / 2K8 R2 / 2012/ 2016/ 2019

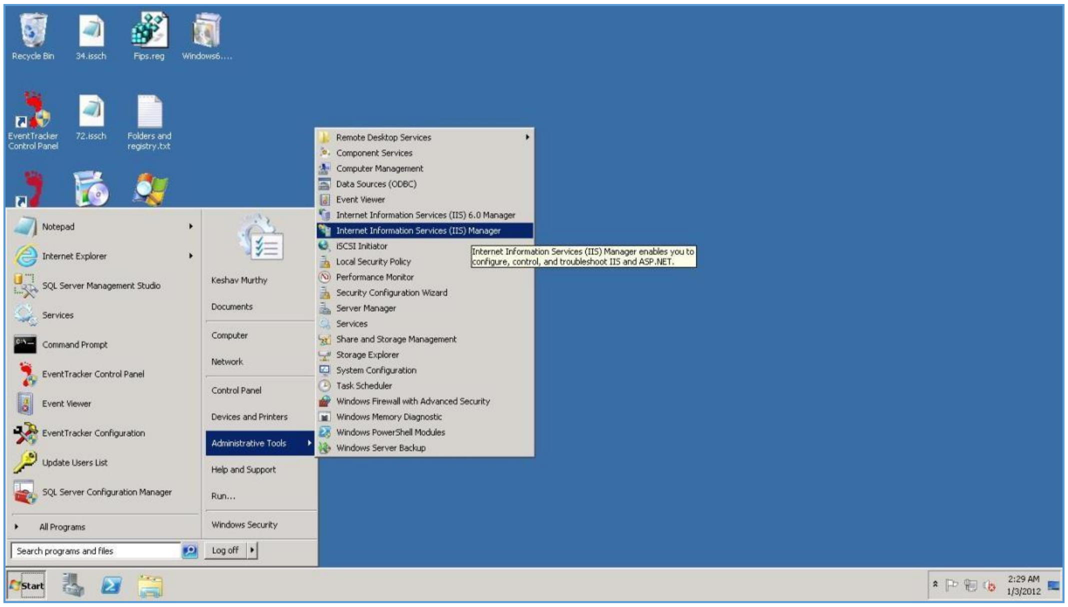
Step 1: Creating the 'Certificate Request'

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

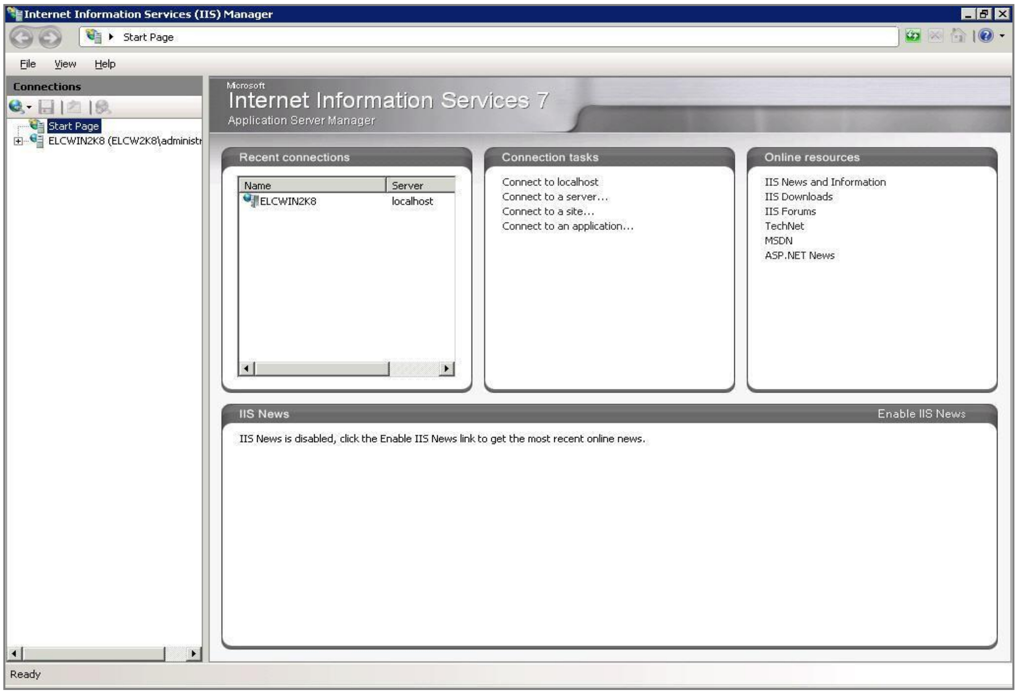
NOTE: In Windows Server 2012, Click the **Start** button, and select **Administrative Tools.**

The screenshot for IIS 8 in Windows 2012 may differ but the features and functionality remain the same.

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

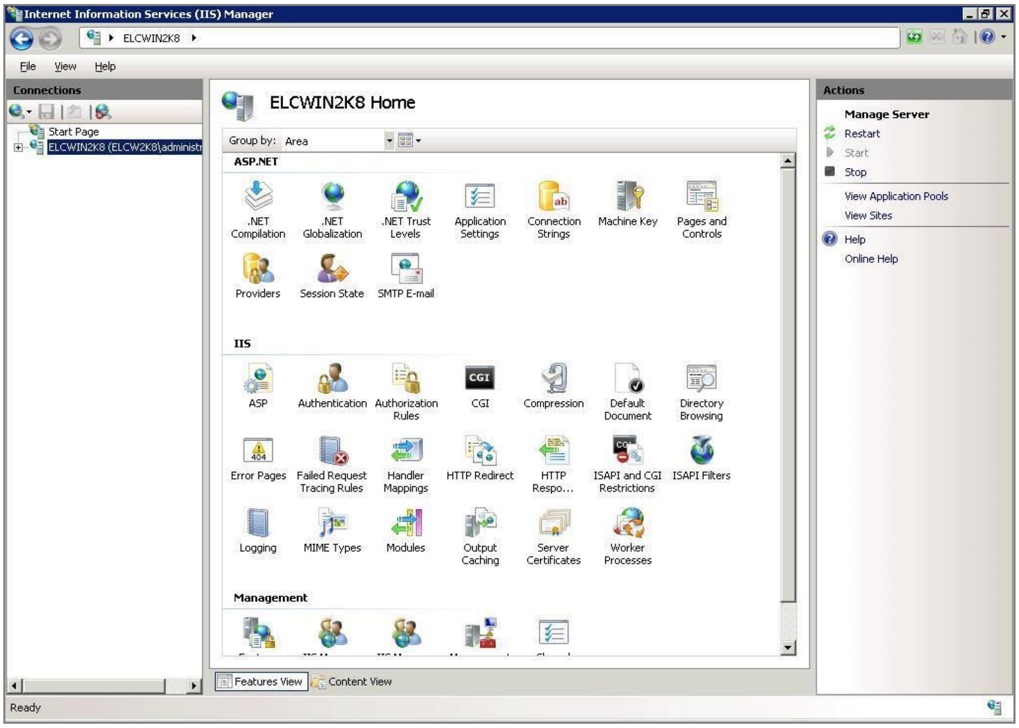


Internet Information Services (IIS) Manager enables you to configure, control, and troubleshoot IIS and ASP.NET.

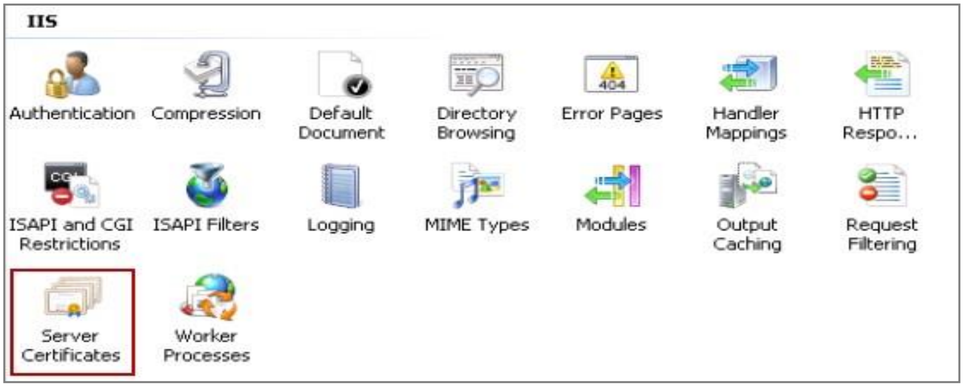


IIS News is disabled, click the Enable IIS News link to get the most recent online news.

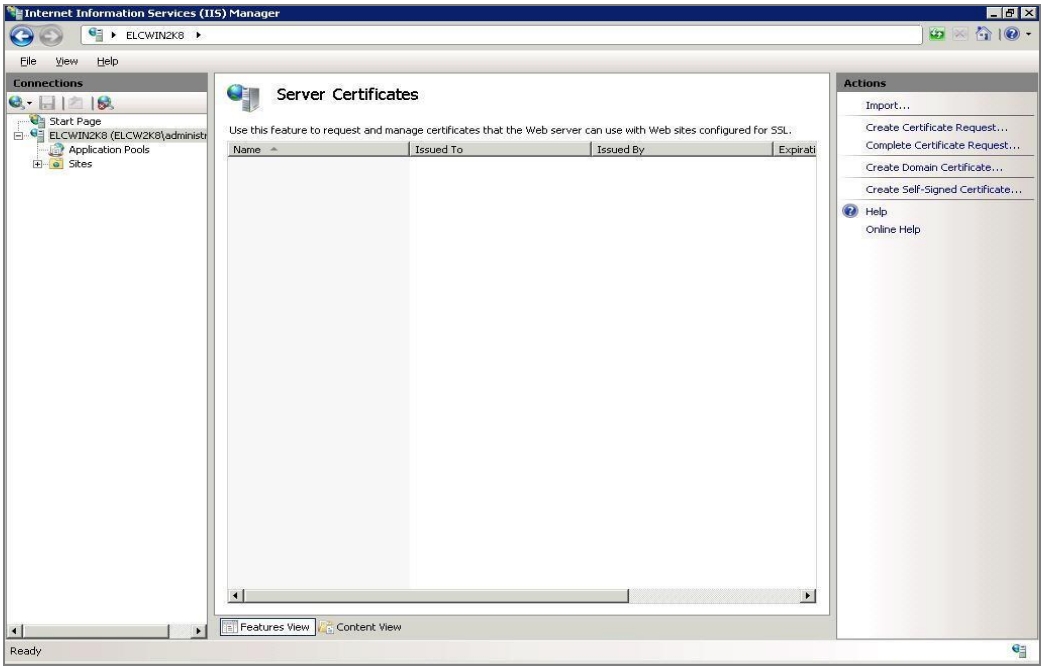
3 Click the server node.



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



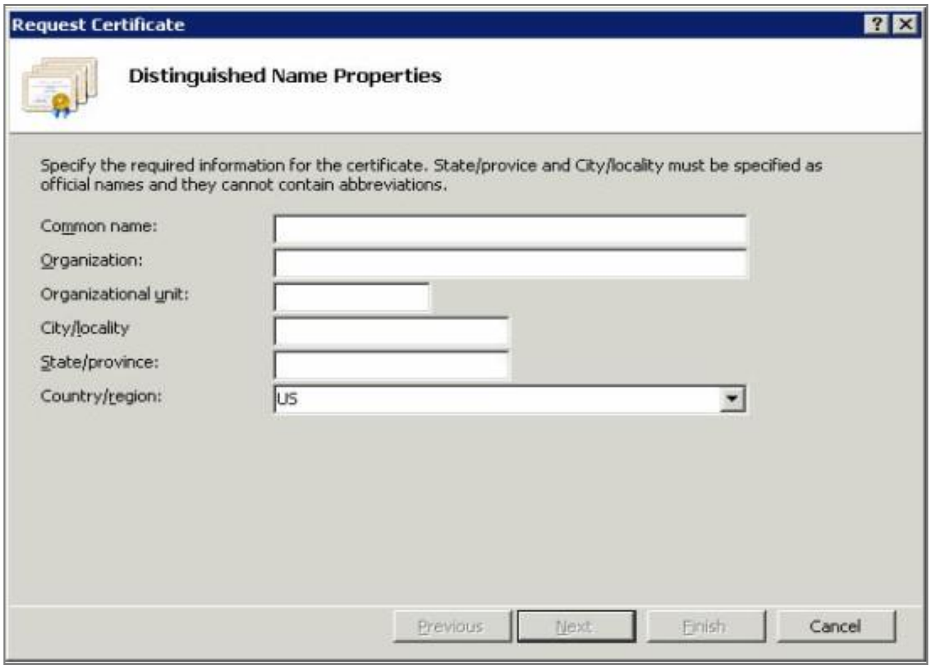
Server Certificates pane displays.


Internet Information Services (IIS) Manager
ELCWIN2K8
File
View
Help
Connections
Start Page
ELCWIN2K8 (ELCW2K8\administr
Application Pools
Sites
Server Certificates
Name
Issued To
Issued By
Expirati
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Ready

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

5 In the **Actions** pane, click **Create Certificate Request** link.

Request Certificate dialog box appears.



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

Common name:

Organization:

Organizational unit:

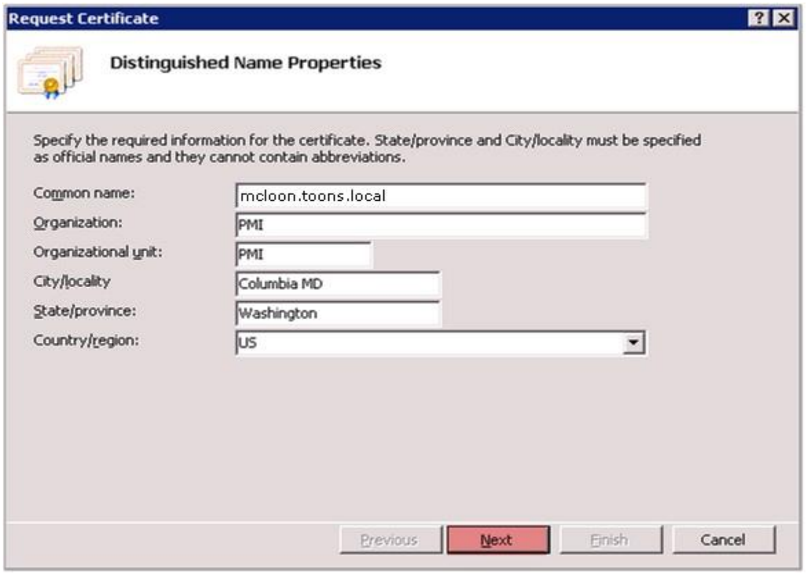
City/locality

State/province:

Country/region: US

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

Example: mcloon.toons.local



Request Certificate

Distinguished Name Properties

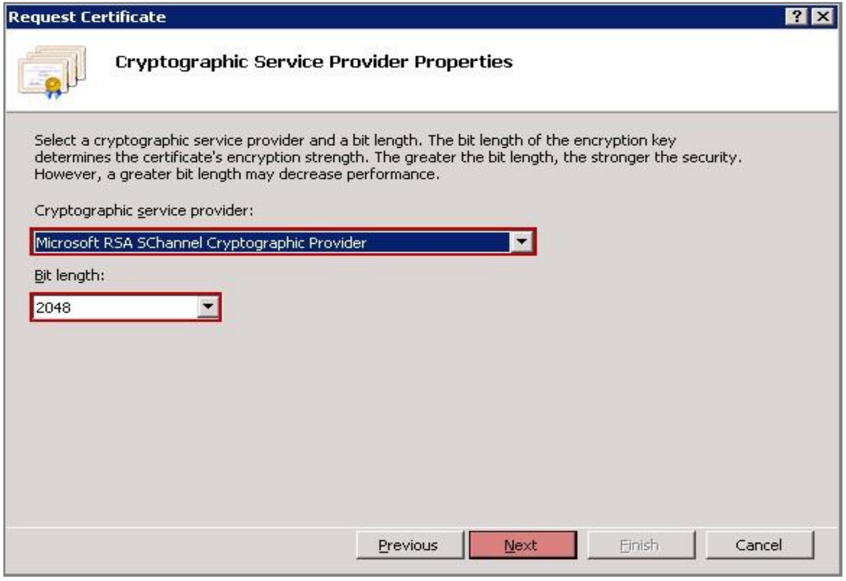
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: mcloon.toons.local
Organization: PMI
Organizational unit: PMI
City/locality: Columbia MD
State/province: Washington
Country/region: US

7 Enter organization and geographical details and click **Next**.

Leave the default selection in **Cryptographic Service Provider Properties** pane.

8 Set bit length to 2048 from the **Bit length** dropdown and click the **Next**.



Request Certificate

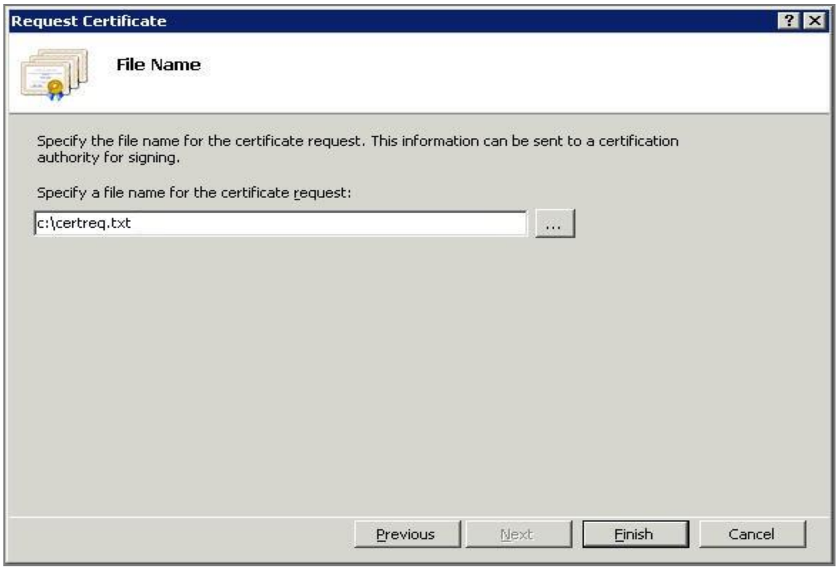
Cryptographic Service Provider Properties

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: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

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



Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

c:\certreq.txt

10 Click **Finish**.

11 Send this request file to the certificate vendor.

Step 2: Installing the certificate

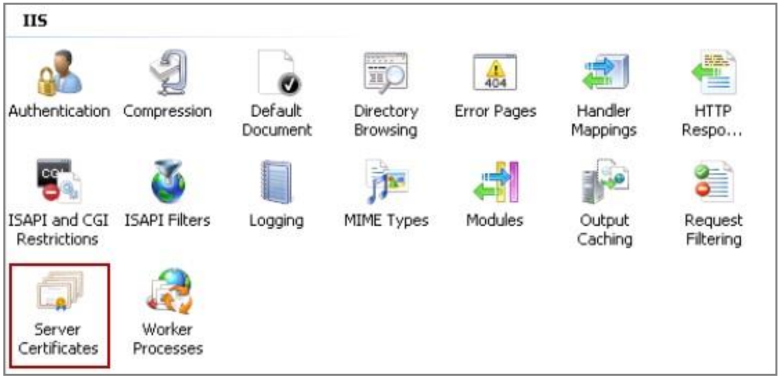
NOTE: Certificate received from the vendor needs to be copied to the system.

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

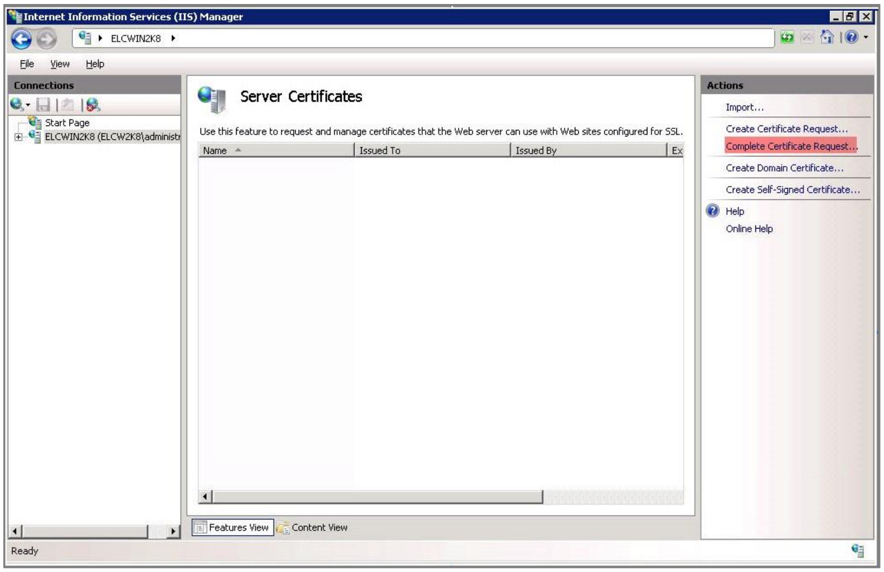
2 Select **Internet Information Services (IIS) Manager**.

‘Internet Information Services (IIS) Manager’ window is displayed.

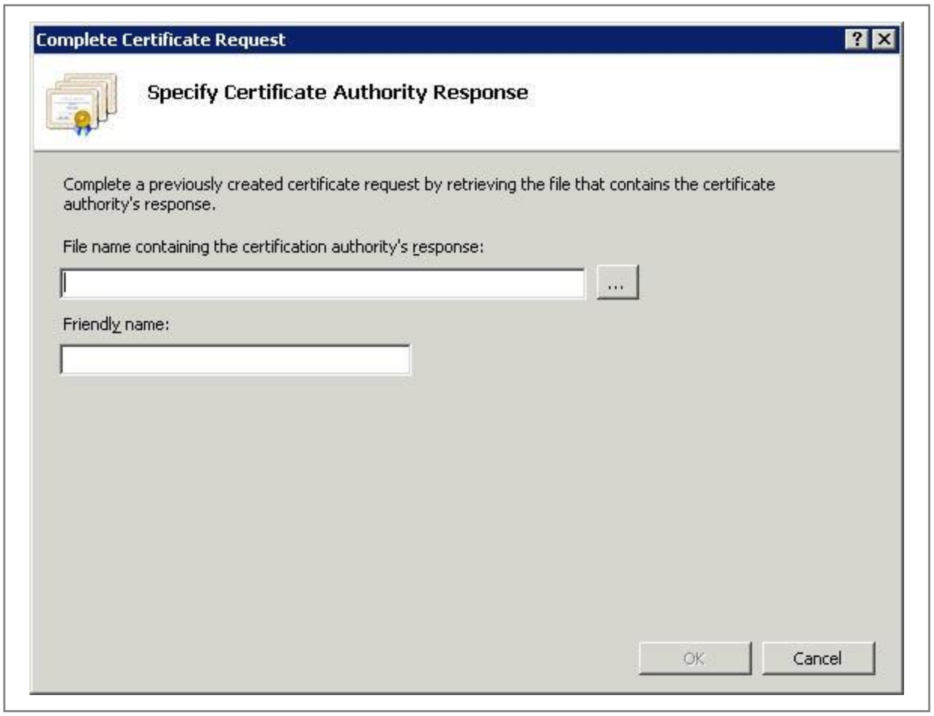
3 Click the server node, and then double click the **Server Certificates** icon in the IIS pane.



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


Internet Information Services (IIS) Manager
ELCWIN2K8
File
View
Help
Connections
Start Page
ELCWIN2K8 (ELCW2K8\administ
Server Certificates
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.
Name
Issued To
Issued By
Ex
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

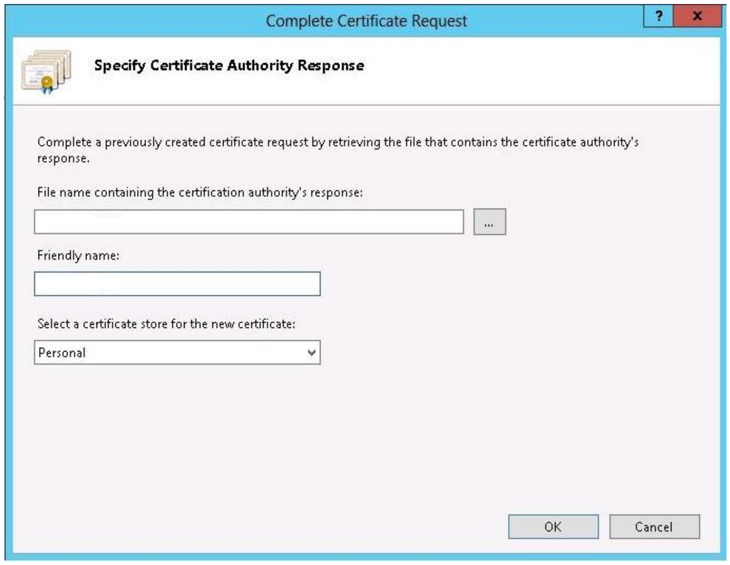
5 In **Complete Certificate Request** dialog box, click the **browse** button.


Complete Certificate Request
?
Specify Certificate Authority Response
...
OK
Cancel

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

Friendly name:



Complete Certificate Request
Specify Certificate Authority Response
OK
Cancel

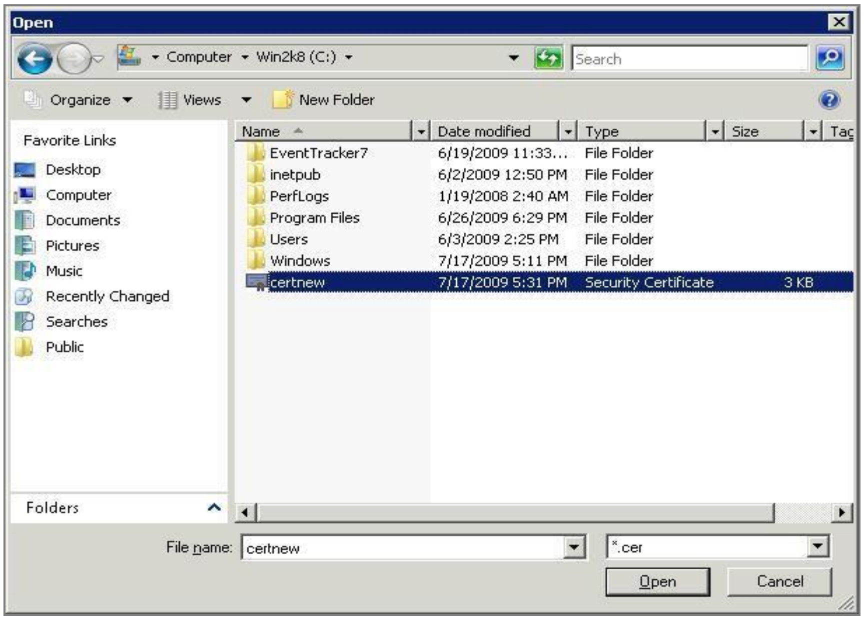
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

Friendly name:

Select a certificate store for the new certificate: Personal

6 Locate the server certificate received from the certificate authority.

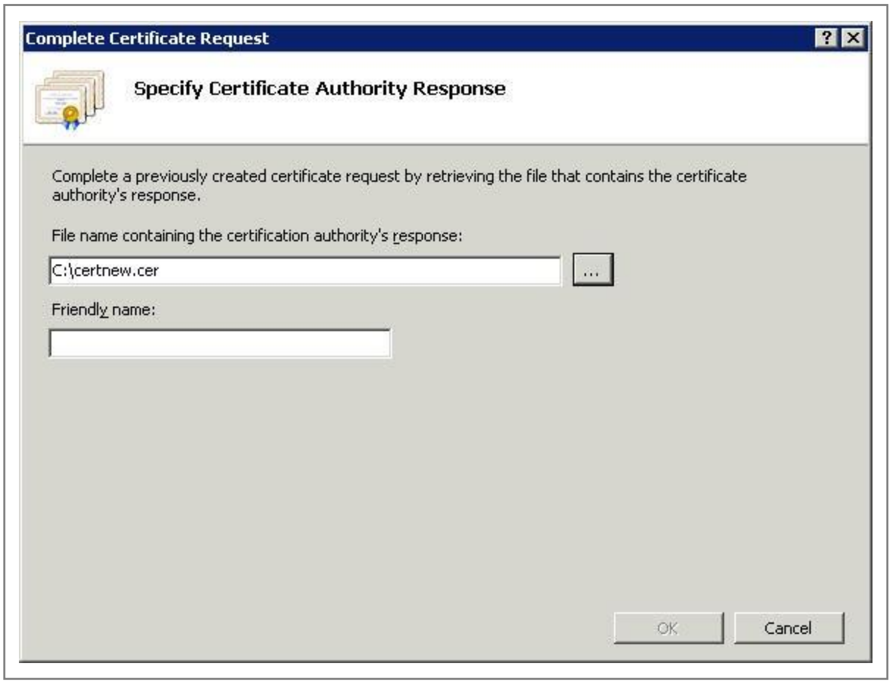


Name	Date modified	Type	Size	Tag
EventTracker7	6/19/2009 11:33...	File Folder		
inetpub	6/2/2009 12:50 PM	File Folder		
PerfLogs	1/19/2008 2:40 AM	File Folder		
Program Files	6/26/2009 6:29 PM	File Folder		
Users	6/3/2009 2:25 PM	File Folder		
Windows	7/17/2009 5:11 PM	File Folder		
certnew	7/17/2009 5:31 PM	Security Certificate	3 KB	

File name: certnew

*.cer

7 Click **Open**.



Complete Certificate Request

Specify Certificate Authority Response

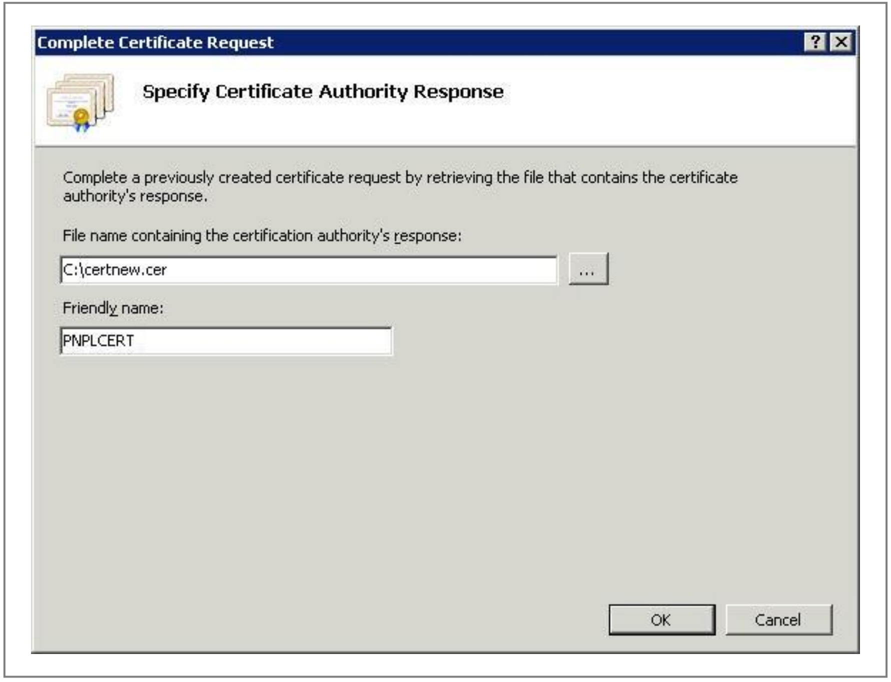
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\certnew.cer

Friendly name:

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



Complete Certificate Request

Specify Certificate Authority Response

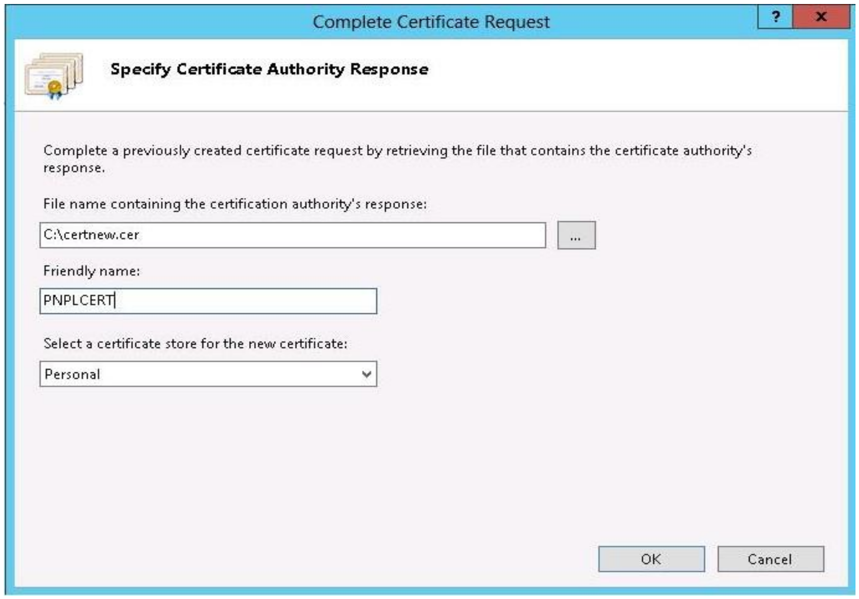
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\certnew.cer

Friendly name:

PNPLCERT



Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

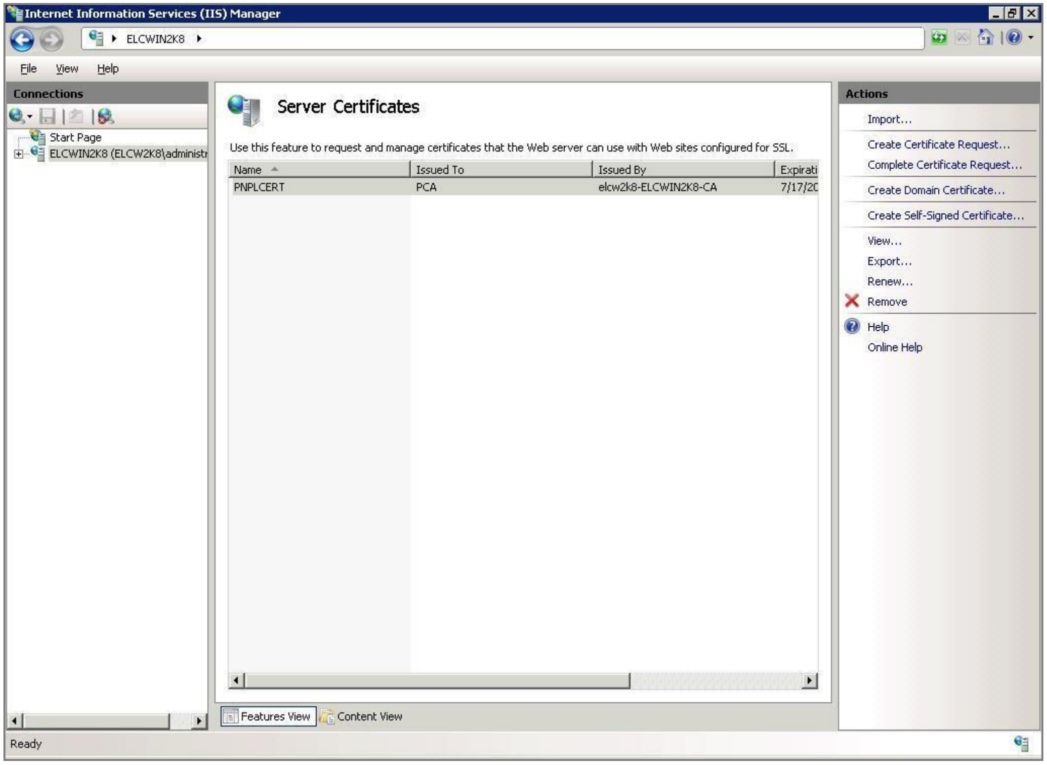
File name containing the certification authority's response: C:\certnew.cer

Friendly name: PNPLCERT

Select a certificate store for the new certificate: Personal

9 Click **OK**.

If successful, the newly installed certificate will be shown in the list. If an error ‘the request or private key cannot be found’ occurs, then ensure that the correct certificate is used and is getting 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.



Internet Information Services (IIS) Manager
ELCWIN2K8
File
View
Help
Connections
Start Page
ELCWIN2K8 (ELCW2K8\administr
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help
Features View
Content View
Ready

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expirati
PNPLCERT	PCA	elcw2k8-ELCWIN2K8-CA	7/17/2C

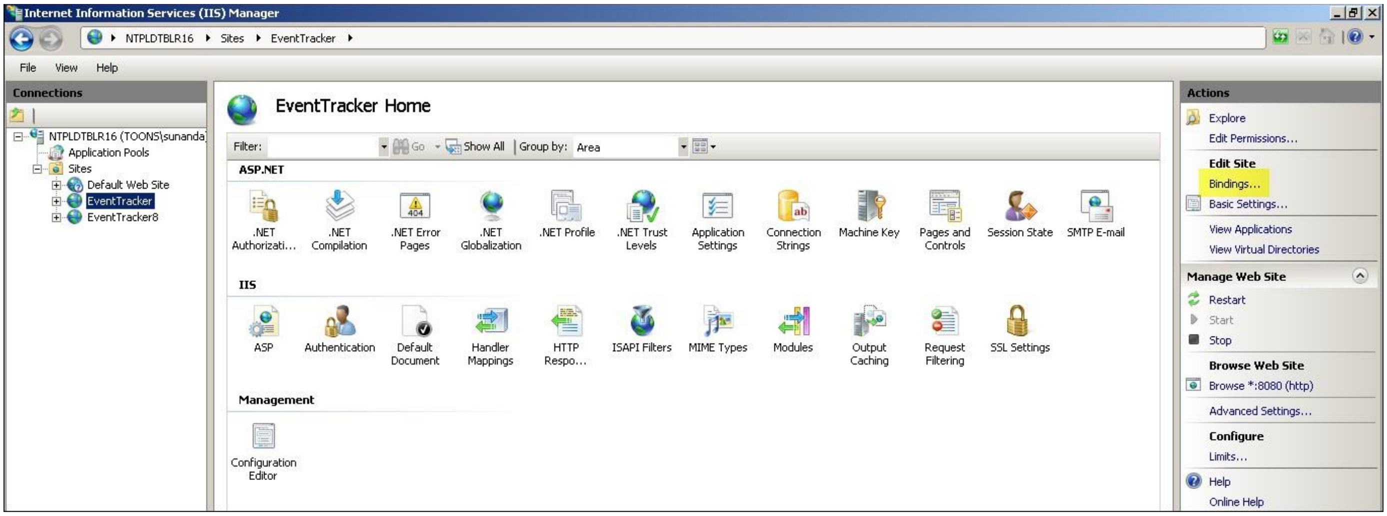
Step 3: Binding the certificate to the 'EventTracker'

1 Expand the server node.

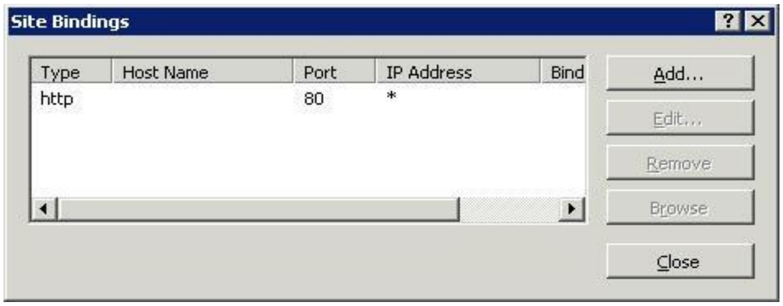
2 Expand the **Sites** node.

3 Click **EventTracker**.

4 In the **Actions** pane, click **Bindings**.



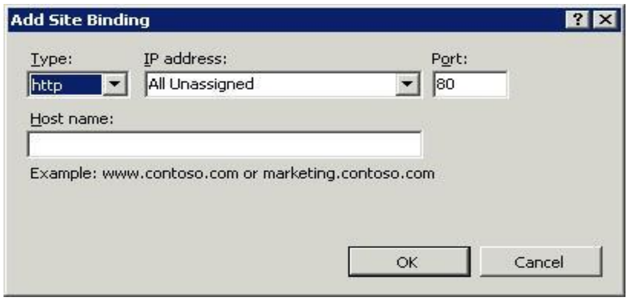
Site Bindings dialog box appears.


Site Bindings

Type	Host Name	Port	IP Address	Bind
http		80	*	

5 Click **Add**.

Add Site Binding dialog box appears.


Add Site Binding

Type: http

IP address: All Unassigned

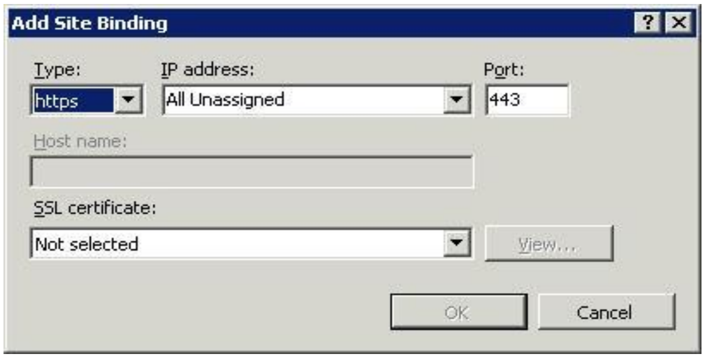
Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

6 Change the **Type** to **https**.

By default, system will select the port number as 443. The default port number can be changed, if required.



Add Site Binding

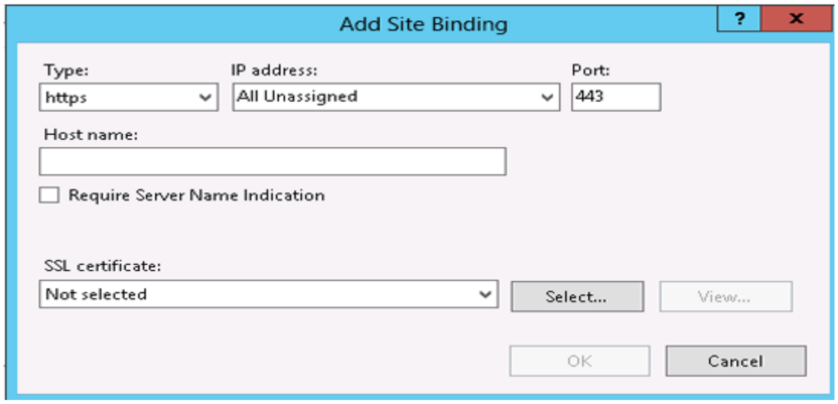
Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: Not selected



Add Site Binding

Type: https

IP address: All Unassigned

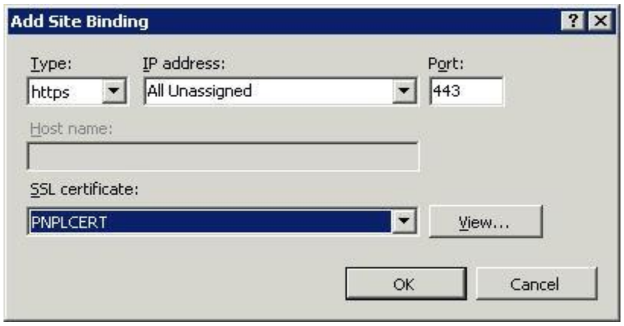
Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: Not selected

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



Add Site Binding

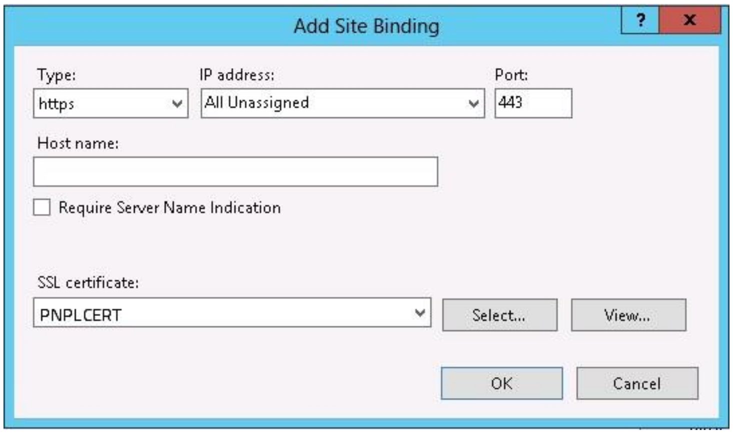
Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: PNPLCERT



Type: https

IP address: All Unassigned

Port: 443

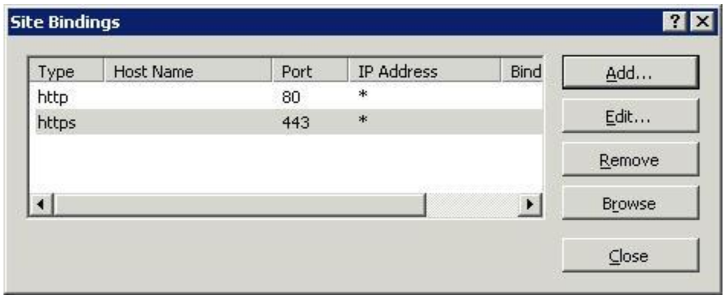
Host name:

□ Require Server Name Indication

SSL certificate: PNPLCERT

8 Click **OK**.

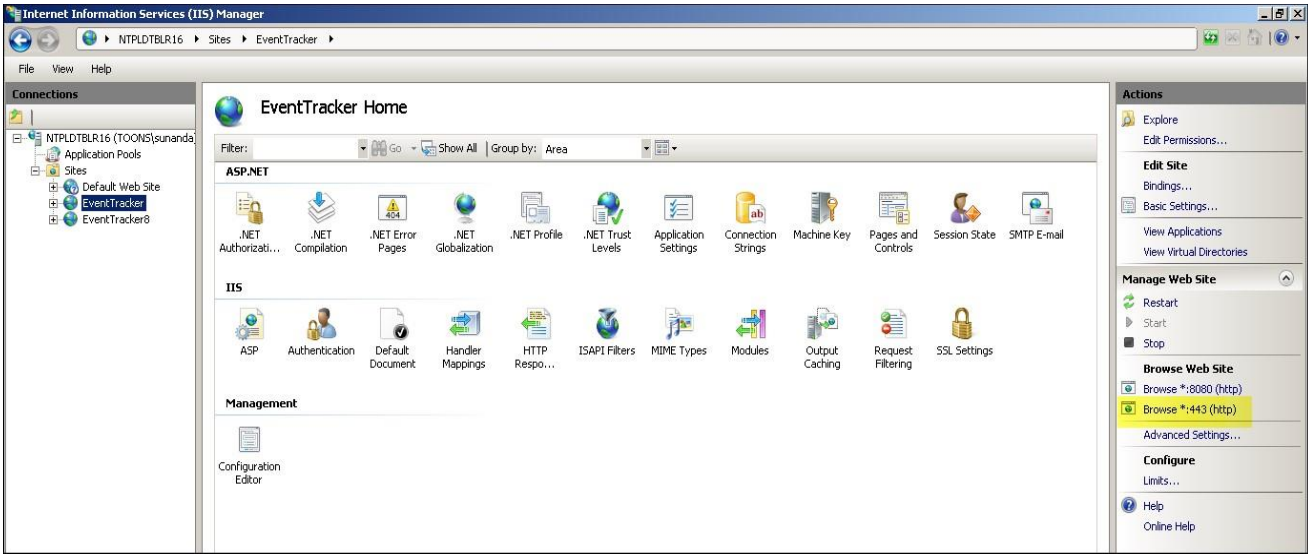
The binding for port 443 is listed.



Type	Host Name	Port	IP Address	Bind
http		80	*	
https		443	*	

9 Click **Close**.

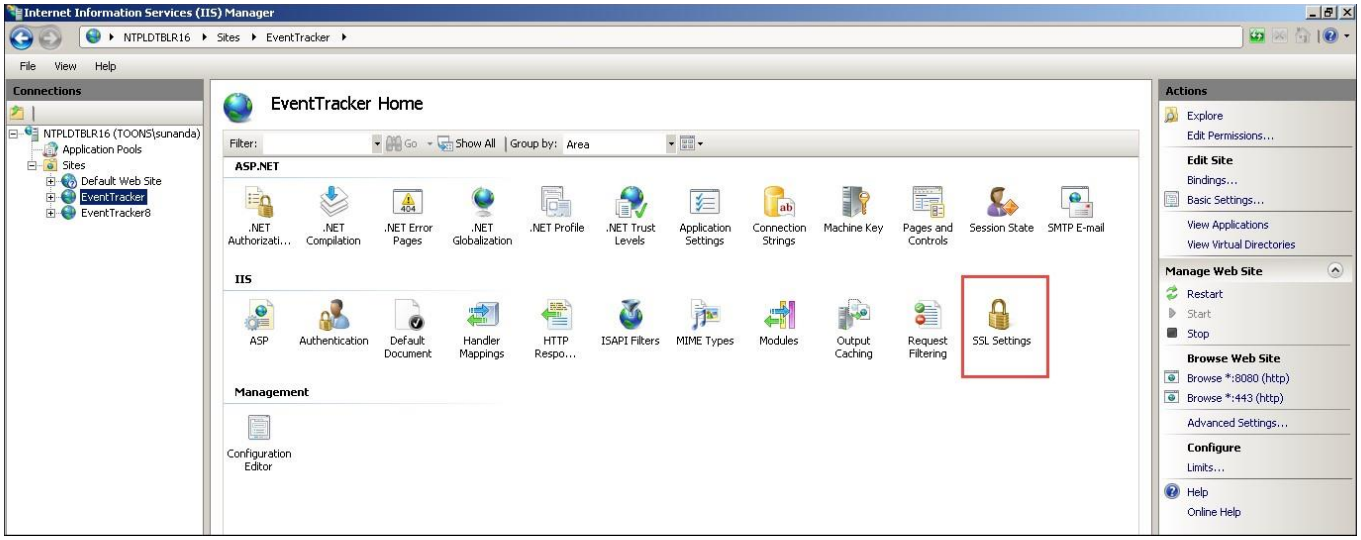
Newly added https website is listed under **Browse Web Site**.



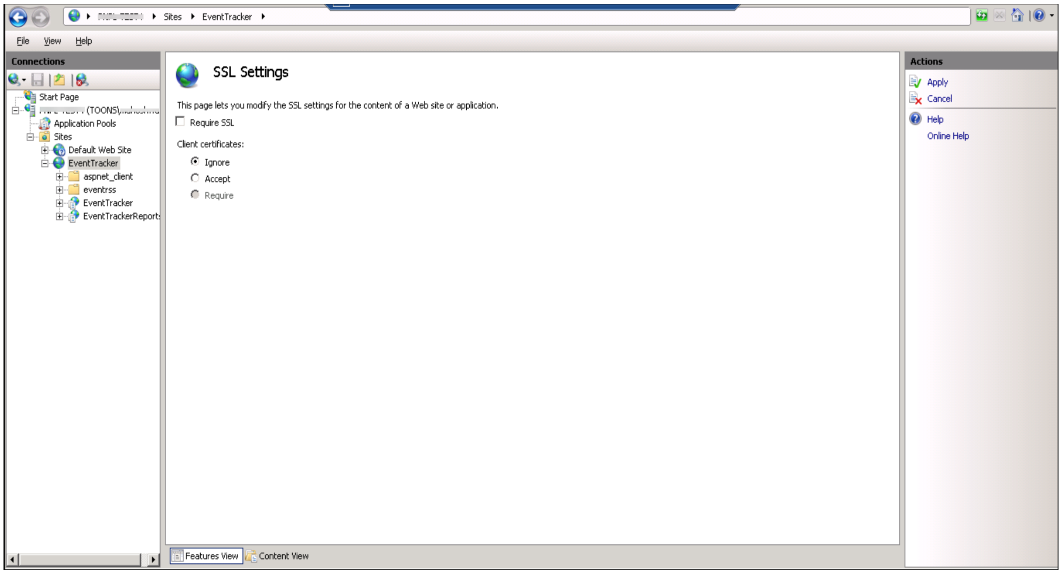
Step 4: Configure 'SSL Settings'

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

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



SSL Settings displays in the middle pane.



This page lets you modify the SSL settings for the content of a Web site or application.

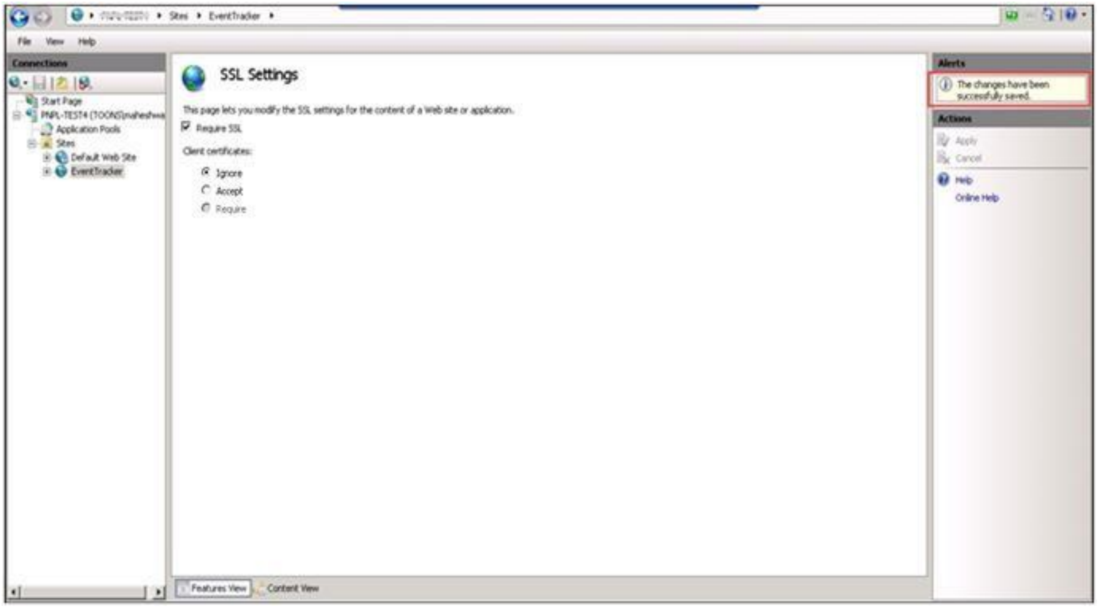
□ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

4. Check the **Require SSL** option.
5. In the **Actions** pane, click **Apply**.

   After successful SSL settings modification, a message will be displayed in the **Alerts** pane.



SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

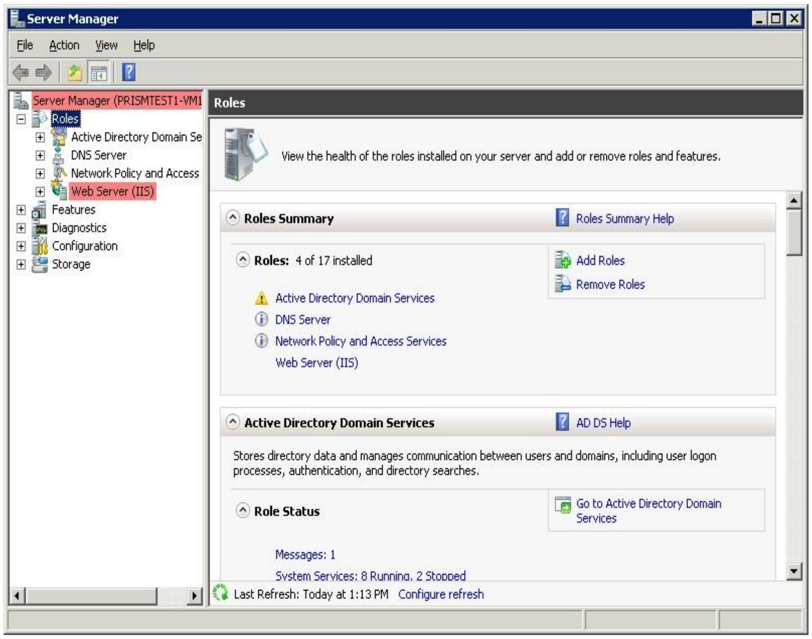
The changes have been successfully saved.

5 Close the **IIS Manager**.

Step 5: Create FTP service

NOTE: Follow step 5 and step 6 only to transfer the custom logs from remote server to the EventTracker server.

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



Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 4 of 17 installed

Active Directory Domain Services
DNS Server
Network Policy and Access Services
Web Server (IIS)

Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

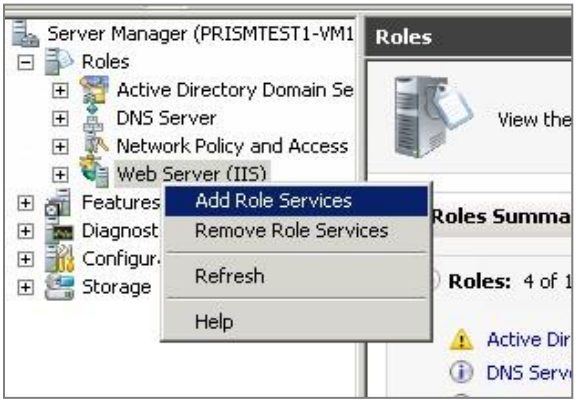
Messages: 1

System Services: 8 Running, 2 Stopped

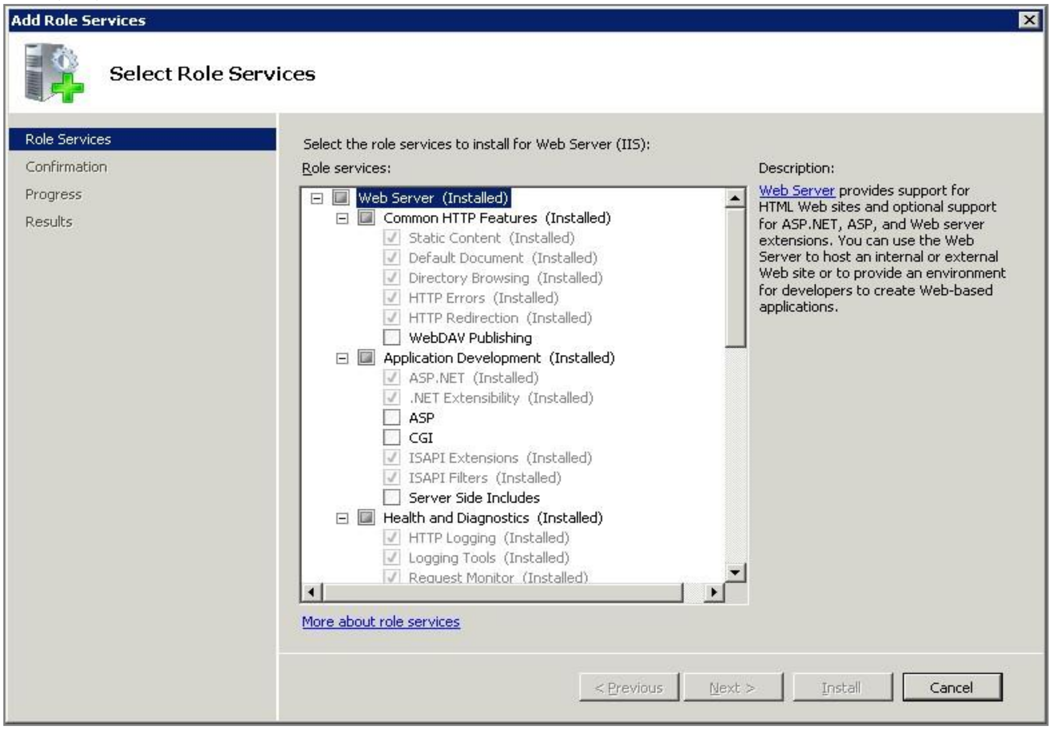
Last Refresh: Today at 1:13 PM

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

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



Server Manager displays **Add Roles Services** wizard.



Select the role services to install for Web Server (IIS):

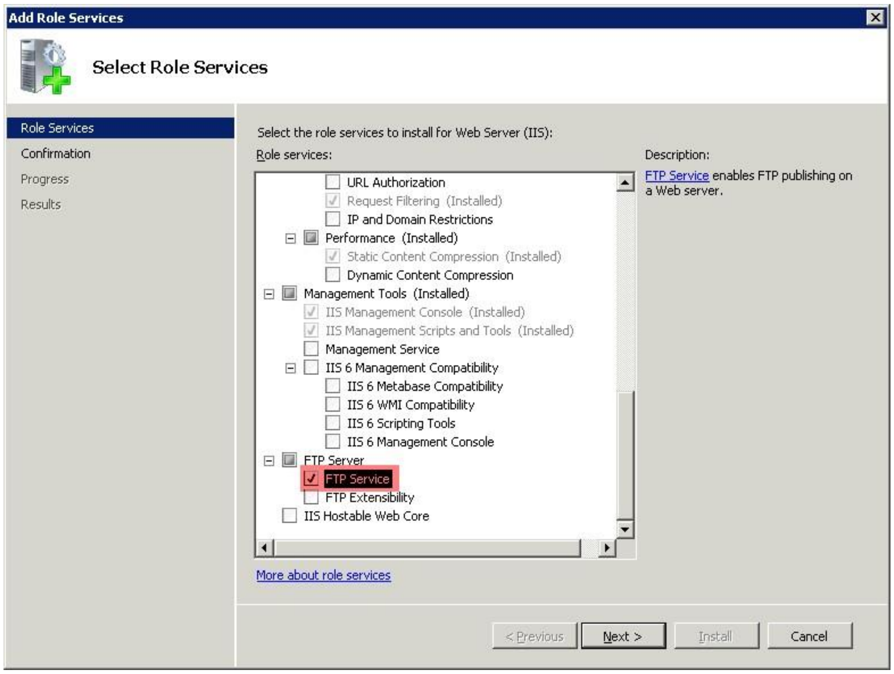
Role services:

- ☑ Web Server (Installed)
  - ☑ Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - ☑ HTTP Redirection (Installed)
    - □ WebDAV Publishing
  - ☑ Application Development (Installed)
    - ☑ ASP.NET (Installed)
    - ☑ .NET Extensibility (Installed)
    - □ ASP
    - □ CGI
    - ☑ ISAPI Extensions (Installed)
    - ☑ ISAPI Filters (Installed)
    - □ Server Side Includes
  - ☑ Health and Diagnostics (Installed)
    - ☑ HTTP Logging (Installed)
    - ☑ Logging Tools (Installed)
    - ☑ Request Monitor (Installed)

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

5. In the **Roles Services** pane, check **FTP service** option, and then click **Next >**.



Add Role Services

Select Role Services

- Role Services
- Confirmation
- Progress
- Results

Select the role services to install for Web Server (IIS):

Role services:

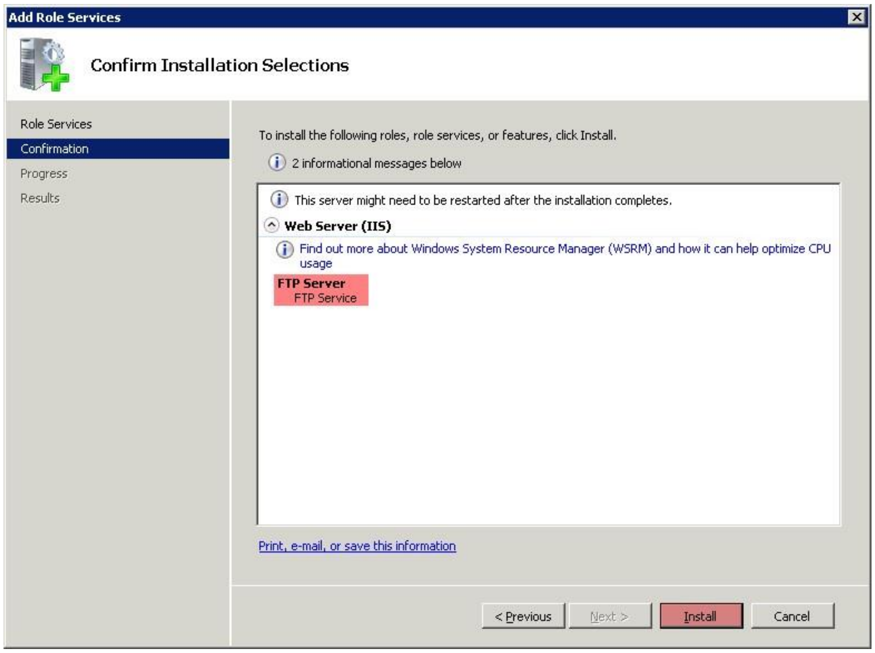
☐ URL Authorization
☑ Request Filtering (Installed)
☐ IP and Domain Restrictions
▣ Performance (Installed)
☑ Static Content Compression (Installed)
☐ Dynamic Content Compression
▣ Management Tools (Installed)
☑ IIS Management Console (Installed)
☑ IIS Management Scripts and Tools (Installed)
☐ Management Service
☐ IIS 6 Management Compatibility
☐ IIS 6 Metabase Compatibility
☐ IIS 6 WMI Compatibility
☐ IIS 6 Scripting Tools
☐ IIS 6 Management Console
▣ FTP Server
☑ FTP Service
☐ FTP Extensibility
☐ IIS Hostable Web Core

Description:

FTP Service enables FTP publishing on a Web server.

More about role services

6. In the **Confirmation** page, click the **Install** button.



Add Role Services

Confirm Installation Selections

- Role Services
- Confirmation
- Progress
- Results

To install the following roles, role services, or features, click Install.

ⓘ 2 informational messages below

ⓘ This server might need to be restarted after the installation completes.

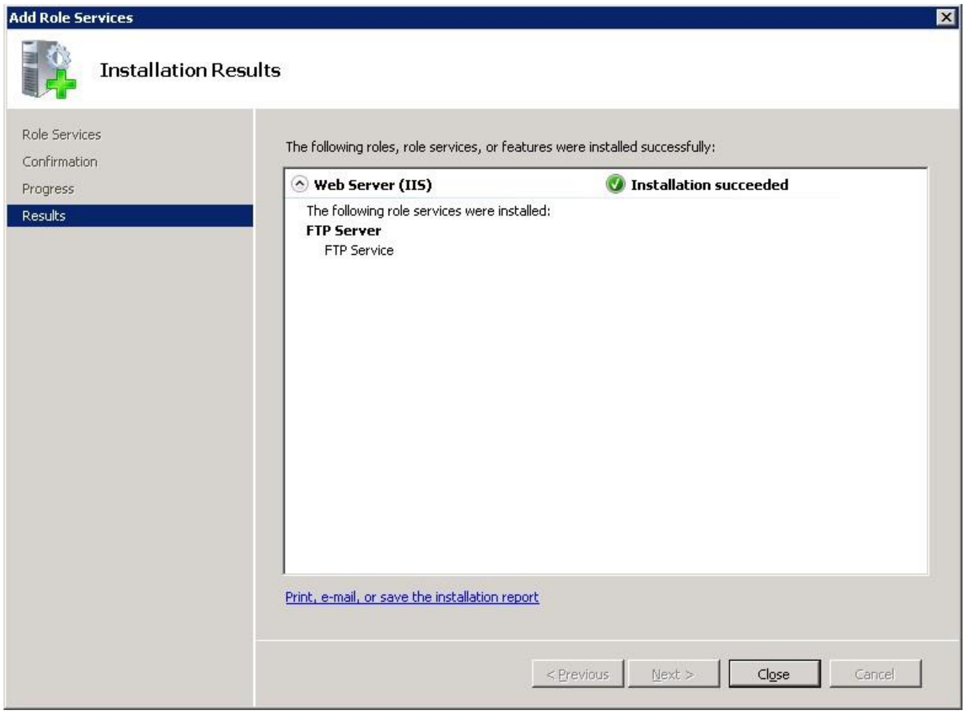
Web Server (IIS)

ⓘ Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

FTP Server
FTP Service

Print, e-mail, or save this information

7. Click the **Close** button after 'Installation Succeeded' message appears on the **Results** page.



The following roles, role services, or features were installed successfully:

Web Server (IIS) ✓ **Installation succeeded**

The following role services were installed:
FTP Server
FTP Service

Step 6: Create an SSL-enabled FTP Site

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

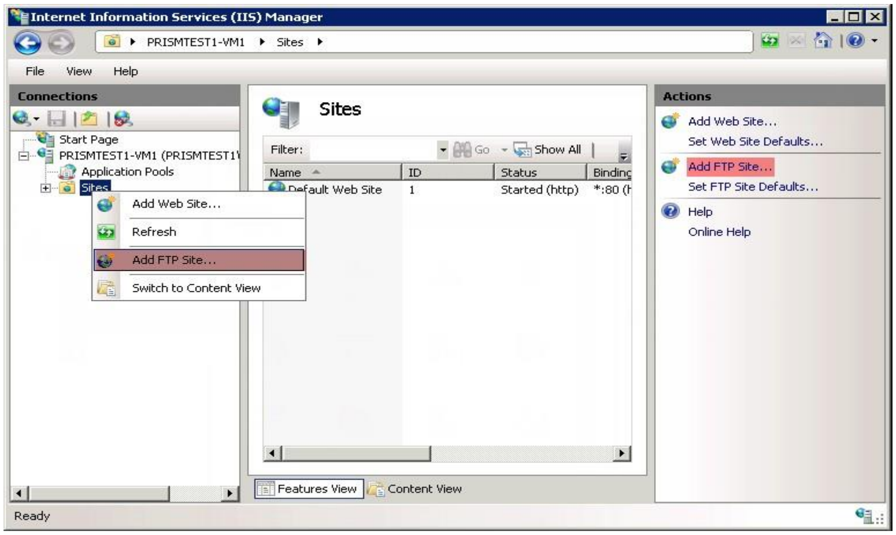
2 Select **Internet Information Services (IIS) Manager**.

3 In the **Connections** pane, select **Sites** node.

4 Right click **Sites** node, and then click **Add FTP Site.**

(OR)

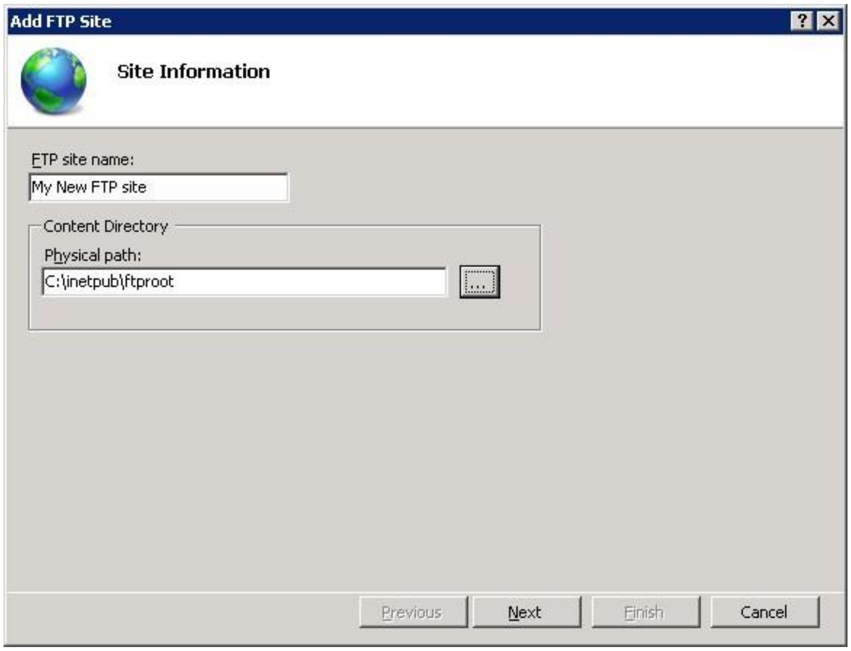
Click **Add FTP Site** in the **Actions** pane.



Name	ID	Status	Binding
Default Web Site	1	Started (http)	*:80 (h

Add FTP Site dialog box appears on the screen.

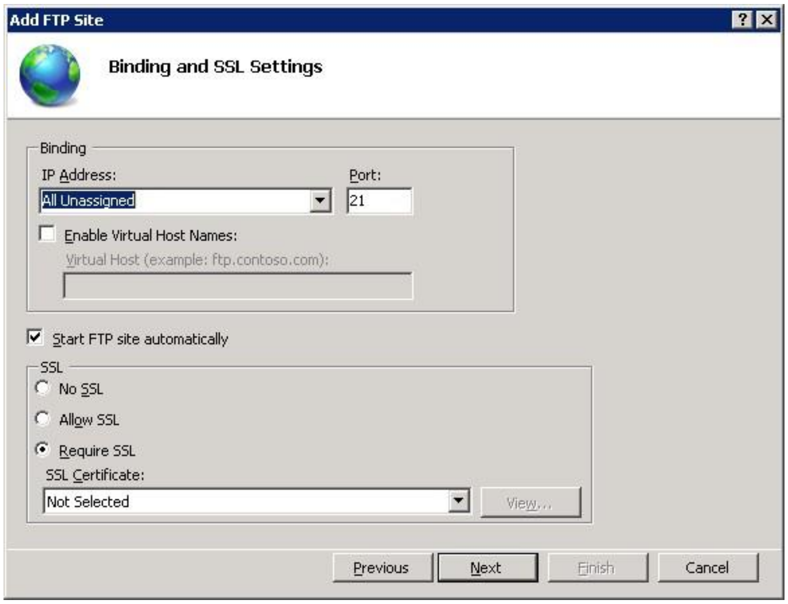
5 In **FTP site name**, type the site name as ‘My New FTP Site’, and then locate the physical path of the ftproot folder.



FTP site name:
My New FTP site

Content Directory
Physical path:
C:\inetpub\ftproot

6 Click the **Next** button.



Binding
IP Address: All Unassigned
Port: 21
☐ Enable Virtual Host Names:
Virtual Host (example: ftp.contoso.com):

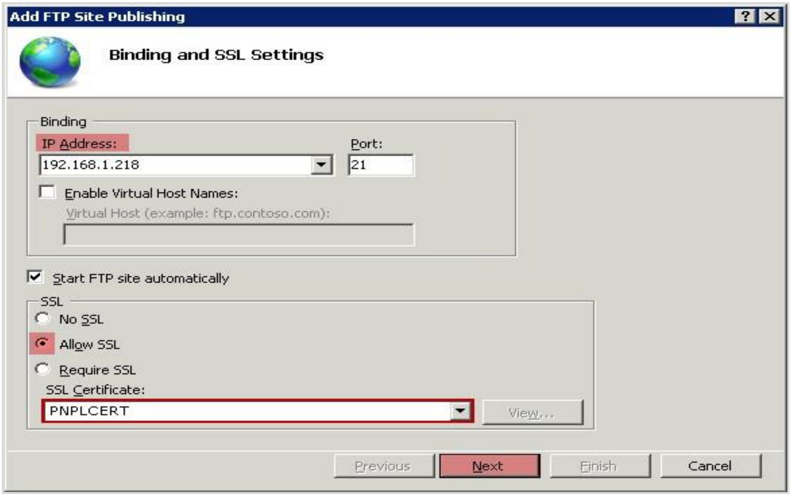
☑ Start FTP site automatically

SSL
○ No SSL
○ Allow SSL
● Require SSL
SSL Certificate:
Not Selected

7 Select a local IP address for FTP site from the **IP Address** drop-down or type 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 **Allow SSL** option, and then click the **View** button to locate the SSL certificate received by the vendor.



Add FTP Site Publishing

Binding and SSL Settings

Binding

IP Address: 192.168.1.218

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

○ No SSL

● Allow SSL

○ Require SSL

SSL Certificate: PNPLCERT

10 Click the **Next** button.

Authentication and Authorization Information page appears.

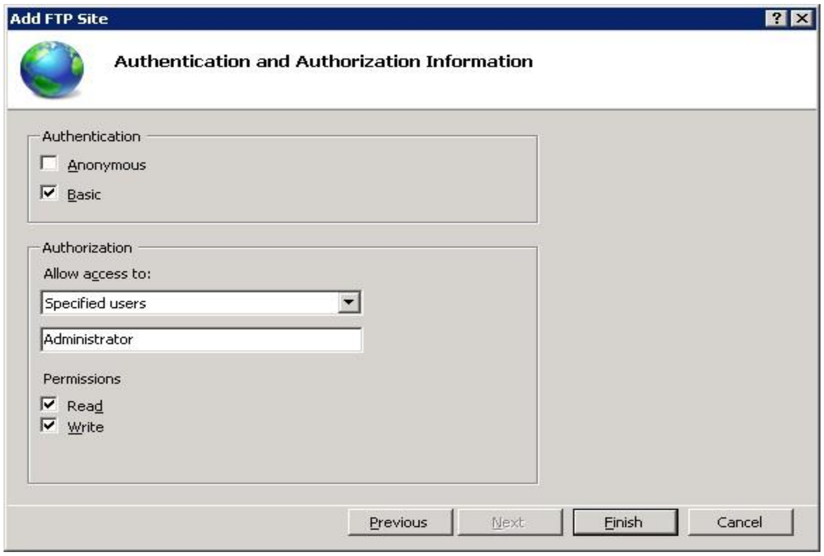
11 In the **Authentication** pane, check the **Basic** option.

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.

For example: Administrator.

14 Check **Read** and **Write** as the **Permissions** option.



Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

☑ Basic

Authorization

Allow access to: Specified users

Administrator

Permissions

☑ Read

☑ Write

15 Click the **Finish** button.

3.3 Restricting EventTracker website

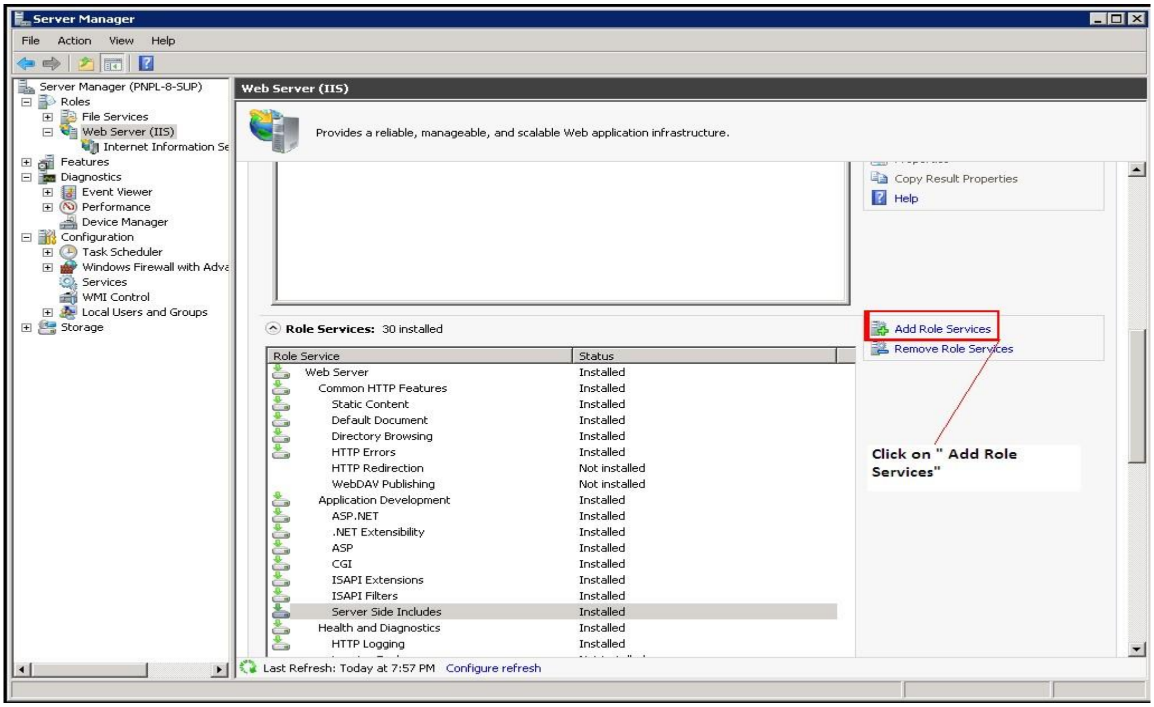
Configuring IP address and domain name restrictions in Internet Information Services (IIS) allows you to permit or deny access to the web server, web sites, folders, or files. Rules can be configured for remote IP addresses or based on the Domain name.

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 IP and Domain Restrictions option by adding the above Role Service as mentioned below.

3.4 Installing IP and Domain Restriction in Windows 2K8, 2K8 R2, 2012, 2016, 2019

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



Provides a reliable, manageable, and scalable Web application infrastructure.

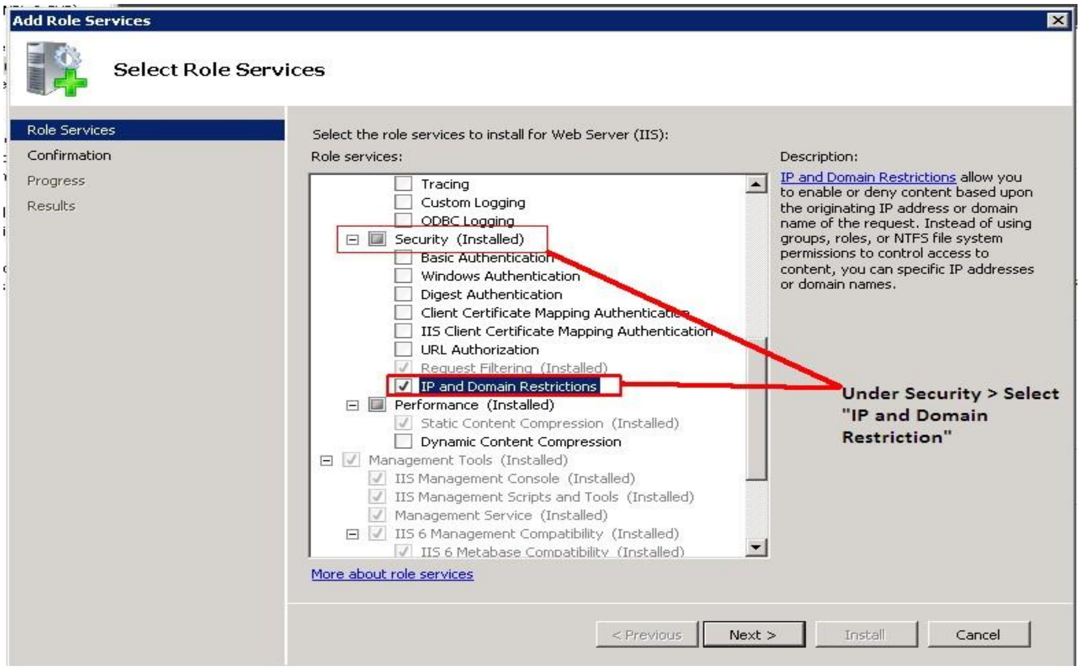
Role Services: 30 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Not installed
WebDAV Publishing	Not installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Installed
CGI	Installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Installed
Health and Diagnostics	Installed
HTTP Logging	Installed

Click on " Add Role Services"

Last Refresh: Today at 7:57 PM

4. In “Security’, select ‘**IP and Domain Restrictions’**, and then select **Next>.**



Add Role Services

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ☐ Tracing
- ☐ Custom Logging
- ☐ ODBC Logging
- ⊟ ▣ Security (Installed)
  - ☐ Basic Authentication
  - ☐ Windows Authentication
  - ☐ Digest Authentication
  - ☐ Client Certificate Mapping Authentication
  - ☐ IIS Client Certificate Mapping Authentication
  - ☐ URL Authorization
  - ☑ Request Filtering (Installed)
  - ☑ IP and Domain Restrictions
- ⊟ ▣ Performance (Installed)
  - ☑ Static Content Compression (Installed)
  - ☐ Dynamic Content Compression
- ⊟ ☑ Management Tools (Installed)
  - ☑ IIS Management Console (Installed)
  - ☑ IIS Management Scripts and Tools (Installed)
  - ☑ Management Service (Installed)
  - ⊟ ☑ IIS 6 Management Compatibility (Installed)
    - ☑ IIS 6 Metabase Compatibility (Installed)

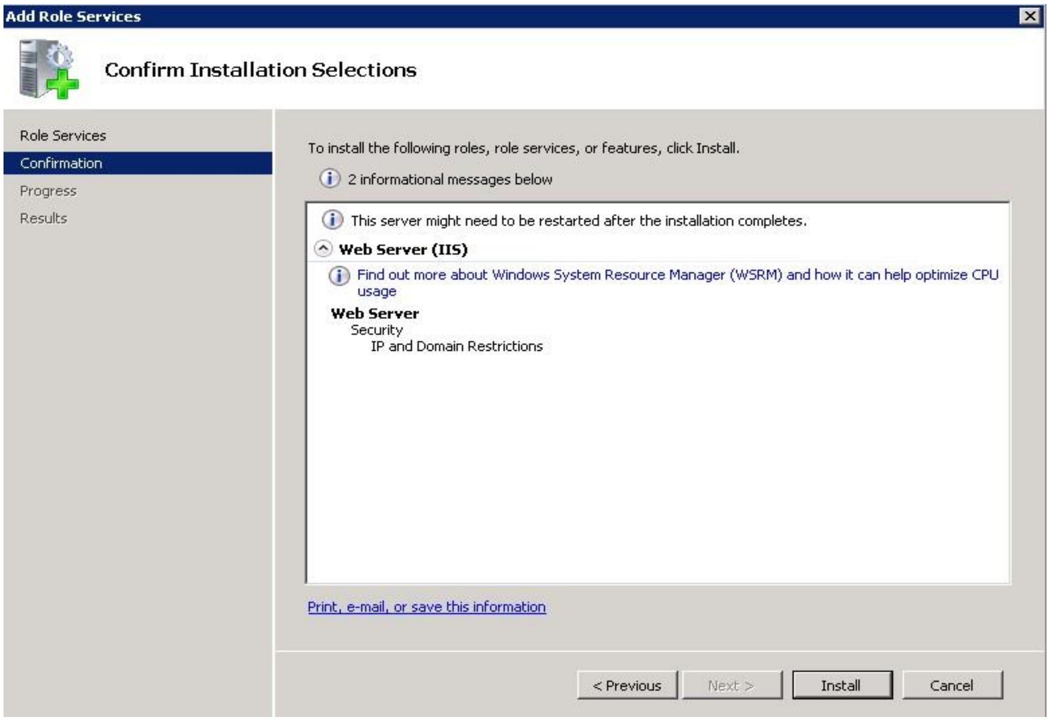
Description:

IP and Domain Restrictions allow you to enable or deny content based upon the originating IP address or domain name of the request. Instead of using groups, roles, or NTFS file system permissions to control access to content, you can specific IP addresses or domain names.

Under Security > Select "IP and Domain Restriction"

More about role services

5. Click the **Install** button.



Add Role Services

Confirm Installation Selections

To install the following roles, role services, or features, click Install.

ⓘ 2 informational messages below

ⓘ This server might need to be restarted after the installation completes.

Web Server (IIS)

ⓘ Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

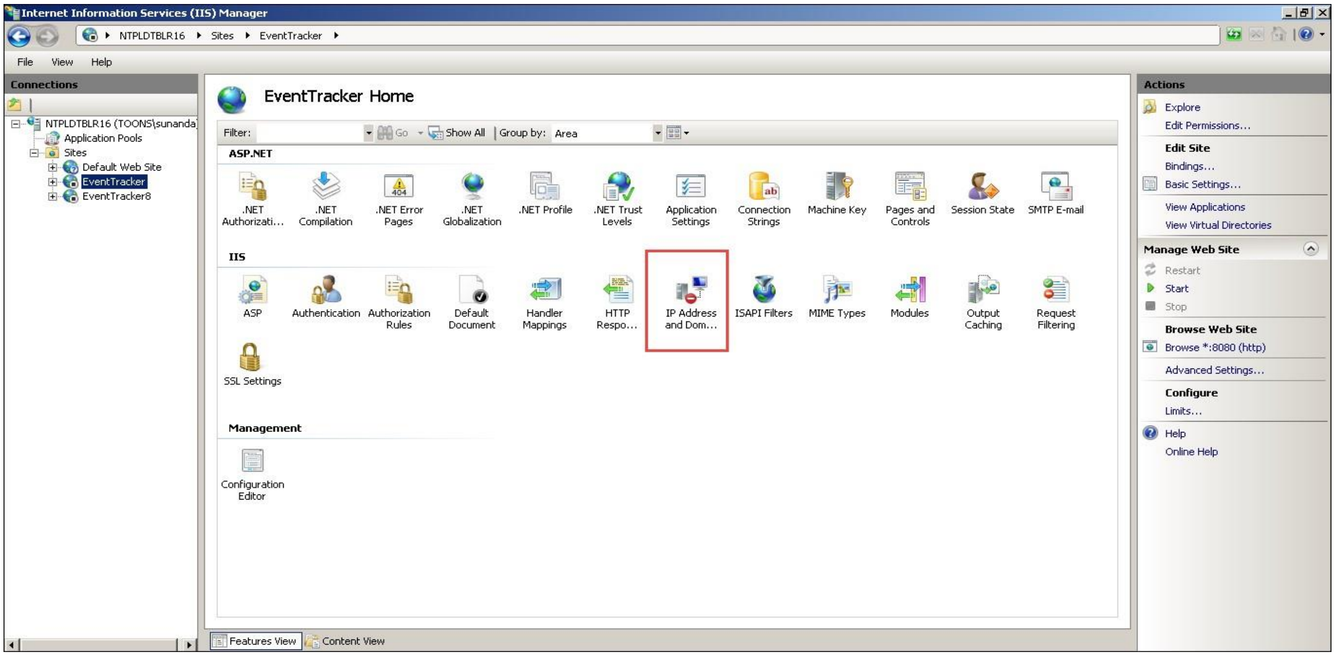
Web Server
Security
IP and Domain Restrictions

Print, e-mail, or save this information

3.5 Configuring IP Address and Domain Restrictions in Windows 2K8, 2K8 R2, 2012/ 2016/ 2019

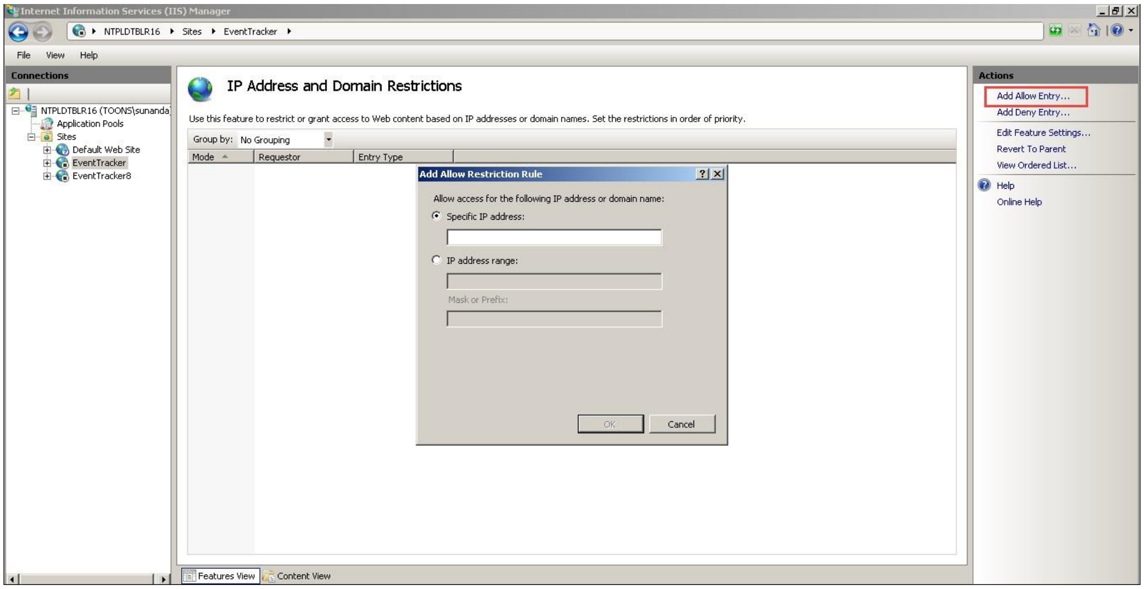
1. Open **IIS Manager**.

2. Select **EventTracker** site**.**

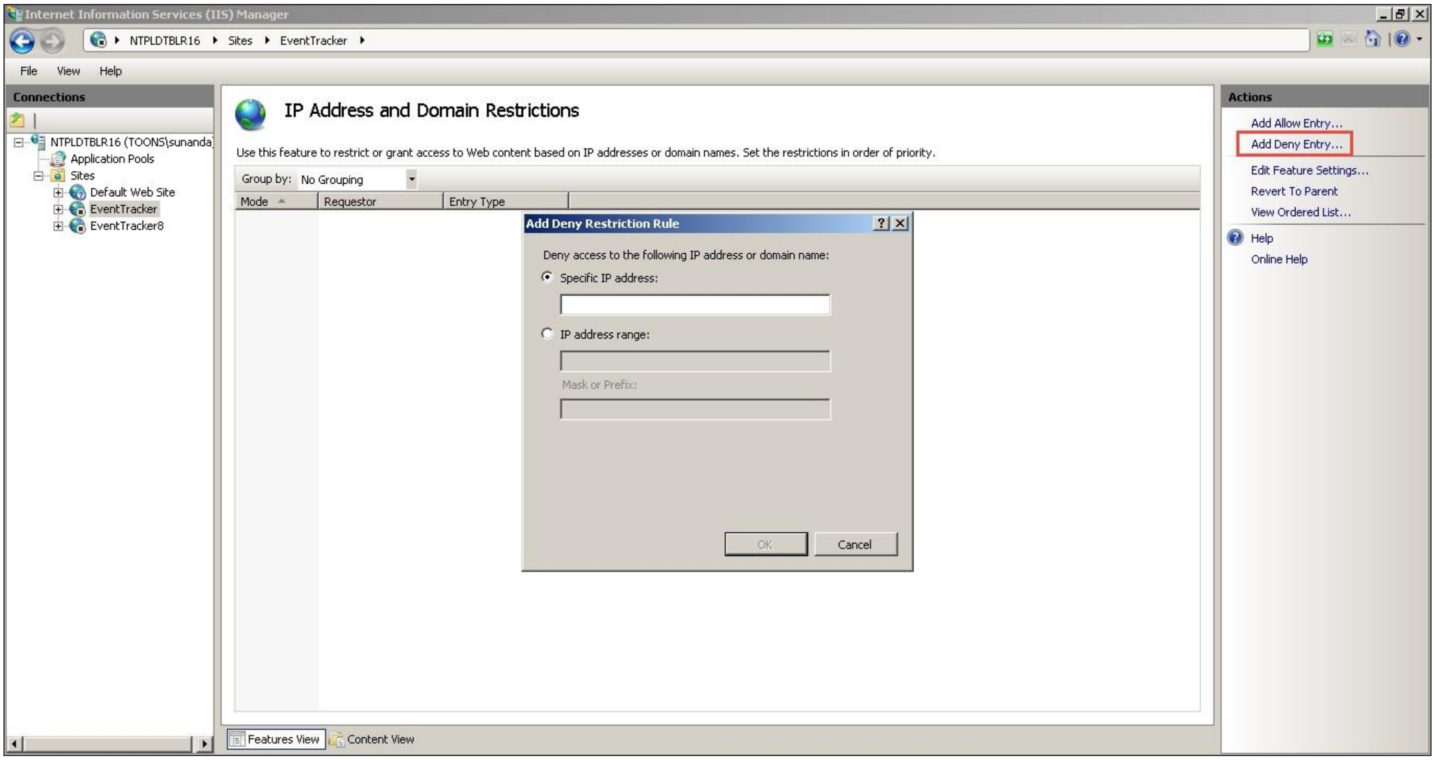


3. In **Features View**, double-click **IP Address and Domain Restrictions**.

4. In **Actions** pane, select "**Add Allow Entry**" or "**Add Deny Entry**" to add Allow or Deny entries.


Internet Information Services (IIS) Manager
NTPLDTBLR16 ▸ Sites ▸ EventTracker ▸
File View Help
Connections
NTPLDTBLR16 (TOONS\sunanda)
Application Pools
Sites
Default Web Site
EventTracker
EventTracker8
IP Address and Domain Restrictions
Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.
Group by: No Grouping
Mode
Requestor
Entry Type
Add Allow Restriction Rule
Allow access for the following IP address or domain name:
Specific IP address:
IP address range:
Mask or Prefix:
OK
Cancel
Features View
Content View
Actions
Add Allow Entry...
Add Deny Entry...
Edit Feature Settings...
Revert To Parent
View Ordered List...
Help
Online Help

(OR)



Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Deny access to the following IP address or domain name:

You can specify an IP address or an IP address range or a Domain Name in above dialog boxes.

NOTE:

Configuring Allow or Deny restrictions using Domain name require 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 Requesting Filtering in IIS 7, 7.5, 8, 8.5 and 10

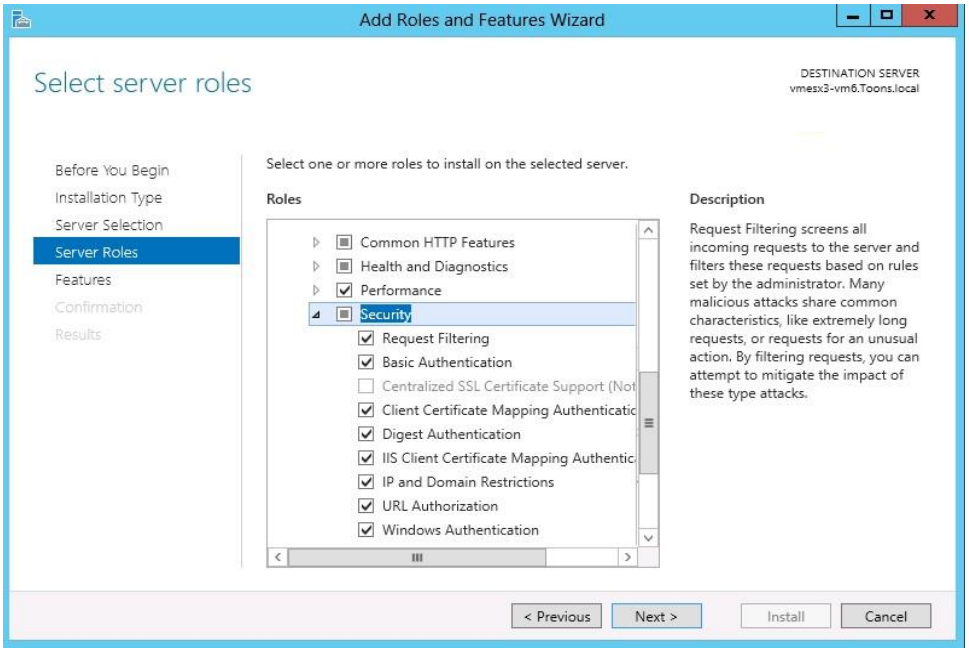
3.6.1 Installing Request Filtering in Windows 2012/ 2016/ 2019

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**, **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 **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 **Security** node, and then select **Request Filtering**, and then click **Next >**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
vmesx3-vm6.Toons.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- ▷ ■ Common HTTP Features
- ▷ ■ Health and Diagnostics
- ▷ ☑ Performance
- ◢ ■ Security
  - ☑ Request Filtering
  - ☑ Basic Authentication
  - □ Centralized SSL Certificate Support (Not
  - ☑ Client Certificate Mapping Authenticatic
  - ☑ Digest Authentication
  - ☑ IIS Client Certificate Mapping Authentic
  - ☑ IP and Domain Restrictions
  - ☑ URL Authorization
  - ☑ Windows Authentication

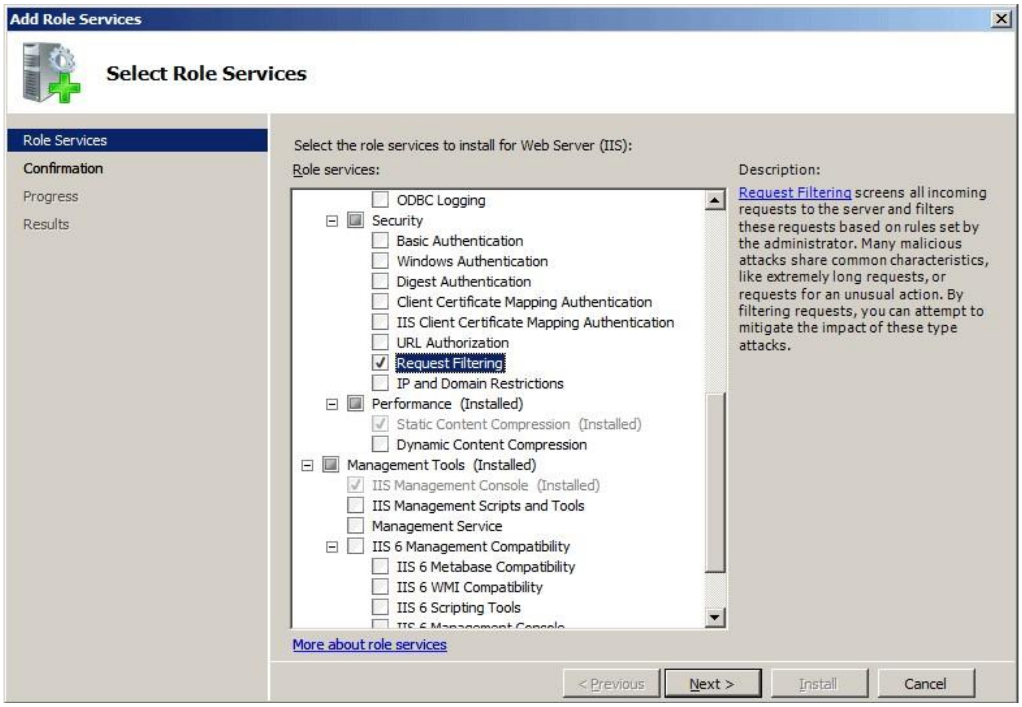
Description

Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, like extremely long requests, or requests for an unusual action. By filtering requests, you can attempt to mitigate the impact of these type attacks.

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

3.6.2 Installing Request Filtering in Windows 2K8 / 2K8 R2/ 2016/ 2019

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 >**.



Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ☐ ODBC Logging
- ⊟ ▣ Security
  - ☐ Basic Authentication
  - ☐ Windows Authentication
  - ☐ Digest Authentication
  - ☐ Client Certificate Mapping Authentication
  - ☐ IIS Client Certificate Mapping Authentication
  - ☐ URL Authorization
  - ☑ Request Filtering
  - ☐ IP and Domain Restrictions
- ⊟ ▣ Performance (Installed)
  - ☑ Static Content Compression (Installed)
  - ☐ Dynamic Content Compression
- ⊟ ▣ Management Tools (Installed)
  - ☑ IIS Management Console (Installed)
  - ☐ IIS Management Scripts and Tools
  - ☐ Management Service
  - ⊟ ☐ IIS 6 Management Compatibility
    - ☐ IIS 6 Metabase Compatibility
    - ☐ IIS 6 WMI Compatibility
    - ☐ IIS 6 Scripting Tools
    - ☐ IIS 6 Management Console

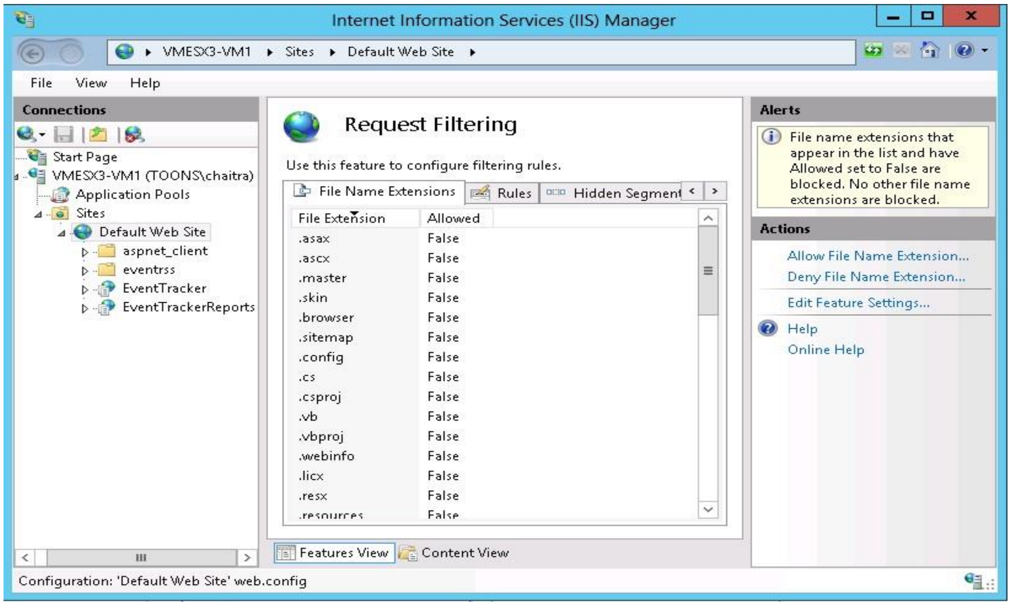
Description:

Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, like extremely long requests, or requests for an unusual action. By filtering requests, you can attempt to mitigate the impact of these type attacks.

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**:
   - o If you are using Windows Server 2008 / 2008 R2 / 2012 /2016/ 2019 :
     - ✦ 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...**.



Request Filtering

Use this feature to configure filtering rules.

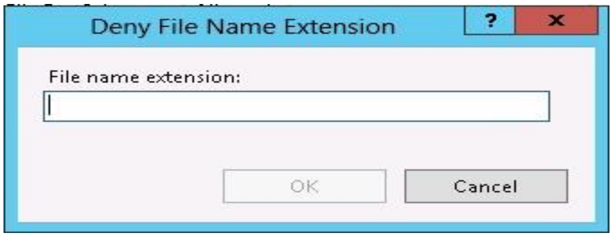
File Extension	Allowed
.asax	False
.ascx	False
.master	False
.skin	False
.browser	False
.sitemap	False
.config	False
.cs	False
.csproj	False
.vb	False
.vbproj	False
.webinfo	False
.licx	False
.resx	False
.resources	False

File name extensions that appear in the list and have Allowed set to False are blocked. No other file name extensions are blocked.

Configuration: 'Default Web Site' web.config

Deny File Name Extension dialog box displays.

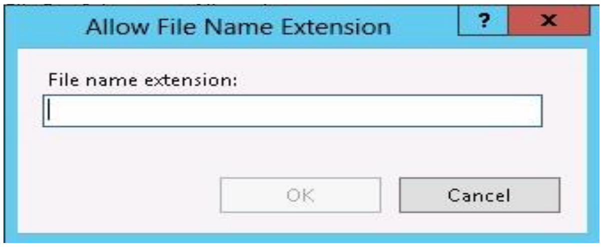
6. Enter the file name extension that you want to block and click **OK**.



File name extension:

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

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



File name extension:

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

4. Securing SQL Database Server - SQL Server 2008 / 2008 R2 / 2012 / 2016 / 2017

4.1 Reducing the Surface Area for SQL Server Components

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

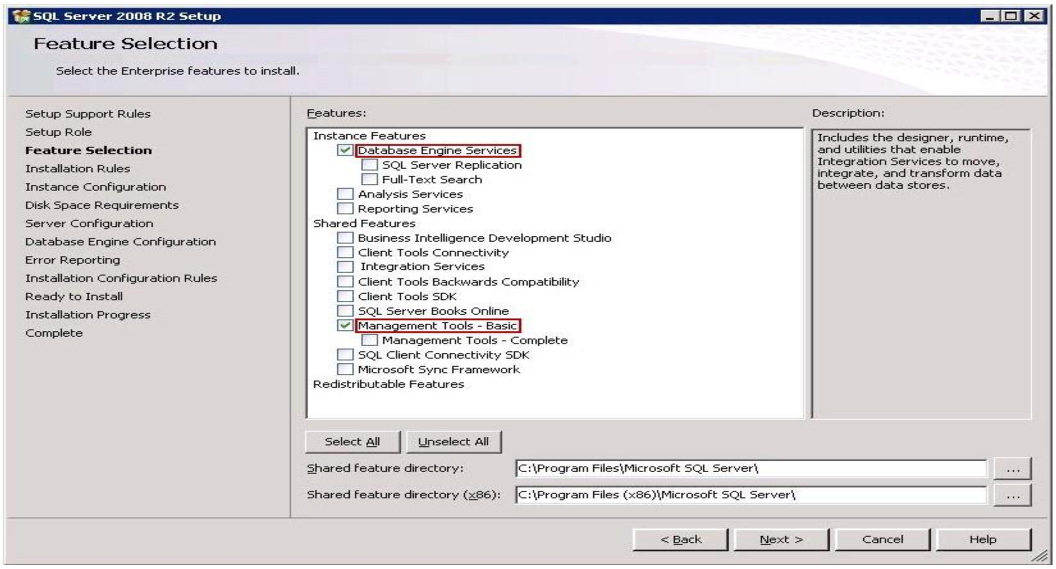
1. **Install only the required SQL Server components.**

   While installing SQL Server, do not include 'Analysis Services', 'Integration Services', and 'Full-Text' engine.

2. **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, web services opens a hole in the security layer.

3. **Install only two features, 'Database Engine Services' and 'Management Tools – Basic'.**



SQL Server 2008 R2 Setup

Feature Selection

Select the Enterprise features to install.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication
  - ☐ Full-Text Search
- ☐ Analysis Services
- ☐ Reporting Services

Shared Features
- ☐ Business Intelligence Development Studio
- ☐ Client Tools Connectivity
- ☐ Integration Services
- ☐ Client Tools Backwards Compatibility
- ☐ Client Tools SDK
- ☐ SQL Server Books Online
- ☑ Management Tools - Basic
  - ☐ Management Tools - Complete
- ☐ SQL Client Connectivity SDK
- ☐ Microsoft Sync Framework

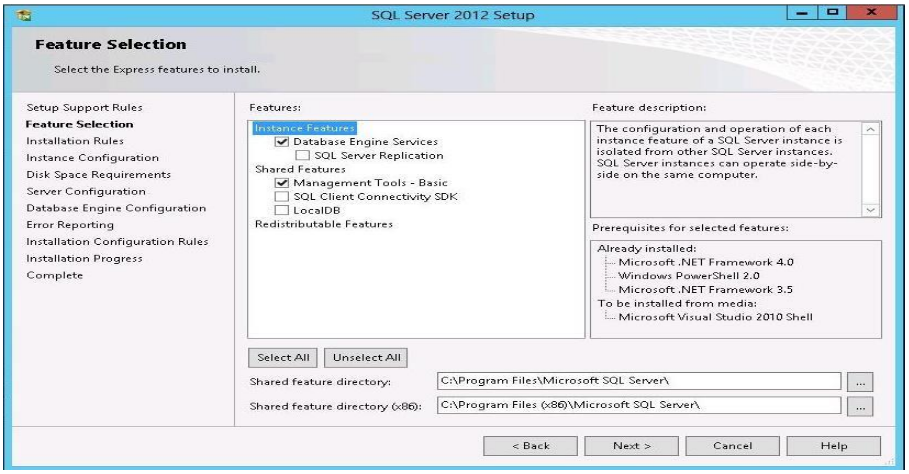
Redistributable Features

Description:

Includes the designer, runtime, and utilities that enable Integration Services to move, integrate, and transform data between data stores.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\



SQL Server 2012 Setup

Feature Selection

Select the Express features to install.

Setup Support Rules
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication

Shared Features
- ☑ Management Tools - Basic
- ☐ SQL Client Connectivity SDK
- ☐ LocalDB

Redistributable Features

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

Prerequisites for selected features:

Already installed:
- Microsoft .NET Framework 4.0
- Windows PowerShell 2.0
- Microsoft .NET Framework 3.5

To be installed from media:
- Microsoft Visual Studio 2010 Shell

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

4. **Disable the following SQL Server services.**

   Disable (or leave disabled) the following services.

   - **SQL Server VSS Writer** service.
   - **SQL Server Browser**.
   - **SQL Active Directory Helper** service.

   Click here for the detailed instruction on how to disable the SQL server services.

5. **Ensure the latest antivirus is configured correctly.**

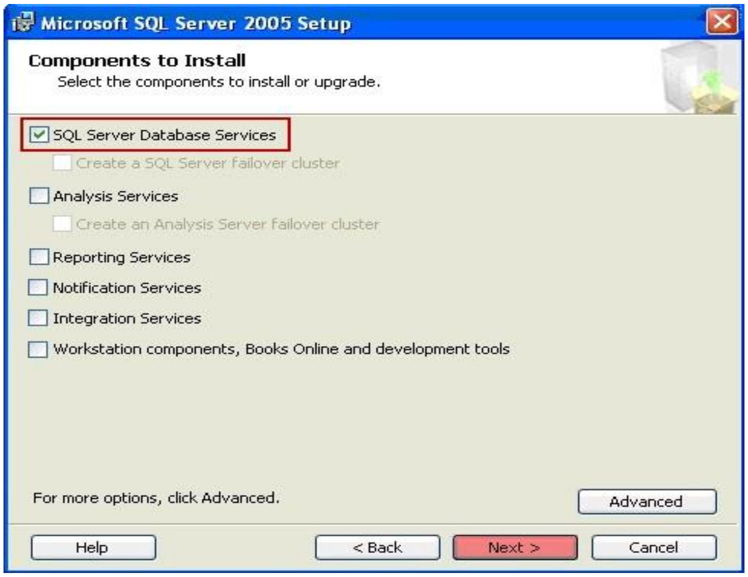
6. **Install the latest critical fixes and service packs for both Windows and SQL Server.**

4.2 Reducing the Surface Area for SQL Server Services

To reduce the surface area of SQL Server, 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.



Microsoft SQL Server 2005 Setup

Components to Install

Select the components to install or upgrade.

☑ SQL Server Database Services

□ Create a SQL Server failover cluster

□ Analysis Services

□ Create an Analysis Server failover cluster

□ Reporting Services

□ Notification Services

□ Integration Services

□ Workstation components, Books Online and development tools

For more options, click Advanced.

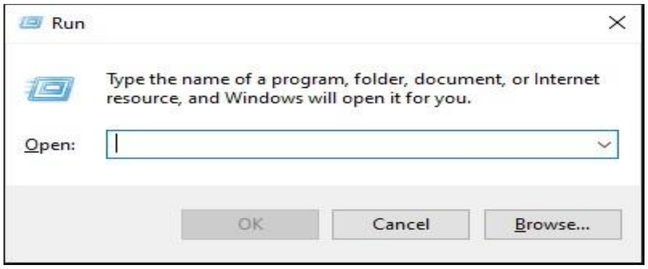
2. **Disable the following SQL Server services.**

   Disable (or leave disabled) the following services.

   - **SQL Server VSS Writer** service.
   - **SQL Active Directory Helper** service.
   - **SQL Server Browser** service.

Follow the steps given below to disable the

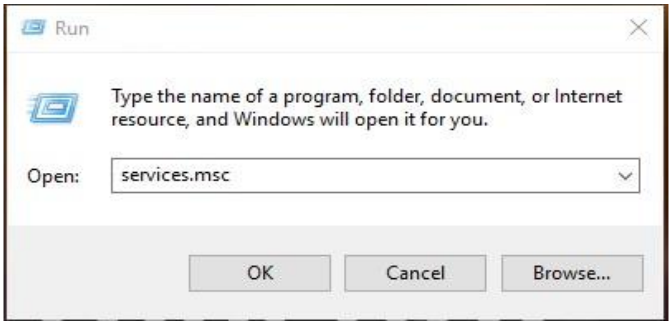
services, 1. Click **Start** button and click **Run**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

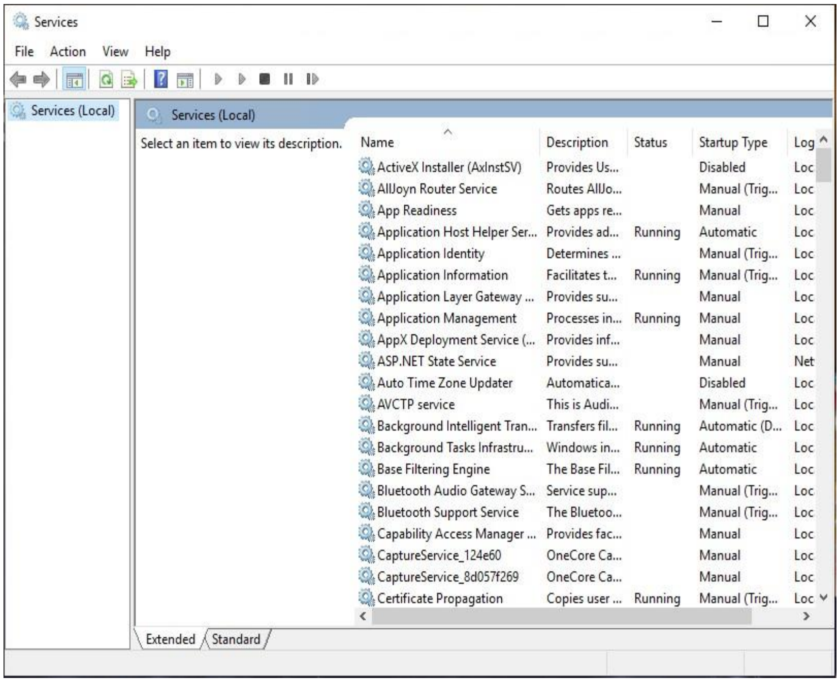
2. In the **Run** dialog box, type '**Services.msc**', and click the **OK** button.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Services window opens.



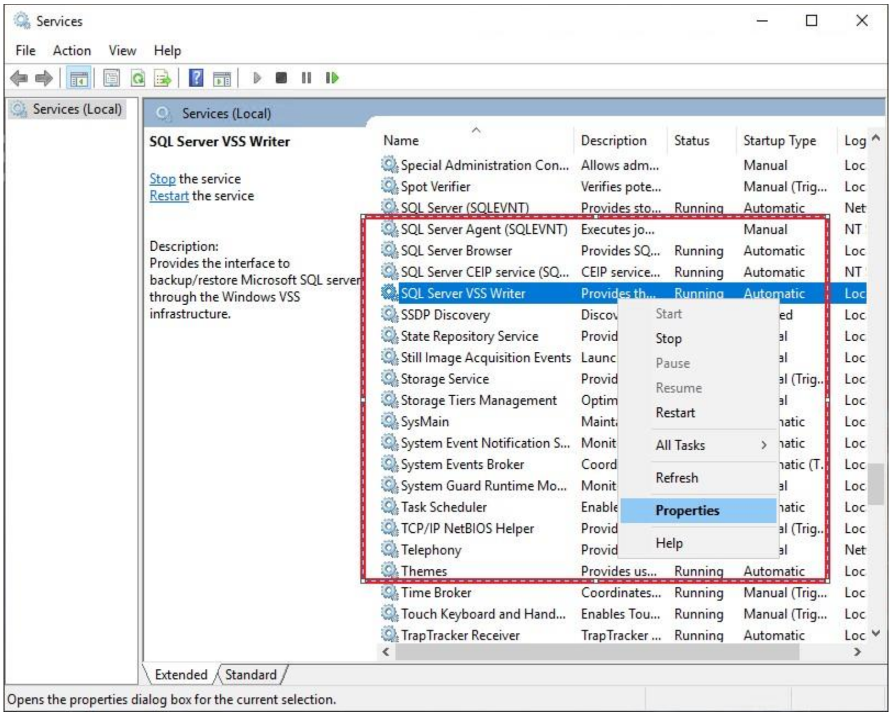
Select an item to view its description.

Name	Description	Status	Startup Type	Log
ActiveX Installer (AxInstSV)	Provides Us...		Disabled	Loc
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Host Helper Ser...	Provides ad...	Running	Automatic	Loc
Application Identity	Determines ...		Manual (Trig...	Loc
Application Information	Facilitates t...	Running	Manual (Trig...	Loc
Application Layer Gateway ...	Provides su...		Manual	Loc
Application Management	Processes in...	Running	Manual	Loc
AppX Deployment Service (...	Provides inf...		Manual	Loc
ASP.NET State Service	Provides su...		Manual	Net
Auto Time Zone Updater	Automatica...		Disabled	Loc
AVCTP service	This is Audi...		Manual (Trig...	Loc
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Loc
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Loc
Capability Access Manager ...	Provides fac...		Manual	Loc
CaptureService_124e60	OneCore Ca...		Manual	Loc
CaptureService_8d057f269	OneCore Ca...		Manual	Loc
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Loc

3. Locate the required service(s) name in the **Name** column.

For example: 'SQL Server VSS Writer' service.

4. Right click the service to be disabled and click **Properties**.



SQL Server VSS Writer

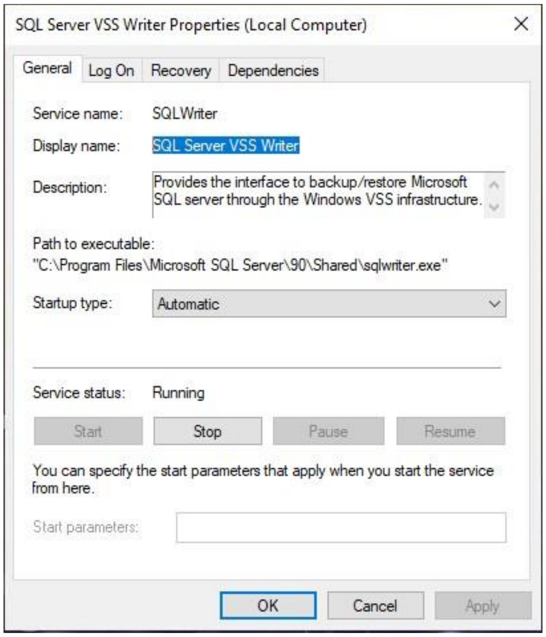
Stop the service
Restart the service

Description:
Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Name	Description	Status	Startup Type	Log
Special Administration Con...	Allows adm...		Manual	Loc
Spot Verifier	Verifies pote...		Manual (Trig...	Loc
SQL Server (SQLEVNT)	Provides sto...	Running	Automatic	Net
SQL Server Agent (SQLEVNT)	Executes jo...		Manual	NT
SQL Server Browser	Provides SQ...	Running	Automatic	Loc
SQL Server CEIP service (SQ...	CEIP service...	Running	Automatic	NT
SQL Server VSS Writer	Provides th...	Running	Automatic	Loc
SSDP Discovery	Discov		ed	Loc
State Repository Service	Provid		al	Loc
Still Image Acquisition Events	Launc		al	Loc
Storage Service	Provid		al (Trig...	Loc
Storage Tiers Management	Optim		al	Loc
SysMain	Maint		natic	Loc
System Event Notification S...	Monit		natic	Loc
System Events Broker	Coord		natic (T...	Loc
System Guard Runtime Mo...	Monit		al	Loc
Task Scheduler	Enable		natic	Loc
TCP/IP NetBIOS Helper	Provid		al (Trig...	Loc
Telephony	Provid		al	Net
Themes	Provides us...	Running	Automatic	Loc
Time Broker	Coordinates...	Running	Manual (Trig...	Loc
Touch Keyboard and Hand...	Enables Tou...	Running	Manual (Trig...	Loc
TrapTracker Receiver	TrapTracker ...	Running	Automatic	Loc

Opens the properties dialog box for the current selection.

SQL Server VSS Writer Properties (Local Computer) dialog box appears.



Service name: SQLWriter

Display name: SQL Server VSS Writer

Description: Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Path to executable:
"C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"

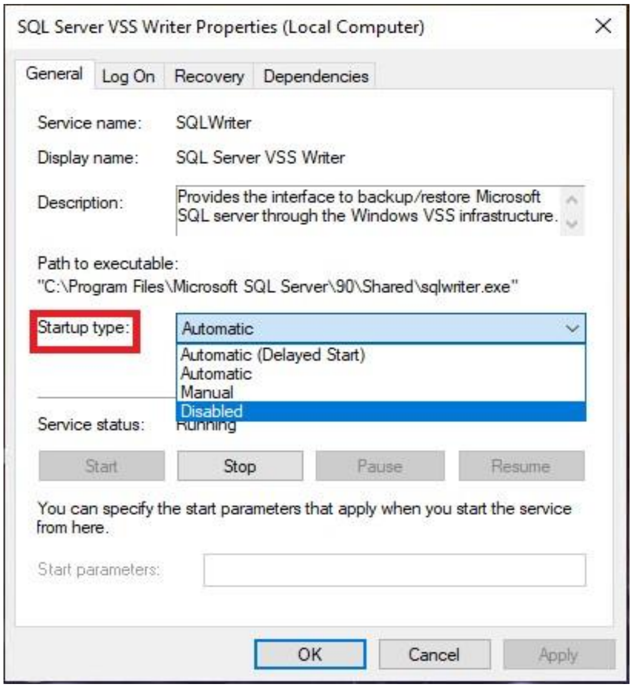
Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

5. Click **Startup type** dropdown and select **'Disabled'**.



Service name: SQLWriter

Display name: SQL Server VSS Writer

Description: Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Path to executable:
"C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"

Startup type: Automatic

- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled

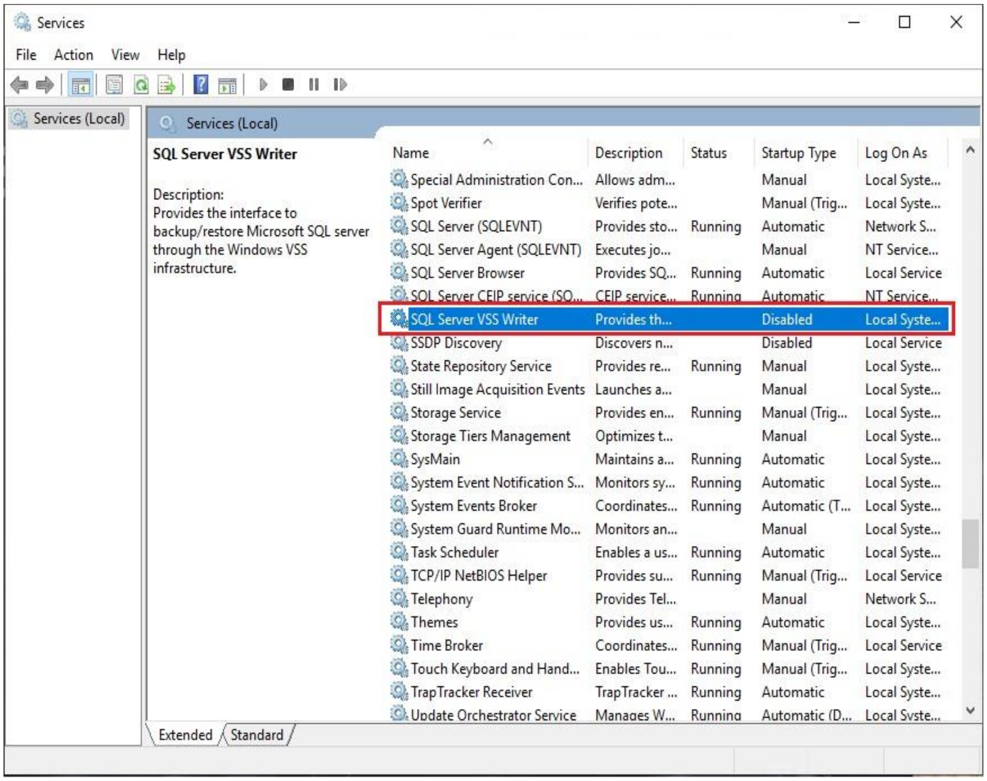
Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6. Click the **Stop** button to stop the service.

7. Click the **Apply** button and click the **OK** button.



SQL Server VSS Writer

Description:
Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Name	Description	Status	Startup Type	Log On As
Special Administration Con...	Allows adm...		Manual	Local Syste...
Spot Verifier	Verifies pote...		Manual (Trig...	Local Syste...
SQL Server (SQLEVNT)	Provides sto...	Running	Automatic	Network S...
SQL Server Agent (SQLEVNT)	Executes jo...		Manual	NT Service...
SQL Server Browser	Provides SQ...	Running	Automatic	Local Service
SQL Server CEIP service (SQ...	CEIP service...	Running	Automatic	NT Service...
SQL Server VSS Writer	Provides th...		Disabled	Local Syste...
SSDP Discovery	Discovers n...		Disabled	Local Service
State Repository Service	Provides re...	Running	Manual	Local Syste...
Still Image Acquisition Events	Launches a...		Manual	Local Syste...
Storage Service	Provides en...	Running	Manual (Trig...	Local Syste...
Storage Tiers Management	Optimizes t...		Manual	Local Syste...
SysMain	Maintains a...	Running	Automatic	Local Syste...
System Event Notification S...	Monitors sy...	Running	Automatic	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...
System Guard Runtime Mo...	Monitors an...		Manual	Local Syste...
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Telephony	Provides Tel...		Manual	Network S...
Themes	Provides us...	Running	Automatic	Local Syste...
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service
Touch Keyboard and Hand...	Enables Tou...	Running	Manual (Trig...	Local Syste...
TrapTracker Receiver	TrapTracker ...	Running	Automatic	Local Syste...
Update Orchestrator Service	Manages W...	Running	Automatic (D...	Local Syste...

NOTE: If remote indexer is enabled in the EventTracker server then,

- ‘SQL server browser’ service should be enabled.
- Need to add ‘sqlbrowser.exe’ & ‘sqlservr.exe’ in firewall exception list.

4.2.1 SQL Server SA Account

- Windows Authentication mode is more secure than SQL Authentication. Hence configure SQL Server to use Windows authentication only.
- If 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 SA Account. Do not use this account for SQL server management.
  - Enforce a strong password policy, while using SQL Authentication.

5. EventTracker Settings

5.1 Securing Agent Configuration and Saving it as Template

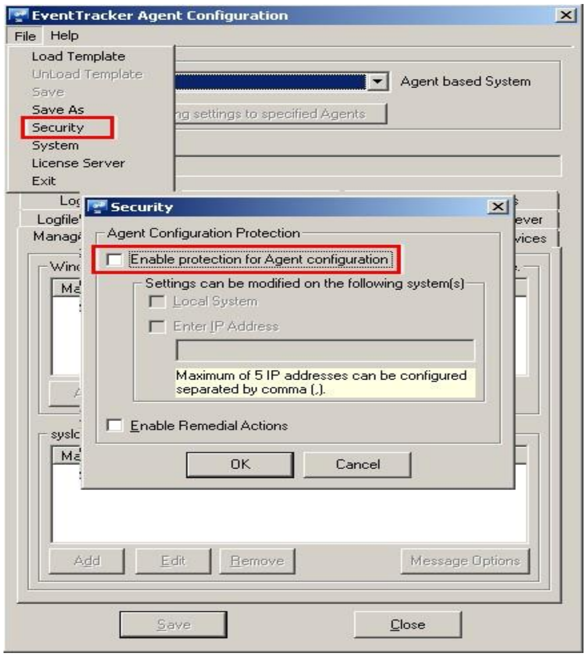
The current agent configuration settings on the local system can be protected from being modified by any unauthorized remote system. In this option, allow only the local system to modify the agent settings or configure up to five IP addresses of remote systems where the modification of agent configuration 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 local system needs to be saved as **‘Template’** first. The template is saved as .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 **EventTracker Control Panel**.
2. Double- click the **EventTracker Agent Configuration**, and then click **File** dropdown.
3. Click the **Security** option.


EventTracker Agent Configuration
File
Help
Load Template
UnLoad Template
Save
Save As
Security
System
License Server
Exit
Agent based System
ng settings to specified Agents
Security
Agent Configuration Protection
□ Enable protection for Agent configuration
Settings can be modified on the following system(s)
□ Local System
□ Enter IP Address
Maximum of 5 IP addresses can be configured separated by comma (,).
□ Enable Remedial Actions
OK
Cancel
Add
Edit
Remove
Message Options
Save
Close

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.

Field	Description
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** box. Up to five IP addresses can be configured, separated by comma (,)
Remedial Action	Remedial actions are scripts or EXEs that can be launched at either the agent or Manager side, in response to events.

4. Check the **Enable protection for Agent configuration** option.

5. Click the **OK** button.

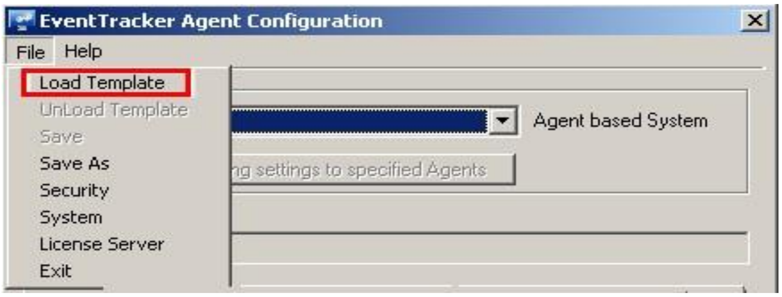
   NOTE: To apply this configuration to the agent systems in the enterprise, click the Apply this configuration to agents button.

5.2.1 Applying Configuration to Agent System(s)

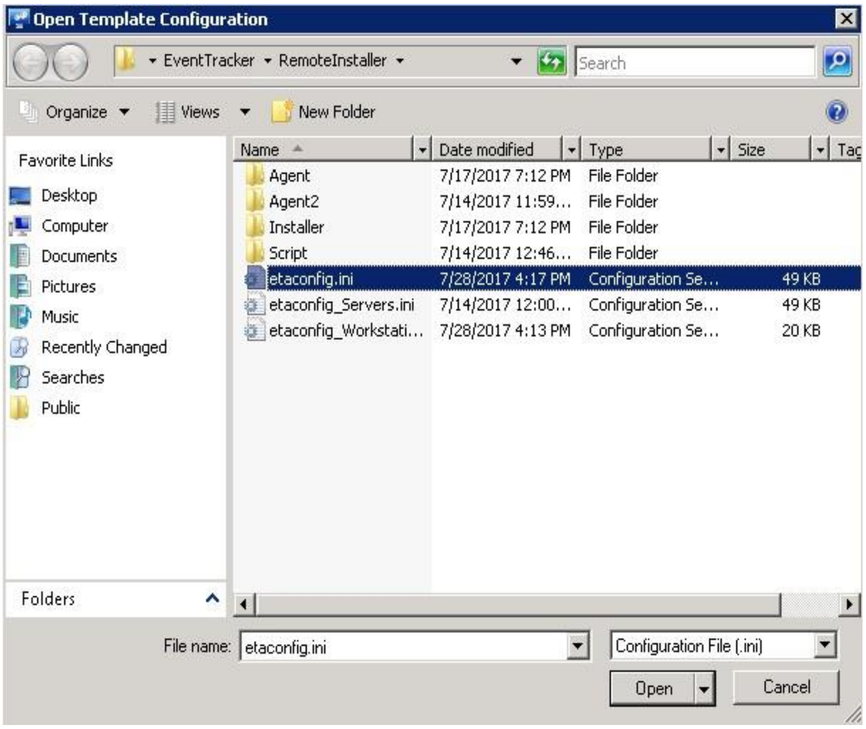
1. Go to **EventTracker Control Panel**.

2. Double- click the **EventTracker Agent Configuration** and click **File** dropdown.

3. Click the **Load Template** button.



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

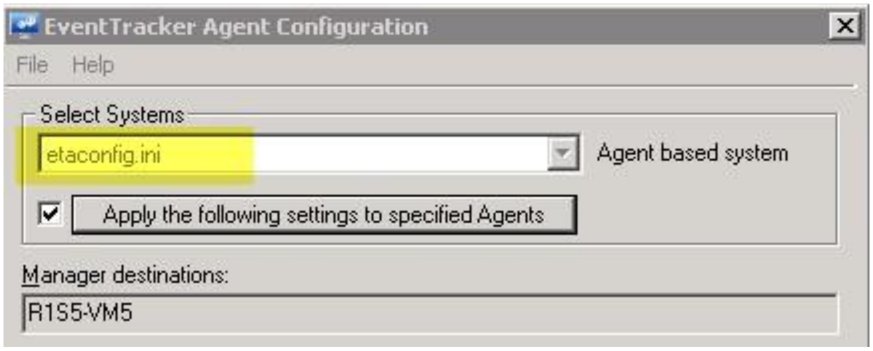


Name	Date modified	Type	Size	Tag
Agent	7/17/2017 7:12 PM	File Folder		
Agent2	7/14/2017 11:59...	File Folder		
Installer	7/17/2017 7:12 PM	File Folder		
Script	7/14/2017 12:46...	File Folder		
etaconfig.ini	7/28/2017 4:17 PM	Configuration Se...	49 KB	
etaconfig_Servers.ini	7/14/2017 12:00...	Configuration Se...	49 KB	
etaconfig_Workstati...	7/28/2017 4:13 PM	Configuration Se...	20 KB	

File name: etaconfig.ini

Configuration File (.ini)

EventTracker loads the selected template configuration.


EventTracker Agent Configuration
File
Help
Select Systems
Agent based system
Apply the following settings to specified Agents

etaconfig.ini

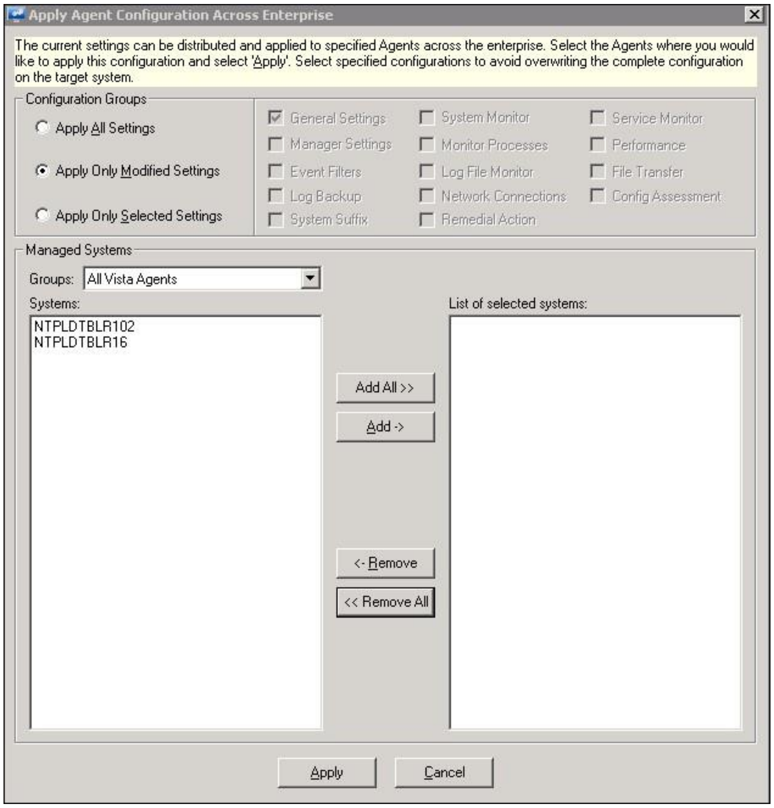
☑ Apply the following settings to specified Agents

Manager destinations:

R1S5-VM5

5. To apply this configuration to the agent systems in the enterprise, click the **Apply the following settings to specified Agents** button.

   Apply client configuration across enterprise dialog box appears.



Apply Agent Configuration Across Enterprise

The current settings can be distributed and applied to specified Agents across the enterprise. Select the Agents where you would like to apply this configuration and select 'Apply'. Select specified configurations to avoid overwriting the complete configuration on the target system.

Configuration Groups

○ Apply All Settings
● Apply Only Modified Settings
○ Apply Only Selected Settings

☑ General Settings
☐ Manager Settings
☐ Event Filters
☐ Log Backup
☐ System Suffix
☐ System Monitor
☐ Monitor Processes
☐ Log File Monitor
☐ Network Connections
☐ Remedial Action
☐ Service Monitor
☐ Performance
☐ File Transfer
☐ Config Assessment

Managed Systems

Groups: All Vista Agents

Systems:

NTPLDTBLR102
NTPLDTBLR16

List of selected systems:

6. Select a system group from **Select a group** dropdown.

EventTracker displays the managed systems associated with the selected group.

7. Check the required system options for which the configuration needs to be applied.

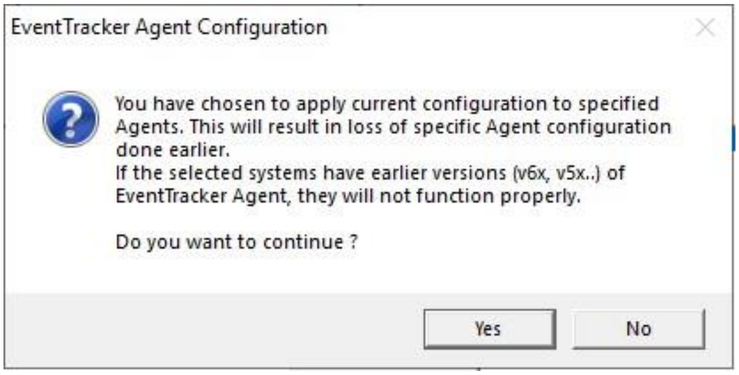
8. Select the **Configuration groups** option as required.

Field	Description
Apply Only Modified Settings	EventTracker selects this option by default. Leave the default selection to apply only modified settings.
Apply All Settings	Select this option to apply all settings including the default and modified settings.

Field	Description
Apply Only Selected Settings	Select this option to apply only the selected settings made under respective tabs. EventTracker enables the checkboxes. Select appropriately and then click **Apply**.

9. Click the **Apply** button.

   EventTracker displays a warning message.



EventTracker Agent Configuration

You have chosen to apply current configuration to specified Agents. This will result in loss of specific Agent configuration done earlier.
If the selected systems have earlier versions (v6x, v5x..) of EventTracker Agent, they will not function properly.

Do you want to continue ?

10. 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 EventTracker administrators/users.

1. **Backup purpose**:

   Provide the full permission for 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.

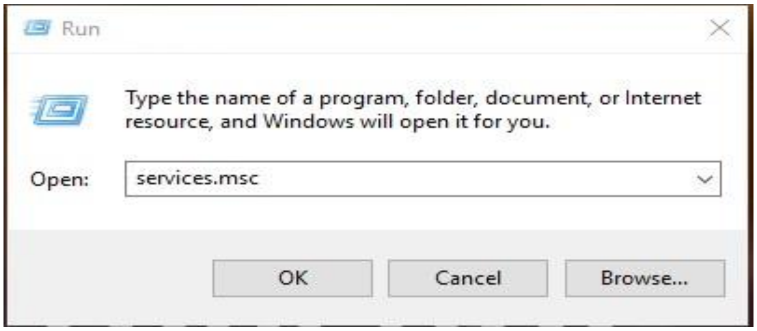
   c. Change the following services to run under the created service account.

      - EventTracker Scheduler
      - EventTracker EventVault
      - EventTracker Reporter
      - EventTracker Indexer

- Event Correlator (if available)

5.3.1 Changing the Service account

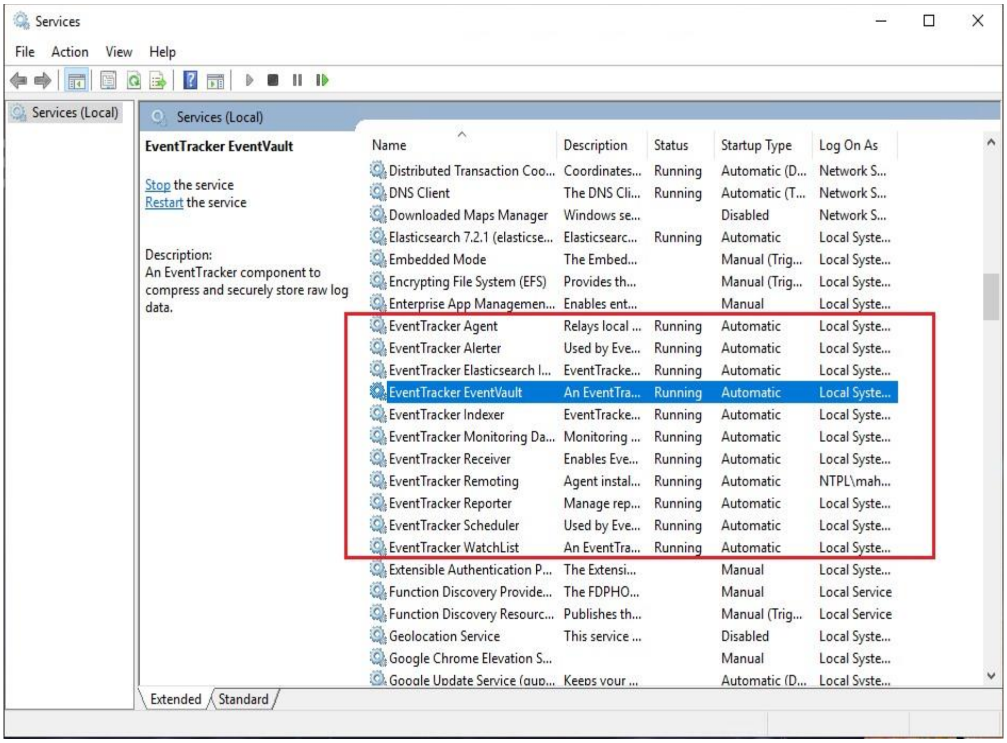
1. Click the **Start** button and select **Run**.
2. Type **services.msc**, and then click the **OK** button.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

3. In the **Services** window, search for EventTracker services.



EventTracker EventVault

Stop the service
Restart the service

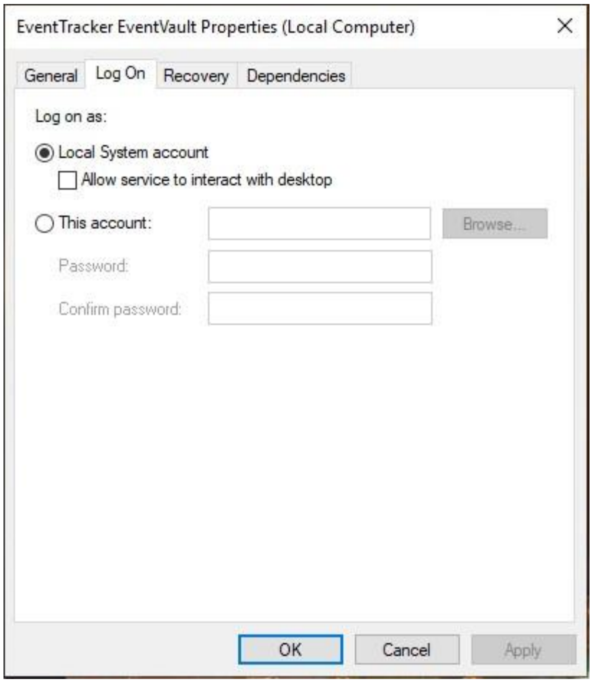
Description:
An EventTracker component to compress and securely store raw log data.

Name	Description	Status	Startup Type	Log On As
Distributed Transaction Coo...	Coordinates...	Running	Automatic (D...	Network S...
DNS Client	The DNS Cli...	Running	Automatic (T...	Network S...
Downloaded Maps Manager	Windows se...		Disabled	Network S...
Elasticsearch 7.2.1 (elasticse...	Elasticsearc...	Running	Automatic	Local Syste...
Embedded Mode	The Embed...		Manual (Trig...	Local Syste...
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Local Syste...
Enterprise App Managemen...	Enables ent...		Manual	Local Syste...
EventTracker Agent	Relays local ...	Running	Automatic	Local Syste...
EventTracker Alerter	Used by Eve...	Running	Automatic	Local Syste...
EventTracker Elasticsearch I...	EventTracke...	Running	Automatic	Local Syste...
EventTracker EventVault	An EventTra...	Running	Automatic	Local Syste...
EventTracker Indexer	EventTracke...	Running	Automatic	Local Syste...
EventTracker Monitoring Da...	Monitoring ...	Running	Automatic	Local Syste...
EventTracker Receiver	Enables Eve...	Running	Automatic	Local Syste...
EventTracker Remoting	Agent instal...	Running	Automatic	NTPL\mah...
EventTracker Reporter	Manage rep...	Running	Automatic	Local Syste...
EventTracker Scheduler	Used by Eve...	Running	Automatic	Local Syste...
EventTracker WatchList	An EventTra...	Running	Automatic	Local Syste...
Extensible Authentication P...	The Extensi...		Manual	Local Syste...
Function Discovery Provide...	The FDPHO...		Manual	Local Service
Function Discovery Resourc...	Publishes th...		Manual (Trig...	Local Service
Geolocation Service	This service ...		Disabled	Local Syste...
Google Chrome Elevation S...			Manual	Local Syste...
Google Update Service (gup...	Keeps your ...		Automatic (D...	Local Syste...

4. Right click the service name and click **Properties**.

For example: Right click **EventTracker EventVault** service

'EventTracker EventVault Properties (Local Computer)' window displays.



EventTracker EventVault Properties (Local Computer)

Log on as:

● Local System account

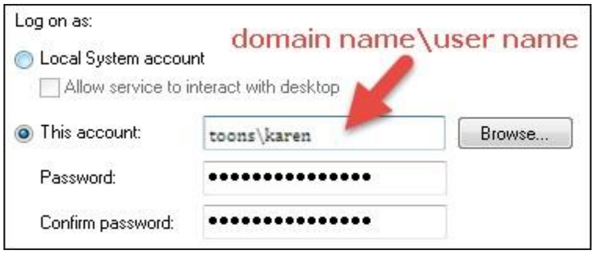
□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

5. Click **Log On** tab and select **This account** option.



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: toons\karen

Password: ●●●●●●●●●●●●●●●

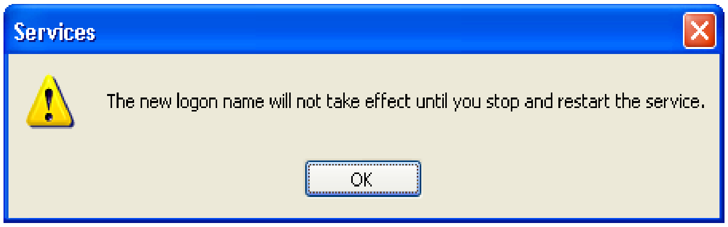
Confirm password: ●●●●●●●●●●●●●●●

6. Enter the user credentials and correct password.

   The username should be in ‘domain name\username’ format.

7. Click the **Apply** button.

   Warning message appears.

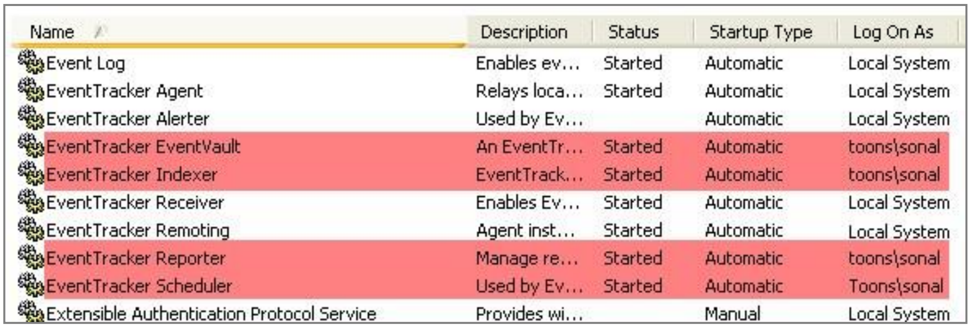


Services

The new logon name will not take effect until you stop and restart the service.

8. Click the **OK** button.
9. To run the service with new logon name, stop and start the service.
10. Likewise, for rest of the services, repeat step 4 to step 10 to change the service account.

The **Log On As** column will display the changed service account name.



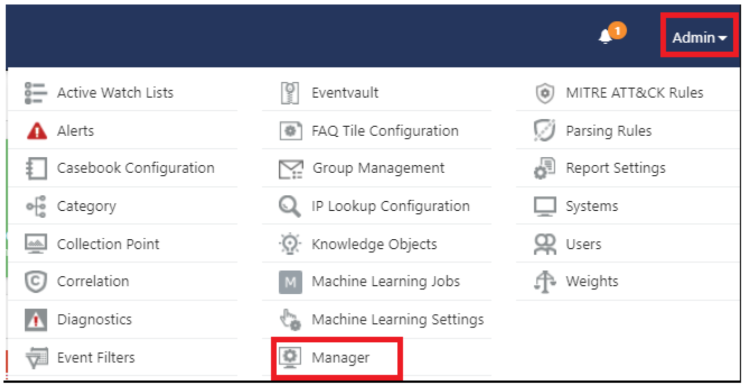
Name	Description	Status	Startup Type	Log On As
Event Log	Enables ev...	Started	Automatic	Local System
EventTracker Agent	Relays loca...	Started	Automatic	Local System
EventTracker Alerter	Used by Ev...		Automatic	Local System
EventTracker EventVault	An EventTr...	Started	Automatic	toons\sonal
EventTracker 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 2FA option for EventTracker Web Login

To enable the 2FA for EventTracker Web Login, follow the steps below:

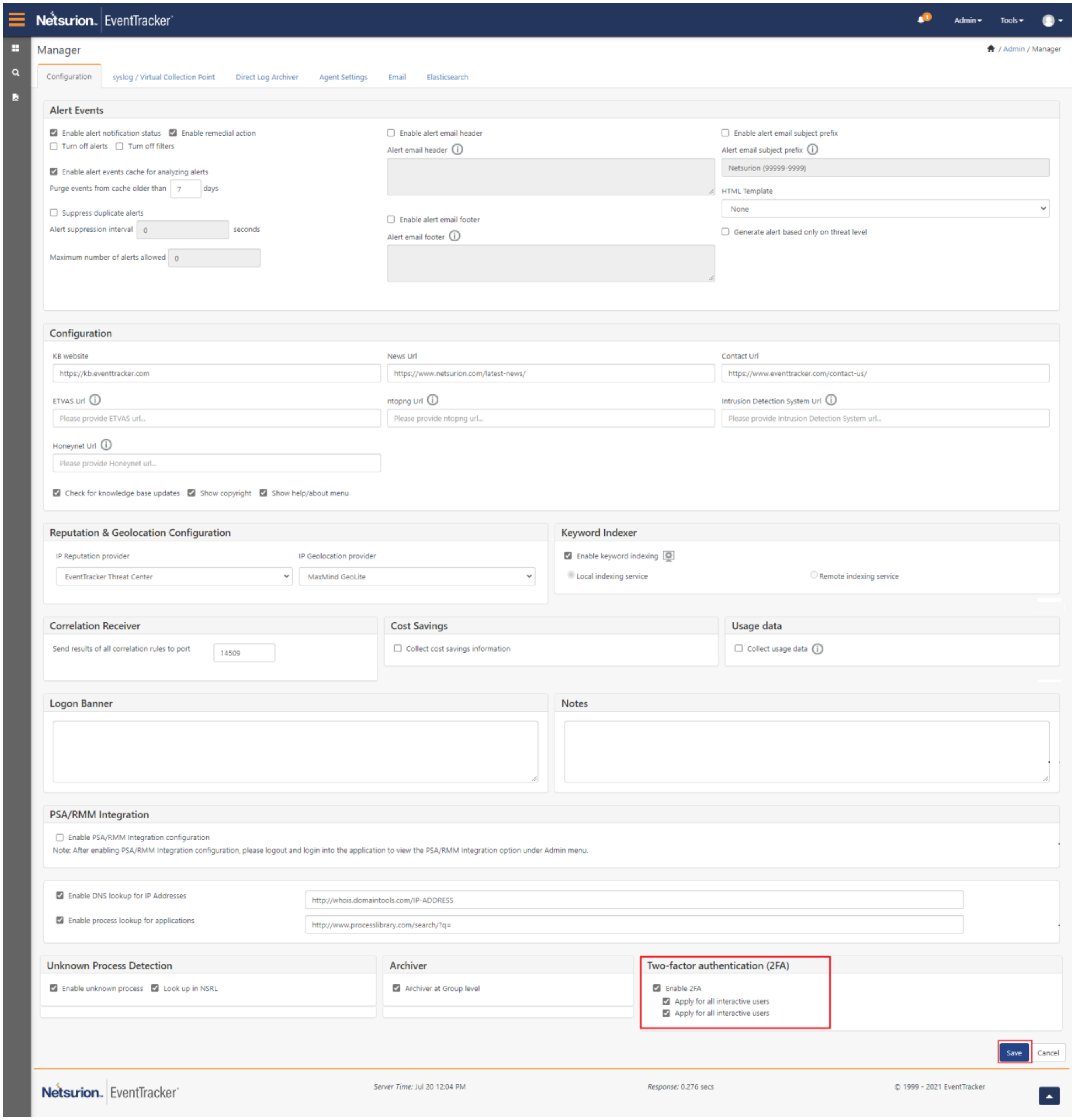
Log into the EventTracker Web UI.

1. Click **Admin > Manager**.



Manager page opens.

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



Alert Events

☑ Enable alert notification status ☑ Enable remedial action
☐ Turn off alerts ☐ Turn off filters

☑ Enable alert events cache for analyzing alerts
Purge events from cache older than 7 days

☐ Suppress duplicate alerts
Alert suppression interval 0 seconds

Maximum number of alerts allowed 0

☐ Enable alert email header
Alert email header

☐ Enable alert email footer
Alert email footer

☐ Enable alert email subject prefix
Alert email subject prefix: Netsurion (99999-9999)
HTML Template: None
☐ Generate alert based only on threat level

Configuration

KB website: https://kb.eventtracker.com
News Url: https://www.netsurion.com/latest-news/
Contact Url: https://www.eventtracker.com/contact-us/
ETVAS Url: Please provide ETVAS url...
ntopng Url: Please provide ntopng url...
Intrusion Detection System Url: Please provide Intrusion Detection System url...
Honeynet Url: Please provide Honeynet url...

☑ Check for knowledge base updates ☑ Show copyright ☑ Show help/about menu

Reputation & Geolocation Configuration

IP Reputation provider: EventTracker Threat Center
IP Geolocation provider: MaxMind GeoLite

Keyword Indexer

☑ Enable keyword indexing
● Local indexing service ○ Remote indexing service

Correlation Receiver

Send results of all correlation rules to port 14509

Cost Savings

☐ Collect cost savings information

Usage data

☐ Collect usage data

Logon Banner

Notes

PSA/RMM Integration

☐ Enable PSA/RMM Integration configuration
Note: After enabling PSA/RMM Integration configuration, please logout and login into the application to view the PSA/RMM Integration option under Admin menu.

☑ Enable DNS lookup for IP Addresses: http://whois.domaintools.com/IP-ADDRESS
☑ Enable process lookup for applications: http://www.processlibrary.com/search/?q=

Unknown Process Detection

☑ Enable unknown process ☑ Look up in NSRL

Archiver

☑ Archiver at Group level

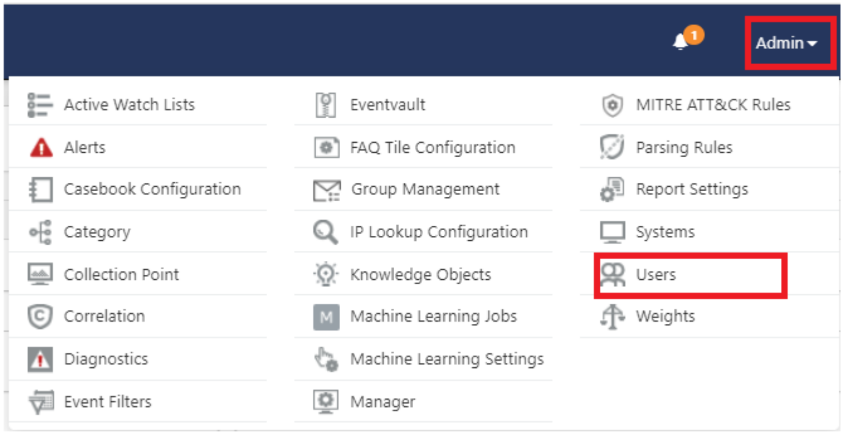
Two-factor authentication (2FA)

☑ Enable 2FA
☑ Apply for all interactive users
☑ Apply for all interactive users

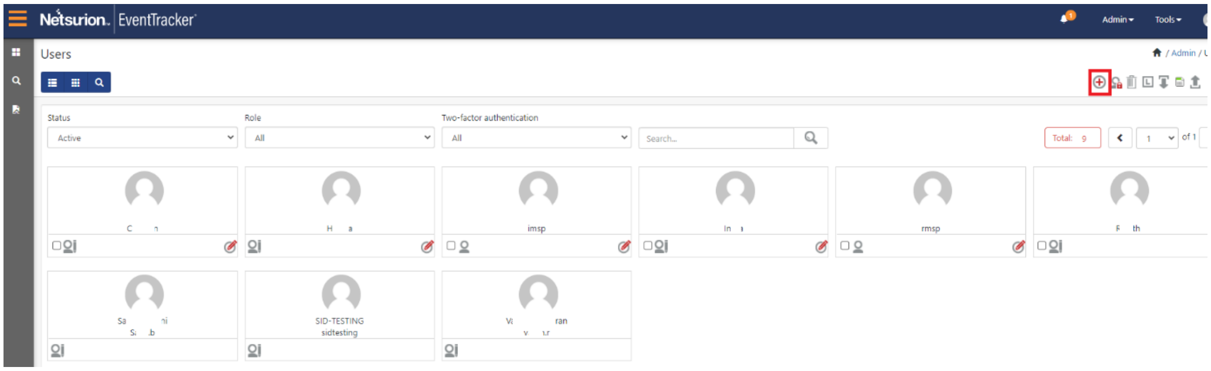
Now the 2FA option is enabled by default while creating the new users.

6.1 Adding New Users

1. Click **Admin > Users**.

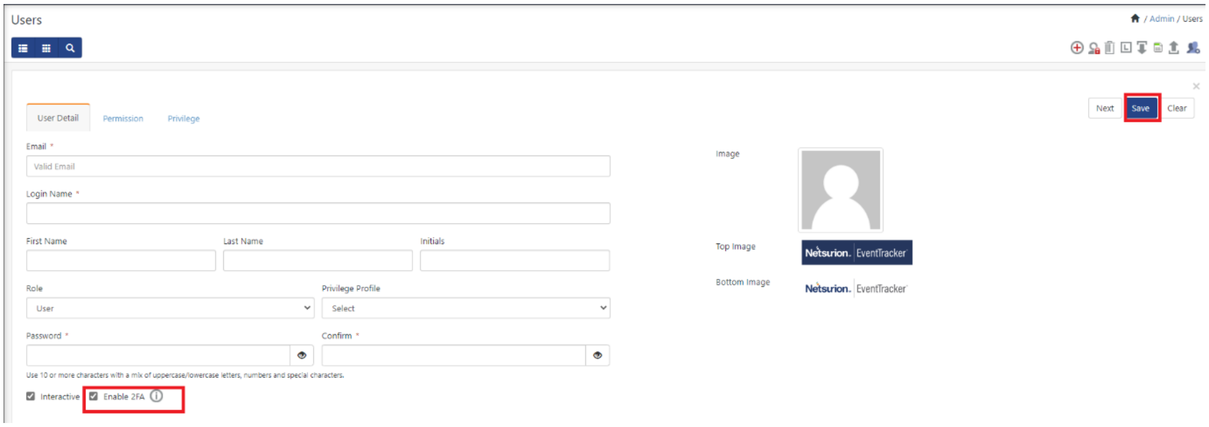


Users page opens.



2. Click ⊕ icon to add a new user.

User Detail page opens. 2FA option is enabled by default for the users.



Email *: Valid Email

Login Name *

First Name | Last Name | Initials

Role: User | Privilege Profile: Select

Password * | Confirm *

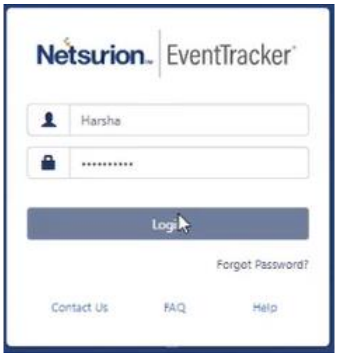
Use 10 or more characters with a mix of uppercase/lowercase letters, numbers and special characters.

☑ Interactive ☑ Enable 2FA ⓘ

4. Enter the required details and click **Save**.

Next time the user logs into the EventTracker Web, the user is asked to provide their authentication to login.

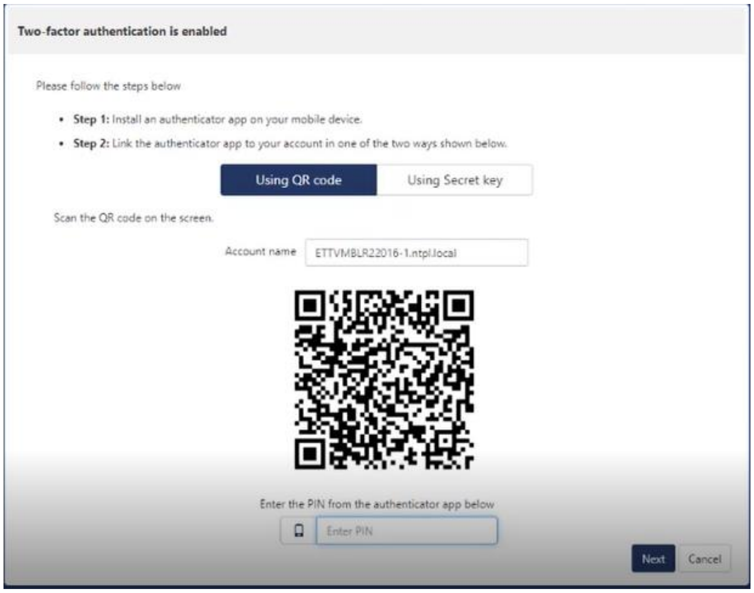
Note: You may also choose to uncheck **Enable 2FA** option to disable the feature.



Netsurion | EventTracker

Harsha

••••••••••



Two-factor authentication is enabled

Please follow the steps below

- **Step 1:** Install an authenticator app on your mobile device.
- **Step 2:** Link the authenticator app to your account in one of the two ways shown below.

Scan the QR code on the screen.

Account name: ETTVMBLR22016-1.ntpl.local

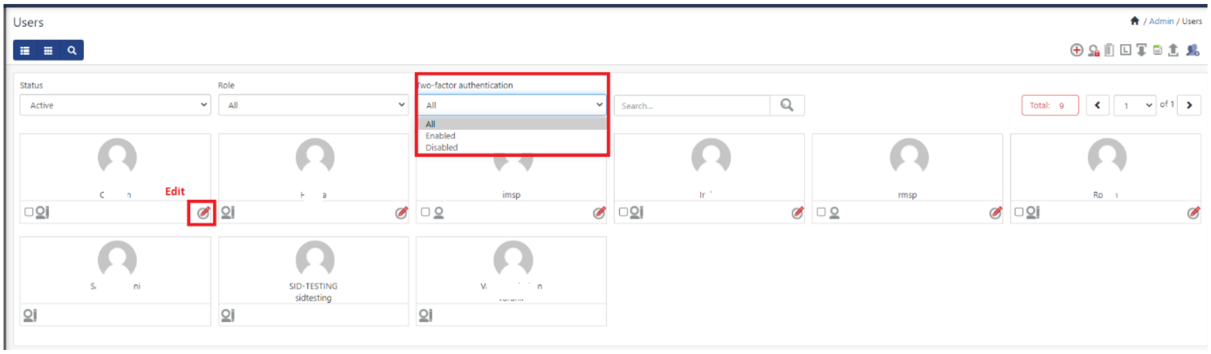
Enter the PIN from the authenticator app below

Refer the following link to configure the authentication app.

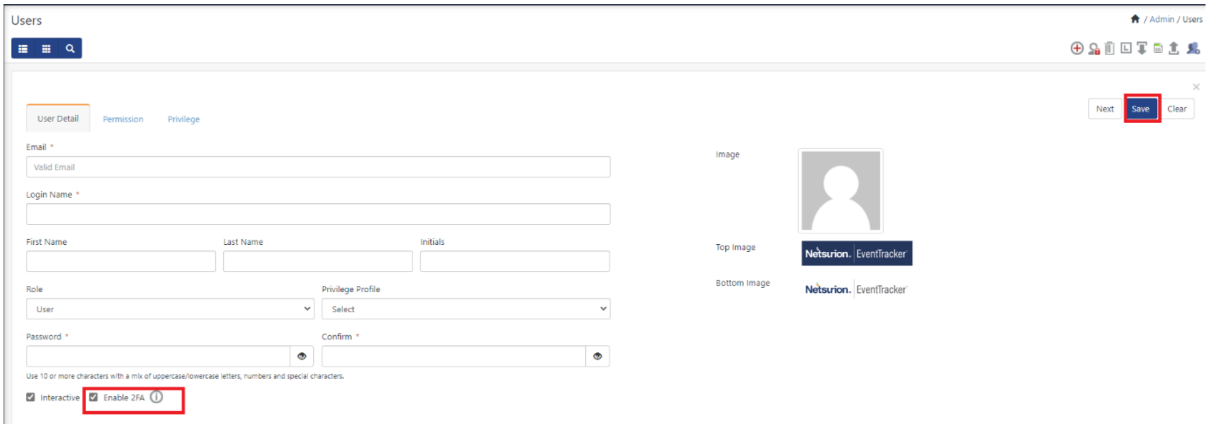
https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Two-factor-Authentication-2FA-User-Guide.pdf

6.2 Enabling 2FA option for Existing Users

1. Click **Admin > Users**.
   Users page opens.
2. In the **two-factor authentication** dropdown, select **Disabled** option.
   All the Users accounts with disabled 2FA account display.

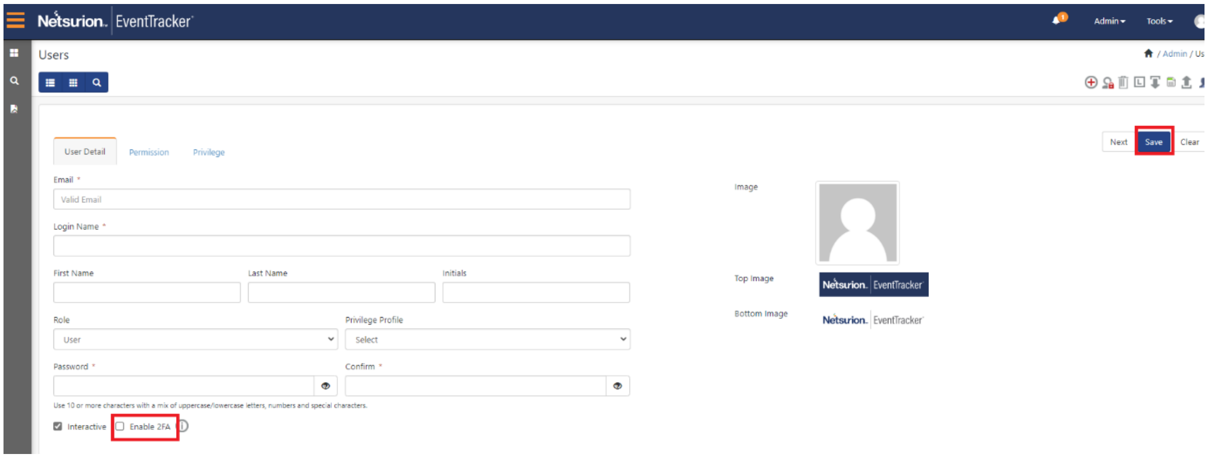


3. Click Edit on the User account for which you want to enable 2FA and then click **Save**. The Two-factor authentication is enabled for the selected user.

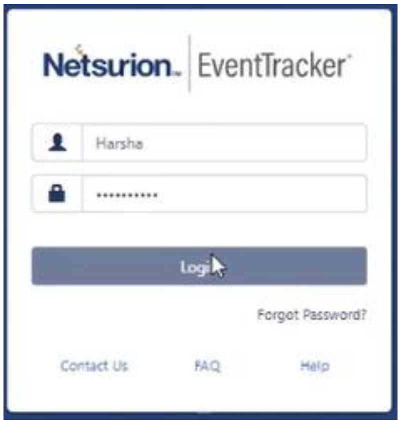


6.3 Disabling the 2FA

1. Click Admin—Users.
2. Click **Add User** in the user page, uncheck the 2FA option to disable the feature and then click **Save**.

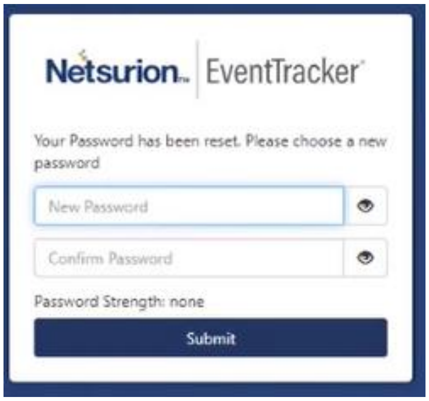


3. Next time when the user logs into EventTracker Web, the user is prompted to reset the password.



Harsha

••••••••••



Your Password has been reset. Please choose a new password

Password Strength: none

7. Checking for Vulnerability Scanner

It is a standard practice to scan critical machines for vulnerabilities. Scan the hardened EventTracker system for vulnerabilities. Some of the following vulnerabilities maybe reported.

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

Vulnerabilities	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 doesn't support encryption or any sort of strong authentication mechanism.	EventTracker uses default port 514 for receiving syslogs messages. Configure the firewall to allow incoming connections on port 514 from trusted hosts or use another port for receiving syslog in EventTracker Manager Configuration.

Vulnerabilities	Impact	Recommended actions
FTP server does not support 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 EventTracker server to transfer custom logs from remote sources. • In case of IIS 6, FTP does not support AUTH command. This is by design, use a third-party FTP that supports 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 event logs	Windows event logs have been configured to allow guest access. 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.	For each event log listed, find the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\[logname] Under this key, add a DWORD value named "RestrictGuestAccess" and set it to 1.
Microsoft IIS default installation/welco me page installed (http-iis-defaultinstall-page)	The IIS default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and not be known about.	Replace default page with relevant content page.

Vulnerabilities	Impact	Recommended actions
TCP timestamp response (generictcp-timestamp)	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.	Disable TCP timestamp responses on Windows. For each event log listed, find the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Under this key, add a DWORD value named "Tcp1323Opts " and set it to 1.
General Security Issue Clear text authentication	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 is able to monitor FTP traffic.	FTP server is installed on the EventTracker server to transfer custom logs from remote sources. • In case of IIS 6, FTP does not support AUTH command. This is by design, either use a thirdparty FTP that supports AUTH command and configure FTP over SSL or configure FTP server to allow connection from trusted host.

* These vulnerabilities are determined by Vulnerability scanners.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support