Hardening Guide

Logcollect 9.4 Server

Publication Date

Nov 25, 2025

Abstract

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

Note:

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

Scope

The configuration details in this guide are consistent with Logcollect 9.4.

Audience

This guide is for the Logcollect users responsible for monitoring and managing network security.

Table of Contents

1 Overview

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

1.1 Applying Group Policies on Windows Server 2019

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

Download WS2019-GPO.zip

Apply the following policies:

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

1.2 Securing IIS Web Server

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

For IIS 7 Web Server,

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

1.3 Securing SQL Server

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

Note

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

1.4 Adding Windows Firewall Exceptions

Add the ports/.exe in use to the firewall exception list. Any number of VCPs can be added based on the system capacity. For Logcollect, 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)	Logcollect Certificate server
14506 (TCP)	Logcollect Agent
14507 (TCP)	Collection Master
443 (TCP)	Logcollect securely access (HTTPS), Logcollect Endpoint Security
514 (UDP/TCP)	Syslog Receiver, Multiple VCP's can be configured
14504	Logcollect Active Watchlist
9200	Elasticsearch-service-x64, Elastic Cross Cluster
9300	Elastic Cross Cluster **Note**: Applicable for Logcollect 9.4 version.
6514	Logcollect Endpoint Security **Note**: This port is configurable. In case of a change in port number, the Logcollect team will notify. **Note**: Applicable for Logcollect 9.4 version.

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

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

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

1.5 Allowing Outbound Access to Public URL’s

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

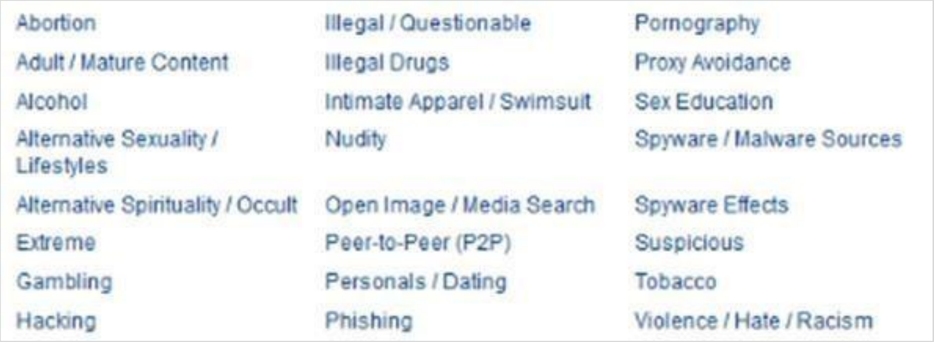
URL/Domain	Port/Protocol/Direction	Purpose
*.logcollect.com	443/TCP/Outbound	Download the Logcollect updates and DSI
certificates.logcollect.com	443/TCP/Outbound	Logcollect Licensing server
ipinfo.io	443/TCP/Outbound	Load the map in Machine Learning Dashboard
geolite.maxmind.com	80/TCP/Outbound	Download the Geolocation details in the Attackers Dashboard

1.6 Checking for Vulnerability Scanner

Scan the hardened Logcollect system for vulnerabilities. This is applicable only if the Vulnerable Scanner is used.

1.7 Restricting Email/File-Sharing Website Access

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

2 Harden Windows Server – Detailed View

Configure the following aspects to harden the Logcollect Manager:

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

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

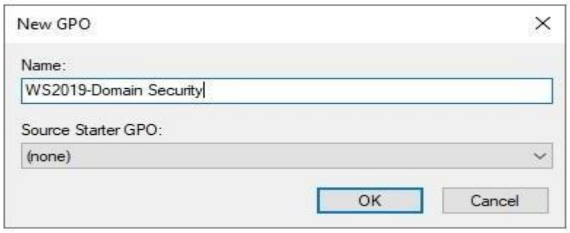
Step 1: Click the link below to download the GPO and extract the contents of the zip file to the system.

Download WS2019-GPO.zip

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

Step 2: Create new Group Policy Objects.

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

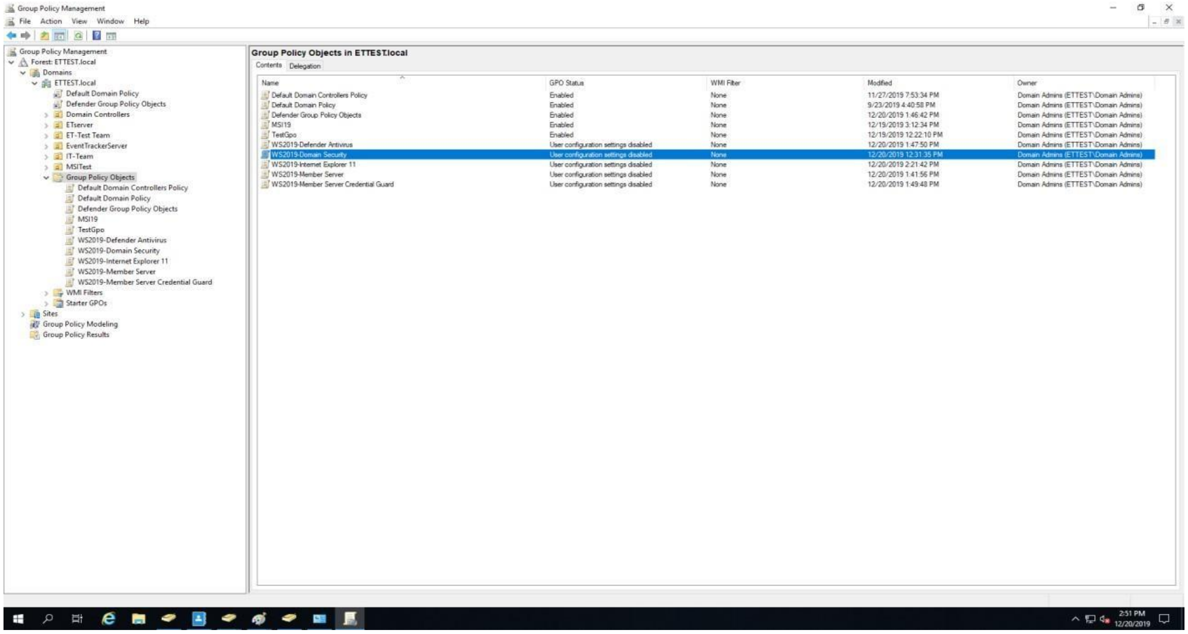


New GPO

Name: WS2019-Domain Security

Source Starter GPO: (none)

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

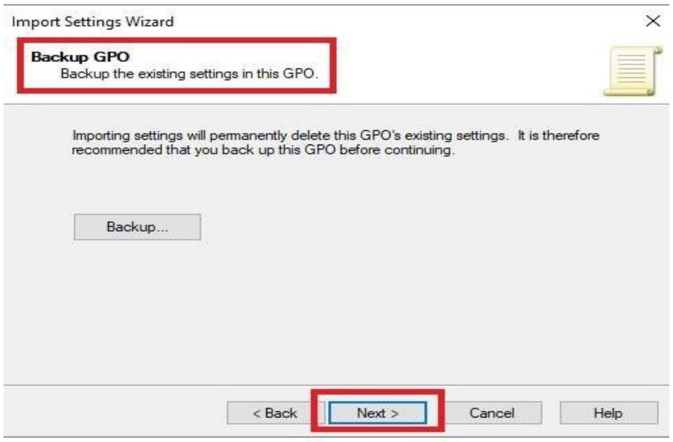


Group Policy Objects in ETTEST.local

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.

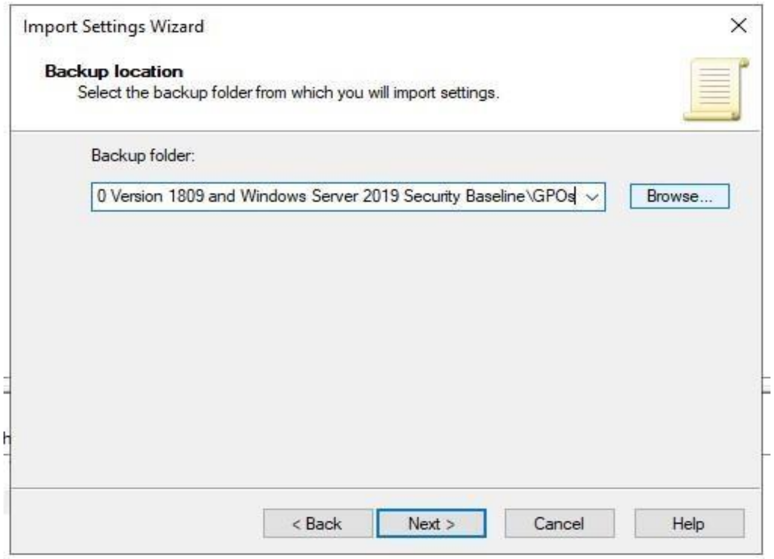
1. Right-click the newly created GPO (For example, **WS2019-Domain Security**), and click **Import settings**.
2. Click the **Next** button to start the importing process.
3. In **Backup GPO**, click the **Next >** button.



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

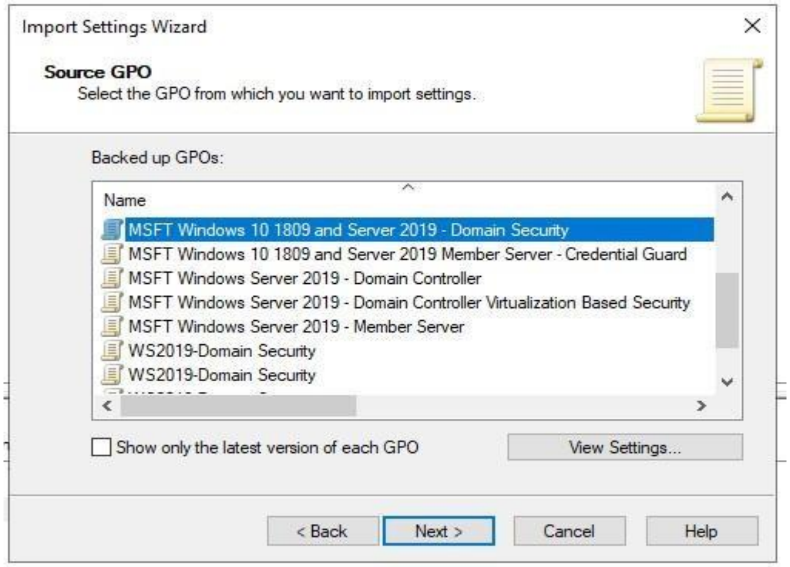
Backup location

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

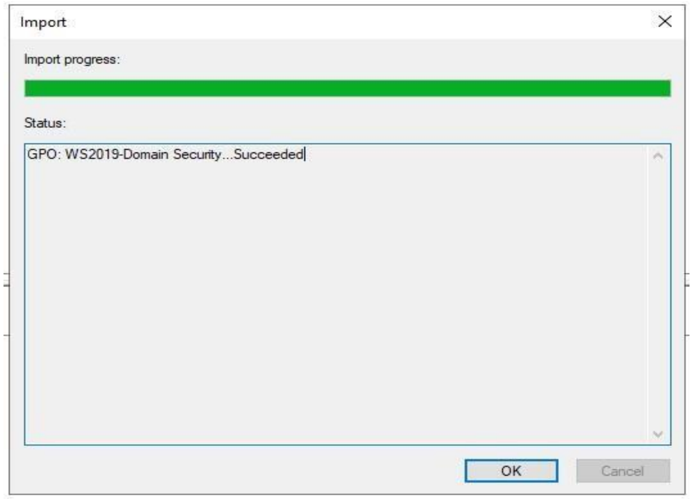
Select the GPO from which you want to import settings.

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 are complete, click the **Next >** button.
9. In **Migrating References**, click the **Next >** button.
10. Click **Finish.**
11. After successfully importing, click the **OK** button.



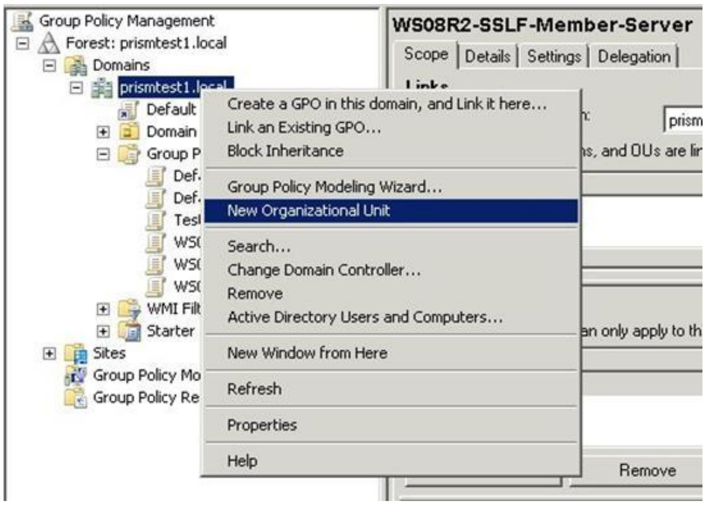
GPO: WS2019-Domain Security...Succeeded

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

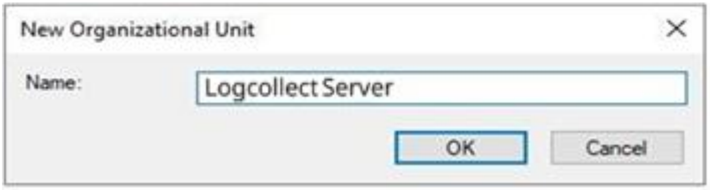
12. Repeat the steps from 1 to 11 to import Group Policy for **WS2019-Member Server, WS2019Defender Antivirus, WS2019-Member Server Credential Guard, and WS2019-Internet Explorer 11- User and Computer.**

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

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



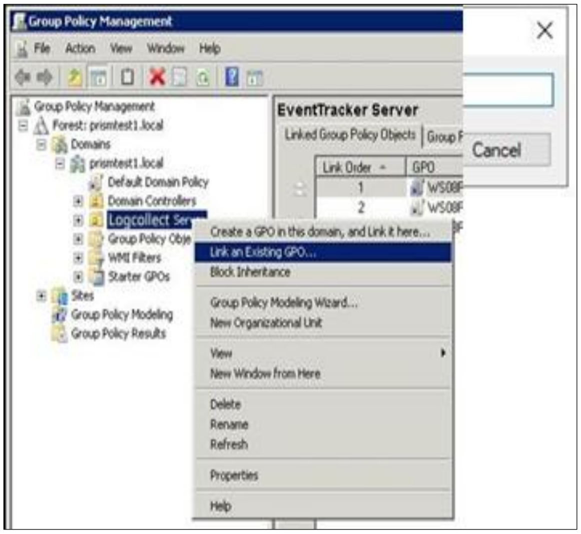
2. Enter the new organizational unit (OU) name and click **OK**. Example: Logcollect Manager



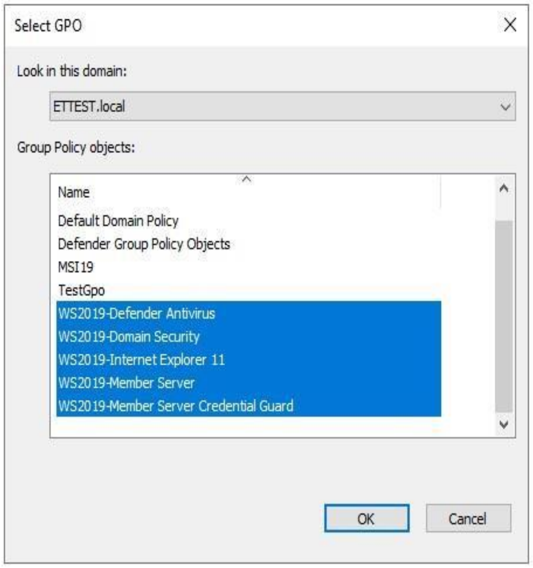
Name: Logcollect Server

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

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



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


Select GPO

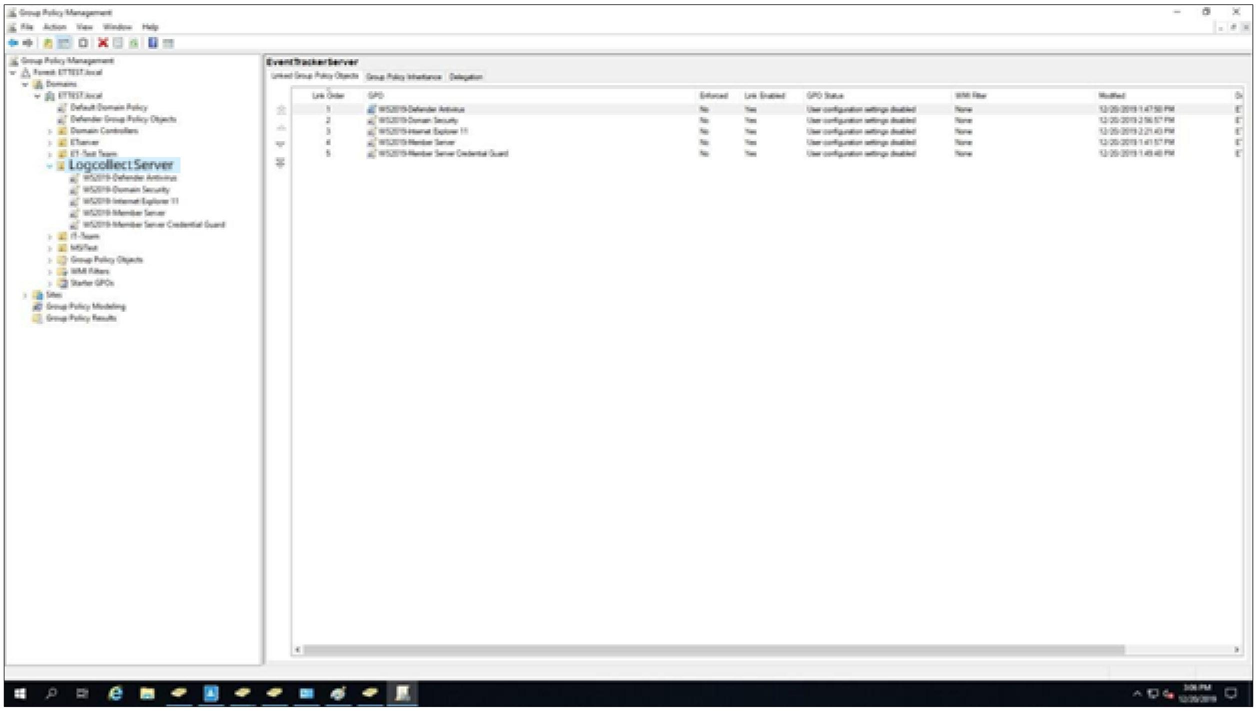
Look in this domain:

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

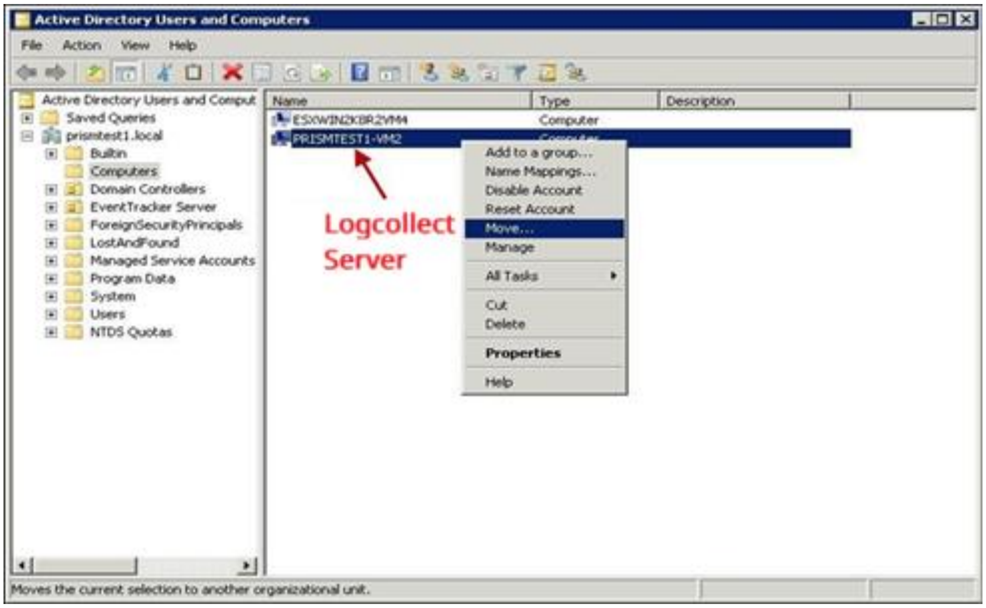
3. The Group Policy objects are now linked to the organizational unit.



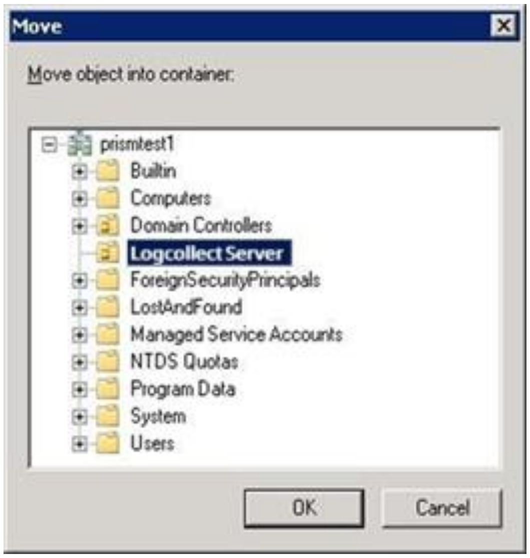
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	WS2019-Defender Antivirus	No	Yes	User configuration settings disabled	None	12/20/2019 1:47:50 PM
2	WS2019-Domain Security	No	Yes	User configuration settings disabled	None	12/20/2019 2:56:57 PM
3	WS2019-Internet Explorer 11	No	Yes	User configuration settings disabled	None	12/20/2019 2:21:43 PM
4	WS2019-Member Server	No	Yes	User configuration settings disabled	None	12/20/2019 1:41:57 PM
5	WS2019-Member Server Credential Guard	No	Yes	User configuration settings disabled	None	12/20/2019 1:49:40 PM

Step 6: Link Logcollect Manager to the newly created OU and reboot the Logcollect Manager system.

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

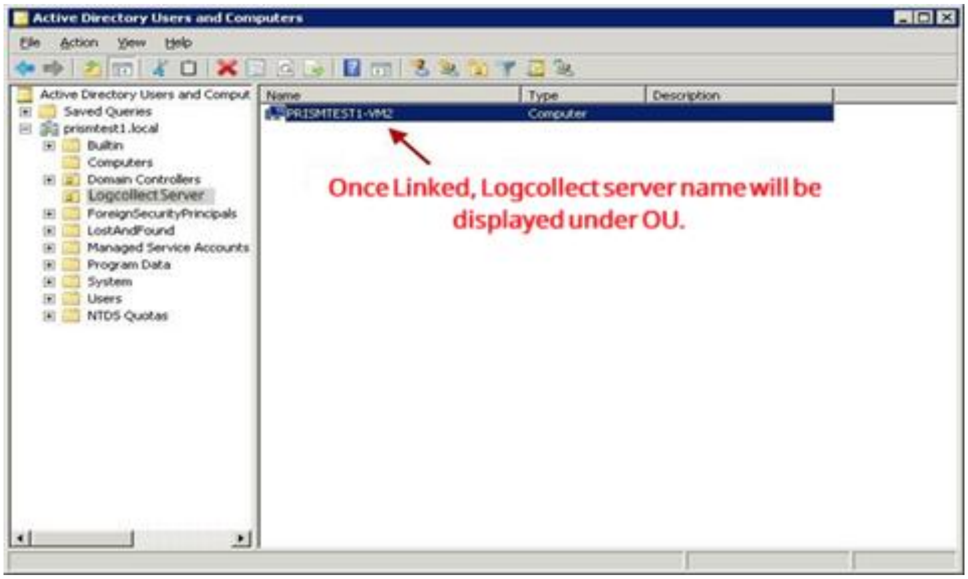


Moves the current selection to another organizational unit.


Move

Move object into container:

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



Name	Type	Description
PRISMTEST1-VM2	Computer	

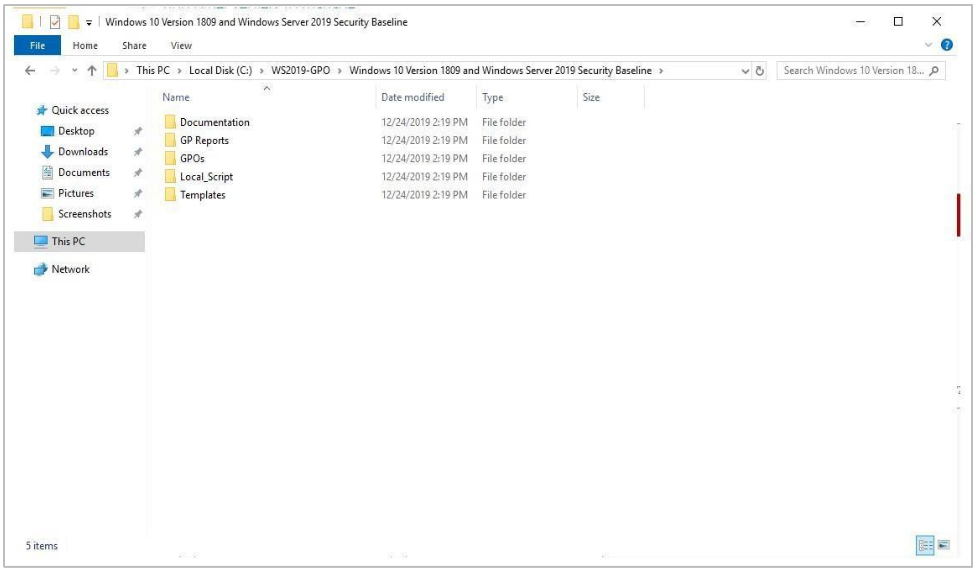
Once Linked, Logcollect server name will be displayed under OU.

7. Reboot the Logcollect Manager system linked to the OU.

2.2 Applying Group Policies in a Workgroup on Windows Server 2019

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

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



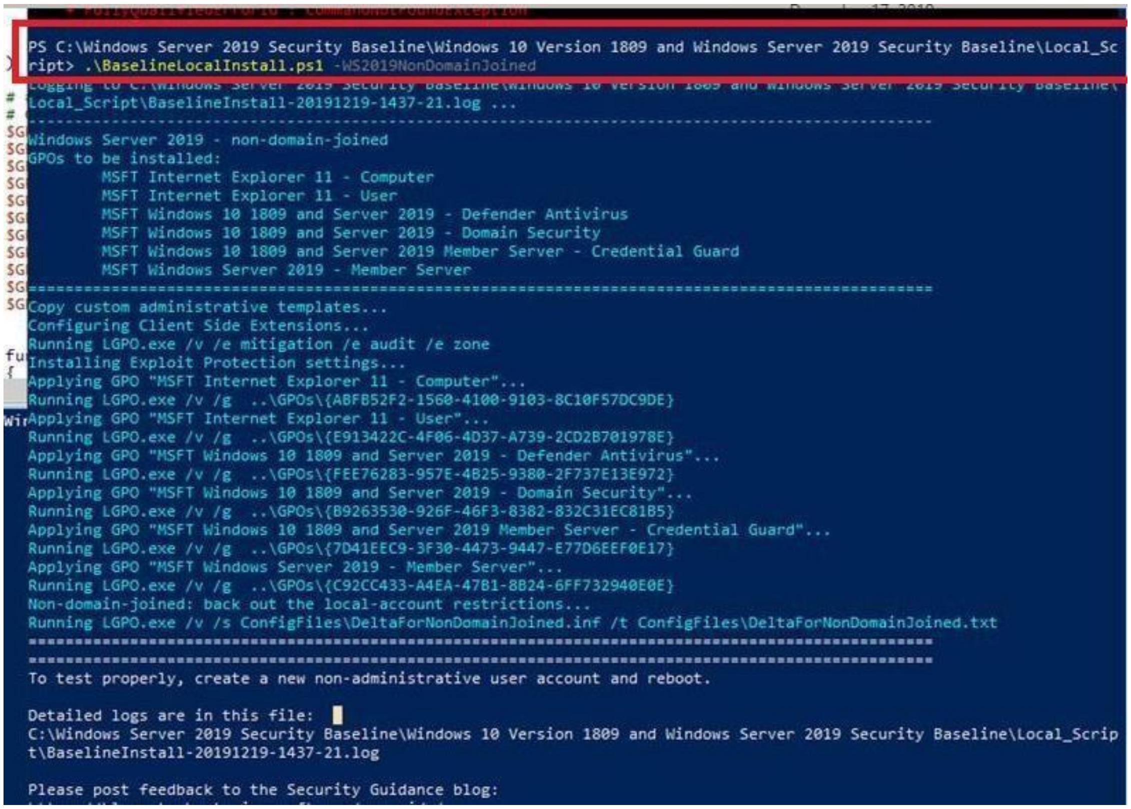
Windows 10 Version 1809 and Windows Server 2019 Security Baseline
File
Home
Share
View
This PC › Local Disk (C:) › WS2019-GPO › Windows 10 Version 1809 and Windows Server 2019 Security Baseline ›
Search Windows 10 Version 18...
Quick access
Desktop
Downloads
Documents
Pictures
Screenshots
This PC
Network
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 the PowerShell script which is available in the downloaded folder.

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

```
.\BaselineLocalInstall.ps1  -WS2019NonDomainJoined
```

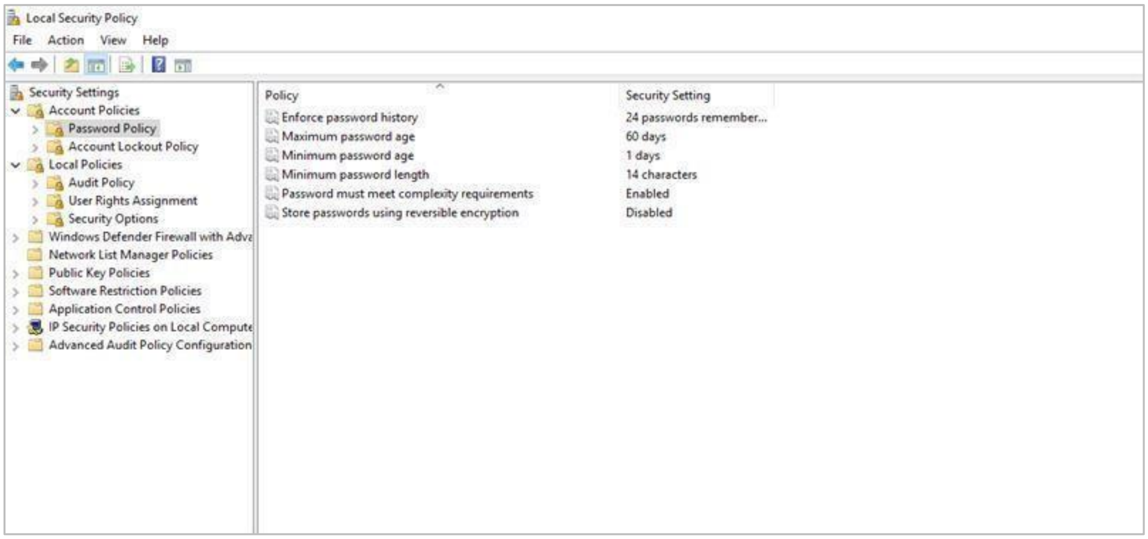


```
PS C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Sc
ript> .\BaselineLocalInstall.ps1 -WS2019NonDomainJoined
Logging to C:\Windows Server 2019 Security Baseline\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\
Local_Script\BaselineInstall-20191219-1437-21.log ...
-------------------------------------------------------------------------------------------------
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:
```

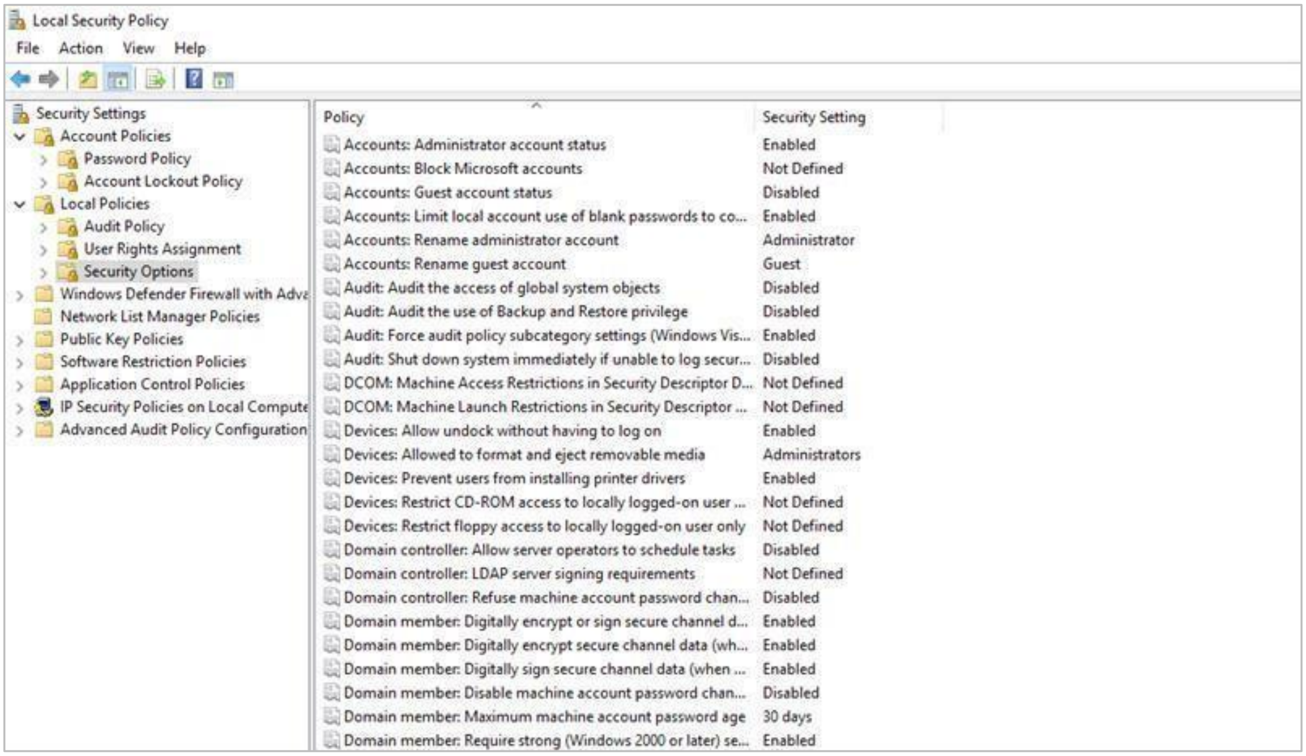
Step 3: Verify the applied Security Policy.

<u>In the Workgroup System</u>

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


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
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



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - 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
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

3 Securing IIS Web Server (10 and 11)

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

3.1 Mandatory Requirements

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

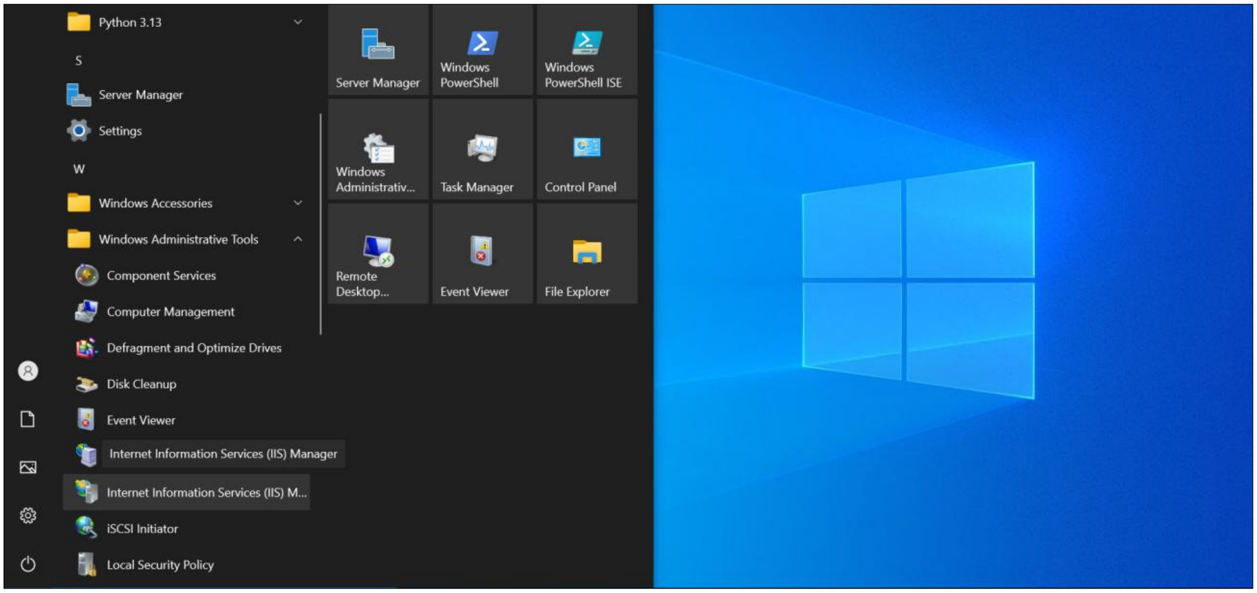
Operating System	Windows Server 2019
Software and Components	• Internet Information Server (IIS) 10 and 11. • Browser, which supports 128-bit encryption (IE 11 or above/ Firefox 3.5 or above).

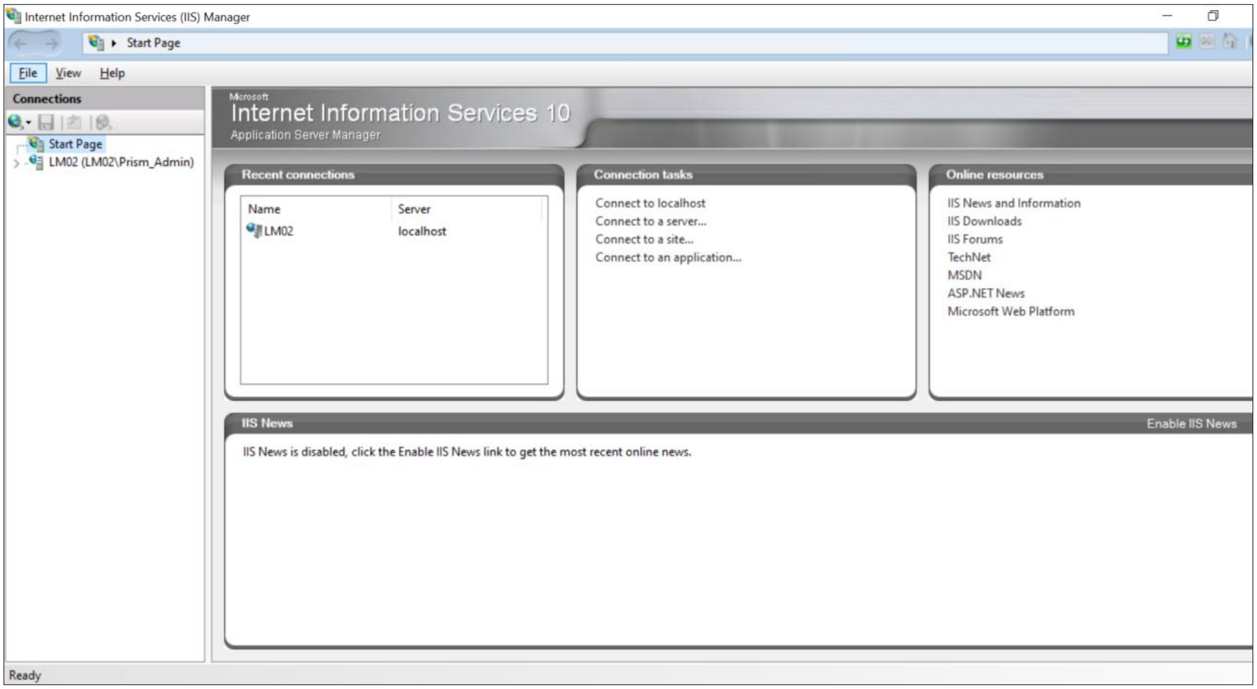
3.2 IIS setup on Windows

Step 1: Creating the ‘Certificate Request’.

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

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

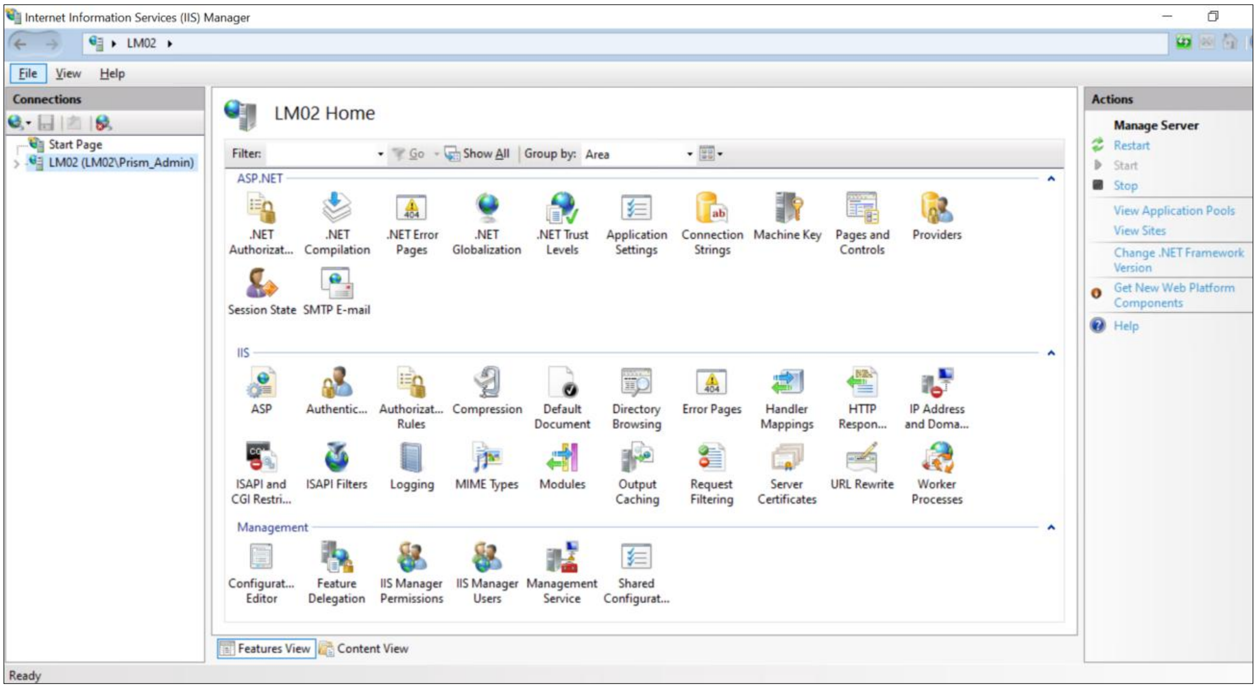




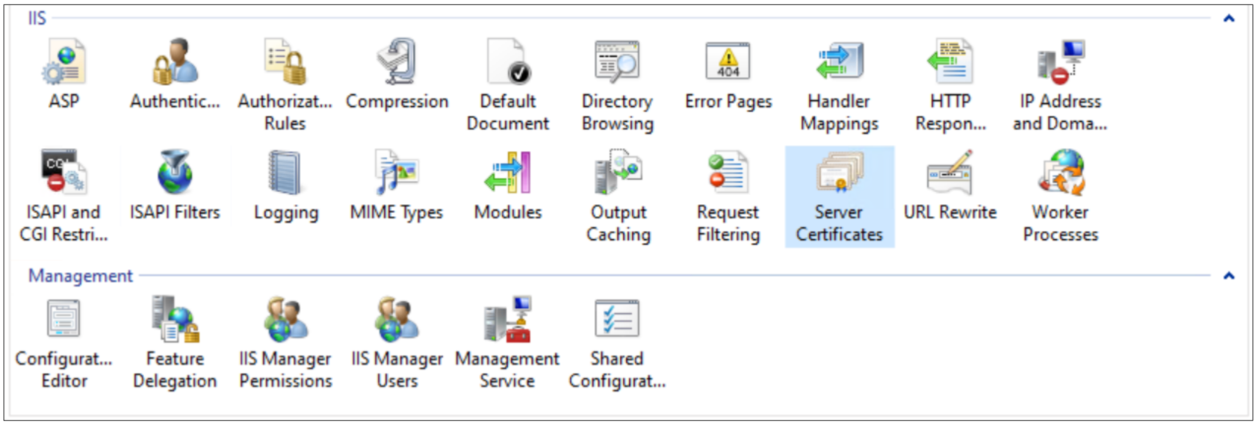
Name	Server
LM02	localhost

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

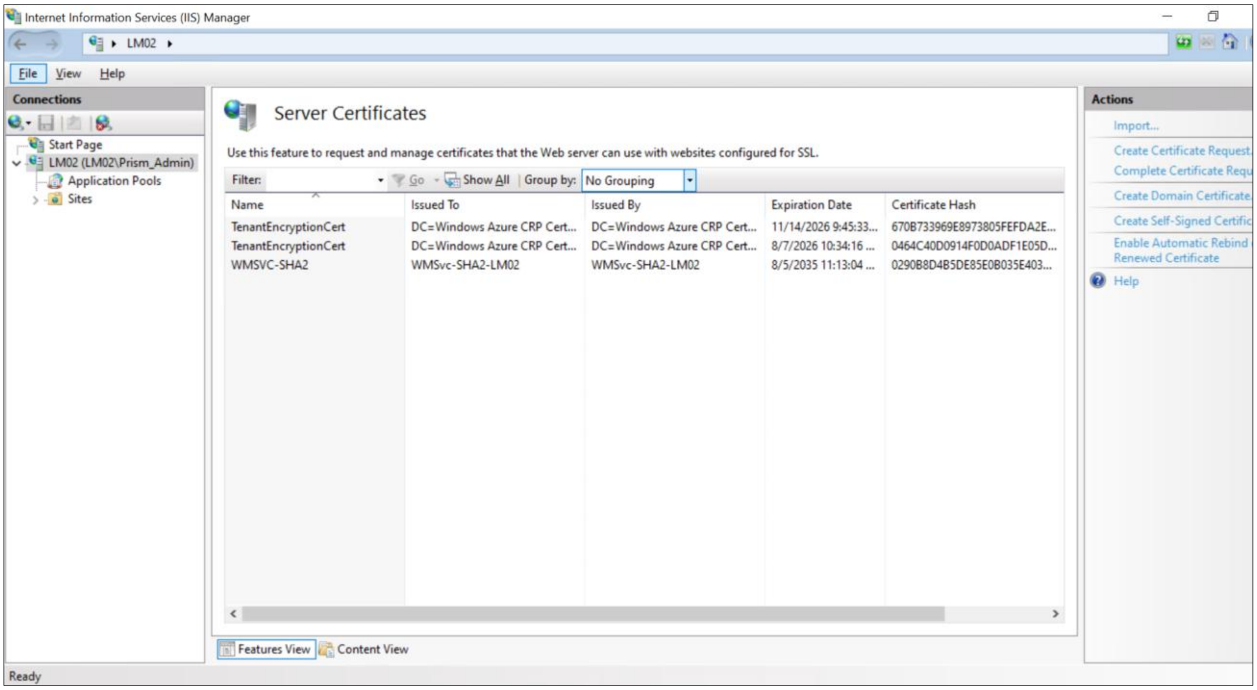
3. Click the server node.



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



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

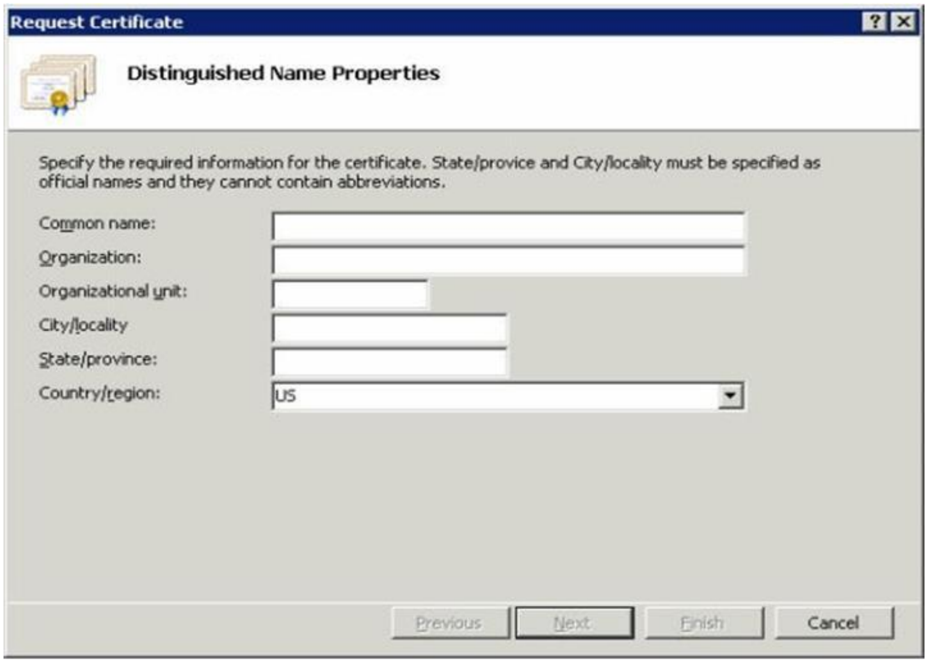


Server Certificates

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

Name	Issued To	Issued By	Expiration Date	Certificate Hash
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	11/14/2026 9:45:33...	670B733969E8973805FEFDA2E...
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	8/7/2026 10:34:16 ...	0464C40D0914F0D0ADF1E05D...
WMSVC-SHA2	WMSvc-SHA2-LM02	WMSvc-SHA2-LM02	8/5/2035 11:13:04 ...	0290B8D4B5DE85E0B035E403...

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



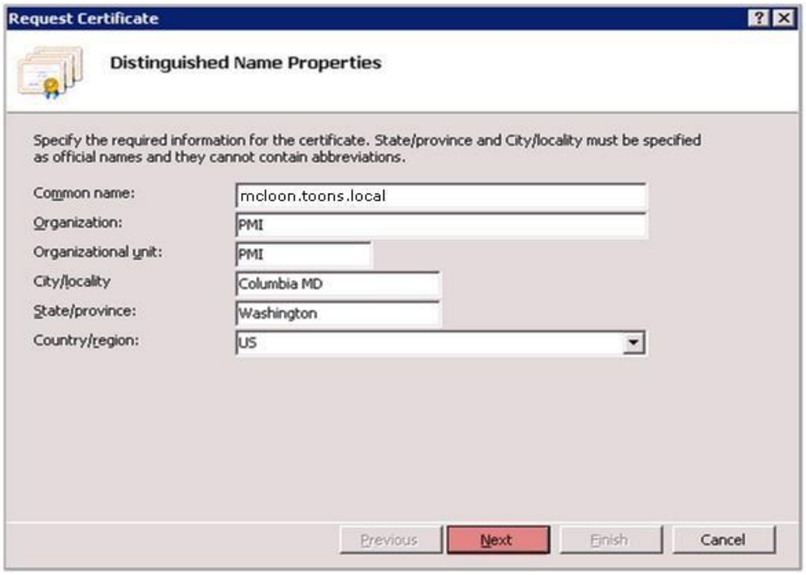
Distinguished Name Properties

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

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

   Example: mcloon.toons.local



Request Certificate

Distinguished Name Properties

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

Common name: mcloon.toons.local

Organization: PMI

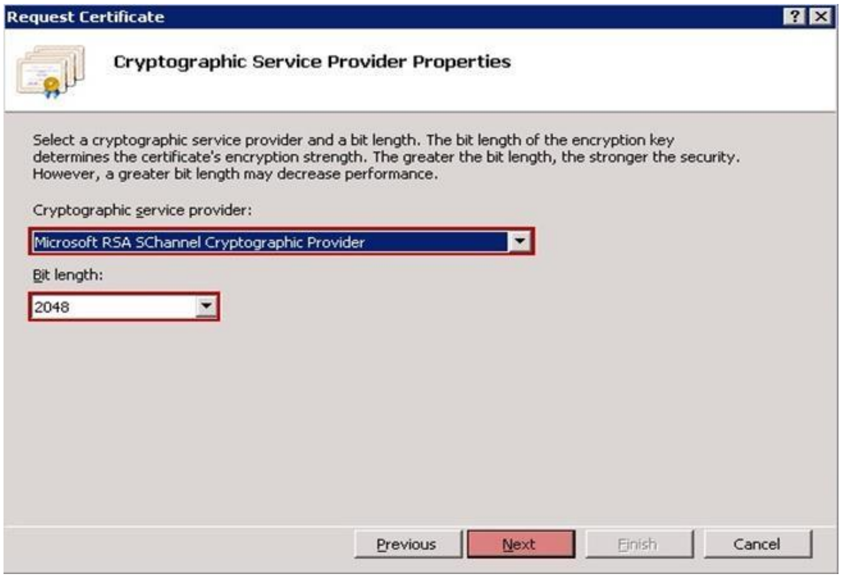
Organizational unit: PMI

City/locality: Columbia MD

State/province: Washington

Country/region: US

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



Request Certificate

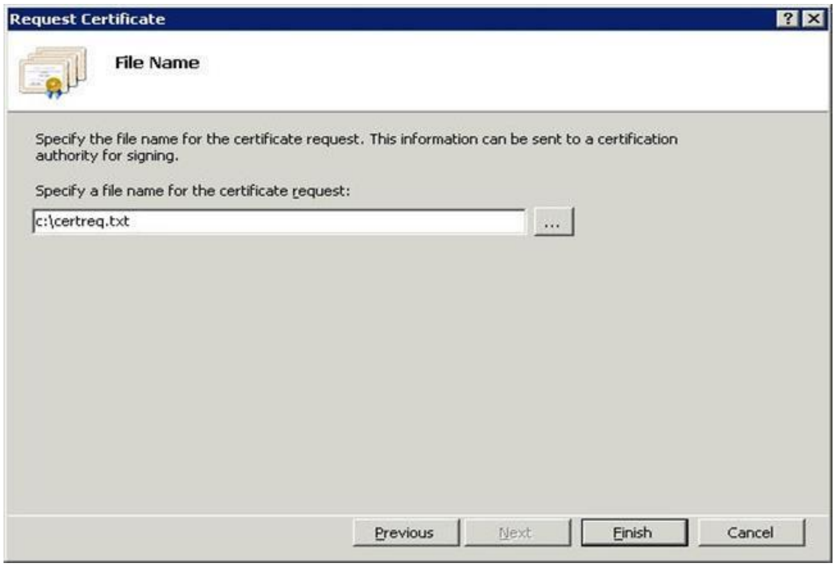
Cryptographic Service Provider Properties

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

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

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



Request Certificate

File Name

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

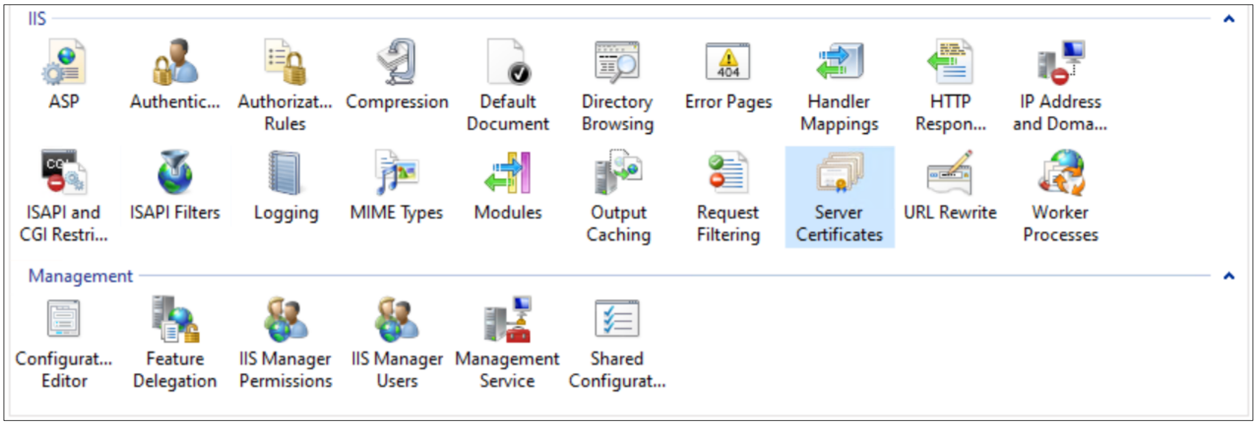
11. Click **Finish**.

12. Send this request file to the certificate vendor.

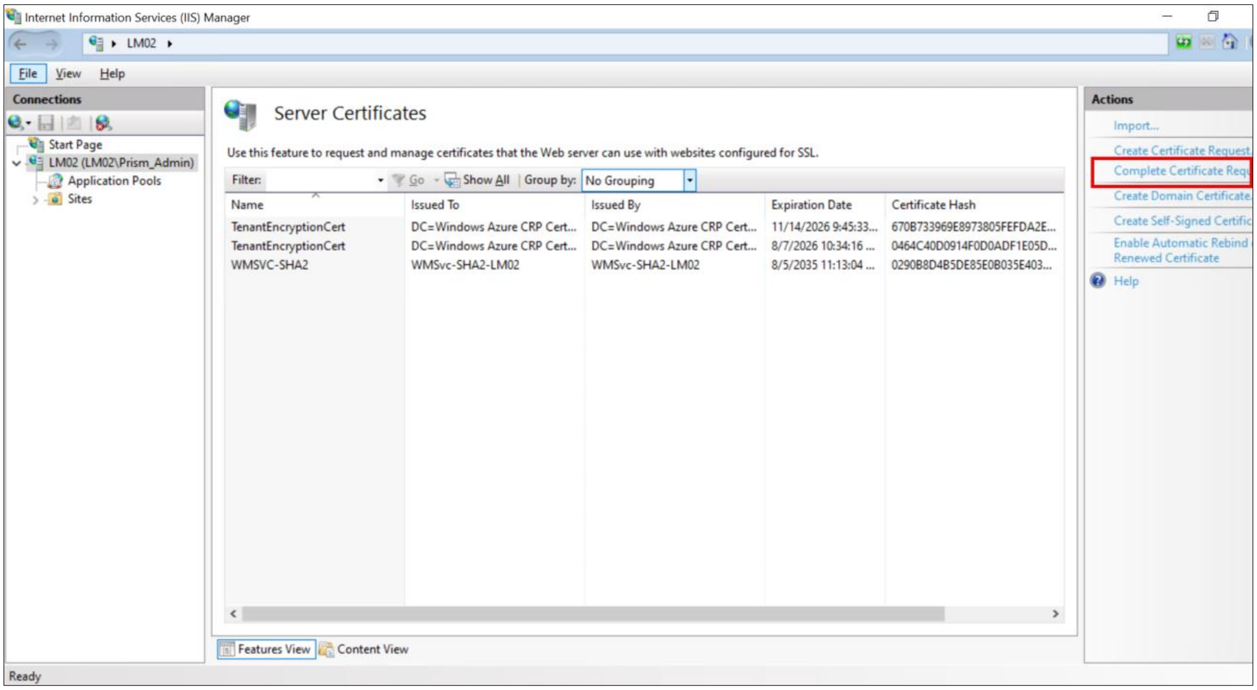
Step 2: Installing the Certificate.

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

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



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


Internet Information Services (IIS) Manager
LM02
File
View
Help
Connections
Start Page
LM02 (LM02\Prism_Admin)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Requ
Create Domain Certificate...
Create Self-Signed Certific
Enable Automatic Rebind Renewed Certificate
Help
Features View
Content View
Ready

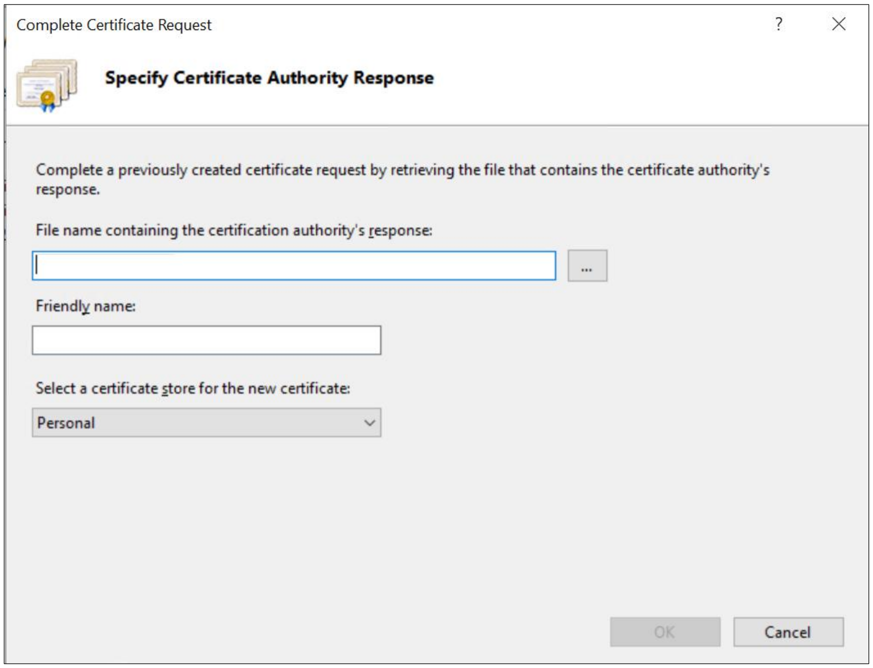
Server Certificates

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

Filter: Go Show All Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Hash
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	11/14/2026 9:45:33...	670B733969E8973805FEFDA2E...
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	8/7/2026 10:34:16 ...	0464C40D0914F0D0ADF1E05D...
WMSVC-SHA2	WMSvc-SHA2-LM02	WMSvc-SHA2-LM02	8/5/2035 11:13:04 ...	0290B8D4B5DE85E0B035E403...

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



Specify Certificate Authority Response

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

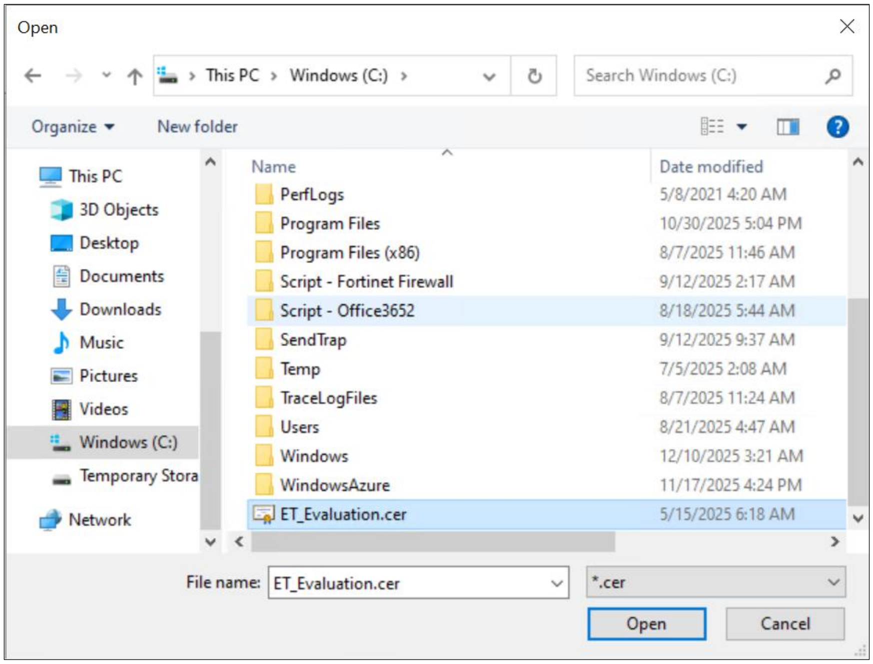
File name containing the certification authority's response:

Friendly name:

Select a certificate store for the new certificate:

Personal

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

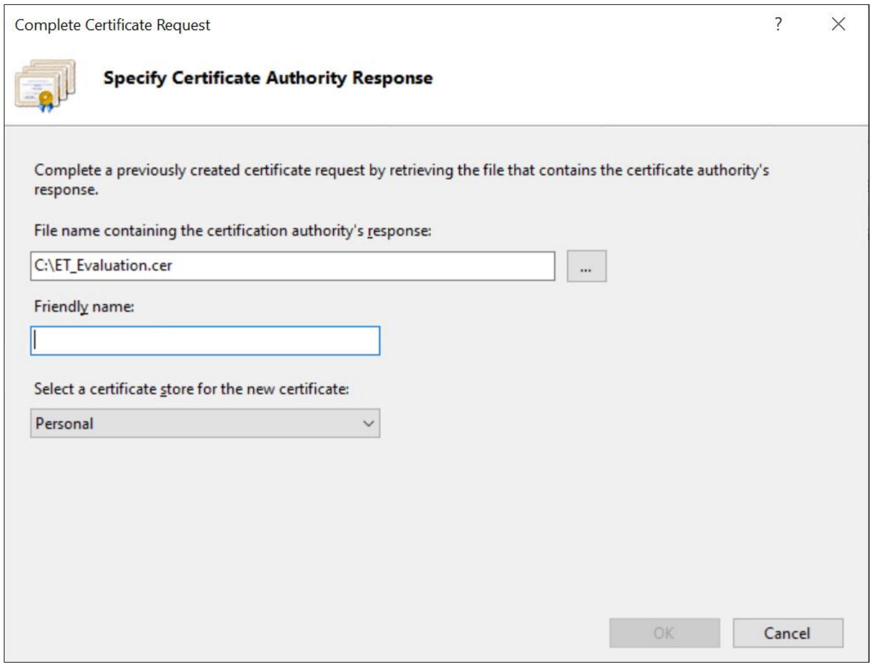


Name	Date modified
PerfLogs	5/8/2021 4:20 AM
Program Files	10/30/2025 5:04 PM
Program Files (x86)	8/7/2025 11:46 AM
Script - Fortinet Firewall	9/12/2025 2:17 AM
Script - Office3652	8/18/2025 5:44 AM
SendTrap	9/12/2025 9:37 AM
Temp	7/5/2025 2:08 AM
TraceLogFiles	8/7/2025 11:24 AM
Users	8/21/2025 4:47 AM
Windows	12/10/2025 3:21 AM
WindowsAzure	11/17/2025 4:24 PM
ET_Evaluation.cer	5/15/2025 6:18 AM

File name: ET_Evaluation.cer

*.cer

7. Click **Open**.



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:

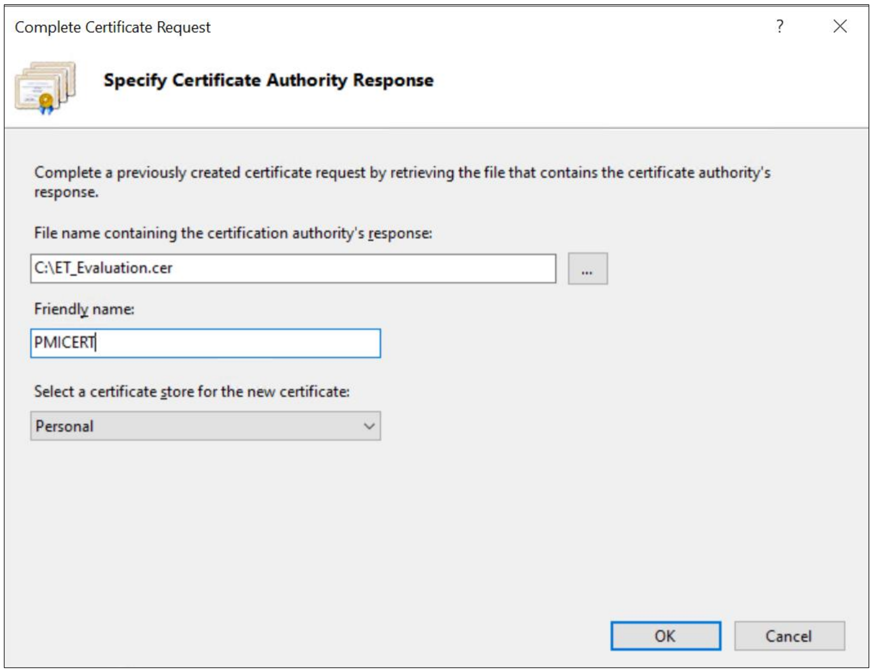
C:\ET_Evaluation.cer

Friendly name:

Select a certificate store for the new certificate:

Personal

8. Type a relevant name in the **Friendly name** field 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.

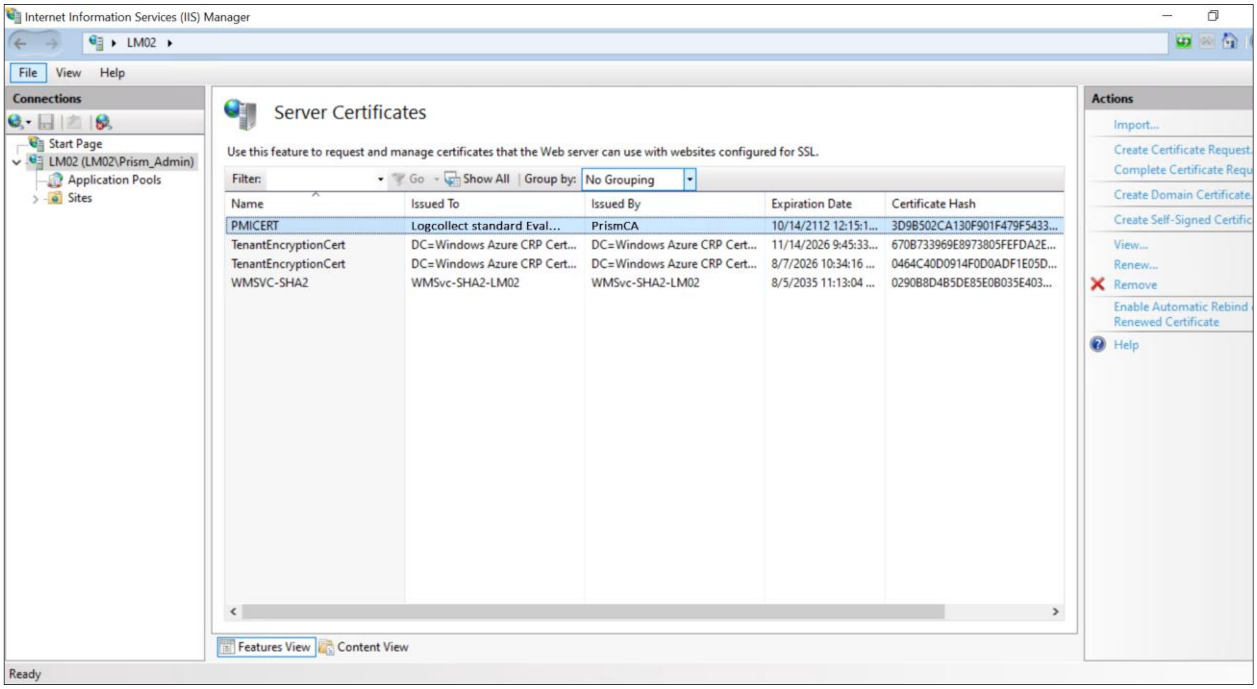
File name containing the certification authority's response: C:\ET_Evaluation.cer

Friendly name: PMICERT

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



Internet Information Services (IIS) Manager

LM02
File
View
Help
Connections
Start Page
LM02 (LM02\Prism_Admin)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Requ
Create Domain Certificate...
Create Self-Signed Certific
View...
Renew...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Server Certificates

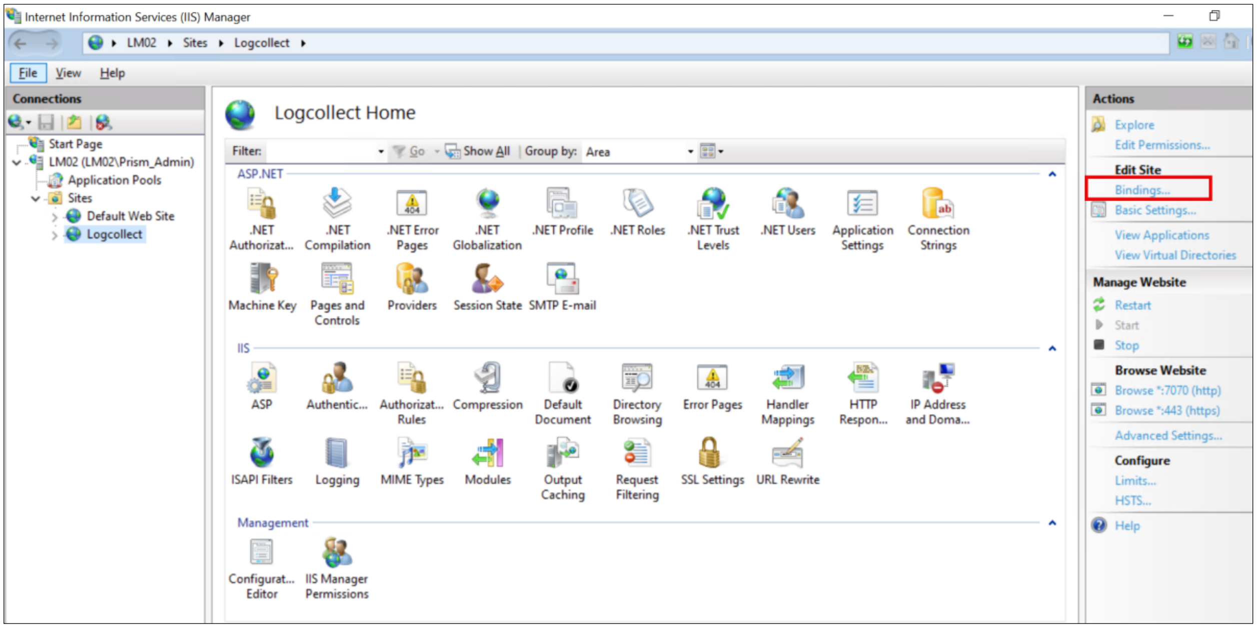
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All Group by: No Grouping

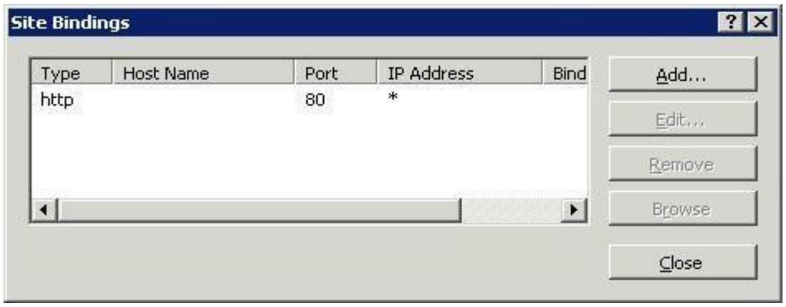
Name	Issued To	Issued By	Expiration Date	Certificate Hash
PMICERT	Logcollect standard Eval...	PrismCA	10/14/2112 12:15:1...	3D9B502CA130F901F479F5433...
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	11/14/2026 9:45:33...	670B733969E8973805FEFDA2E...
TenantEncryptionCert	DC=Windows Azure CRP Cert...	DC=Windows Azure CRP Cert...	8/7/2026 10:34:16 ...	0464C40D0914F0D0ADF1E05D...
WMSVC-SHA2	WMSvc-SHA2-LM02	WMSvc-SHA2-LM02	8/5/2035 11:13:04 ...	0290B8D4B5DE85E0B035E403...

Step 3: Binding the certificate to Logcollect.

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

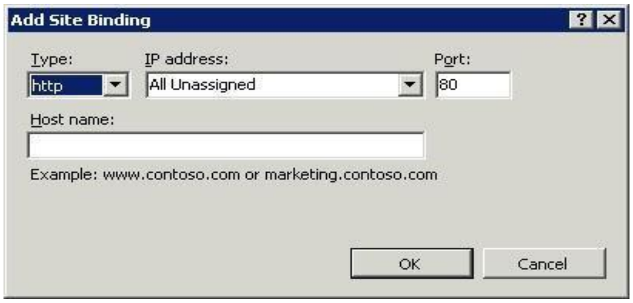


5. The **Site Bindings** dialog box appears as shown below:


Site Bindings

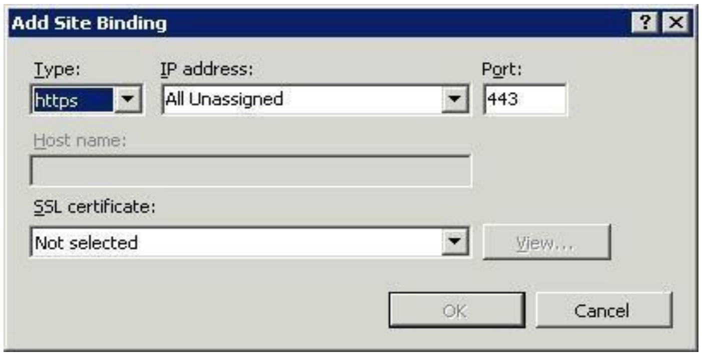
Type	Host Name	Port	IP Address	Bind
http		80	*	

6. Click **Add**.

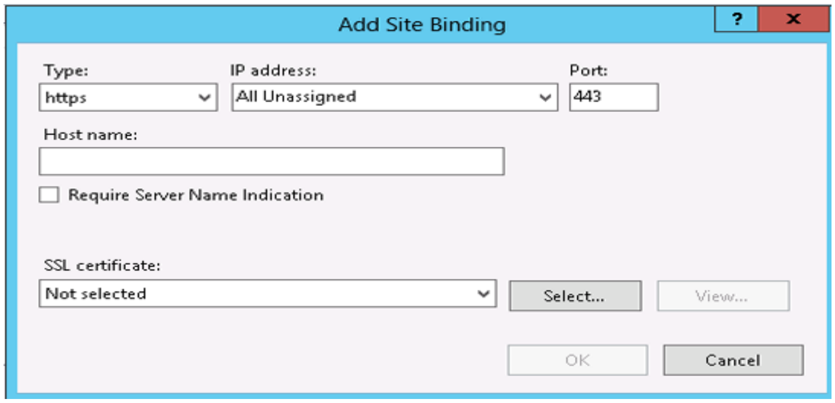

Add Site Binding

Type: http
IP address: All Unassigned
Port: 80
Host name:
Example: www.contoso.com or marketing.contoso.com

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

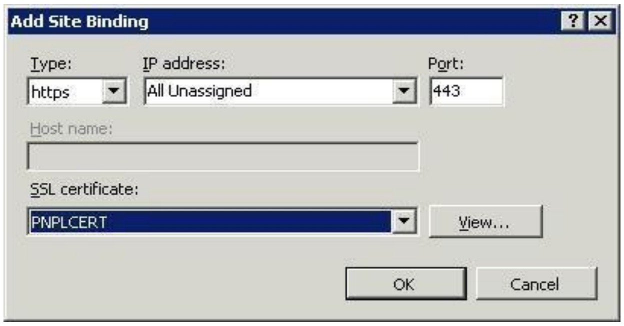


Type: https
IP address: All Unassigned
Port: 443
Host name:
SSL certificate: Not selected

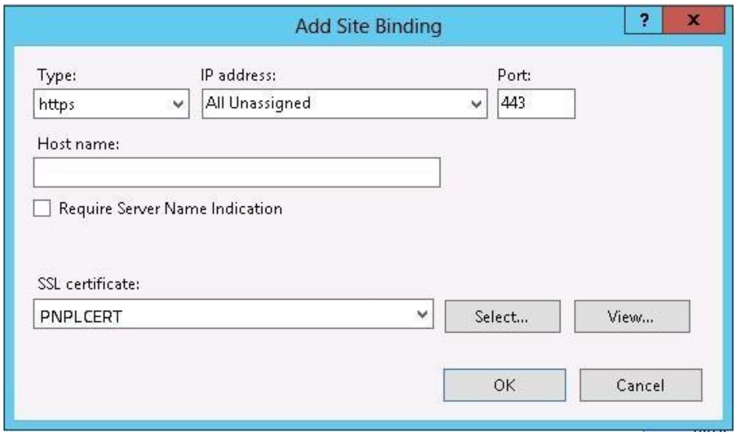


Type: https
IP address: All Unassigned
Port: 443
Host name:
☐ Require Server Name Indication
SSL certificate: Not selected

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

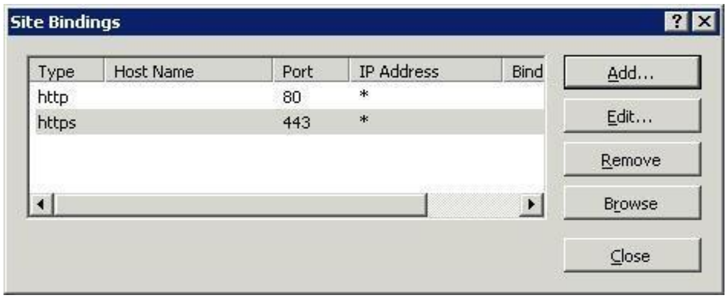


Type: https
IP address: All Unassigned
Port: 443
Host name:
SSL certificate: PNPLCERT



Type: https
IP address: All Unassigned
Port: 443
Host name:
☐ Require Server Name Indication
SSL certificate: PNPLCERT

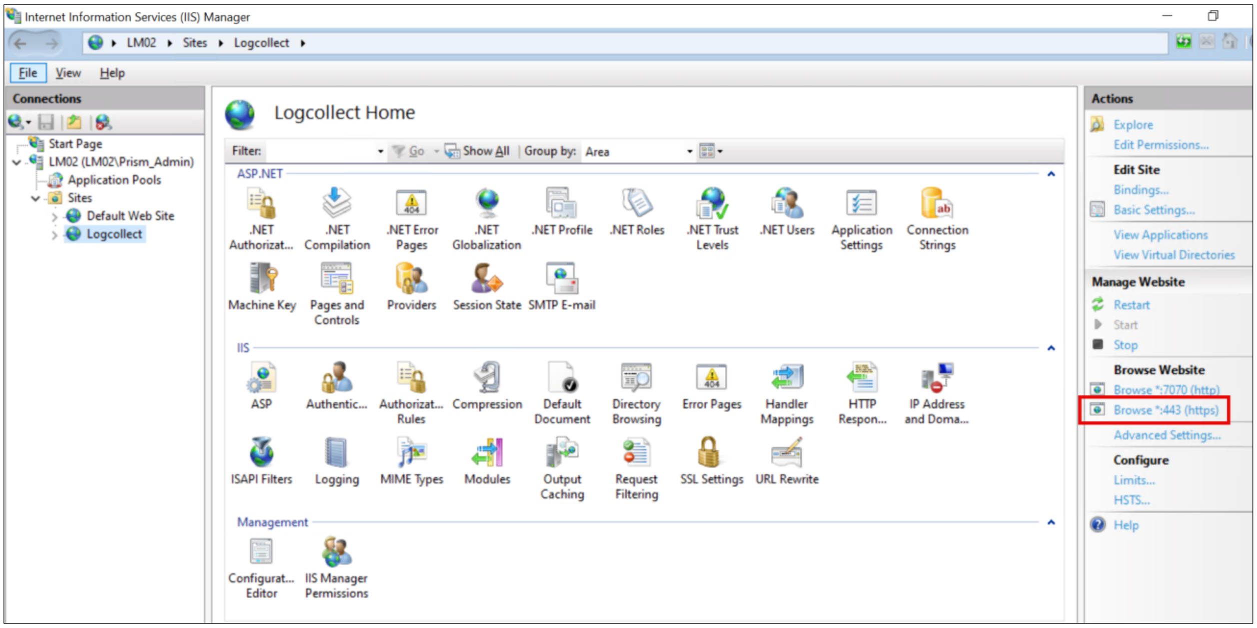
9. Click **OK**. The binding for port 443 will be listed.



Site Bindings

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

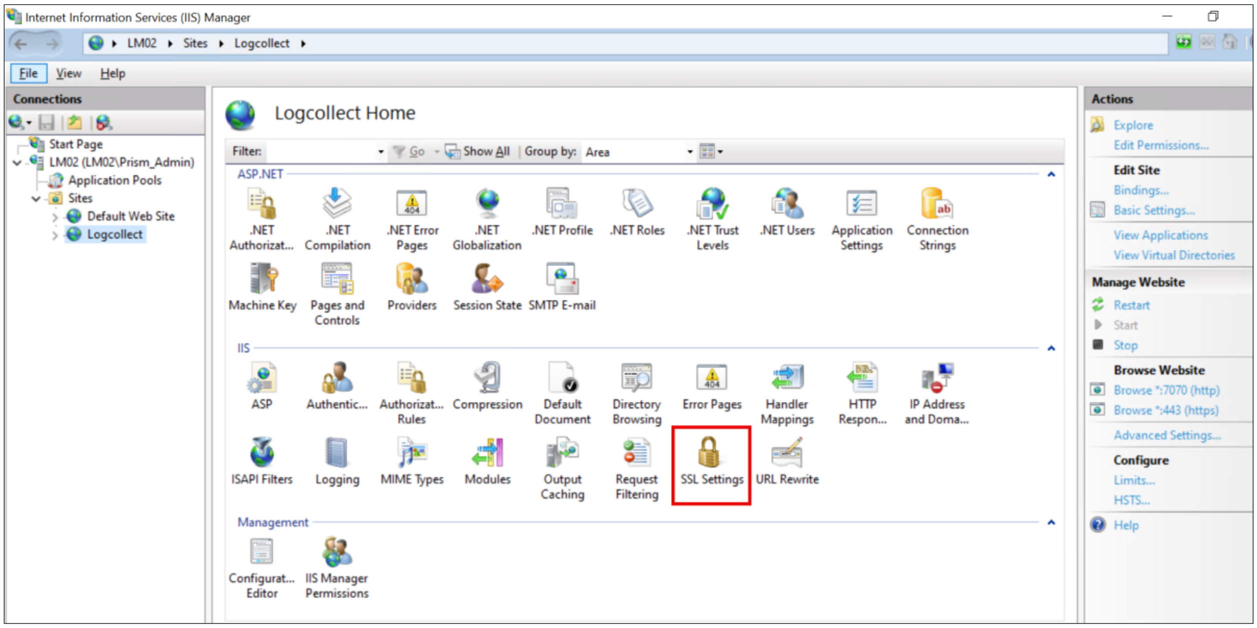
10. Click **Close**. The newly added https website will be listed under **Browse Web Site**.



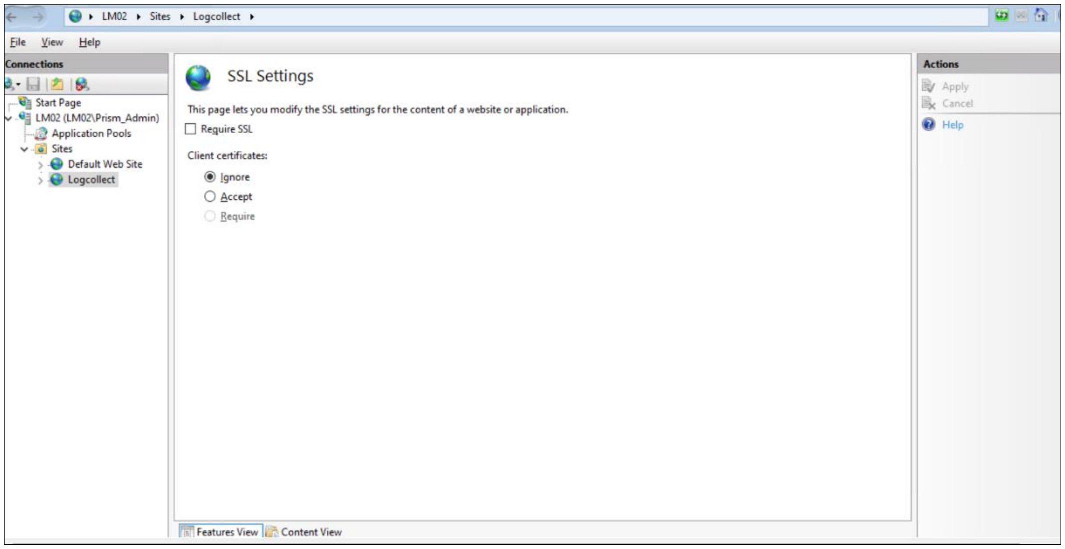
Step 4: Configure SSL Settings.

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

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



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



SSL Settings

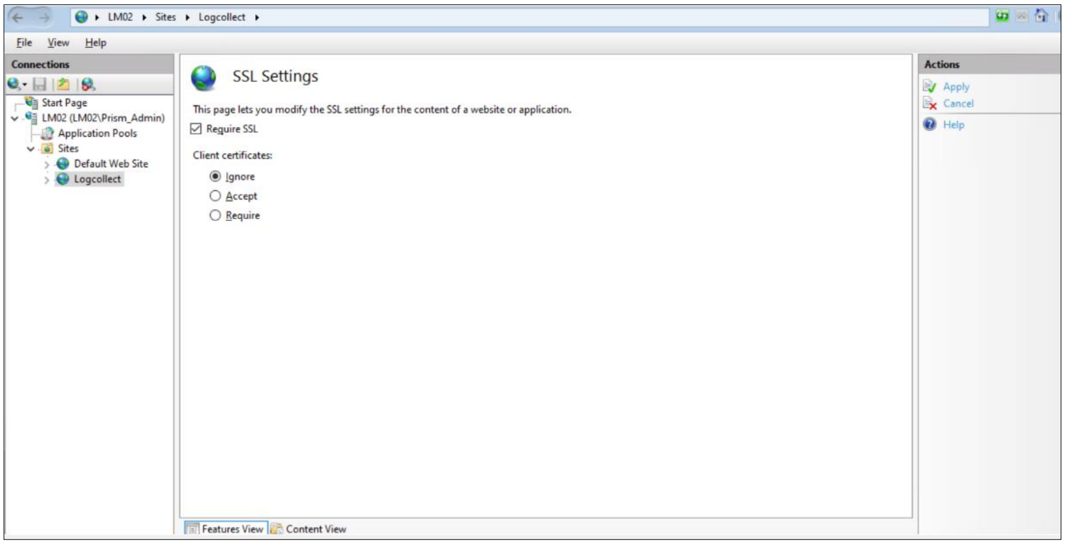
This page lets you modify the SSL settings for the content of a website or application.

☐ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

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



SSL Settings

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

☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

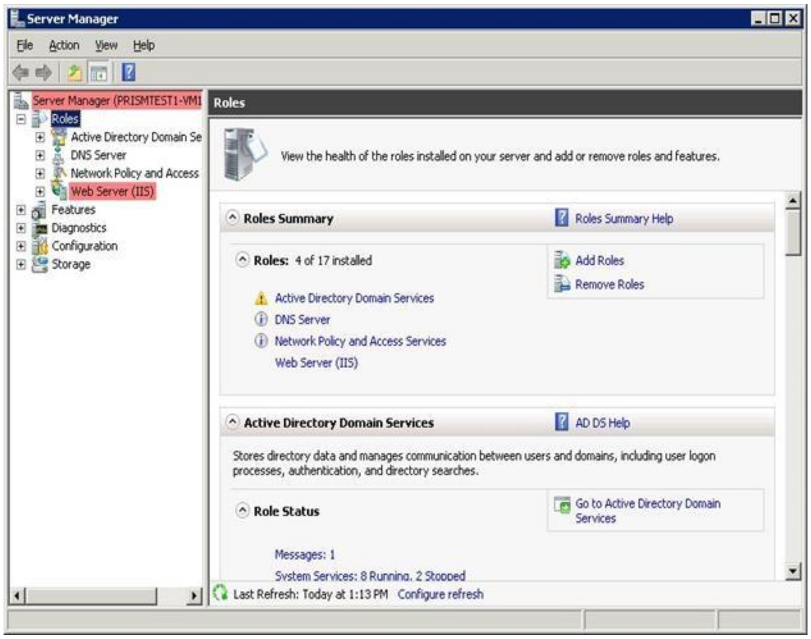
7. Close the **IIS Manager**.

Step 5: Create FTP Service.

Note

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

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.

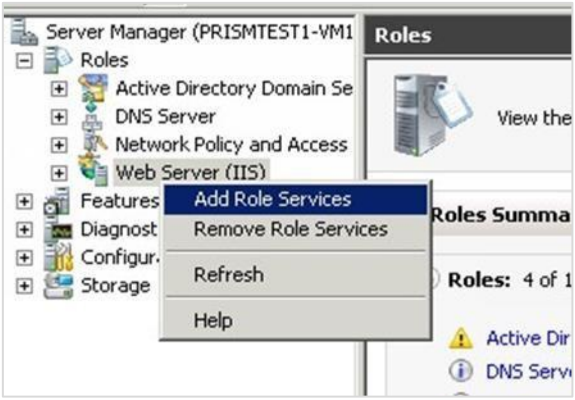
Role Status

Messages: 1
System Services: 8 Running, 2 Stopped

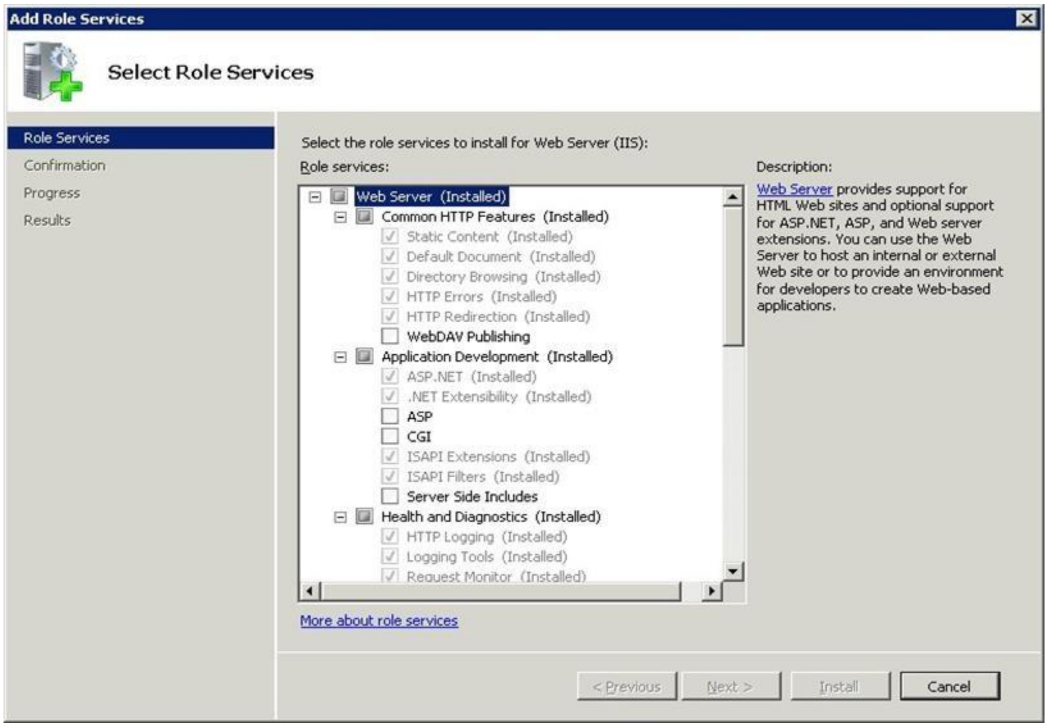
Last Refresh: Today at 1:13 PM

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

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



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



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

Role services:

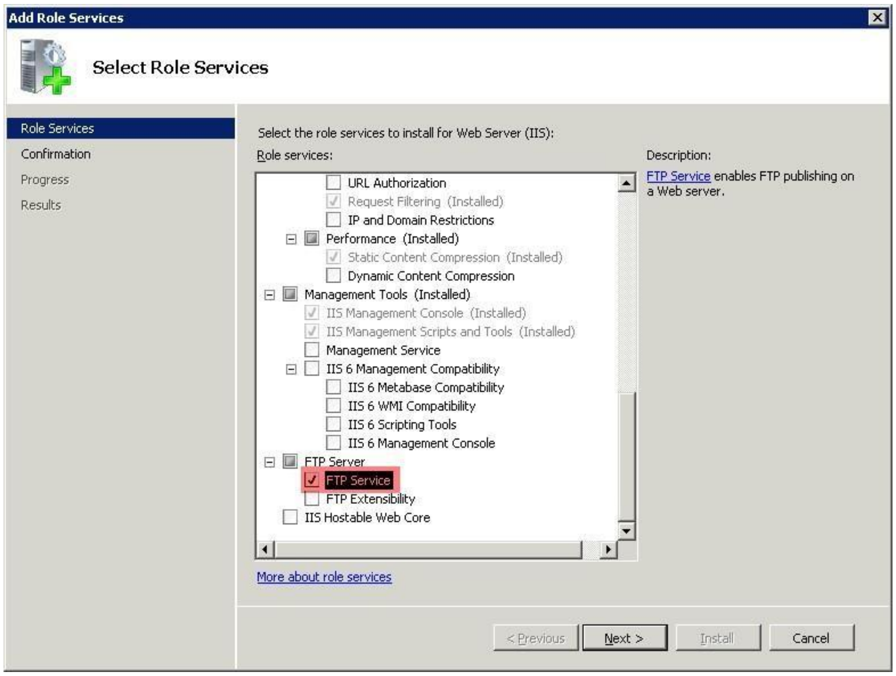
▣ Web Server (Installed)
  ▣ Common HTTP Features (Installed)
    ☑ Static Content (Installed)
    ☑ Default Document (Installed)
    ☑ Directory Browsing (Installed)
    ☑ HTTP Errors (Installed)
    ☑ HTTP Redirection (Installed)
    □ WebDAV Publishing
  ▣ Application Development (Installed)
    ☑ 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.

More about role services

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



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

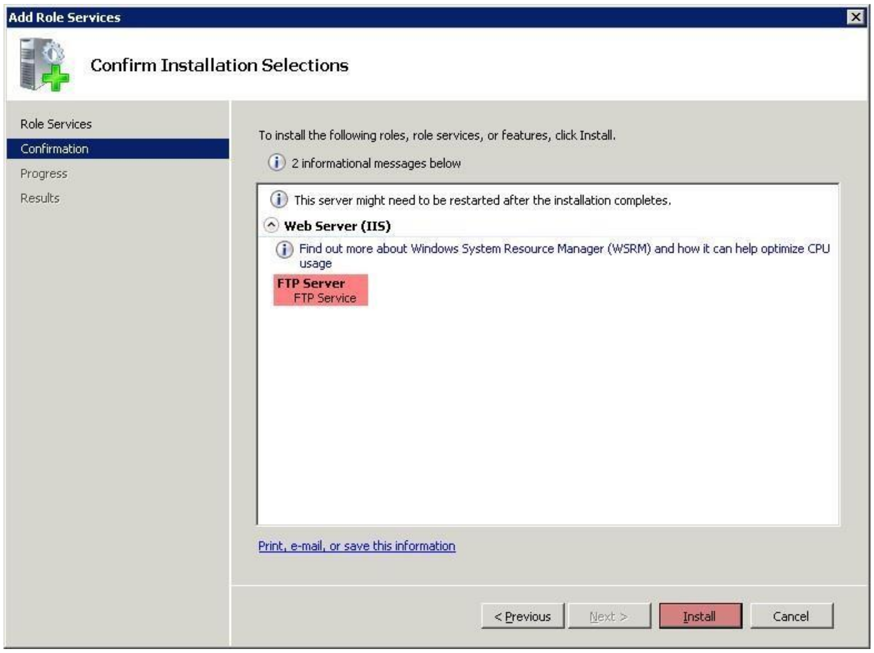
Role services:

- ☐ 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.

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



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

ⓘ 2 informational messages below

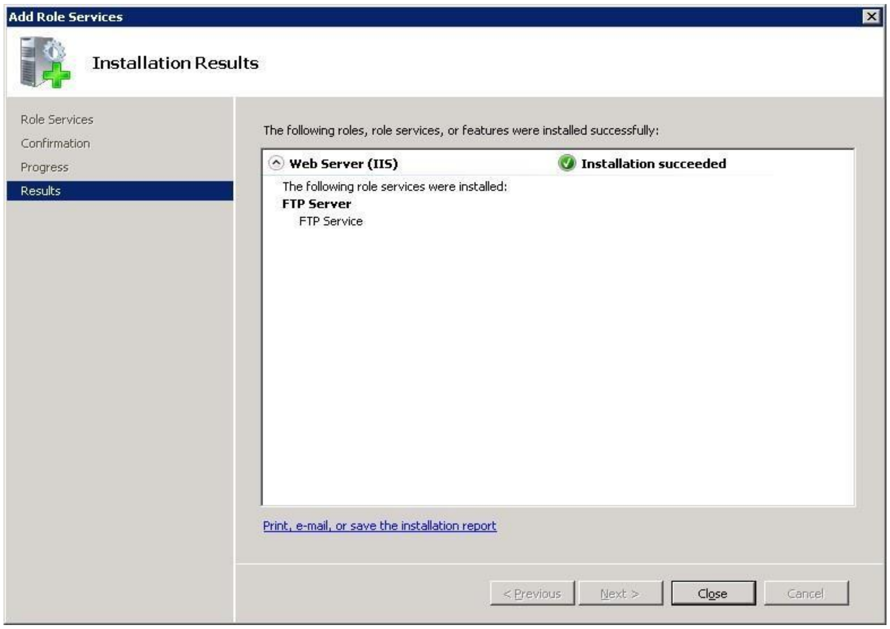
ⓘ This server might need to be restarted after the installation completes.

Web Server (IIS)

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

FTP Server
FTP Service

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



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

Web Server (IIS) — Installation succeeded

The following role services were installed:

FTP Server

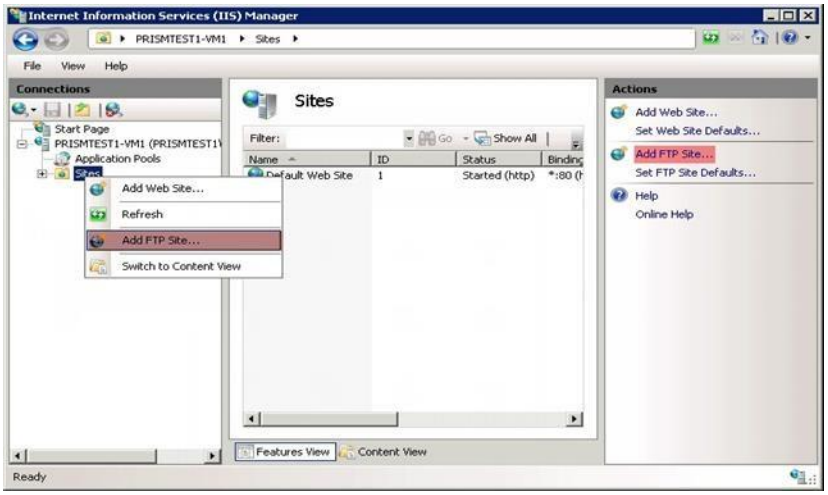
FTP Service

Step 6: Create an SSL-enabled FTP Site.

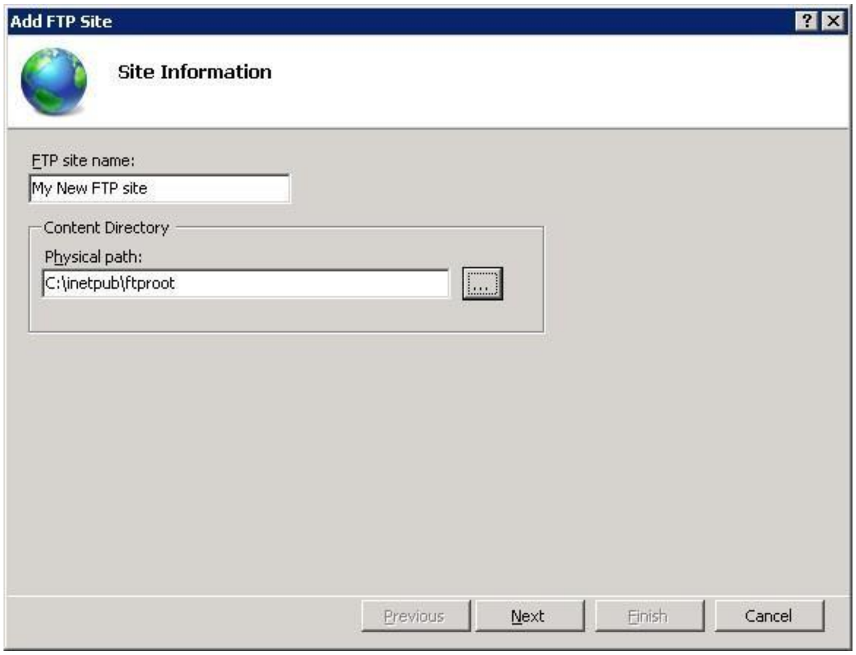
1. Click the **Start** button, select **Programs,** and then select **Administrative Tools.**
2. Select **Internet Information Services (IIS) Manager**.
3. In the **Connections** pane, select **Sites** node.
4. Right-click the **Sites** node, and then click **Add FTP Site.**

   (OR)

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



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



Add FTP Site

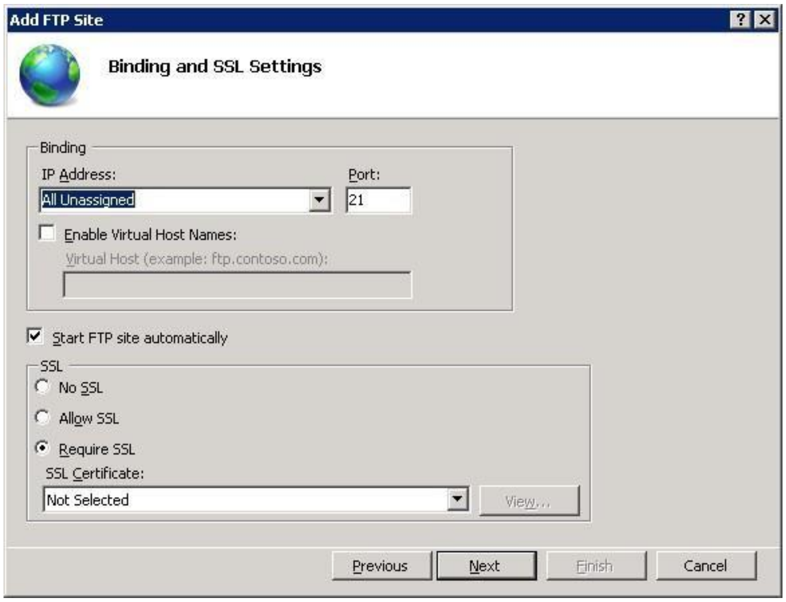
Site Information

FTP site name: My New FTP site

Content Directory

Physical path: C:\inetpub\ftproot

6. Click the **Next** button.



Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 21

□ Enable Virtual Host Names:

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

☑ Start FTP site automatically

SSL

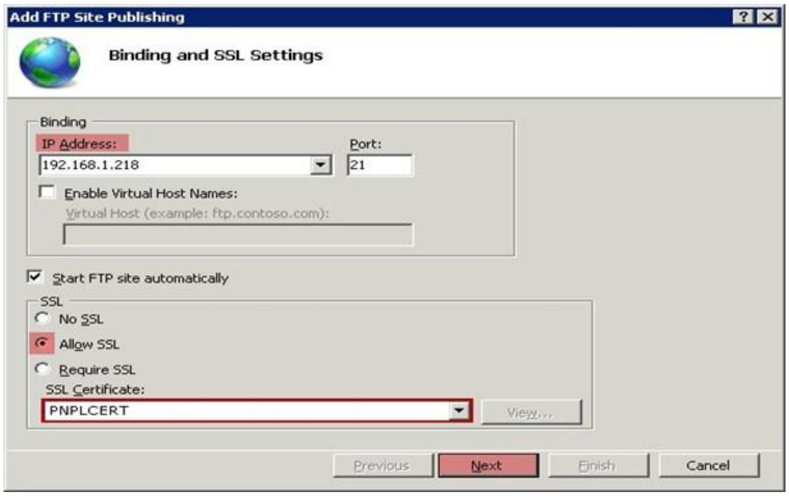
○ No SSL

○ Allow SSL

● Require SSL

SSL Certificate: Not Selected

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



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

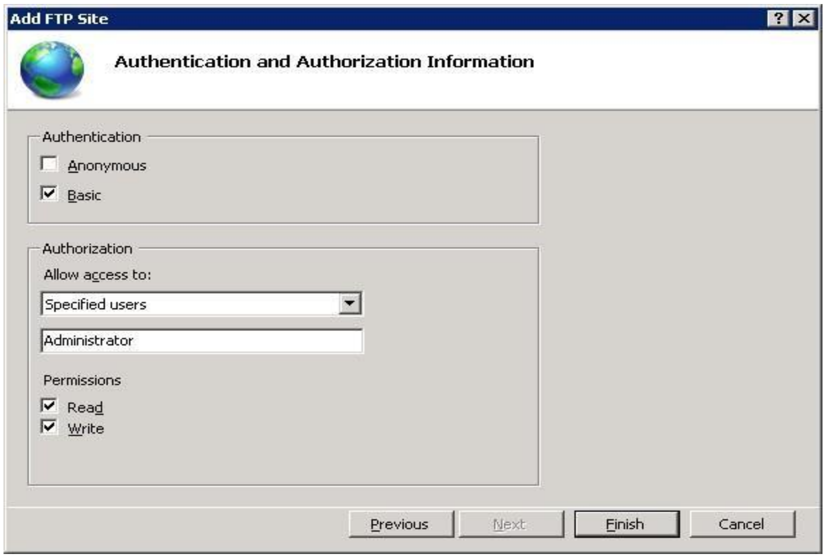
○ No SSL

● Allow SSL

○ Require SSL

SSL Certificate: PNPLCERT

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



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.

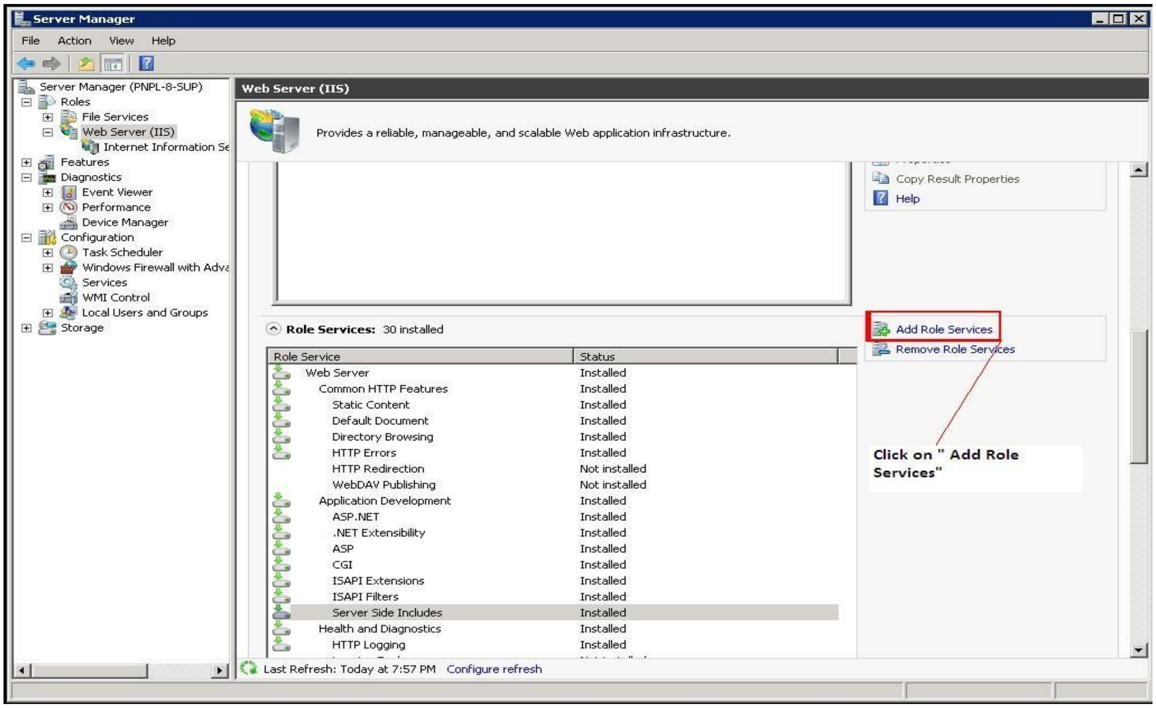
3.3 Restricting Logcollect Web Console Access

Configuring IP address and domain name restrictions in Internet Information Services (IIS) allows you to permit or deny access to the web server, websites, folders, or files. The rules can be configured for remote IP addresses or based on the Domain name.
When a remote client that is not permitted access requests a resource i.e. a 403.6 (“Forbidden: IP address of the client has been rejected”) or 403.8 (“DNS name of the client is rejected”), HTTP status will be logged by Internet Information Services (IIS).

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

3.4 Installing IP and Domain Restriction in Windows

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



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

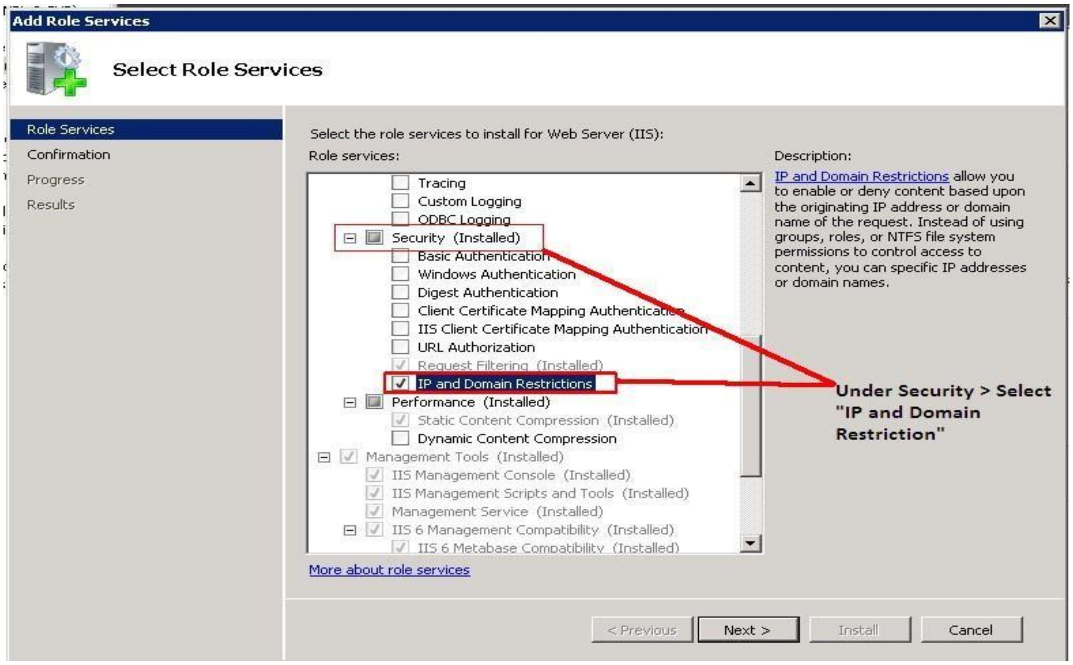
Role Services: 30 installed

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



Add Role Services

Select Role Services

Role Services
Confirmation
Progress
Results

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

Role services:

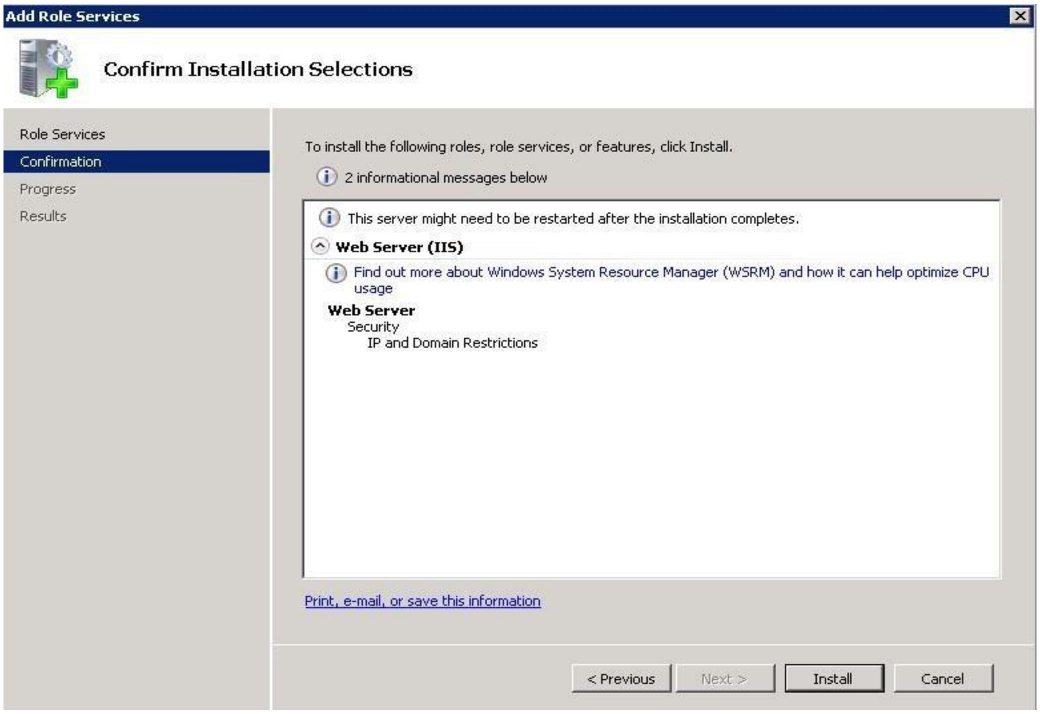
- □ Tracing
- □ Custom Logging
- □ ODBC Logging
- ⊟ ▣ Security (Installed)
  - □ Basic Authentication
  - □ Windows Authentication
  - □ Digest Authentication
  - □ Client Certificate Mapping Authentication
  - □ IIS Client Certificate Mapping Authentication
  - □ URL Authorization
  - ☑ Request Filtering (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.

More about role services

5. 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)

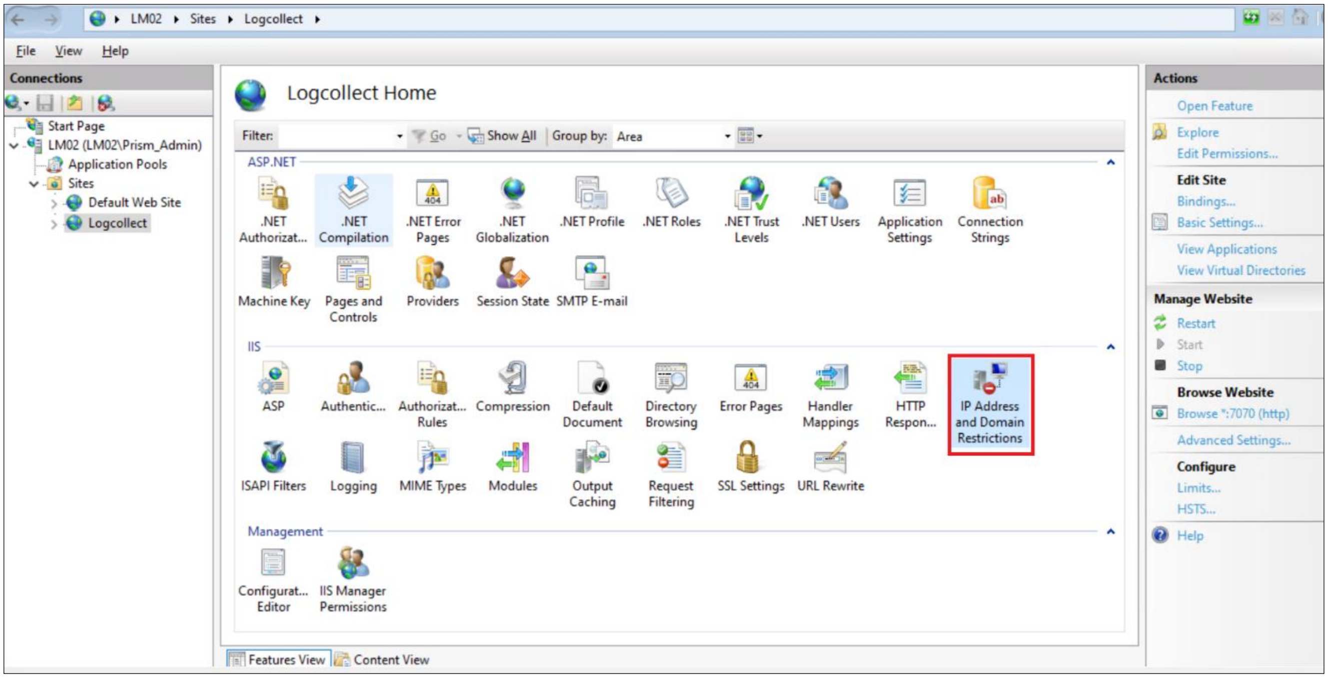
ⓘ Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
Security
IP and Domain Restrictions

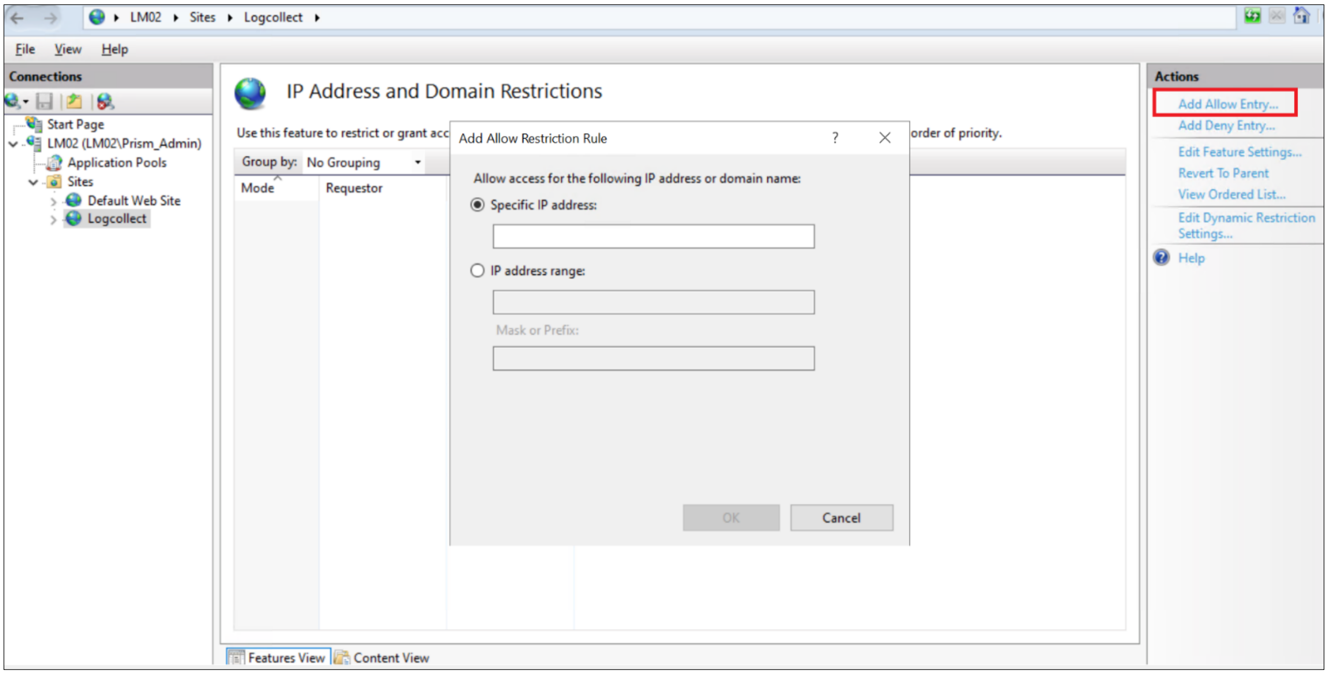
Print, e-mail, or save this information

3.5 Configuring IP Address and Domain Restrictions in Windows

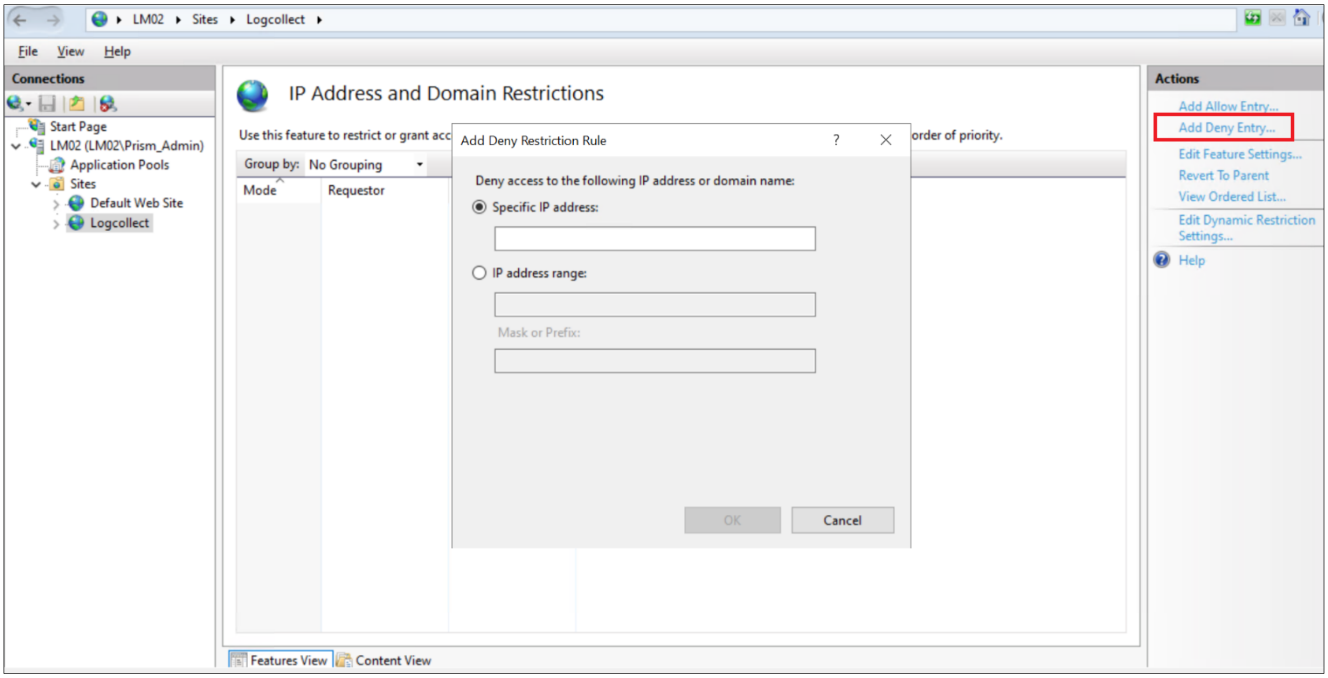
1. Open **IIS Manager**.
2. Select the **Logcollect** site.



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



(OR)



IP Address and Domain Restrictions

Use this feature to restrict or grant acc... order of priority.

Group by: No Grouping

Add Deny Restriction Rule

Deny access to the following IP address or domain name:

● Specific IP address:

○ IP address range:

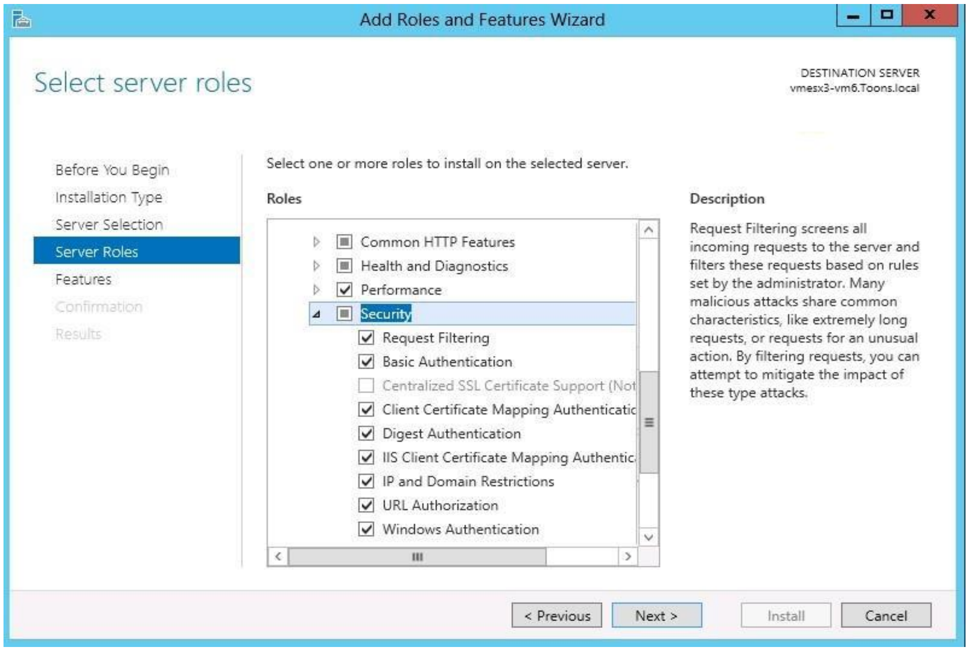
Mask or Prefix:

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

3.6 Request Filtering in IIS 10 and 11

3.6.1 Installing Request Filtering in Windows

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



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
vmesx3-vm6.Toons.local

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

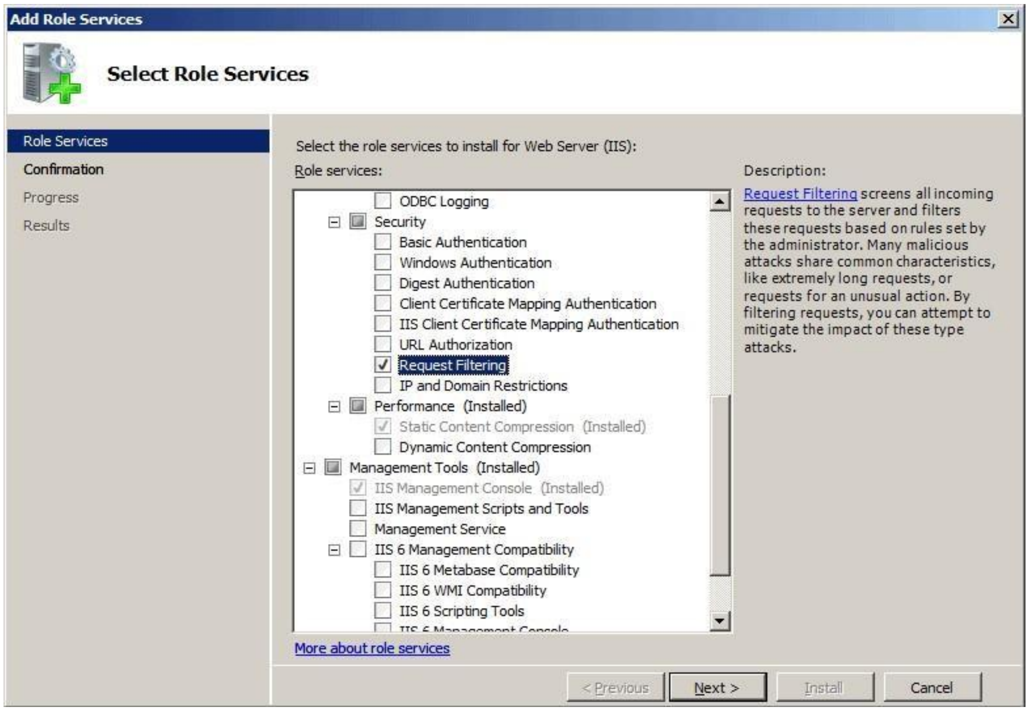
Description

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

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 >**.



Add Role Services

Select Role Services

Role Services
Confirmation
Progress
Results

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:

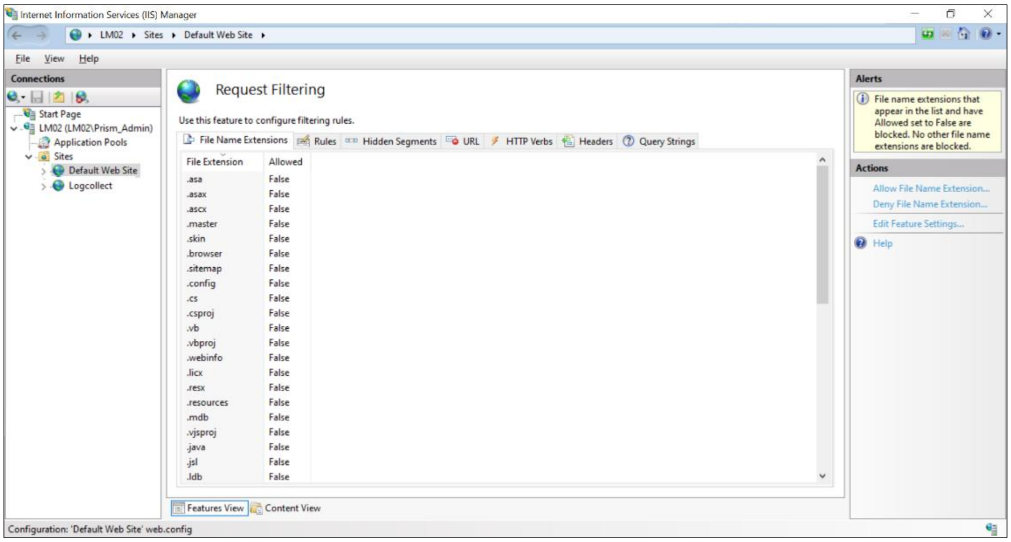
Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, like extremely long requests, or requests for an unusual action. By filtering requests, you can attempt to mitigate the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

More about role services

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

3.6.3 Allowing/Denying Access to a Specific File Name Extension

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



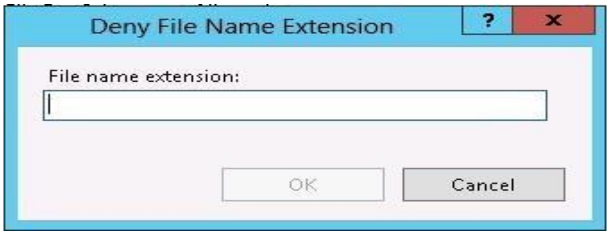
Use this feature to configure filtering rules.

File Extension	Allowed
.asa	False
.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
.mdb	False
.vjsproj	False
.java	False
.jsl	False
.ldb	False

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

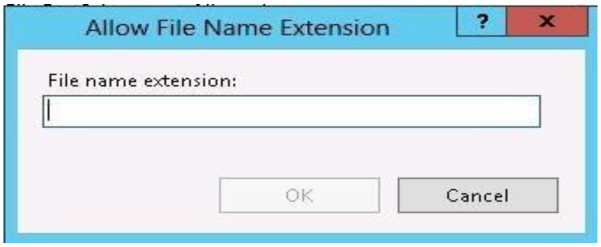
Configuration: 'Default Web Site' web.config

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



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

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



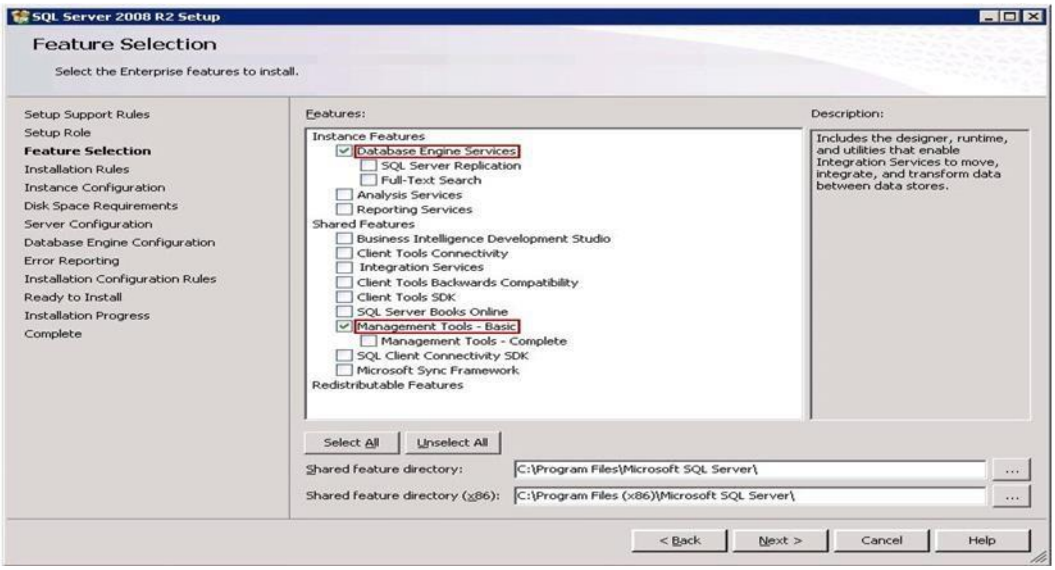
8. Enter the file name extension that you want to allow and click **OK**.

4 Securing SQL Database Server

4.1 Reducing the Surface Area for SQL Server Components

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

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



Select the Enterprise features to install.

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

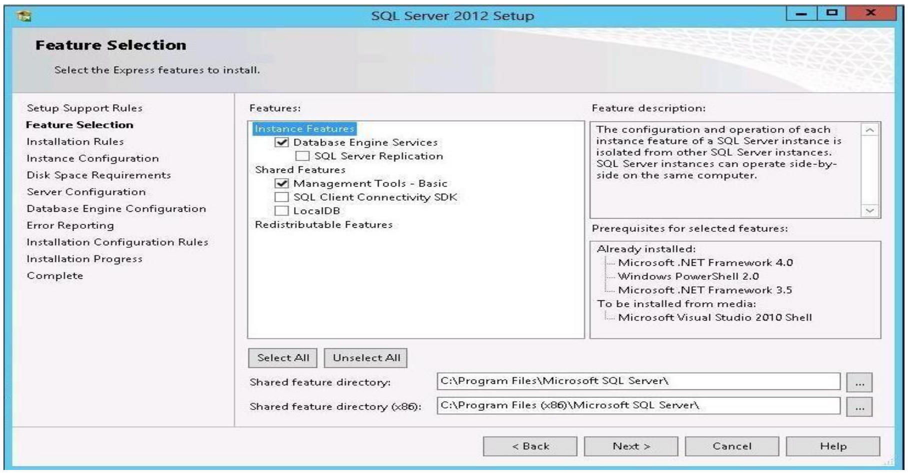
Shared Features
- ☐ Business Intelligence Development Studio
- ☐ Client Tools Connectivity
- ☐ Integration Services
- ☐ Client Tools Backwards Compatibility
- ☐ Client Tools SDK
- ☐ SQL Server Books Online
- ☑ Management Tools - Basic
  - ☐ Management Tools - Complete
- ☐ SQL Client Connectivity SDK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

Redistributable Features

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\



Select the Express features to install.

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

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

Redistributable Features

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.

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\

5. Disable the following SQL Server services.

- **SQL Server VSS Writer** service

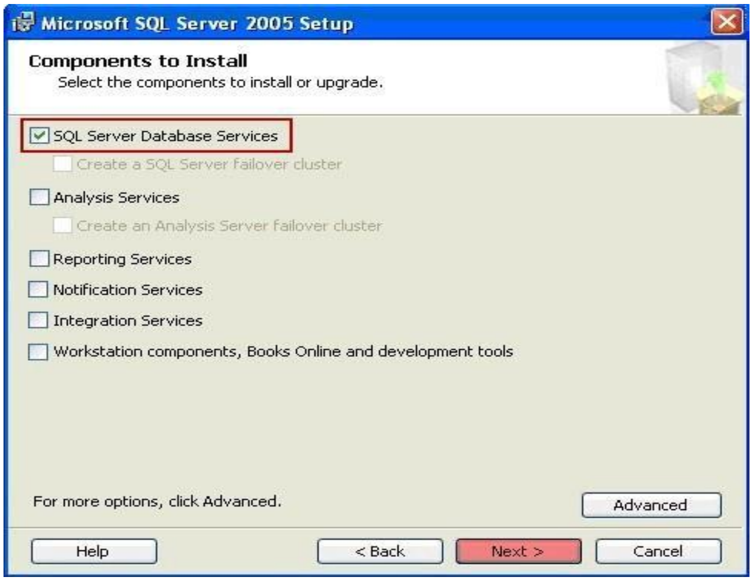
- **SQL Server Browser**
- **SQL Active Directory Helper** service

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

4.2 Reducing the Surface Area for SQL Server Services

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

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



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

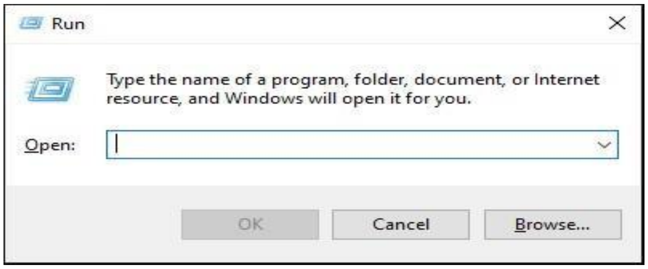
□ Workstation components, Books Online and development tools

For more options, click Advanced.

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

Follow the steps given below to disable the services.

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

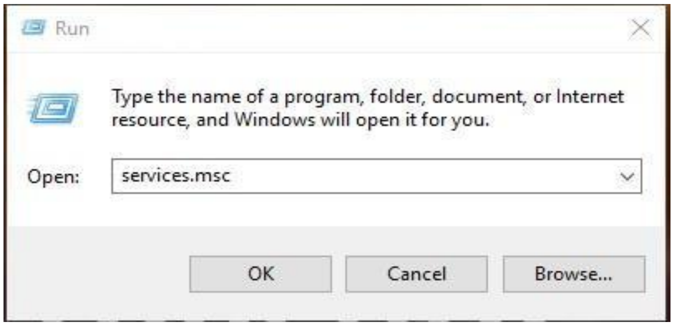


Run

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

Open:

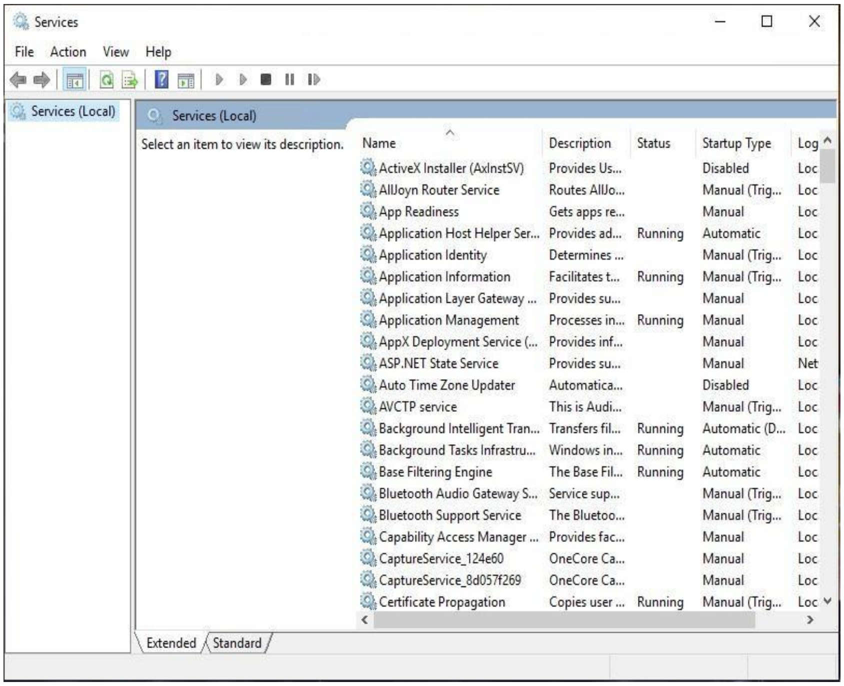
2. In the **Run** window, type '**Services.msc**', and click the **OK** button.



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

Open: services.msc

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



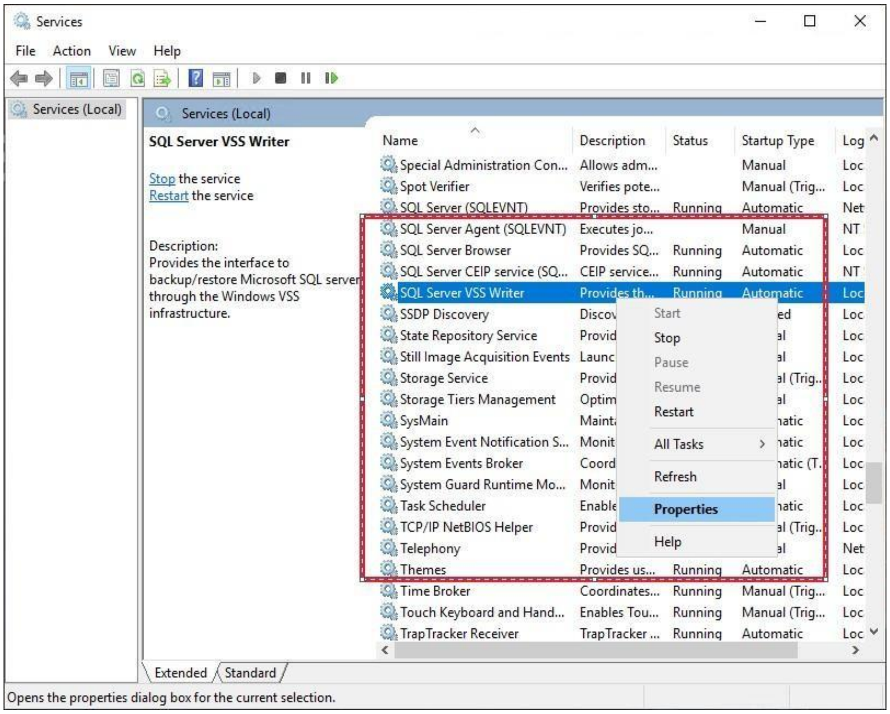
Select an item to view its description.

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

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

   Example: SQL Server VSS Writer service.

5. Right-click the service to be disabled and click **Properties**.



SQL Server VSS Writer

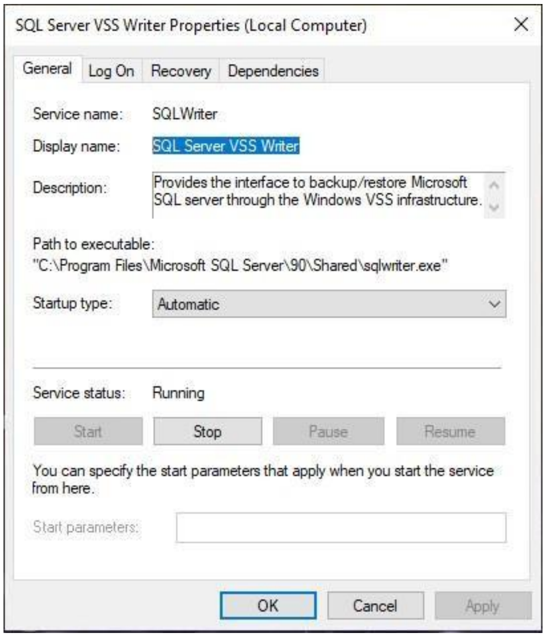
Stop the service
Restart the service

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.

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



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"

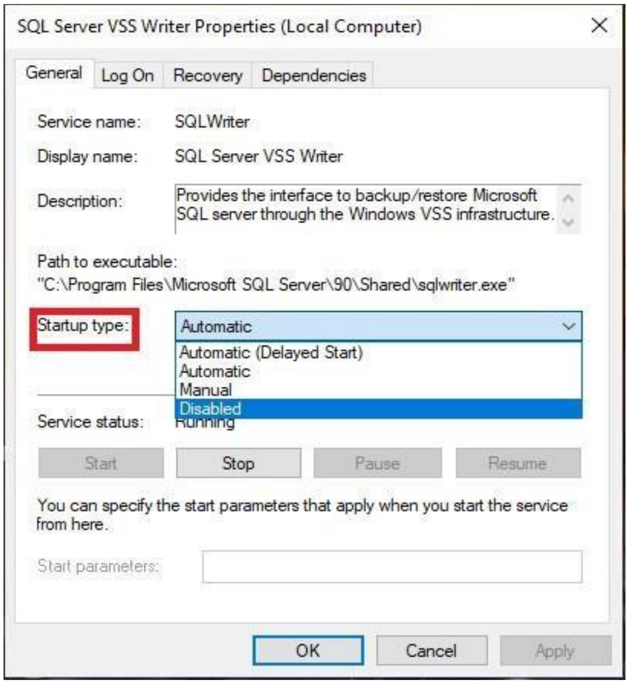
Startup type: Automatic

Service status: Running

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

Start parameters:

7. Click the **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

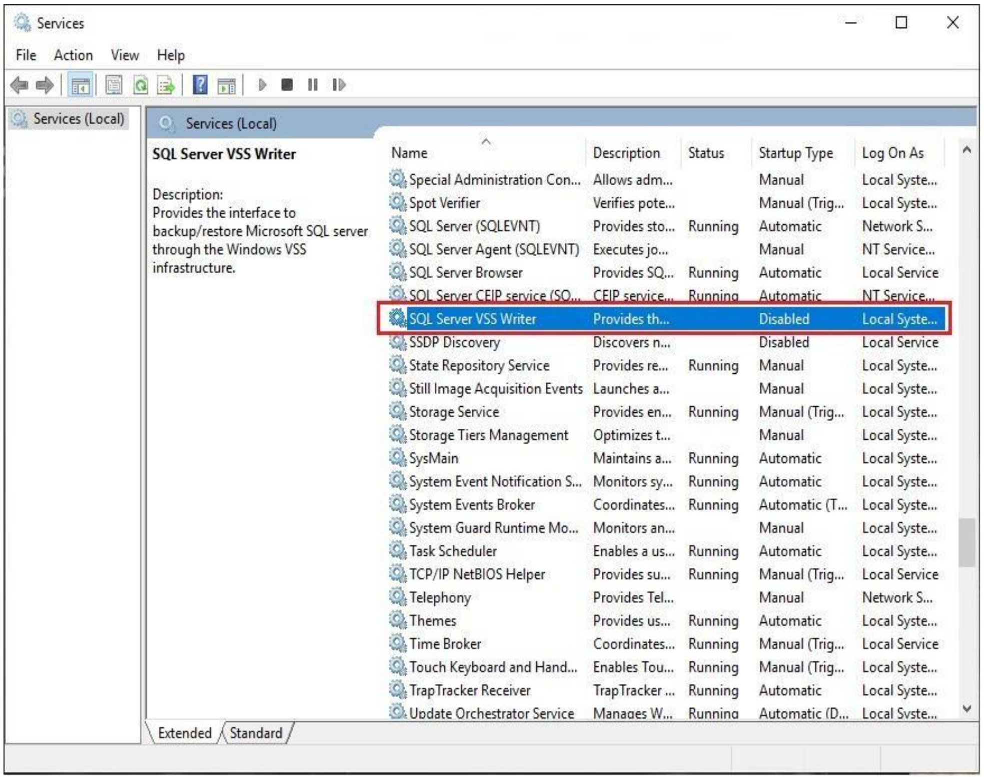
- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled

Service status: Running

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

Start parameters:

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



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 the remote indexer is enabled in the Logcollect Manager then,

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

4.2.1 SQL Server SA Account

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

5 Logcollect Settings

5.1 Securing Agent Configuration and Saving it as a Template

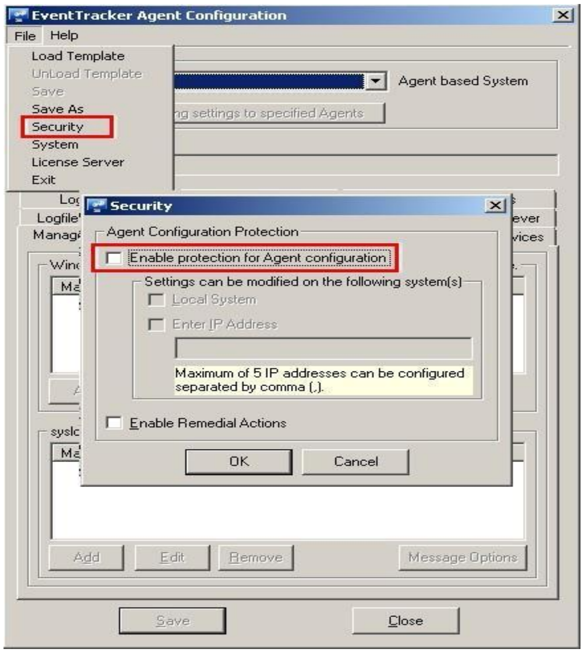
The current Agent configuration settings on the local system can be protected from being modified by any unauthorized remote system. This option allows only the local system to modify the agent settings or configure up to five IP addresses of remote systems where the modification of agent configuration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

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

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

5.2 Protecting the Current Configuration Settings for Local System

1. Go to the **Logcollect** Control Panel.
2. Double-click the **Logcollect Agent Configuration**, and then click the **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
Logfile
Manag
Win
sysl
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

Need to change this image

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

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

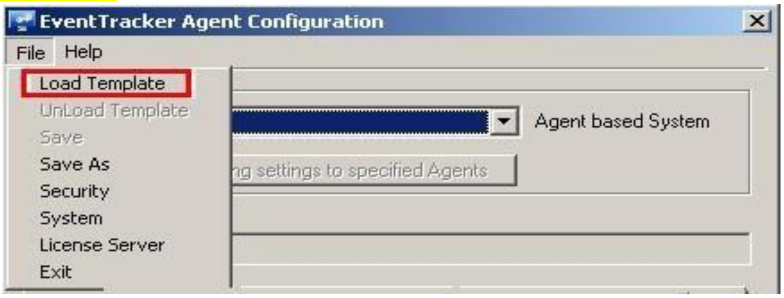
Note

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

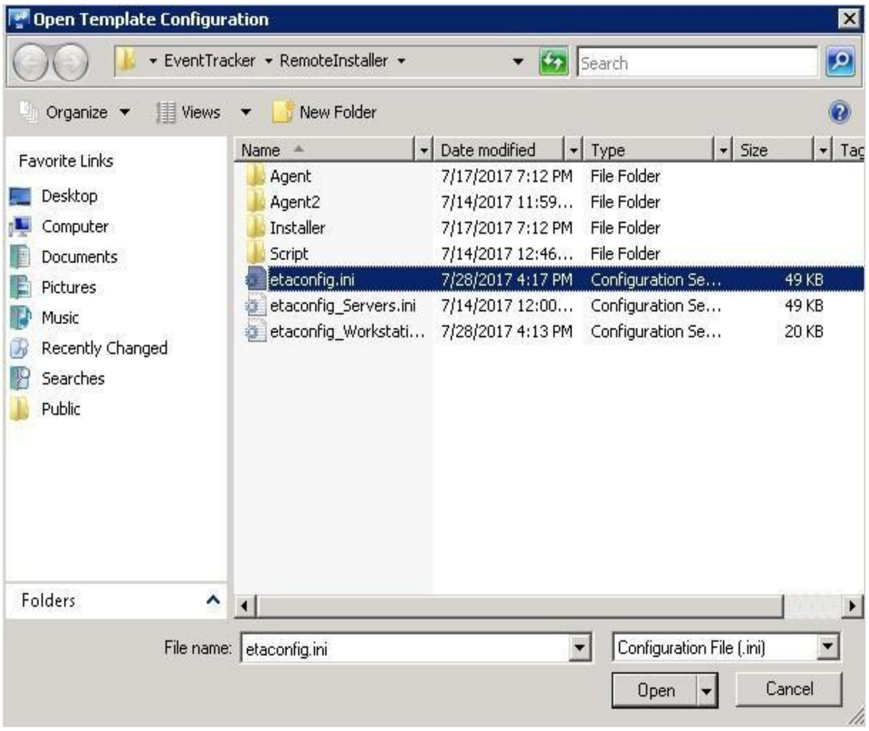
5.2.1 Applying Configuration to Agent System(s)

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

Need to change the below image



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

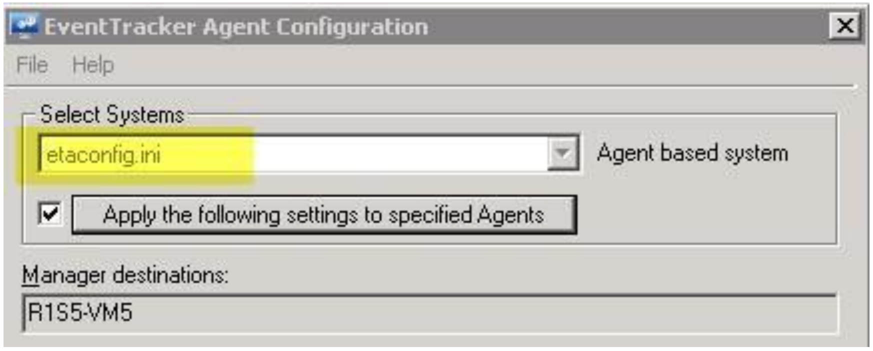


Name	Date modified	Type	Size	Tag
Agent	7/17/2017 7:12 PM	File Folder		
Agent2	7/14/2017 11:59…	File Folder		
Installer	7/17/2017 7:12 PM	File Folder		
Script	7/14/2017 12:46…	File Folder		
etaconfig.ini	7/28/2017 4:17 PM	Configuration Se…	49 KB	
etaconfig_Servers.ini	7/14/2017 12:00…	Configuration Se…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

File name: etaconfig.ini

Configuration File (.ini)

5. Logcollect loads the selected template configuration.



EventTracker Agent Configuration

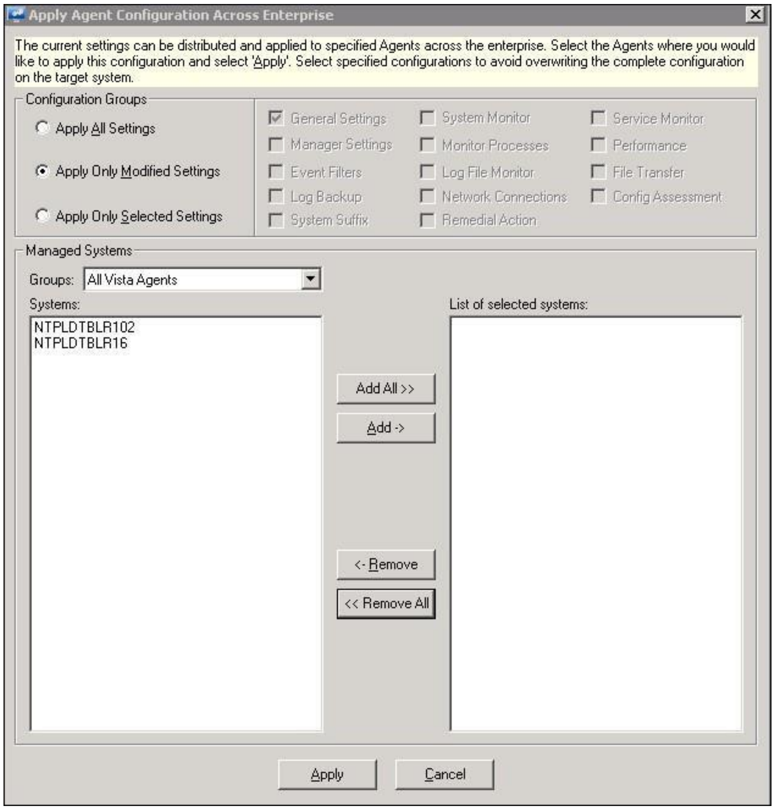
Select Systems: etaconfig.ini — Agent based system

☑ Apply the following settings to specified Agents

Manager destinations: R1S5-VM5

Need to change

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



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

Managed Systems

Groups: All Vista Agents

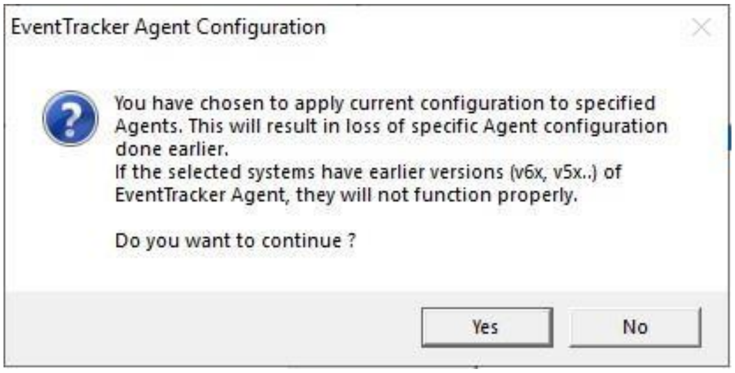
Systems:
NTPLDTBLR102
NTPLDTBLR16

List of selected systems:

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

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

11. Click the **Apply** button. Logcollect displays a warning message as shown below: Need to change the image



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 ?

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

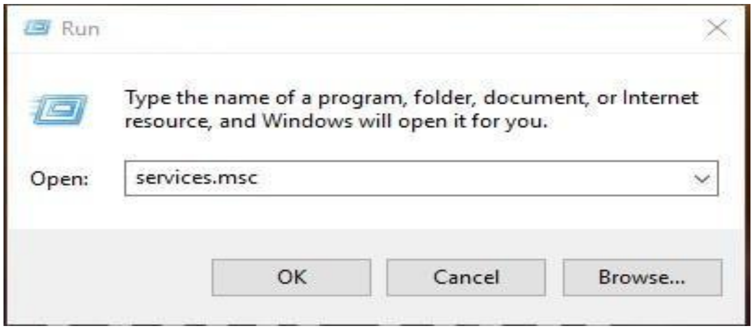
5.3 Securing EventVault Storage

Provide EventVault storage access only to the required Logcollect administrators/users.

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

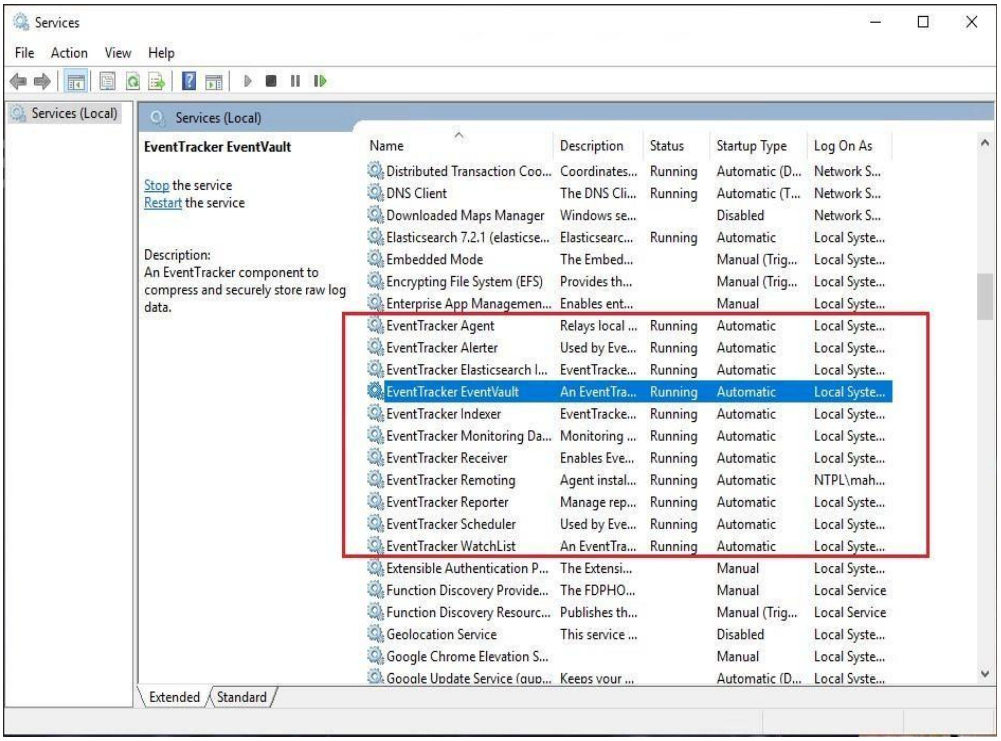


Run

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 Logcollect services. Need to change when we change the service name



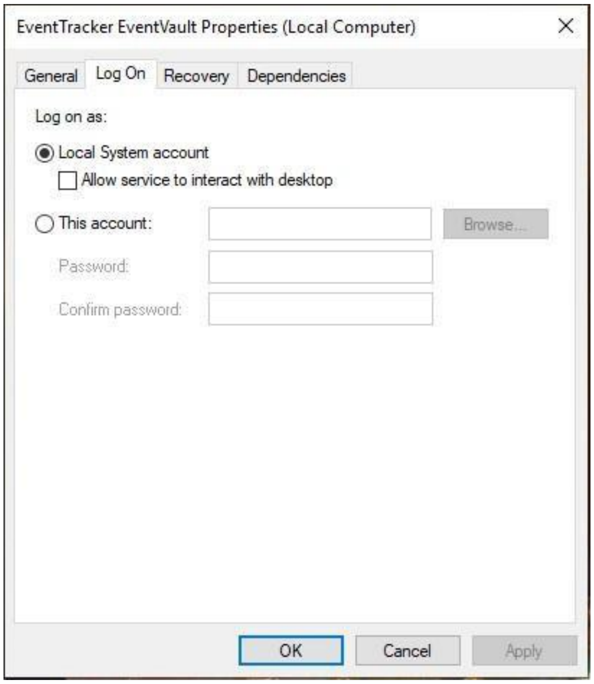
EventTracker EventVault

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 **Logcollect EventVault** service
5. The Logcollect EventVault Properties (Local Computer)' window will be displayed as shown below.



EventTracker EventVault Properties (Local Computer)

Log on as:

● Local System account

□ Allow service to interact with desktop

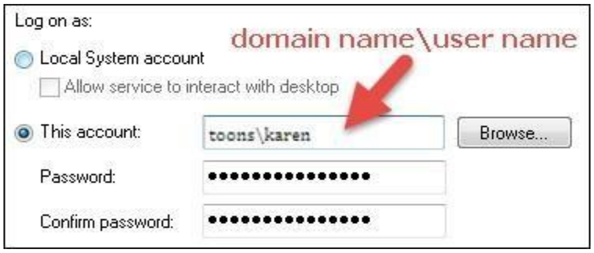
○ This account:

Password:

Confirm password:

Need to change the image

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



Log on as:

○ Local System account

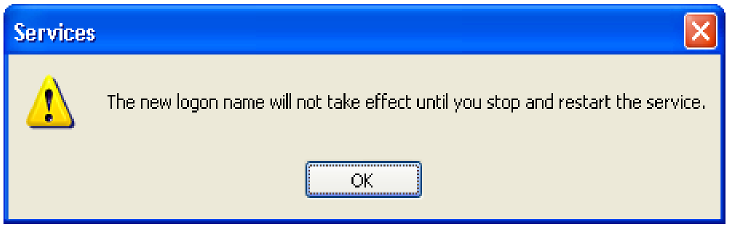
□ Allow service to interact with desktop

● This account: toons\karen

Password: •••••••••••••••

Confirm password: •••••••••••••••

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



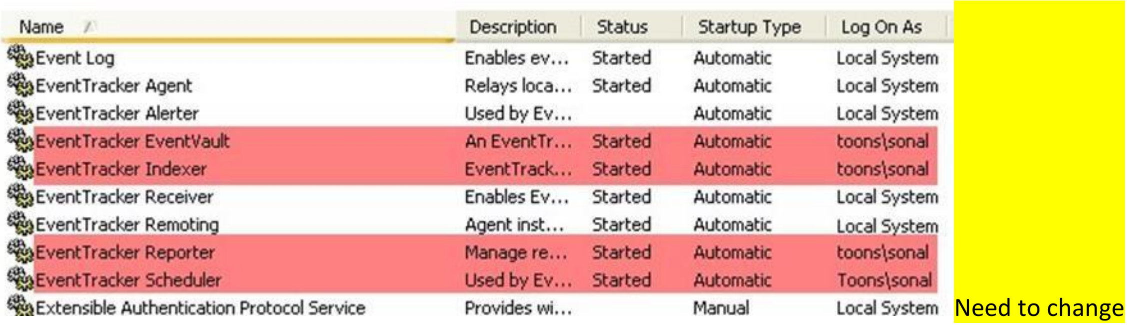
Services

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

9. Click the **OK** button.

10. To run the service with a new login name, stop and start the service.

11. Likewise, for the rest of the services, repeat steps 4 to 10 to change the service account. The **Log On As** column will display the changed service account name.



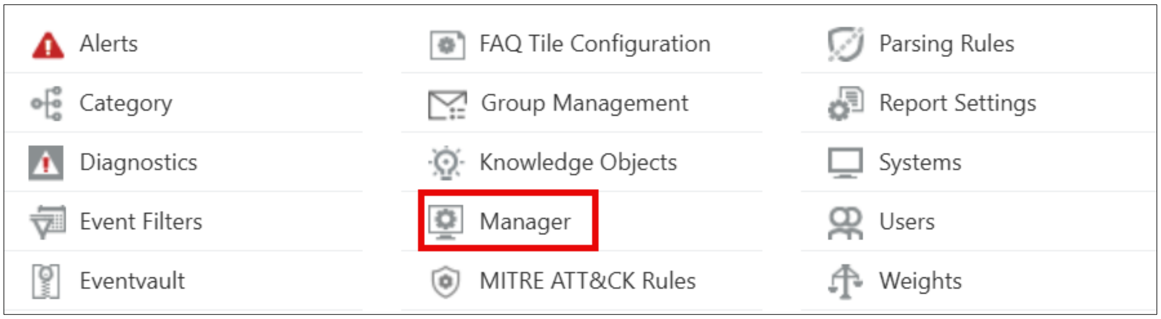
Name	Description	Status	Startup Type	Log On As
Event Log	Enables ev...	Started	Automatic	Local System
EventTracker Agent	Relays loca...	Started	Automatic	Local System
EventTracker Alerter	Used by Ev...		Automatic	Local System
EventTracker EventVault	An EventTr...	Started	Automatic	toons\sonal
EventTracker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

Need to change

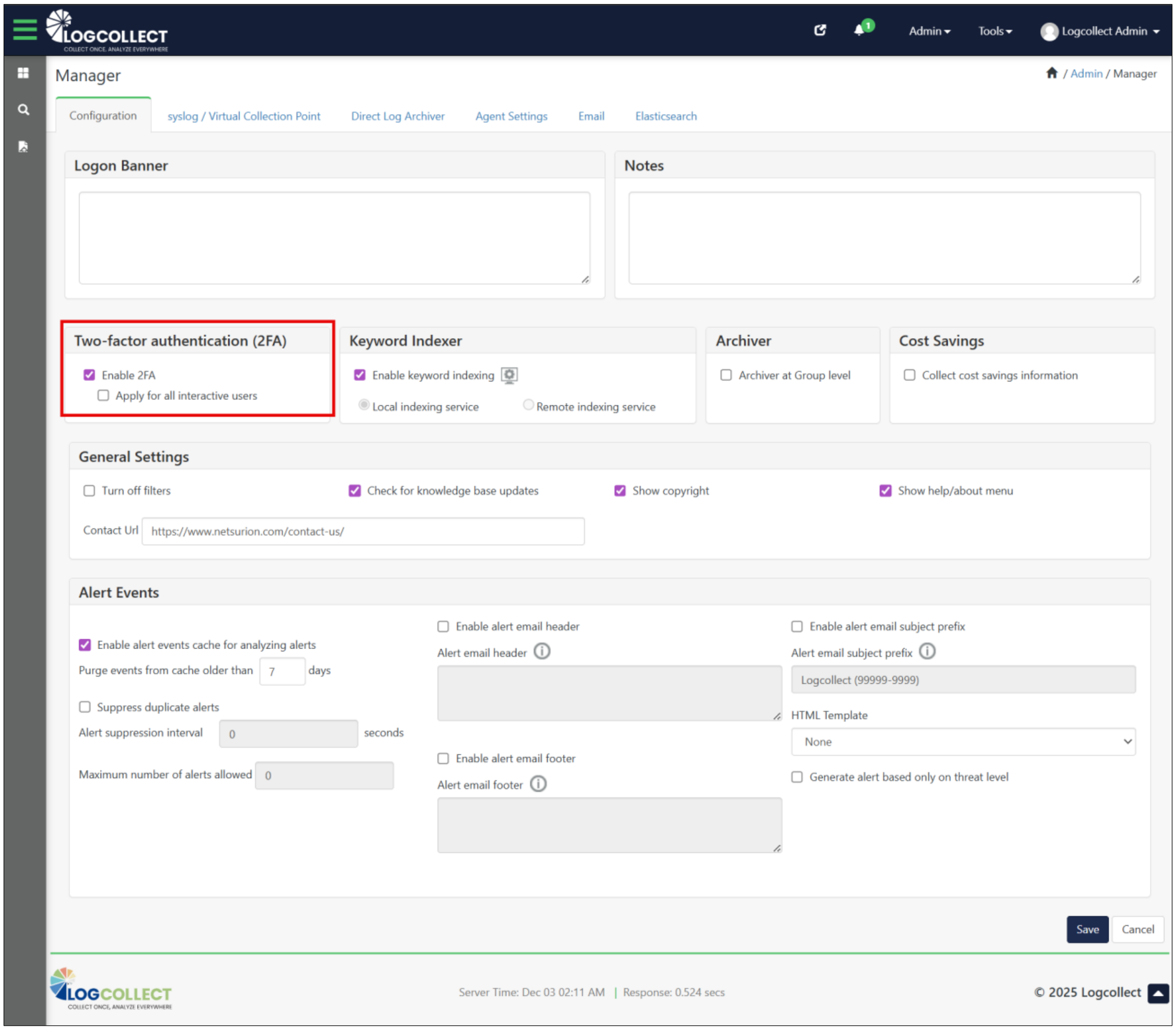
6 Enabling Two-Factor Authentication in Logcollect Web Console

To enable Two-Factor Authentication in Logcollect Web Console, perform the following steps:

1. Log into the Logcollect Web Console.
2. Click **Admin > Manager**.



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



Manager

Configuration | syslog / Virtual Collection Point | Direct Log Archiver | Agent Settings | Email | Elasticsearch

Logon Banner

Notes

Two-factor authentication (2FA)

☑ Enable 2FA
☐ Apply for all interactive users

Keyword Indexer

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

Archiver

☐ Archiver at Group level

Cost Savings

☐ Collect cost savings information

General Settings

☐ Turn off filters ☑ Check for knowledge base updates ☑ Show copyright ☑ Show help/about menu

Contact Url https://www.netsurion.com/contact-us/

Alert Events

☑ 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 ⓘ Logcollect (99999-9999)
HTML Template None
☐ Generate alert based only on threat level

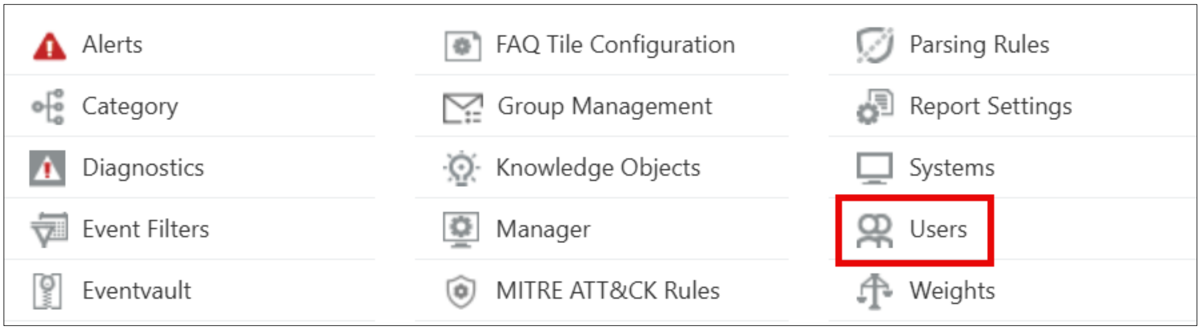
Server Time: Dec 03 02:11 AM | Response: 0.524 secs

© 2025 Logcollect

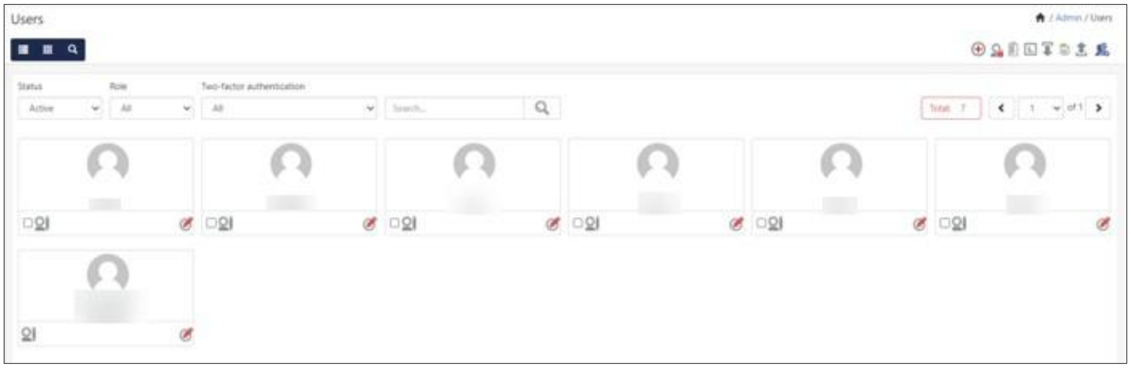
4. Now the 2FA option will be enabled by default while creating new users.

6.1 Adding New Users

1. Click **Admin > Users**.



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



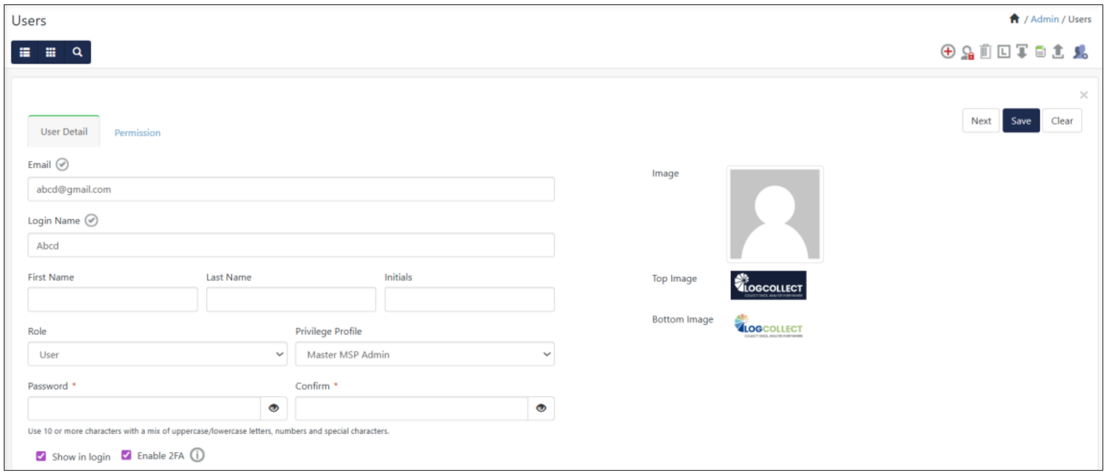
Users

/ Admin / Users

Status: Active | Role: All | Two-factor authentication: All | Search...

Total 7 | 1 of 1

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



Users

/ Admin / Users

Email: abcd@gmail.com

Login Name: Abcd

First Name:

Last Name:

Initials:

Role: User

Privilege Profile: Master MSP Admin

Password *

Confirm *

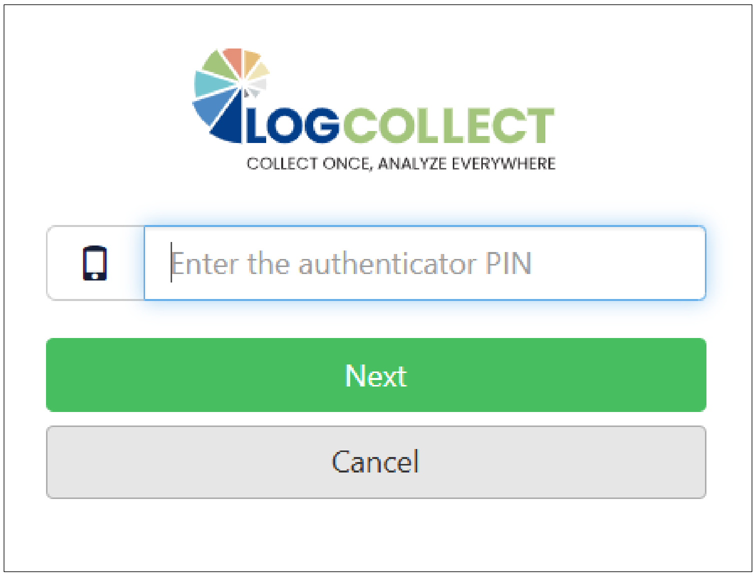
Use 10 or more characters with a mix of uppercase/lowercase letters, numbers and special characters.

☑ Show in login ☑ Enable 2FA

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

Note

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

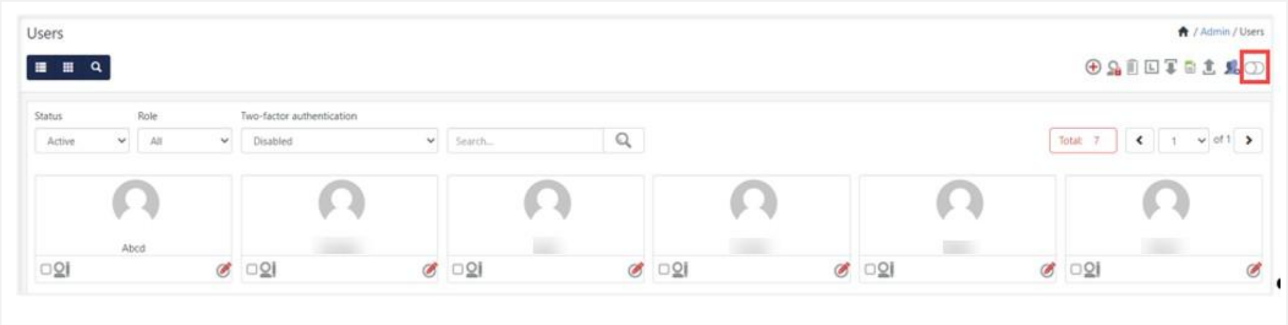


Refer to the following link to configure the Authenticator App.

https://logcollect.com/wp-content/uploads/support-docs/How-To-Configure-Two-Factor-Authentication-using-Authenticator-App-Logcollect.pdf

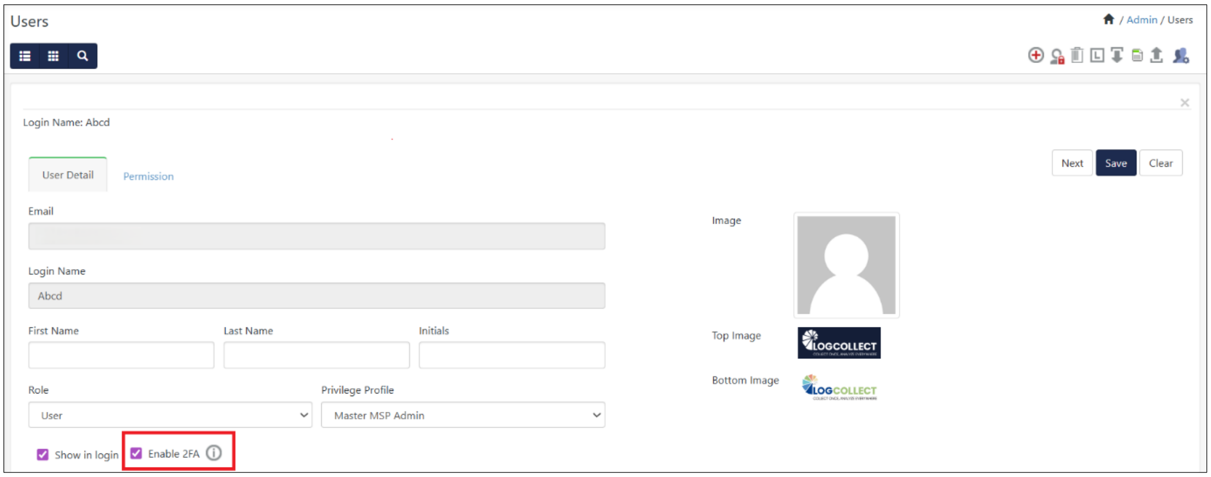
6.2 Enabling 2FA Option for Existing Users

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



Status: Active
Role: All
Two-factor authentication: Disabled

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



Users

/ Admin / Users

Login Name: Abcd

Email: [redacted]

Login Name: Abcd

First Name:

Last Name:

Initials:

Role: User

Privilege Profile: Master MSP Admin

☑ Show in login ☑ Enable 2FA

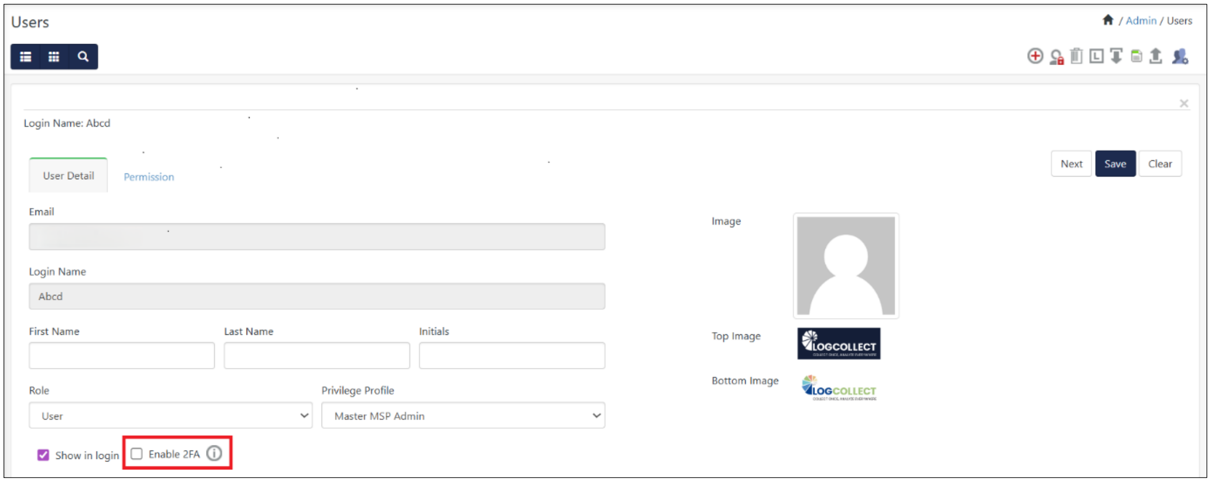
Image

Top Image

Bottom Image

6.3 Disabling 2FA

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



Users

/ Admin / Users

Login Name: Abcd

Email: [redacted]

Login Name: Abcd

First Name:

Last Name:

Initials:

Role: User

Privilege Profile: Master MSP Admin

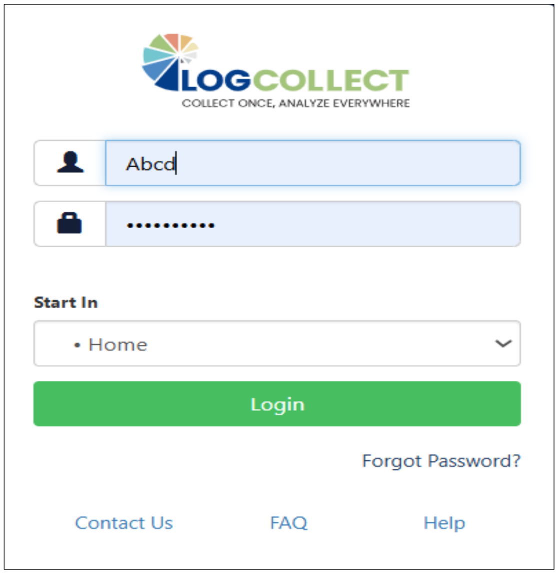
☑ Show in login ☐ Enable 2FA

Image

Top Image

Bottom Image

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

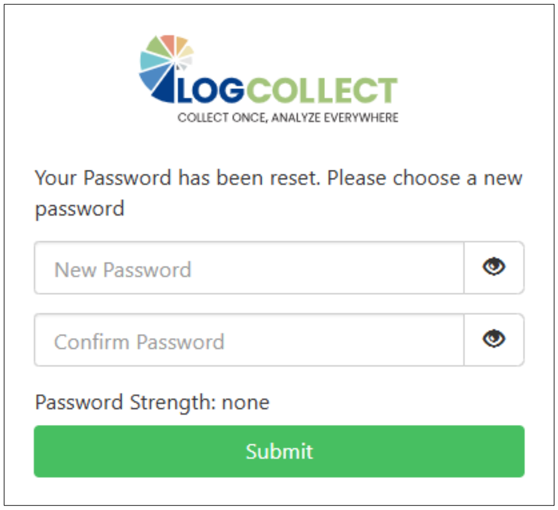


Abcd

••••••••••

Start In

• Home



Your Password has been reset. Please choose a new password

New Password

Confirm Password

Password Strength: none

7 Checking for Vulnerability Scanner

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

Note

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

Vulnerability	Impact	Recommended actions
'rsh' Remote Shell Service Enabled (service-rsh) (CVE1999-0651)	This is a legacy service often configured to blindly trust some hosts and IPs. The protocol does not support encryption or any sort of strong authentication mechanism.	Logcollect uses default port 514 for receiving syslog messages. Configure the firewall to allow incoming connections on port 514 from trusted hosts or use another port for receiving syslog in Logcollect Manager Configuration.
The FTP server does not support the AUTH command (ftpgeneric-0007)	By default, FTP clients send user credentials (user ID and password) in clear text to the FTP server. This allows malicious users to intercept the credentials if they can eavesdrop on the connection.	FTP server is installed on the Logcollect Manager to transfer custom logs from remote sources. In the case of IIS 6, FTP does not support the AUTH command. Use a third-party FTP that supports the AUTH command and configure FTP over SSL.
Untrusted TLS/SSL server X.509 certificate (tlsuntrusted-ca)	The server's TLS/SSL certificate is signed by a Certification Authority (CA) whose publisher is not known or a trusted one. It could indicate that a TLS/SSL man-in-the-middle is taking place and is eavesdropping on TLS/SSL connections.	Obtain a new certificate signed by trusted certificate authorities, such as Thawte or Verisign.
Guest access allowed to Windows	Windows event logs have been configured to allow guest access.	For each event log listed, find the following registry key:
event logs	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.	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\[logname] Under this key, add a DWORD value named "RestrictGuestAccess" and set it to 1.
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 the 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.

Vulnerability	Impact	Recommended actions
Microsoft IIS default installation/welcome 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 that has not yet been configured properly and is not known about.	Replace the default page with a relevant content page.
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 can monitor FTP traffic.	FTP server is installed on the Logcollect Manager to transfer custom logs from remote sources. In case of IIS 6, FTP does not support the AUTH command. Either use a third-party FTP that supports the AUTH command and configure FTP over SSL or configure the FTP server to allow connection from a trusted host.

About Logcollect

Logcollect is a software-only telemetry pipeline which supports the collection, enrichment, transformation and routing of security data from sources to multiple destinations. It is targeted to security operations that are struggling with distributing large volumes of disparate data, high operational costs, alert fatigue and missed threats. It is available as a software license or hosted in AWS. It is backed by a team that has extensive experience with security logging, SIEM and regulatory compliance. Collect once, analyze everywhere.

Headquartered in Ft. Lauderdale, FL, Logcollect is a leader in Log Collection. Learn more at www.Logcollect.com.

Contact Us

Corporate Headquarters

Prism Microsystems
920 NE 17th Way
Fort Lauderdale, FL 33304

https://www.Logcollect.com/support