AppViewX Windows Gateway Setup Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

Trademarks

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
2.0	Updated release of document for release v2022.1.0 FP2 Beta	November 2022
1.0	Initial release of document for release v2022.1.0.	July 2022

About this Guide

This guide outlines the steps for installing the AppViewX Windows Gateway for enabling communication between AppViewX and Windows. It also includes the steps for installing and using the AppViewX validator to validate the accessibility of the target machine on which the AppViewX Windows Gateway will be installed.

Audience

This guide is intended for AppViewX's customers deploying its products on Windows-based machines.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Overview

AppViewX Windows Gateway

The AppViewX Windows Gateway is packaged with two components:

- AppViewX Windows Gateway Service
- AppViewX Windows Gateway Troubleshooting tool

AppViewX Windows Gateway service is a Windows Communication Foundation service that enables secure communication between AppViewX and Windows server infrastructure. Following are the key features of the that are supported by AppViewX for Windows Server Infrastructure:

- Certificate Life Cycle Management (CLM) on Windows servers (version 2012 R2 and above), Microsoft CA Servers, IBM Websphere, and Weblogic.
- Binding of certificates to IIS (Version 7.5 and above)
- Discovering certificates from the file system
- Executing custom scripts on PowerShell

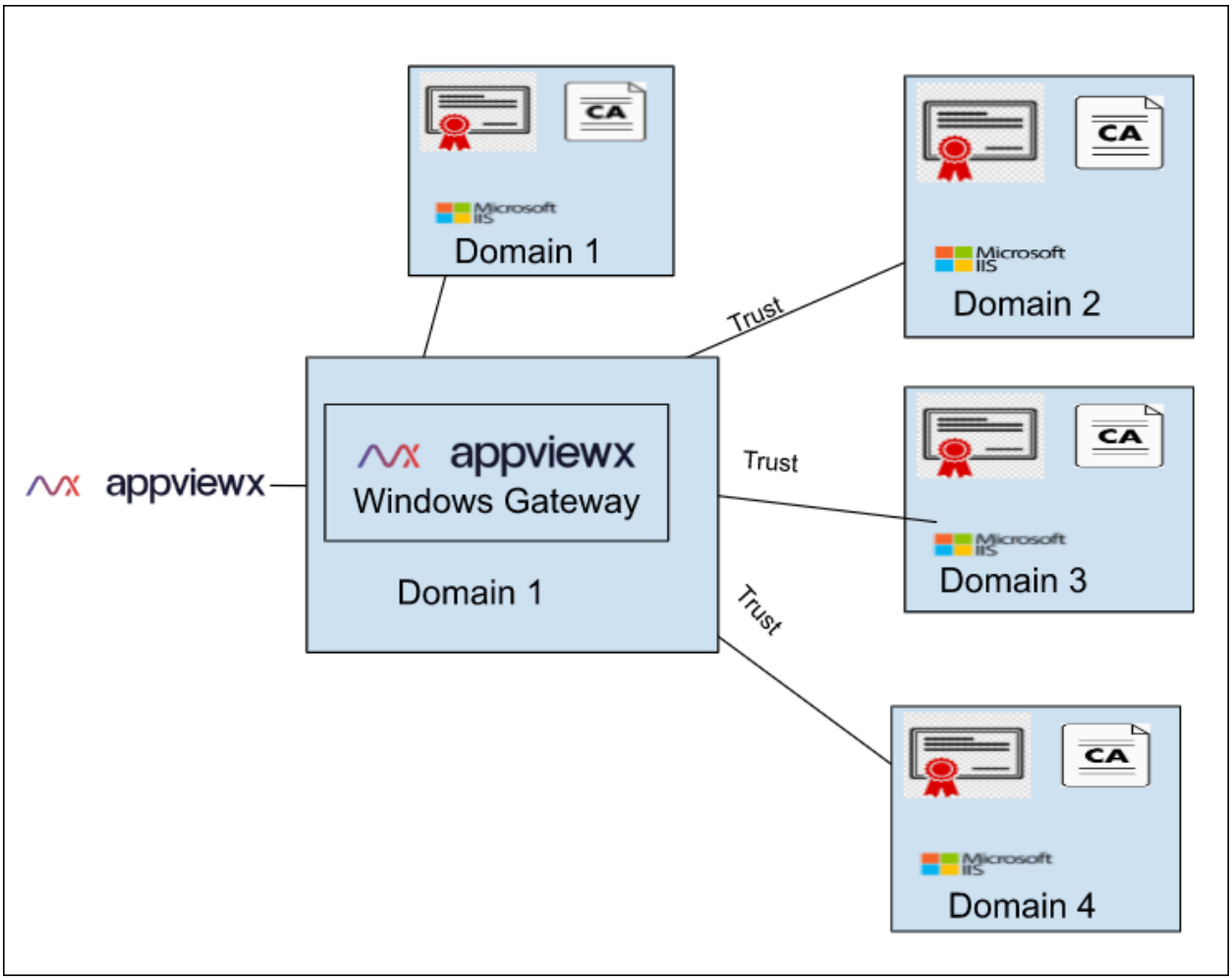
AppViewX Windows Gateway Troubleshooting tool facilitates the trouble shooting of any issues in the communication between AppViewX Windows Gateway service and the Windows server infrastructure in your premises.

Deployment Modes

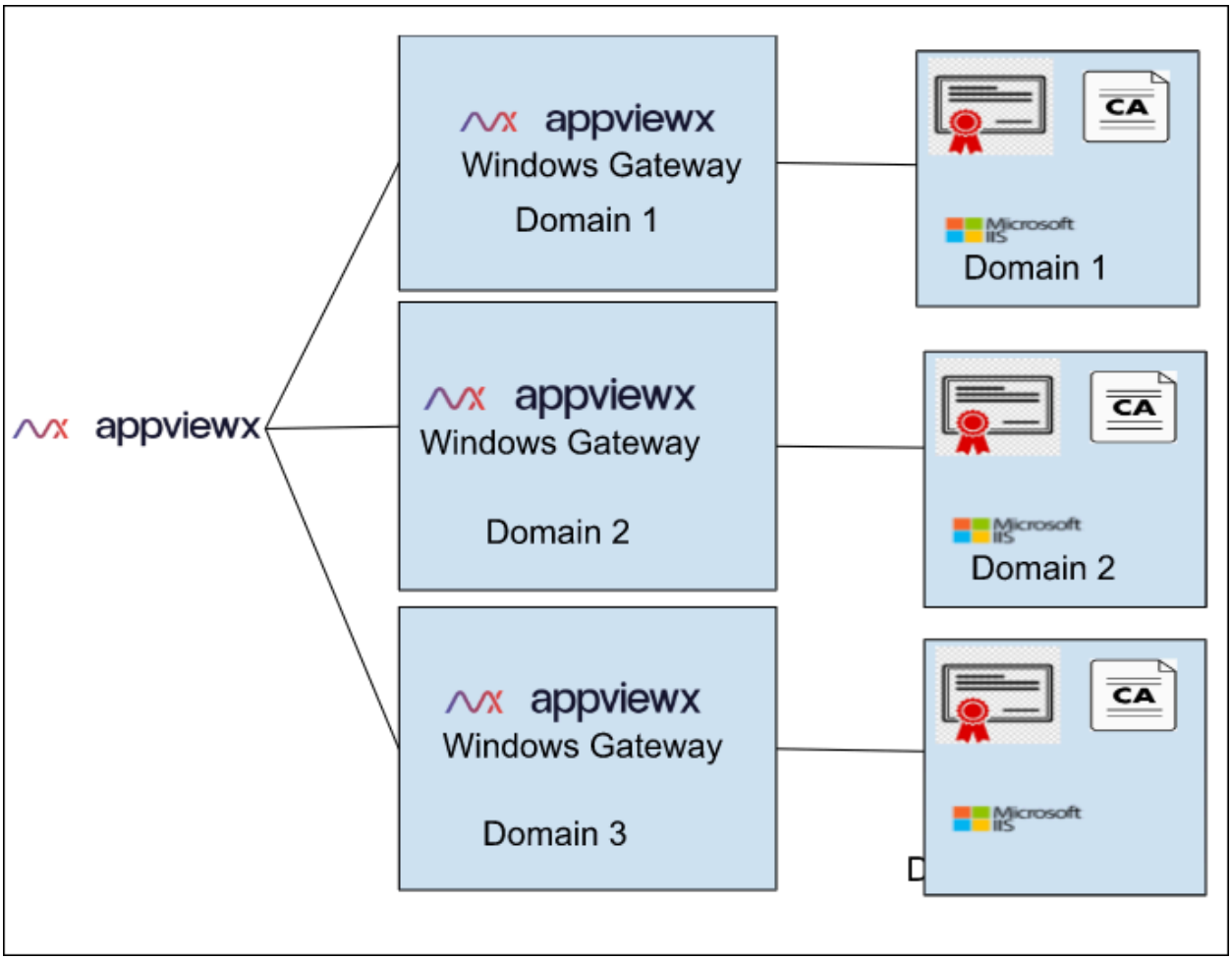
AppViewX WG installation is different for trusted and untrusted domains.

Trusted Domains

If your organization has multiple domains and each of these domains are trusted, then as depicted in the following figure, one installation of the AWG would be sufficient to manage the Windows server infrastructure of all the domains.



Alternatively, if the domains are independent, then at least one installation of the AWG is needed for each such untrusted domain, as shown in the figure below.



Chapter 2: Setting up the AppViewX Windows Gateway

Step 1: Checking Prerequisites

Software

Name	Description
Operating System	AppViewX Windows Gateway is supported Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.
.NET framework	.NET framework version 4.5.2 is required.
Admin access	Administrator privilege is needed to install AppViewX Windows Gateway.
PowerShell	Powershell version version 4.0 is needed

Hardware

Hardware	Capability
RAM	8 GB
HDD	10 GB
CPU	Intel or AMD processor with 64-bit support, 1.8 GHz or faster processor

Firewall

The firewall must not block the following port and the respective port must open on the Agent.

Component	Port
Default Port communication from AppViewX to a AppViewx Windows Gateway	8999

Note: During the installation of AppViewX Windows Gateway, the default port can be reconfigured. For more details refer Step 3 of installation.

Step 2: Downloading the AppViewX Windows Gateway Installer

Download and unarchive the **AppViewX.CertPlus.Installer.zip** file from the release portal. The download package consists of the following files:

File Name	Description
AppViewX.CertPlus.Installer.exe	Installer executable
ClientCertificateGateway.pfx	Default client certificate
ServerCertificateGateway.pfx	Default server certificate
config.xml	Application configuration settings that will override the default settings after the AppViewX Windows Gateway is installed.
Readme.txt	Help file with details of the AppViewX Windows Gateway.

File Name	Description
stallationLog.txt	Logs the success and error messages from the installation process.

Step 3: Installing the AppviewX Windows Gateway

Before you Begin

Certificate Customization

By default, the AppViewX Windows Gateway securely communicates with AppViewX using the server/client certificates that are shipped along with the AppViewX Windows Gateway installer. If you choose to use a different server and client certificate for authentication, then follow the steps below:

1. From Windows explorer, browse to the location where you have unarchived the AppViewX Windows Gateway installer package.
2. Rename the default server certificate “ServerCertificateGateway.pfx” as “ServerCertificateGateway-Backup.pfx” and client certificate file “ClientCertificateGateway.pfx” as “ClientCertificateGateway-Backup.pfx”.
3. Copy the server and client certificates that you intend to use in this directory.
4. Rename the server certificate file as “ServerCertificateGateway.pfx” and client certificate file as “ClientCertificateGateway.pfx”, and then replace the default certificates in the installation folder.

Note: While installing the AppViewX Windows Gateway, you will be prompted to provide the server and client passwords.

CAUTION: If the certificate is replaced, ensure that the respective password has been provided to add the certificate to the store. The incorrect password during the installation of AppViewX Windows Gateway will cause the Windows Agent installation to fail.

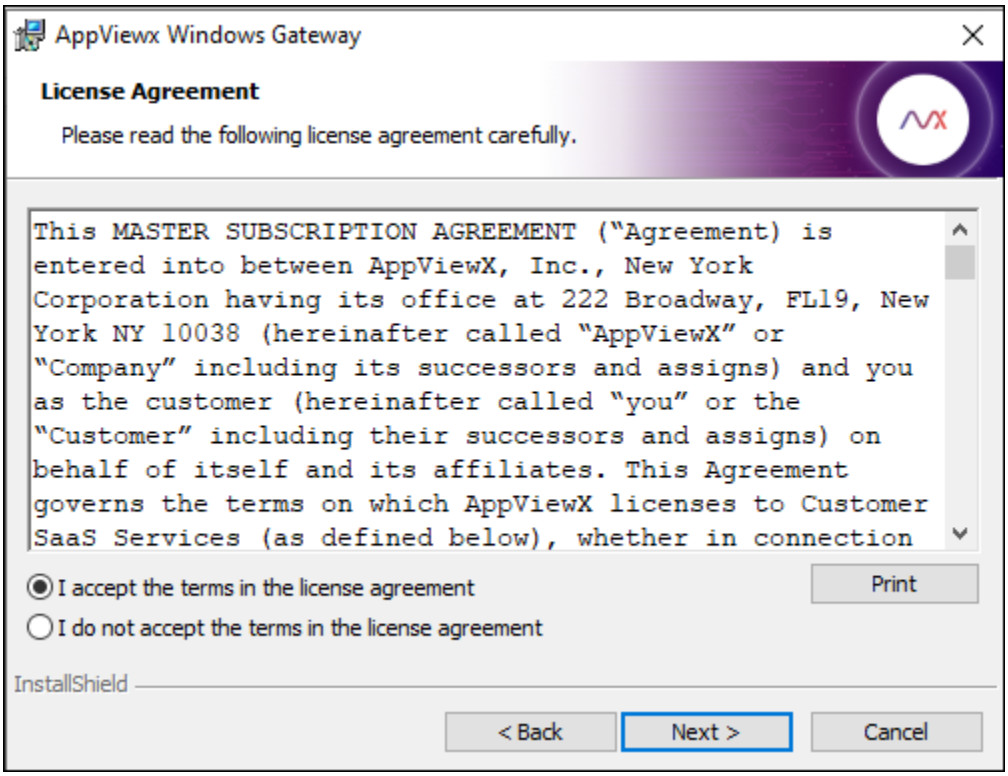
Navigating through the Installation

1. Execute the **AppViewX.CertPlus.Installer.exe** file.

   The following welcome screen for the setup wizard is displayed.

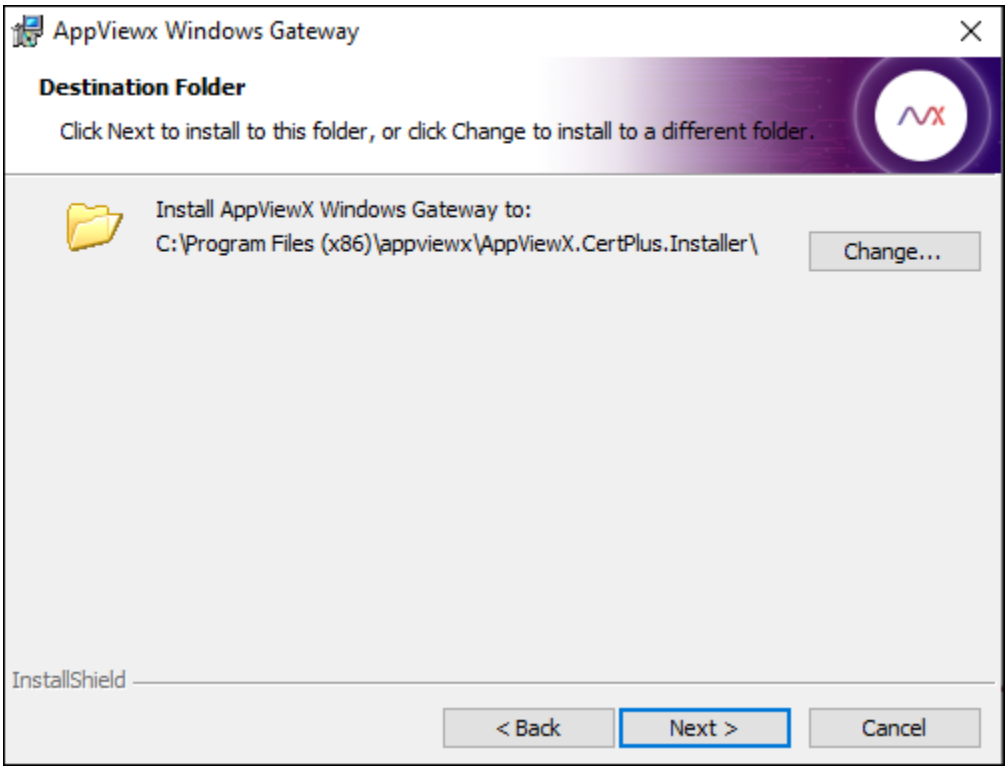
2. Click **Next**.

   The **License Agreement** is displayed.



3. Select **I accept the terms in the license agreement**.
4. Click **Next**.

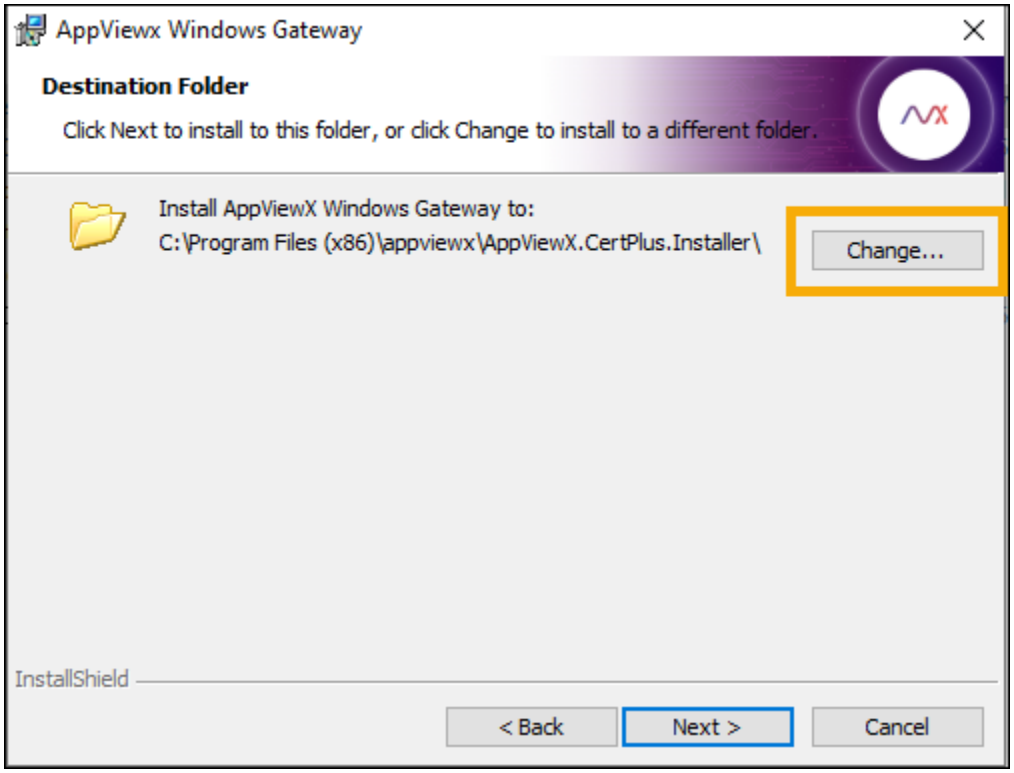
   The **Destination Folder** screen is displayed.



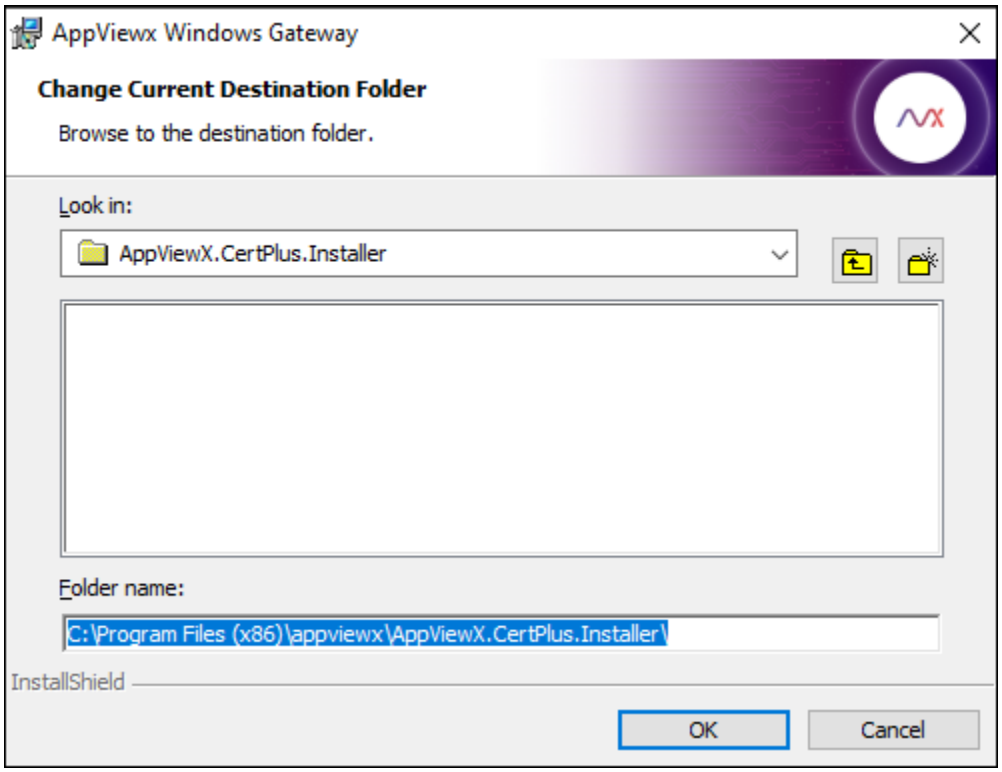
5. To install the AppViewX Windows Gateway at the default location, click **Next**.

   To change the default destination folder:

a. Click **Change**.

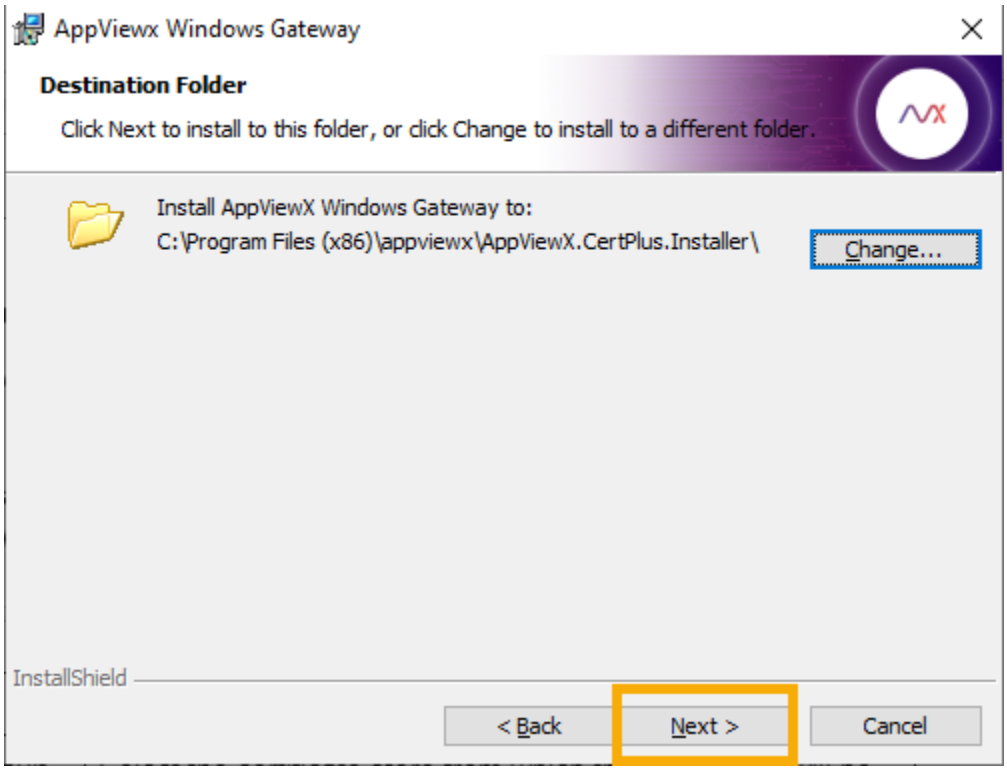


b. On the **Change Current Destination Folder** screen, use the **Look in** dropdown list/  (up one level) icon/  (create new folder) icon to navigate to/create the required destination folder.

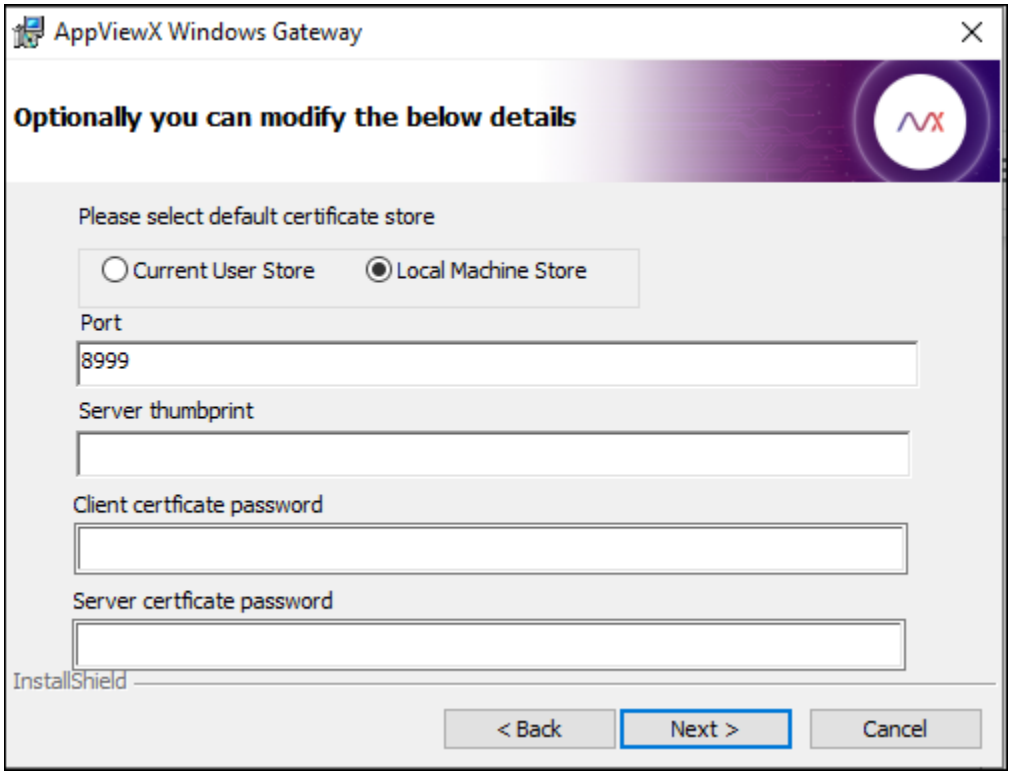


c. Click **OK**.

d. On the **Destination Folder** screen, click **Next**.



The **Optionally you can modify the below details** screen is displayed.



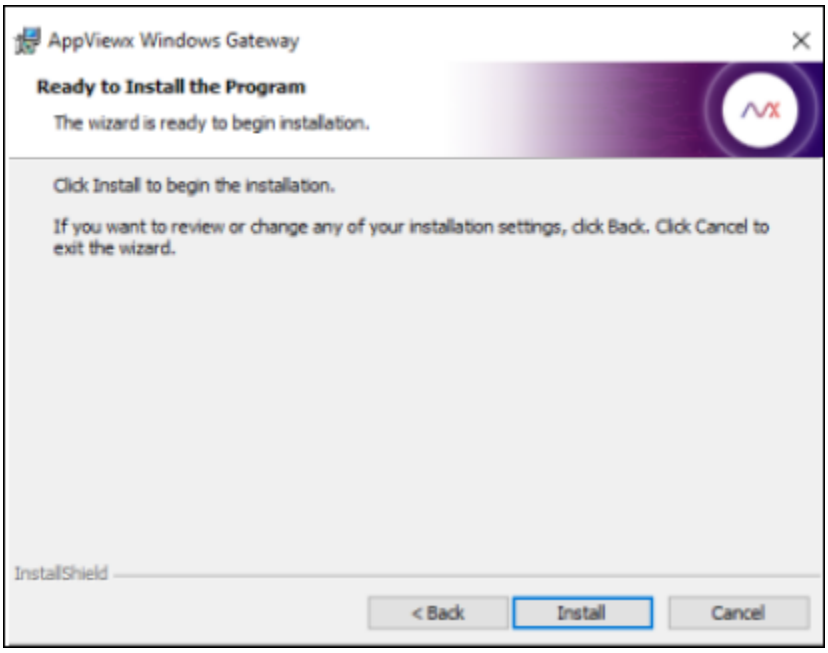
Enter the following details (optional):

Field	Description
Please select default certificate store	Select the certificate store from which the certificates will be discovered and pushed to by AppViewX from the following options: • Current User Store This type of certificate store is local to a user account on a computer. It is located in the registry under the HKEY_CURRENT_USER root. • Local Machine Store (default) This type of certificate store is local to a computer and global to all the user accounts

Field	Description
	on the computer. It is located in the registry under the HKEY_LOCAL_MACHINE root. This configures the gateway for communicating with the appropriate certificate store.
Port	Port for accessing the service. Default value: 8999 (can be modified if required)
Server certificate thumbprint	If you are using a custom certificate, enter the corresponding server certificate thumbprint value.
Client certificate password	Password for accessing the client certificate For custom client certificates, enter the certificate password.
Server certificate password	Password for accessing the server certificate For custom server certificates, enter the certificate password.

Note: Refer Before you Begin section of this section to use custom server and client certificates.

6. Click **Next**.
   The Ready to Install the Program screen is displayed.



7. Click **Install**.

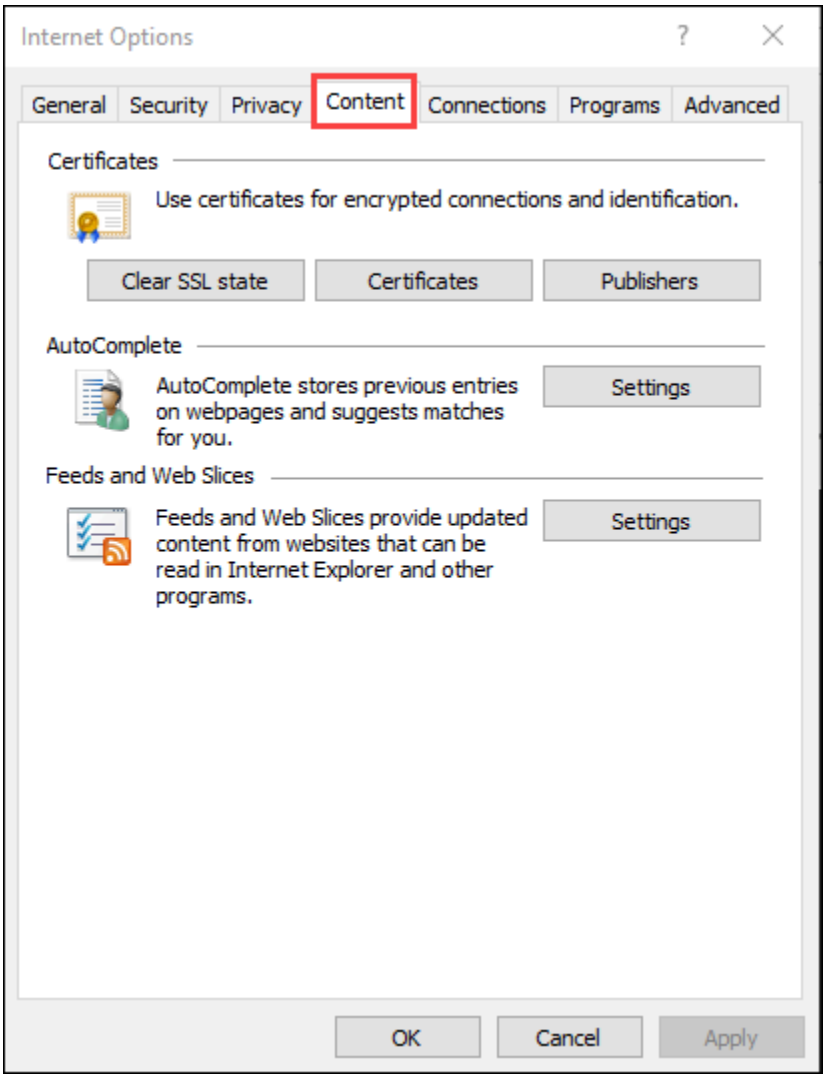
   This will:

   • Install the AppView Windows Gateway Troubleshooter tool

   • AppViewX Windows Gateway service.

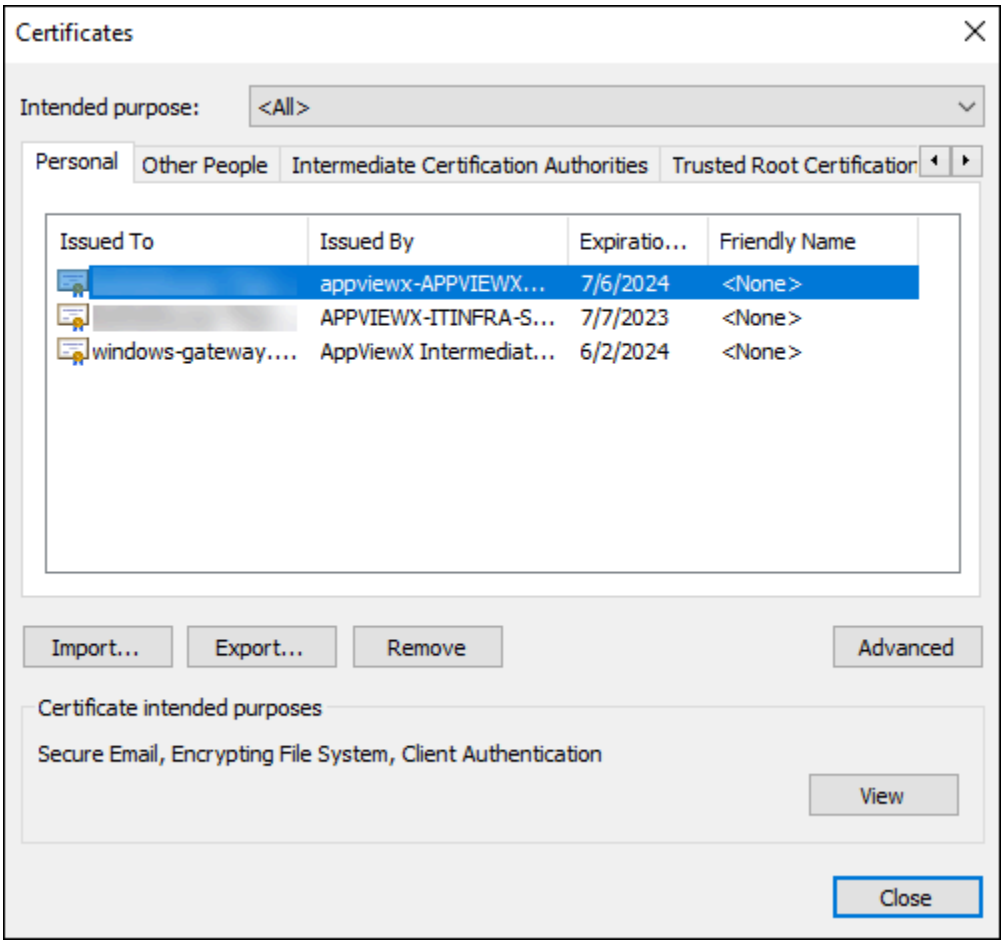
Step 4: Verifying the AppviewX Windows Gateway Installation

1. To verify the Windows AppViewX Gateway installation on Internet Explorer, import the client authentication certificate **ClientCertificateGateway.pfx**, from the download package (password: **appviewx**).
2. Navigate to Internet Explorer's **Settings** > **Internet Options**, and then click the **Content** tab.

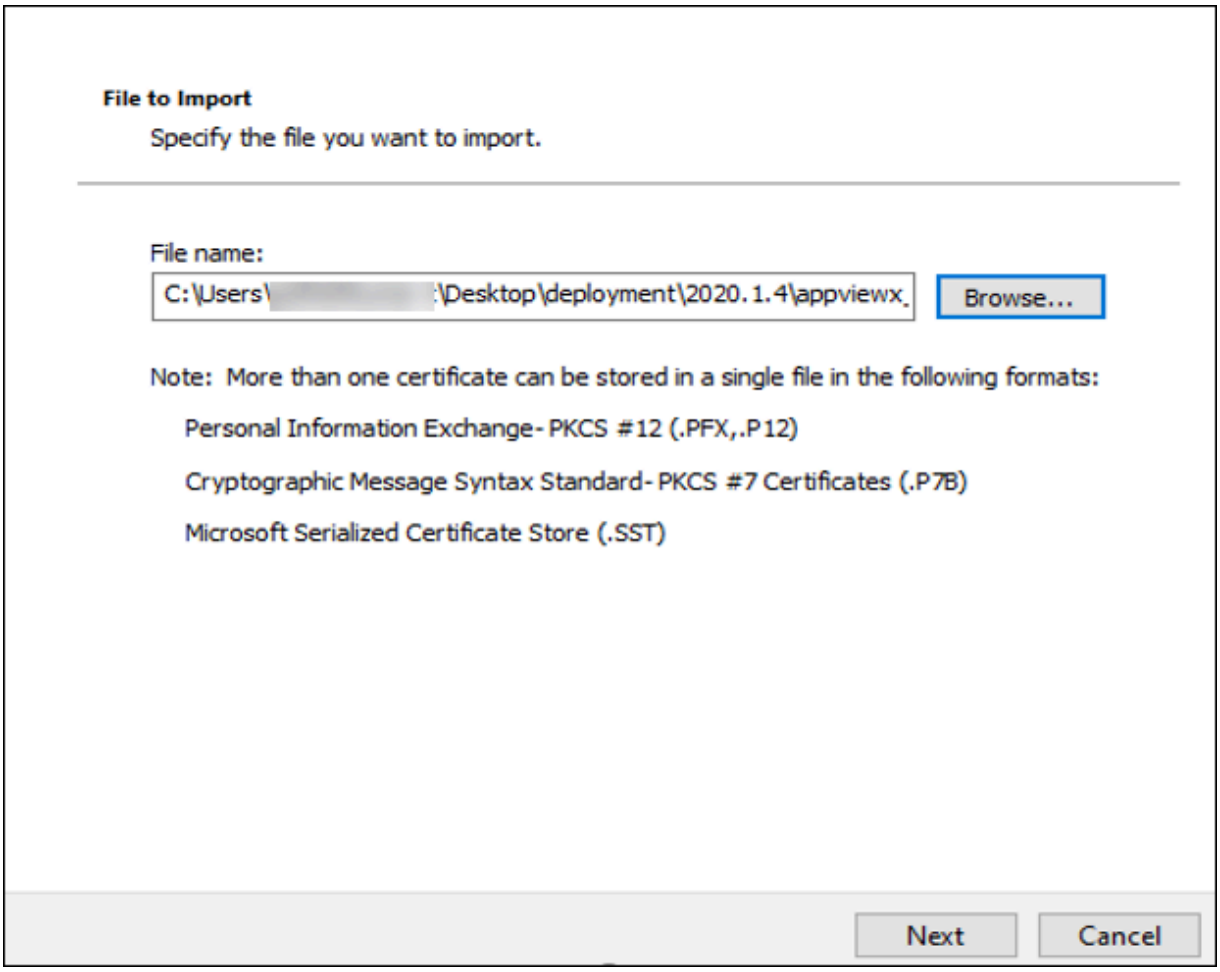


3. Click the **Certificates** button.

   The **Certificates** popup window opens.



4. Click the **Import** button on the **Certificates** page.



5. Navigate to the following URL: https://hostname:portnumber/appviewx/rest/help. For example: https://10.10.10.10:8999/appviewx/rest/help

   The page displayed confirms the accessibility and installation of the service.

Operations at https://localhost:8999/appviewx/rest

This page describes the service operations at this endpoint.

Uri	Method	Description
BindCertificateToGateway	POST	Service at https://localhost:8999/appviewx/rest/BindCertificateToGateway
BindCertificateToSite	POST	Service at https://localhost:8999/appviewx/rest/BindCertificateToSite
BindSQLServerCertificate	POST	Service at https://localhost:8999/appviewx/rest/BindSQLServerCertificate
BootPropertiesReader	POST	Service at https://localhost:8999/appviewx/rest/BootPropertiesReader
CertDeviceInfo	POST	Service at https://localhost:8999/appviewx/rest/CertDeviceInfo
CheckConnection	POST	Service at https://localhost:8999/appviewx/rest/CheckConnection
CreateAndSubmitRequest	POST	Service at https://localhost:8999/appviewx/rest/CreateAndSubmitRequest
CreateCSR	POST	Service at https://localhost:8999/appviewx/rest/CreateCSR
CreateCSRKey	POST	Service at https://localhost:8999/appviewx/rest/CreateCSRKey
DeleteFile	POST	Service at https://localhost:8999/appviewx/rest/DeleteFile
DeleteKeys	POST	Service at https://localhost:8999/appviewx/rest/DeleteKeys
DeviceInfo	POST	Service at https://localhost:8999/appviewx/rest/DeviceInfo
DiscoverCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverCertificates
DiscoverCertStoreCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverCertStoreCertificates
DiscoverFileCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverFileCertificates
DiscoverIBM	POST	Service at https://localhost:8999/appviewx/rest/DiscoverIBM
DiscoverKeys	POST	Service at https://localhost:8999/appviewx/rest/DiscoverKeys
ExecuteScriptInPowershell	POST	Service at https://localhost:8999/appviewx/rest/ExecuteScriptInPowershell
ExecuteWLSTScript	POST	Service at https://localhost:8999/appviewx/rest/ExecuteWLSTScript
ExtractCertificate	POST	Service at https://localhost:8999/appviewx/rest/ExtractCertificate
GetCertStores	POST	Service at https://localhost:8999/appviewx/rest/GetCertStores
LatestLog	POST	Service at https://localhost:8999/appviewx/rest/LatestLog
MicrosoftCAs	POST	Service at https://localhost:8999/appviewx/rest/MicrosoftCAs
MqConnector	POST	Service at https://localhost:8999/appviewx/rest/MqConnector
Ping	GET	Service at https://localhost:8999/appviewx/rest/Ping
PushAndBindCertificate	POST	Service at https://localhost:8999/appviewx/rest/PushAndBindCertificate
PushCertificate	POST	Service at https://localhost:8999/appviewx/rest/PushCertificate
PushDiscoveredCertificates	POST	Service at https://localhost:8999/appviewx/rest/PushDiscoveredCertificates
ReadFile	POST	Service at https://localhost:8999/appviewx/rest/ReadFile
ReadMultipleFiles	POST	Service at https://localhost:8999/appviewx/rest/ReadMultipleFiles
RemoveCertificateFromStore	POST	Service at https://localhost:8999/appviewx/rest/RemoveCertificateFromStore
RemoveSiteBinding	POST	Service at https://localhost:8999/appviewx/rest/RemoveSiteBinding
RevokeCertificate	POST	Service at https://localhost:8999/appviewx/rest/RevokeCertificate
SaveKeys	POST	Service at https://localhost:8999/appviewx/rest/SaveKeys

Note: In the event that a custom client authentication certificate is used, ensure that the CRL mentioned in the certificate is reachable from the AppViewX Windows Gateway hosting server.

Note: The steps to import the client certificate will differ depending on the web browser.

6. To register the AppView Windows Gateway with AppViewX, navigate to the AppViewX Cert+ (on the SaaS deployment) admin UI/UX, and then **Settings** > **Certificate**.

Note: To add the AppViewX Windows Gateway for

- Mocrosoft Enterprise CA integration, see ***Microsoft Enterprise CA*** section under chapter **CERT+ Setup** > **Configuring CA Settings** in Cert Admin guide.
- Mocrosoft Standalone CA integration, see ***Microsoft Standalone CA*** section under chapter **CERT+ Setup** > **Configuring CA Settings** in Cert Admin guide.
- Mocrosoft Device integrations, see ***Microsoft Devices Integration*** section under chapter **CERT+ Setup** in Cert Admin guide.

7. Register the gateway using the following URL format: https://hostname:portnumber/appviewx. For example: https://10.10.10.10:8999/appviewx

Note:

- The AppViewX's custom client authentication uses CRL and OCSP as proposed by Microsoft. If you choose to use Microsoft's client authentication then comment the config file as below:

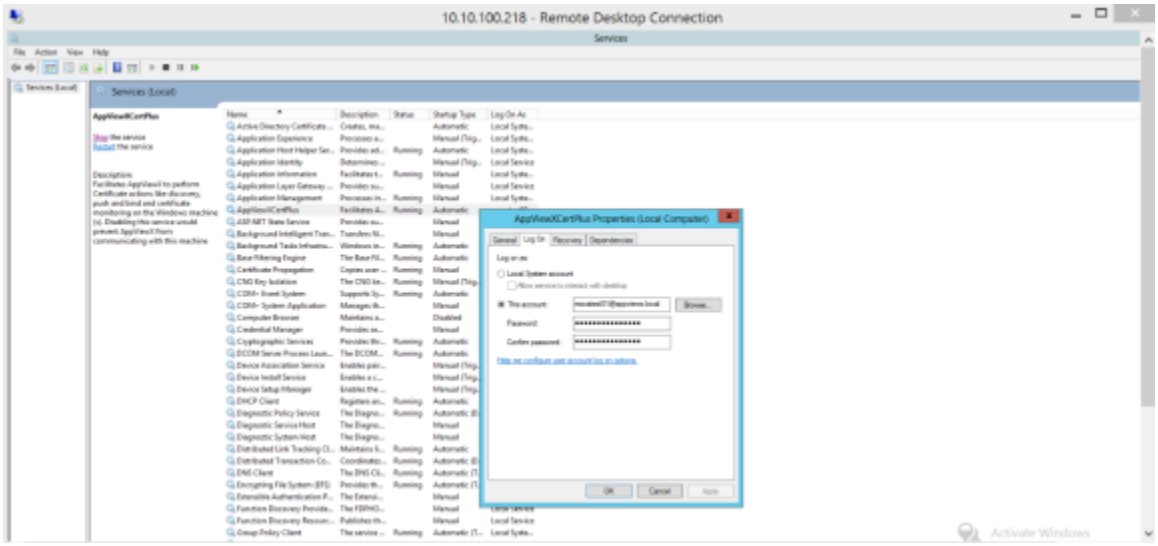
```
<!--<serviceCredentials>
<clientCertificate>
<authentication certificateValidationMode="Custom"
customCertificateValidatorType="AppViewX.CertPlus.Service.CustomValidator,  AppViewX.CertPlus.Service" />
</clientCertificate>
</serviceCredentials>-->
```

- AppViewX recommends customers not to change this default authentication configuration provided by AppViewX.
- Refer Appendix A for the Prerequisites for Managing the Windows Server Infrastructure and Appendix B for Troubleshooting the Target Machine.

Non-Admin Service Account

- The AppViewX Windows Gateway can be installed using a service account that is part of the local administrator group or domain admin account.
- If the network has a policy that the service account cannot be part of the administrator group or that the service account is only a part of the user group, then:

- The AppViewX Windows Gateway is installed using an admin account.
- It is then associated with the service account in **services.msc**, by adding the account in the properties of the AppViewXCert Plus service. Refer to the following image.

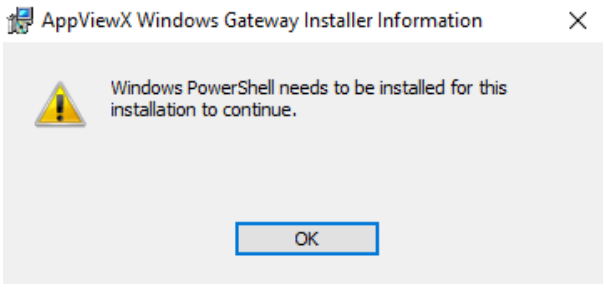
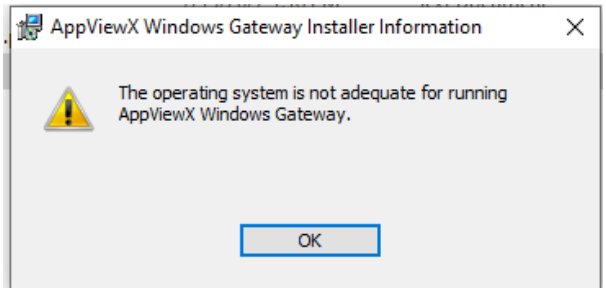
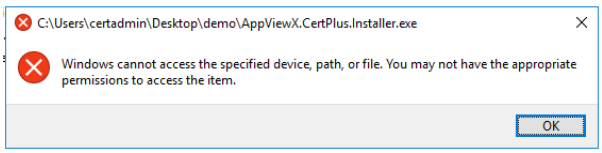


- In this case, the following command has to be executed from the PowerShell:

```
netsh http add urlacl url=https://+:8999/appviewx/user=Username@domainname
```

- In the above command, the value for `user = <domainserviceaccount>` and the `URL` must be changed respectively.
- On the Regedit path, "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\AppViewXCertPlus" add the service account and give Full Control permission.
- C:/Logs Folder gives the service account permission to read and write.
- On the Installation path of the application, the user needs permission to read and write.
- Once this is done, stop and start the `AppViewXCertPlus Service` in `services.msc`.

Troubleshooting the AppViewX Windows Gateway

Error	Solution
	Install Windows Powershell before proceeding with the AppViewX Windows Gateway installation.
	Ensure that the operating system on the target machine fulfills the software requirements for installing the AppViewX Windows Gateway.
	The user attempting to access the specified device, path, or file should have admin access.
	If you see the following message in the **InstallationLog.txt** file: **The specified network password is not correct**, check your username and password. **Note:** The **InstallationLog.txt** can be found in the download package for the installer (downloaded in step 1 here).
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <machine name> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <name> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly,	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command setspn -s http/ machinename domainusername.

Error	Solution
and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<machine name> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation.	• This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.
Retrieving the COM class factory for remote component with CLSID.	• The component used for accessing CA (certadm.dll) is not installed or has permission issues. • Check if the DLL is available in C:WindowsSystem32 folder or else, install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. For example, for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot process the request. The following error with error code 0x80090322 occurred while using Negotiate authentication: An unknown security error occurred.	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command setspn -s http/machinename domainusername.

Error	Solution
	• This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service.	• Check if the WinRM service is running. • Go to the Powershell on the target machine and run the command WinRM QuickConfig. • Execute the command Enable-PSRemoting -force. • Execute the command netsh winhttp show proxy and if a proxy is configured, it must be reset using the command netsh winhttp reset proxy.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <machine name> failed with the following error message : Access is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command WinRM QuickConfig. • Execute the command Enable-PSRemoting -force.

Error	Solution
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".	• Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command WinRM QuickConfig. • Execute the command Enable-PSRemoting -force.
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE).	Go to the target machine and start the RPC service if it is stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. .	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command WinRM QuickConfig. • Execute the command Enable-PSRemoting -force.

Error	Solution
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path '\\<machine name>\C$\\Windows\\Temp\ \qgwwkqi3.fff' is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.

More than five connections are not allowed.	• Run Powershell as an administrator.
	• Check existing config winrm get winrm/config.
	• Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring.
	  • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'
	  • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'
	  • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'

Connecting to remote server failed with the following error message: The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	• Run Powershell as an administrator. • Check existing config winrm get winrm/config. • Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring.

Error	Solution
	• winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Client Certificate gives Permission Denied 403 errors. This can happen in a certain environment and its intermittent.	• Check if the client certificate is installed correctly by validating the chain in the Personal Store. • The root of the client certificate must be available in the Trusted Root Certification Store of the server. • The intermediate of the client certificate must be available in the Intermediate Certification authorities of the server. • If all of the above are fine, go to the agent server and complete the following steps: 1. MMC 2. Add/Remove SnapIn 3. Select certificate 4. Select LocalMachine 5. Go to Personal Store and click on client certificate. 6. Go to chain 7. Export the root certificate and save as Root.cer in a location 8. Import the Root.cer into trusted root back again. 9. If this does not solve the issue, then check if the trusted root contains and non- root certificates.

Error	Solution
	10. Click on "Trusted Root" store and check if there any certificate which has IssuedTo and IssuedBy different. 11. Take a backup of such certificates and move it to respective stores. 12. If it does not solve the issue, then add the root certificate to the "Client Certificate Issuers".
The permission on the certificate template do not allow the current user to enroll for this type of certificate.	1. Go to the CA server. 2. Open Certificate Authority and select the CA Server. 3. Right-click on properties and select the Security tab. 4. Check if the user used in Agent has the necessary permissions to read, issue, manage, and request certificate(s). 5. If the user is a part of a group, then ensure that the group has the required permissions. 6. Click on the Certificate Templates and right-click to manage the template. 7. Right-click on the template which has the issue and navigates to security. 8. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	In the CA server, navigate to the registry through the regedit command and set the following: • HKLMSYSTEMCurrentControlSetServices CertSvcConfigurationDBSessionCount to 64 hex (100 Dec)

Error	Solution
	• HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.rn	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect.	The user name or password is incorrect.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits accesses to remote computers within the same local subnet.	• WinRM service is already running on the following location of the machine: C:Windowssystem32>WinRM quickconfig. • If WinRM is not set up to allow remote access to this machine for management, the following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y
There is not enough space on the disk.	Ensure that your hard disk has enough free space.

Error	Solution
Management Connect to remote machine <machine name> as user failed with the following error User credentials cannot be used for local connections.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group. • Configure the credentials in AppViewX.CertPlus.Service Logon option.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Use template name instead of the template display name.
Device Communication failed while using Native option to connect to CA remotely.	1. Go to the agent machine. 2. Open services.msc using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add the account as "Log on as service". Click "OK" and save changes.

Error	Solution
	8. Click on restart the service. 9. Remove the username and password from AppViewX.
Certificate Request (CSR) is using a different account to request a certificate from CA as compared to the account configured in AppViewX.	1. Go to the agent machine. 2. Open services.msc using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add the account as "Log on as service". Click "OK" and save changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.

Chapter 3: Uninstalling the AppViewX Windows Gateway

Uninstallation of AppViewX Windows Gateway involves the following steps:

1. Go to Windows control panel, select **Add or Remove program**.
2. Select **AppViewX.CertPlus.Installer**, and then click on **Uninstall** button.

Chapter 4: Updating AppViewX Windows Gateway

Before updating the AppViewX Windows Gateway to a newer version, the old version of the AppViewX Windows Gateway should be uninstalled. Follow the instructions in Chapter 5 to uninstall AppViewX Windows Gateway.

After Uninstallation of the older version of AppViewX Windows Gateway, proceed with the installation of the new AppViewX Windows Gateway. Refer Chapter 2 for instructions on Installing the AppViewX Windows Gateway.

Chapter 1: Appendix A

- Prerequisites for Managing the Windows Server Infrastructure

Prerequisites for Managing the Windows Server Infrastructure

General Prerequisites

1. If a device that has the AppViewX Microsoft Gateway installed on it has to be managed in AppViewX, communication mode reset to WMI always.

2. Below are the additional prerequisites and these can be validated manually or by the AppViewX Windows Gateway Troubleshooting tool provided as part of the AppViewX Windows Gateway setup.

Component	Description	Scripts
.Net Framework 4.5 and above	Download dotnet-framework-runtime from Microsoft software download center.	
POWERSHELL 4+	Download PowerShell from Microsoft software download center.	Powershell $PSVersionTable.PSVersion
Certadm.dll (Applicable ONLY if CA servers to be managed)	Check if dll is available in the C: WindowsSystem32 folder or install the Microsoft Remote Server Administration Tools (RSAT) for the respective OS from Microsoft software download center.	cd C:WindowsSystem32 and then dir certadm.dll
CertUtil	File will be available at the System32 folder.	Run certutil in the command prompt.

Component	Description	Scripts
NetSH	Copy to the System32 folder if it is not available.	Run netsh in the command prompt.
RPC	Start the Remote procedure call in the services	net start RpcSs
WMI	Start the Windows Management Instrumentation in the services.	net start Winmgmt
WinRM	Start the Windows Remote Management.	net start WinRM
User Permission	When the users are added in the Group and the machine is not restarted a permission error will occur. Ensure that the machine is restarted when the user is added to a group.	Gwmi win32_groupuser -computer ptpll594|? {$_.groupcomponent -like '*""Administrators""'} \|select PartComponentnet localgroup administratorsCheck if user can access C$/windows/temp or admin$/Temp Local admin addition needs to restart.
	When the users are added in the Group and the machine is not restarted a permission error will occur. Ensure that the machine is restarted when the user is added to a group.	Gwmi win32_groupuser -computer ptpll594|? {$_.groupcomponent -like '*""Administrators""'} \|select PartComponent net localgroup administratorsCheck if user can access C$/windows/temp or admin$/Temp Local admin addition needs to restart.
File Operations		Check if the user can access C$/windows/temp or admin $/temp. If you do not have c-drive then change the configuration to the available drive.

Component	Description	Scripts
Port	Check if the port is already in use.	netstat -an |find ""8999" Check the Firewall outbound rules for the port Ping test from AppViewX Antivirus block for the port Turn off the local firewall Check the server, client, root, and intermediate certificates Check if the C: Logs folder exists and the permissions If you check in the Internet Explorer then the enhanced security must be disabled in the server role local server.
Powershell Remoting		Enter-PSSession -ComputerName <computername> -Credential <username>

Firewall Requirements

The firewall must not block the following ports:

Component	Port
Powershell	5985
WMI	5985 and 135

Minimum Permissions Required for Communication

The AppViewX Windows Gateway agent communicates with the CAs via the following three communication modes:

- WMI
- Native API
- PowerShell

WMI

Note: For communication through WMI, ensure that the C$ share is enabled.

For the following use cases, this section lists the minimum permissions required for the AppViewX Windows Gateway to communicate with the CAs via WMI:

- Discovery
- Create CSR
- Create Certificate
- Create Certificate-Upload CSR
- Renew Certificate
- Revoke Certificate
- Certificate Push
- Certificate Bind

Discovery

- Microsoft CA
- IIS
- Microsoft PC
- Microsoft Server

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Full control permission to **C:\Windows\Temp** • Read permission at CA level for the service account or the service account group
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability
Ports	NA	135, 445, or 139

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
User permission		Full control permission to **C:\Windows\Temp**
Services	WMI Service	WMI Service
Ports	NA	135

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
User permission		Full control permission to **C:\Windows\Temp**

Requirement	AppViewX Windows Gateway	Microsoft PC
Services	WMI Service	WMI Service
Ports	NA	135

Microsoft Server

Requirement	AppViewX Windows Gateway	Microsoft Server
User account type	Service account	Service account
User permission	NA	• Full control permission to **C:\Windows\Temp** • Read permission at CA level for the service account or the service account group
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability
Ports	NA	135, 445, or 139

Create CSR

- IIS
- Microsoft PC

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	WMI Service	WMI Service
Ports	NA	445

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
Services	WMI Service	WMI Service
Ports	NA	445

Create Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability
Ports	NA	135, 445, or 139

Create Certificate-Upload CSR

• Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability
Ports	NA	135, 445, or 139

Renew Certificate

• Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service ac-

Requirement	AppViewX Windows Gateway	Microsoft CA
		count group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability
Ports	NA	135, 445, or 139

Revoke Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	WMI Service, certutil.exe command availability	WMI Service, certutil.exe command availability

Requirement	AppViewX Windows Gateway	Microsoft CA
Ports	NA	135, 445, or 139

Certificate Push

- IIS
- Microsoft PC
- Microsoft Server

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	WMI Service	WMI Service
Ports	NA	445 or 139

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
Services	WMI Service	WMI Service
Ports	NA	445 or 139

Microsoft Server

Requirement	AppViewX Windows Gateway	Microsoft Server
User account type	Service account	Service account

Requirement	AppViewX Windows Gateway	Microsoft Server
User permission	NA	• Full control permission to **C:\Windows\Temp** • Read permission at CA level for the service account or the service account group
Services	WMI Service	WMI Service
Ports	NA	445 or 139

Certificate Bind

- IIS

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	WMI Service	WMI Service
Ports	NA	135

Native API

For the following use cases, this section lists the minimum permissions required for the AppViewX Windows Gateway to communicate with the CAs via Native API:

- All Operations
- Discovery
- Create Certificate
- Create Certificate-Upload CSR

- Renew Certificate
- Revoke Certificate

All Operations

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Read, request certificates, and issue and manage certificates permission at the CA level for the service account/service account group /authenticated users • Enroll permission at the certificate template level for the service account/service account group/ authenticated users
Services	RPC Service	RPC Service, certutil.exe command availability
Ports	NA	135 as incoming port

Discovery

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Read permission at the CA level for the service account or the service account group
Services	RPC Service	RPC Service, certutil.exe command availability
Ports	NA	135 as incoming port

Create Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	RPC Service	RPC Service, certutil.exe command availability

Requirement	AppViewX Windows Gateway	Microsoft CA
Ports	NA	135 as incoming port

Create Certificate-Upload CSR

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	RPC Service	RPC Service
Ports	NA	135 as incoming port

Renew Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at the CA level for the service account or the service account group or the authenticated users • Enroll permission at the certificate template level for the service account or the service account group or the authenticated users
Services	RPC Service	RPC Service, certutil.exe command availability
Ports	NA	135 as incoming port

Revoke Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	Issue and manage certificates permission at CA level for the service account or the service account group or the authenticated users

Requirement	AppViewX Windows Gateway	Microsoft CA
Services	RPC Service	RPC Service,certutil.exe command availability
Ports	NA	5985

PowerShell

For the following use cases, this section lists the minimum permissions required for the AppViewX Windows Gateway to communicate with the CAs via PowerShell:

- Discovery
- Create CSR
- Create Certificate
- Create Certificate-Upload CSR
- Renew Certificate
- Revoke Certificate
- Certificate Push
- Certificate Bind

Discovery

- Microsoft CA
- IIS
- Microsoft PC
- Microsoft Server

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account

Requirement	AppViewX Windows Gateway	Microsoft CA
User permission	NA	• Full control permission to **C:\Windows\Temp** • Read permission at CA level for the service account or the service account group
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
Ports	NA	5985

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting`	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985

Microsoft Server

Requirement	AppViewX Windows Gateway	Microsoft Server
User account type	Admin account	Admin account
User permission	NA	Read permission for the folder to be discovered
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985

Create CSR

- IIS
- Microsoft PC

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting`	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting

Requirement	AppViewX Windows Gateway	Microsoft PC
Ports	NA	5985

Create Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at CA level for the service account/service account group/ authenticated users • Enroll permission at the certificate template level for the service account/service account group/ authenticated users
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
Ports	NA	5985

Create Certificate-Upload CSR

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at CA level for the service account/service account group/ authenticated users • Enroll permission at the certificate template level for the service account/service account group/ authenticated users
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
Ports	NA	5985

Renew Certificate

- Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	• Request certificates permission at CA level for the service account/service account group/ authenticated users

Requirement	AppViewX Windows Gateway	Microsoft CA
		• Enroll permission at the certificate template level for the service account/service account group/ authenticated users
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
Ports	NA	5985

Revoke Certificate

• Microsoft CA

Microsoft CA

Requirement	AppViewX Windows Gateway	Microsoft CA
User account type	Service account	Service account
User permission	NA	Issue and manage certificates permission at CA level for the service account or the service account group or the authenticated users
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
Ports	NA	5985

Certificate Push

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
User permission	NA	Full control permission to **C:\Windows\Temp**
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985, 445, or 139

Microsoft PC

Requirement	AppViewX Windows Gateway	Microsoft PC
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting`	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985, 445, or 139

Microsoft Server

Requirement	AppViewX Windows Gateway	Microsoft Server
User account type	Admin account	Admin account
User permission	NA	Write permission for the folder to be discovered

Requirement	AppViewX Windows Gateway	Microsoft Server
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting`	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985, 445, or 139

Certificate Bind

- IIS

IIS

Requirement	AppViewX Windows Gateway	IIS
User account type	Admin account	Admin account
Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting
Ports	NA	5985

Chapter 2: Appendix B

- Troubleshooting the Target Machine

Troubleshooting the Target Machine

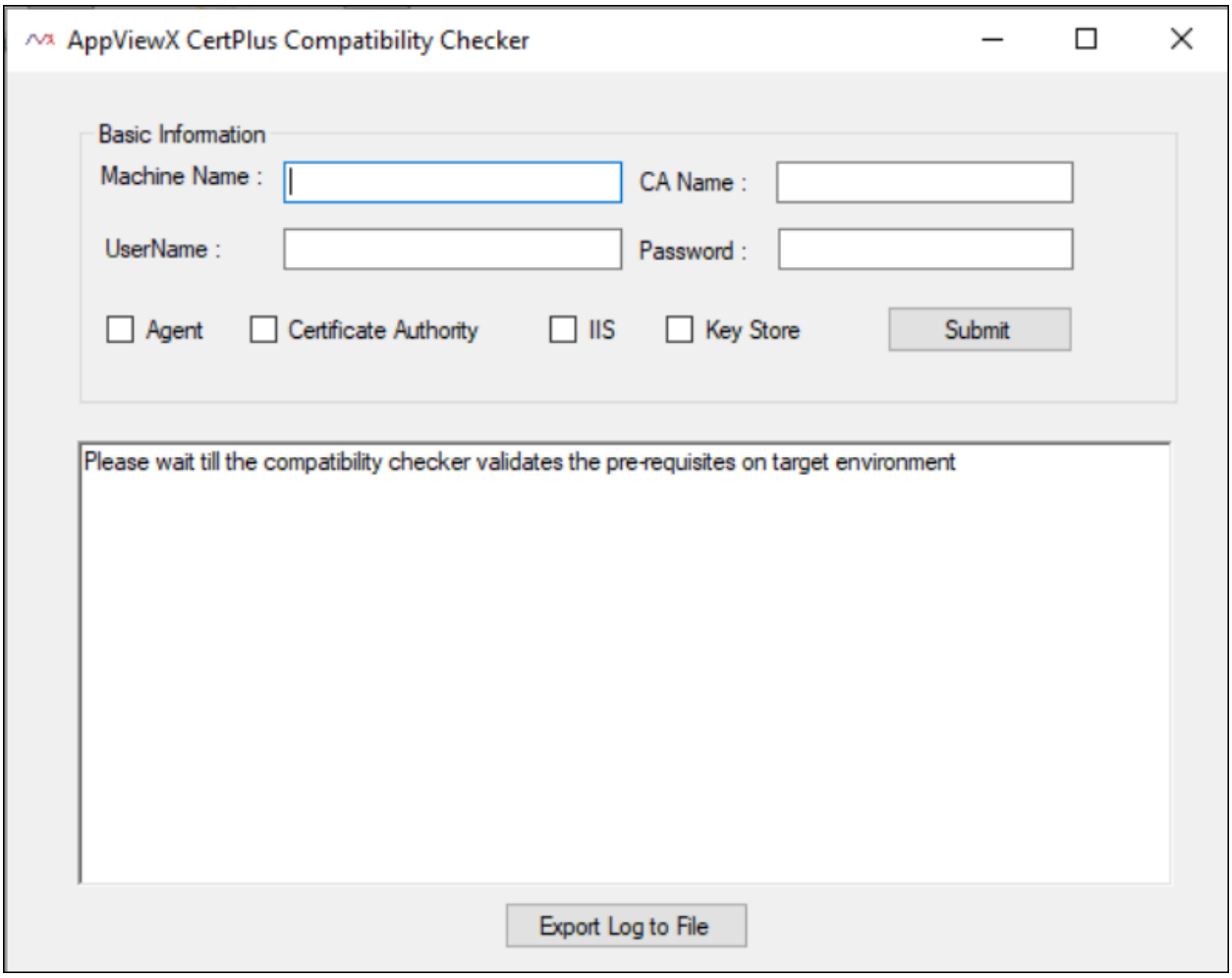
Overview: AppViewX Windows Gateway Troubleshooting Tool

The AppViewX Troubleshooting tool is used to analyze the accessibility of the target machine, to which the AppViewX communicates.

Accessing the Validator

To launch the validator,

From the Windows **Start** menu, execute the **AppViewX.CertPlus.Validator.exe** file.
The **AppViewX CertPlus Compatibility Checker** screen is displayed.



Validating the Target Machine

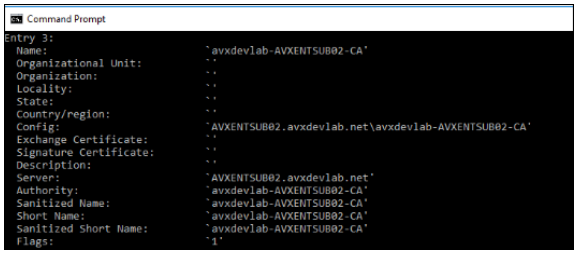
1. On the **AppViewX CertPlus Compatibility Checker** screen, in the **Basic Information** section:
   a. Enter the following details:

Name	Description	Condition
Machine Name	Enter the hostname of the target machine for validation.	Mandatory field.
CA Name	Enter the name of the Certificate Authority from the CA Config.	Mandatory only when the **Certificate Authority** option (explained in the next step) is selected .

Name	Description	Condition
User Name	Enter the username for accessing the target machine.	Mandatory field Format: username@domainname
Password	Enter the password for accessing the target machine.	Mandatory field

b. From the following choices, select one or more options as required:

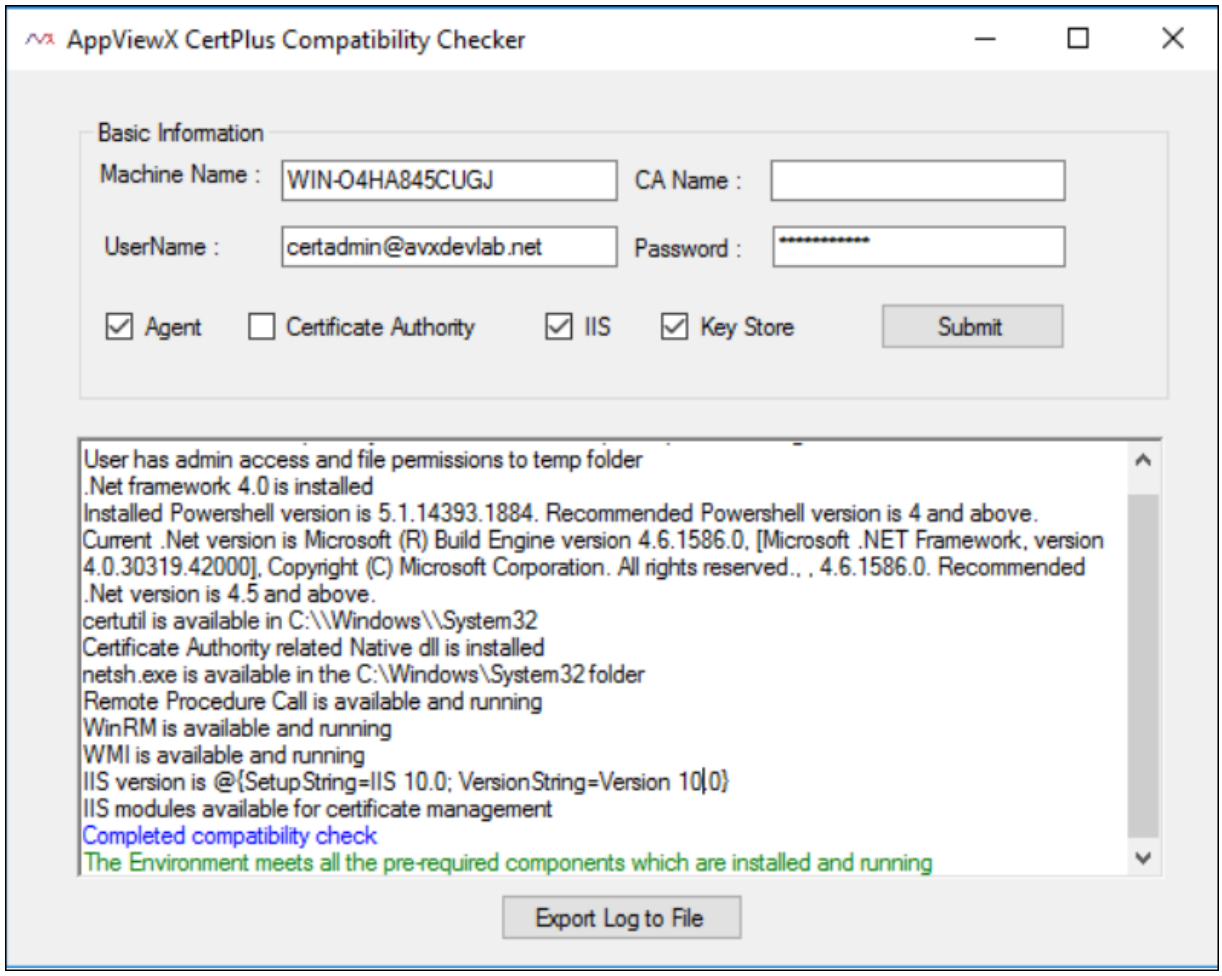
Option	Description
Agent	To install the AppViewX Windows Gateway in the target machine, select this option. This will validate the prerequisites required for the installation. The machine name will be entered in the **Machine Name** field.
Certificate Authority	To validate the Certificate Authority-related functionality, select this option. The CA Name is mandatory only in this case. Use the `certutil -dump` command in a cmd window to get the CA Name. In the output, the value for **Server** is the Machine Name and the value for **Name** is the CA Name. In the sample screenshot shown below, the machine name is **AVXENTSUB02.avxdevlab.net** and the CA Name is **avxdevlab-AVXENTSUB02-CA**.

Option	Description
	
IIS	To validate the IIS-sites related functionality, select this option.
Key Store	To validate only the Microsoft Certificate-store related functionality, select this option.

2. Click **Submit**.

> **Note:** Mandatory fields (from **Machine Name**, **CA Name**, **UserName**, and **Password**) that have been missed will be highlighted in red after you click **Submit**.

The validation summary is displayed in the text box below the **Basic Information** section, as shown in the image below:



The validation summary follows the color code explained below:

Color	Indicates
Black	Success information and output
Red	An error or warning
Blue	Completion of the validation process
Green	Successful completion of the process

3. To export the validation summary into a log file, click **Export Log to File**.

   Following are the validations performed by the AppViewX Windows Troubleshooting tool:

Validate	Description	Agent	CA	IIS	Keystore
User	The validator will connect to the target	Yes	Yes	Yes	Yes

Validate	Description	Agent	CA	IIS	Keystore
	machine with the username and password specified, and check if the target machine has admin access.				
.Net framework	The validator will check if .Net framework version 4.5.2+ is installed. It will also display the current version installed.	Yes	Yes	Yes	Yes
PowerShell	The validator will check if PowerShell is installed. It will also display the current version of PowerShell installed.	Yes	Yes	Yes	Yes
CertUtil	The validator will check if the certutil component is available. The certutil component is used to retrieve the CA name and the corresponding templates.	Yes	Yes	No	No
Certadm.dll	The validator will check if this component, a native component to access the CA, is available in the **C:\Windows\System32** folder. Sometimes, while trying to access	Yes	Yes	No	No

Validate	Description	Agent	CA	IIS	Keystore
	this component during verification, it will return an error. Therefore, a manual check must be performed.				
netsh.exe	This is used to bind the certificate to the installed agent port (8999).	Yes	No	No	No
RPC	The validator will check if the Remote Procedure Call (RPC) service is installed and running on the target machine. This service should be running to perform all remote operations.	Yes	Yes	Yes	Yes
WinRM	The validator will check if the Windows Remote Management service is installed and running on the target machine. This service is required for the PowerShell execution.	Yes	Yes	Yes	Yes
WMI	The validator will check if the Windows Management Instrumentation service	Yes	Yes	Yes	Yes

Validate	Description	Agent	CA	IIS	Keystore
	is installed and running on the target machine. This service is required for the WMI and PowerShell execution.				
IIS	The validator will check if the IIS server is installed and, if yes, the current IIS version.	No	No	Yes	No