# MaaS360 Cloud Extender

## Common Criteria Guide

## Abstract

**Guide to Set up the Cloud Extender to Meet NIAP Common Criteria Requirements**

**Version 1.0, 20 July 2022**

## Table of Contents

# 1 Introduction

This guide describes installation and configuration of the MaaS360 Cloud Extender in the Common Criteria evaluated configuration. In general, this guide supplements information found in standard product guidance, but in any case, where differing information is provided, this guide takes precedence over all other product guidance when installing and using the Cloud Extender in the evaluated configuration.

To get started, visit the MaaS360 site (https://m1.maas360.com/tryMDM/SK_MDM_C) and click on Free Trial. This will create your MaaS360 account. Once you start the Free Trial, you will receive emails with the links to download the software and a license key required to activate the software. The Free Trial version is frequently updated and is most likely not the same version as the evaluated product. To obtain a distribution of the evaluated product and guidance, you will need to contact MaaS360 Customer Support at (https://www.ibm.com/mysupport/s/topic/0TO0z000000YckSGAS/maas360?language=en_US&_ga=2.171360096.1558214632.1654015637-840974718.1610459656) and request the Common Criteria evaluated version of Cloud Extender. Obtain the product and guidance, then return to this guide for specific configuration steps to put the product into the evaluated configuration.

## 1.1 Intended Audience

This guide is intended for MaaS360 administrators with experience in the configuration and maintenance of Windows servers. Knowledge of networking and user-management configuration is assumed. This document explains the administrative tasks for the software and is solely intended for MaaS360 administrators.

## 1.2 Evaluated Versions

The following Cloud Extender version and the pertaining components mentioned below were evaluated for Common Criteria.

- IBM MaaS360 v 2.106.500.016 Cloud Extender.
    - Core installer.
    - Cloud Extender Configuration Tool
    - Cloud Extender Modules
        - Exchange Integration for Managing ActiveSync Devices
        - Corporate Directory Authentication
        - Corporate User Visibility
        - Certificate Authority

The evaluation was performed using the following Operating Systems (OS).

- Microsoft Windows Server 2019 Standard version 1809 (x64).

The evaluation was performed on the following hardware.

- Dell PowerEdge R740 with an Intel Xeon Gold 5118 processor

## 1.3 Cryptographic Acknowledgment

The Cloud Extender uses cryptographic services provided by both the Windows platform and OpenSSL. The Target of Evaluation is bound to OpenSSL, and it is not possible to remove OpenSSL or replace its function with another cryptographic component. Only these two cryptographic services were tested as part of the Evaluated Configuration.

The cryptographic functionality included with the Cloud Extender (OpenSSL) cannot be configured or modified. The TOE, including the Configuration Tool, provides no functions to alter these cryptographic algorithms, key schemes, or key sizes.

The cryptographic functionality provided by the Windows platform must be configured as described in section 2.1 during installation of the TOE. Only the key schemes and sizes listed there are to be included in the evaluated configuration.

## 1.4 Security Objectives and Assumptions

The security objectives and assumptions have been taken from “Protection Profile for Application Software Version 1.3”. They are reproduced here for the convenience of the reader.

### 1.4.1 Platform

The Cloud Extender relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the Cloud Extender.

### 1.4.2 Proper User

The user of the application software is not willfully negligent or hostile and uses the software within compliance of the applied enterprise security policy.

### 1.4.3 Proper Admin

The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

## 1.5 Managing Updates and Known Vulnerabilities

Timely installation of vendor-provided or vendor-approved updates or patches is always recommended to maintain protection against new flaws or attacks as they may be discovered.

## 1.6 TOE Security Functionality

In the evaluated configuration, the TOE supports the following security functionality.

### 1.6.1 Cryptographic Support

The Cloud Extender provides cryptographic support using the Windows platform provided cryptographic services via the Cryptography API: Next Generation (CNG) for the following features.

- TLS connections: CNG is used by Secure Channel (SChannel), enabling the Cloud Extender to communicate with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2, and only using a subset of the TLS 1.2 ciphers.
- Protecting data-at-rest using the Encrypted File System (EFS) to the C:\ProgramData\MaaS360\ directory that contains all configuration and log information.
- Encrypting registry entries using the Data Protection Application Programming Interface (DAPI).
- Generating an Exchange Server certificate during the installation process.

The inclusion of the OpenSSL libraries with the TOE provides cryptographic functionality for the following functions.

- TLS connections to the MaaS360 Portal and SCEP certificate servers only (HTTPS using cURL).
- Encryption of configuration profiles, but as these are stored within an EFS directory above it is not the enforcing SFR.
- Device and User Certificate generation for certificate signing requests to a SCEP server using the Device and User templates. The Cloud Extender generates a certificate based on requirements and pushes that certificate to the mobile device.

Entropy to generate random numbers is obtained from the Windows Operating System and provides a security strength of 256 bits.

### 1.6.2 User Data Protection

The application provides user data protection services through restricting access by the application to only those platform-based resources (sensitive data repositories, and network communications) that are needed to provide the needed application functionality.

Sensitive application data is encrypted using platform-provided encrypted file system (EFS) services, when stored in non-volatile memory, such as the hard disk drive(s).

### 1.6.3 Identification and Authentication

The TOE supports authentication by X.509 certificates by the application and using the platform API.

### 1.6.4 Security Management

The Cloud Extender application provides the ability to set various configuration options for the TOE. These options are stored, as recommended by Microsoft, in the Windows Registry and are protected using the Data Protection application programming interface (DPAPI).

During installation, the files installed on the platform are allocated appropriate file-permissions, supporting the protection of the application, and its data from unauthorized access.

### 1.6.5 Privacy

The Cloud Extender application does not specifically request Personally Identifiable Information (PII).

### 1.6.6 Protection of the TSF

The Cloud Extender application uses only documented Windows APIs, and it is packaged with third-party libraries which provide supporting functionality.

The Cloud Extender application is packaged and delivered in the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process using the Microsoft Sign Tool.exe (v6.3). It is compiled by IBM with stack-based buffer overflow protection enabled.

The Cloud Extender application does not write user-modifiable files to directories that contain executable files.

### 1.6.7 Trusted Path/Channels

The Cloud Extender application protects all transmitted data by using TLS 1.2 protected trusted channels. Protocols used within these trusted channels may include additional protection and include HTTPS, and LDAPS.

## 1.7 Excluded Functionality

The following modules are not part of the evaluated configuration.

- IBM Traveler module

- Exchange Integration for Real-time Mail Notifications module
- BlackBerry Enterprise Server (BES) module
- Mobile Enterprise Gateway (MEG) module
- MaaS360 VPN module
- Zebra Printer Management module

# 2 Protect Cloud Extender Communications When Using HTTPS

The following sections document the steps required so the Cloud Extender can communicate to the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2, and only using a subset of the TLS 1.2 ciphers.

Do not install the Cloud Extender now. Installing the Cloud Extender will happen during the folder encryption steps.

## 2.1 Make TLS 1.2 the System Default on Windows Server 2019

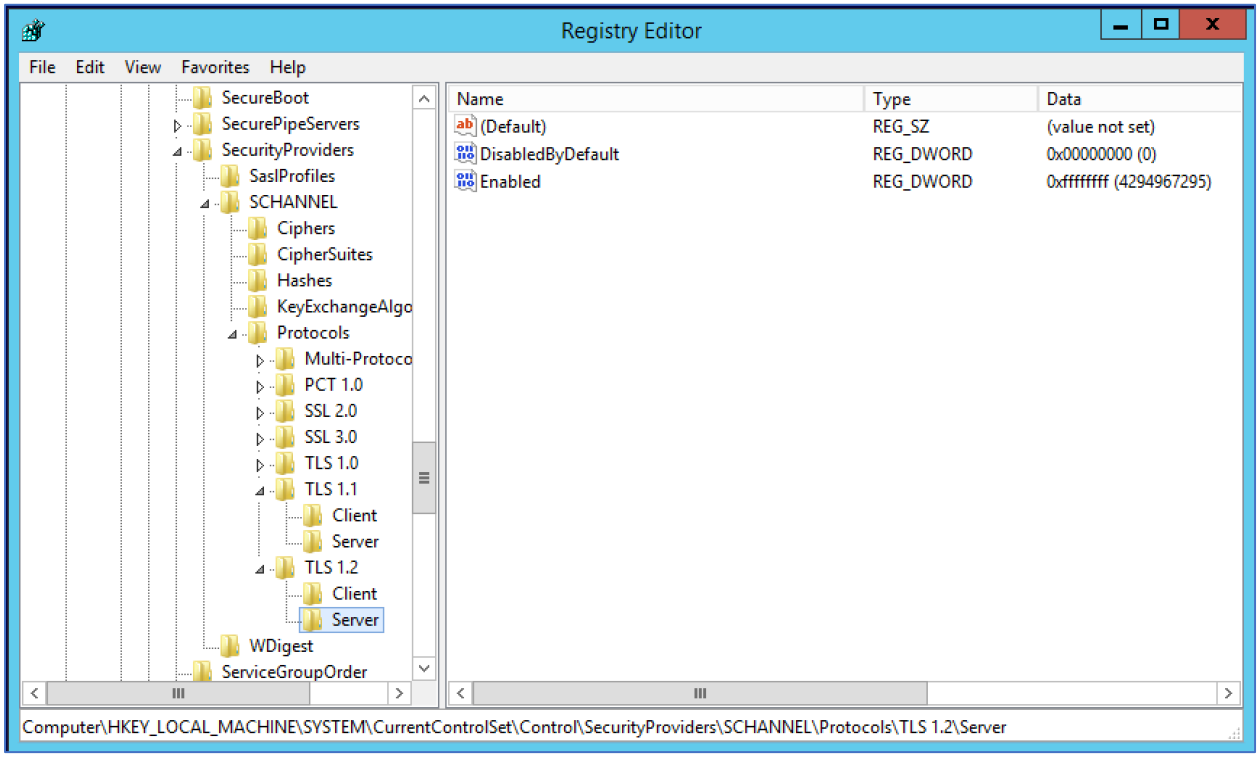
By default, the Windows Operating System (OS) will negotiate all the Transport Layer Security (TLS) and SSL protocols when creating an HTTPS session. Follow the steps listed below to restrict the OS to use just TLS 1.2 and to limit the cryptographic ciphers to those specified in the Software Application Protection Profile v1.3, which can be downloaded from NIAP at: (https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429).

There are three exported registry settings, described in Appendix A that can be used to create .reg files to run on the Cloud Extender server. After running these three files you can open the registry editor to view the changes required to limit the protocol to TLS 1.2 and specific ciphers.

Perform the following steps.

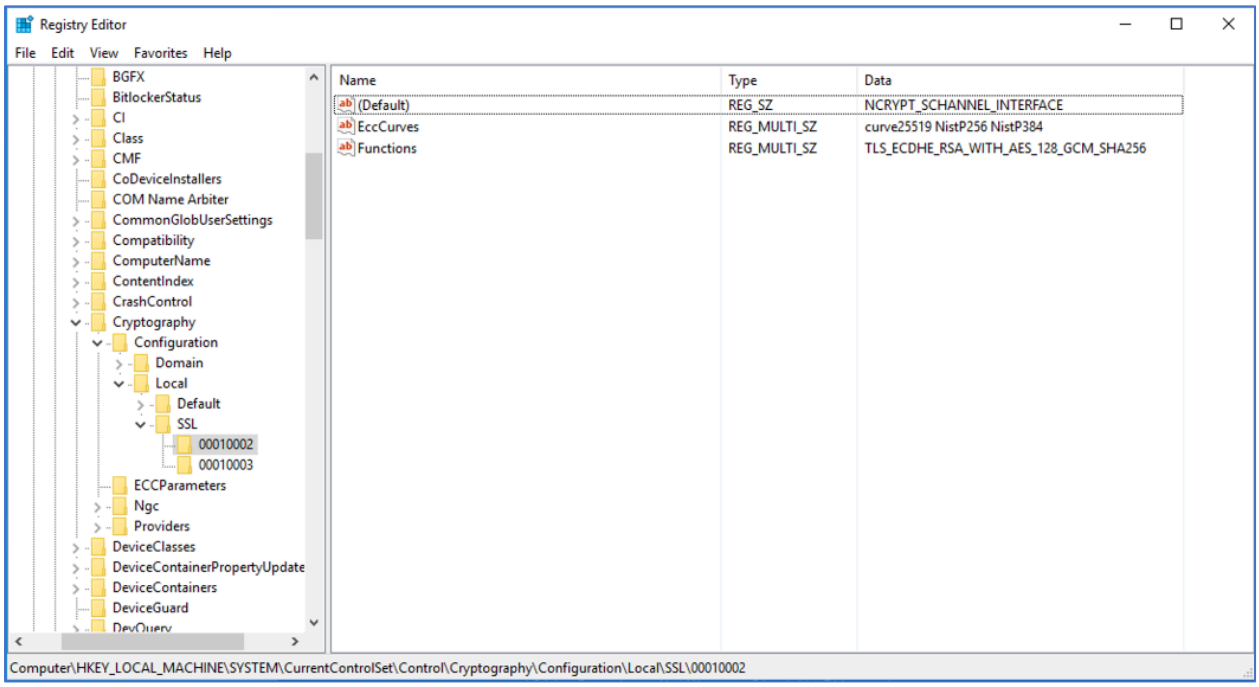
- Create three .reg files as described in Appendix A: Protocols.reg, CipherAvail.reg, and CCCiphers.reg.
- Use Remote Desktop to access the Cloud Extender server and copy these three files to a temp folder.
- Run each of the files and select **Yes** to the prompt **Are you sure you want to modify the registry**…
- Reboot the server after running all three reg files. The changes will not take effect until after a reboot

After running Protocols.reg open the Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`. Only TLS 1.2/Server will have **Enabled** to **0xffffffff**. TLS 1.1, and as shown below, will have **Enabled** set to **0**.




After running CipherAvail.reg open the Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002`. Only the following cipher is enabled:

`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`



After running CCCiphers.reg open the Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Fiberlink\V360\NIAP_SSL_Ciphers`. This shows the TLS ciphers that will be offered to the server during TLS handshaking:

| | | |
|---|---|---|
| NIAP_SSL_Ciphers | REG_SZ | ECDHE-RSA-AES128-GCM-SHA256 |

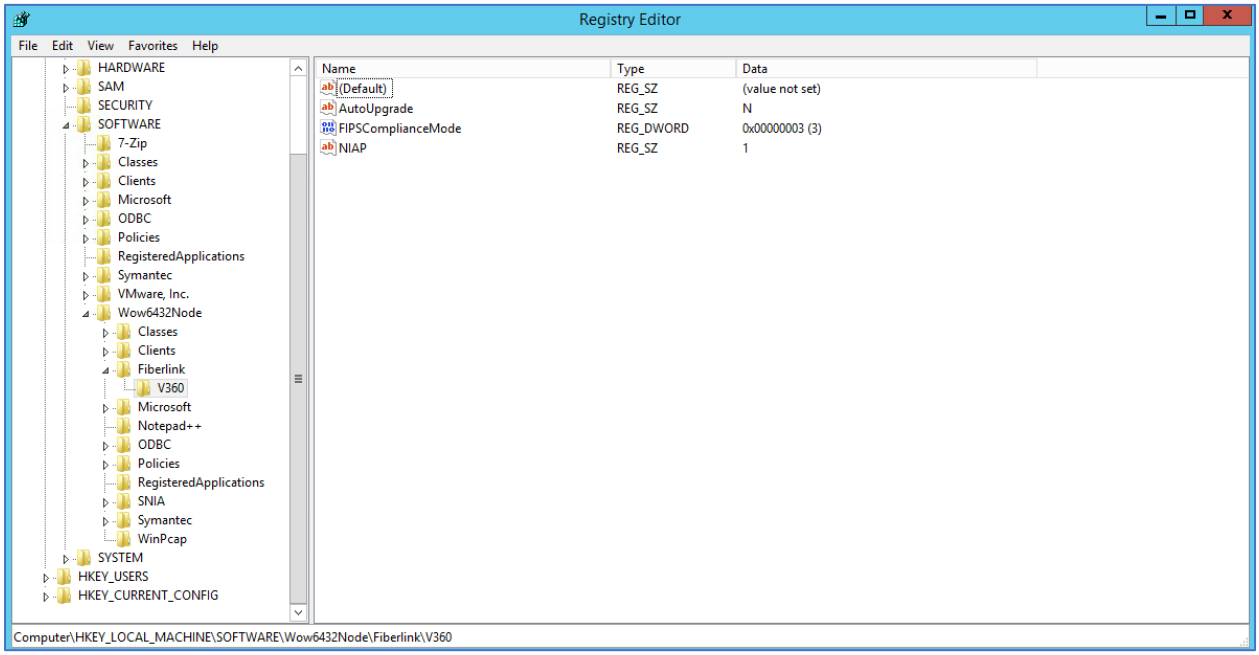
Remember to reboot the server after running the reg files.

## 2.2 Enable FIPS and NIAP Modes and disable module updates

By default, the Cloud Extender does not limit HTTPS to the TLS 1.2 protocol and limited ciphers. FIPS is also disabled by default and modules updates are enabled by default. To make the necessary changes for the evaluated configuration, perform the following steps:

- Create a .reg files from Appendix B: NIAP=1_FIPS=3.reg
- Use Remote Desktop to access the Cloud Extender server and copy this file to a temp folder
- Run this .reg file and select **Yes** to the prompt **Are you sure you want to modify the registry …**
- Restart the Cloud Extender (emsagent) service to pick up these new settings

The FIPSComplianceMode key is now set to **3**, the NIAP key is now set to **1**, and the **AutoUpgrade** key is set to N as shown in the following screenshot.



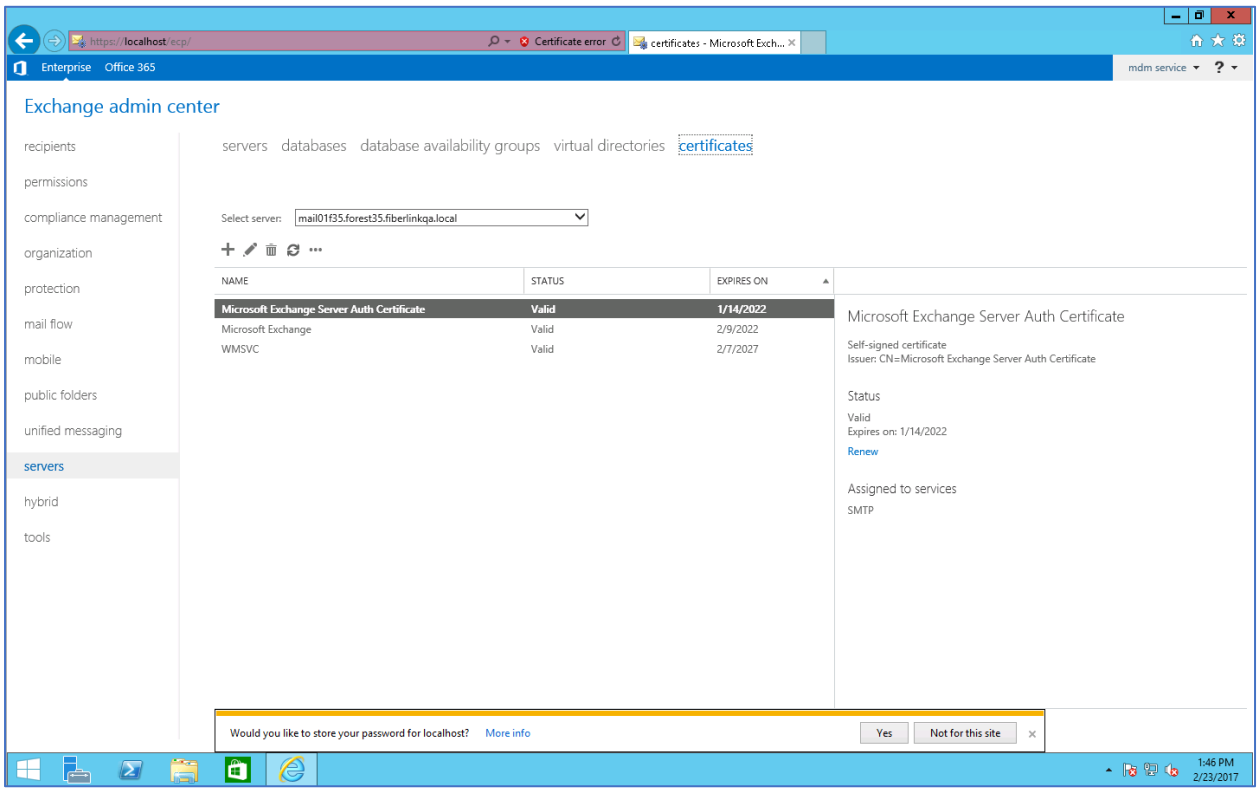
If the Cloud Extender is uninstalled these registry keys will be deleted, so run the NIAP=1_FIPS=3.reg before reinstalling the Cloud Extender again.

## 2.3 Exchange Server Certificate

In the evaluated configuration, the Cloud Extender supports RSA certificates with key size of 2048 bits or greater, and signed with SHA-256 and SHA-384.

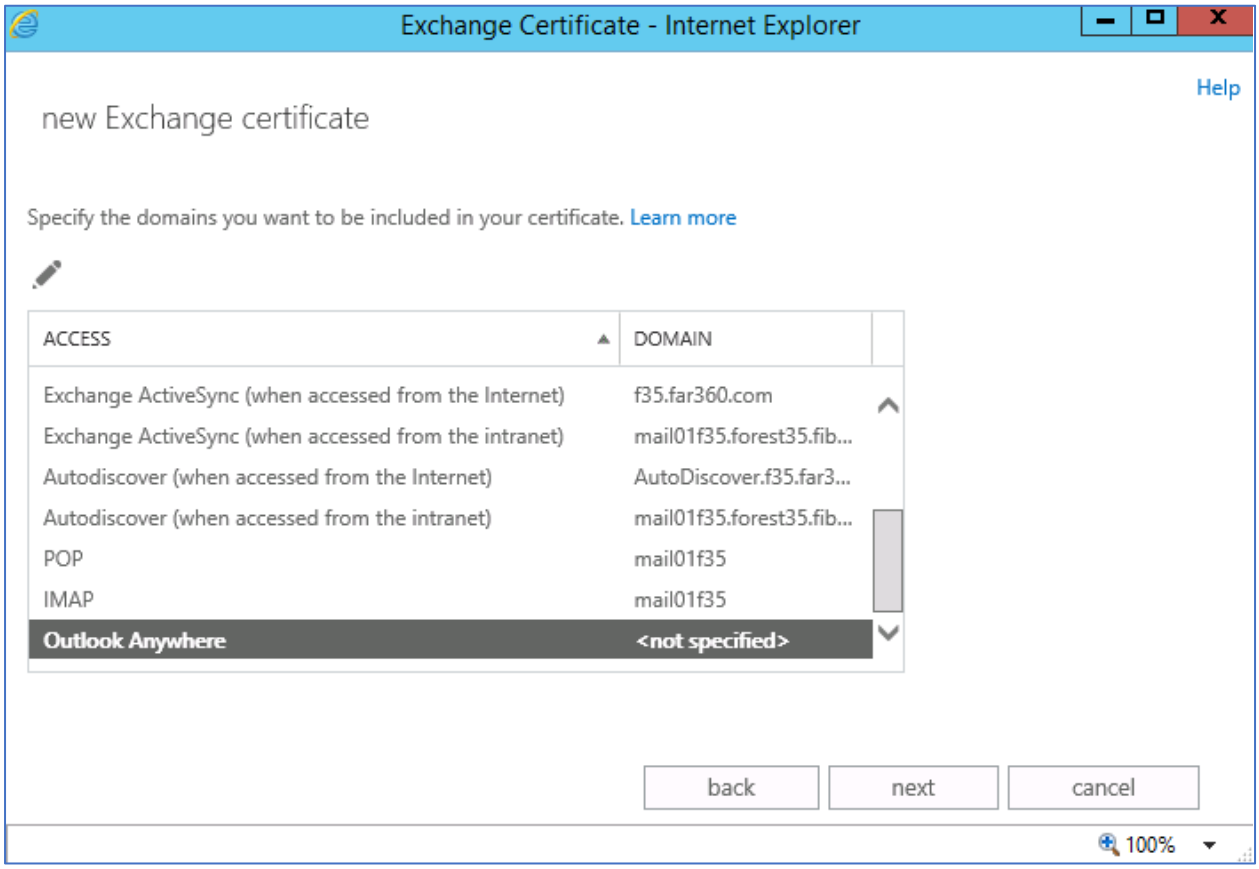
Perform the following steps to create an Exchange certificate and enable it for HTTPS communications:

- Using a browser log in to the Microsoft Exchange Control Panel with an account that has organization admin privileges
- Navigate to Servers > Certificates as seen in the screenshot below

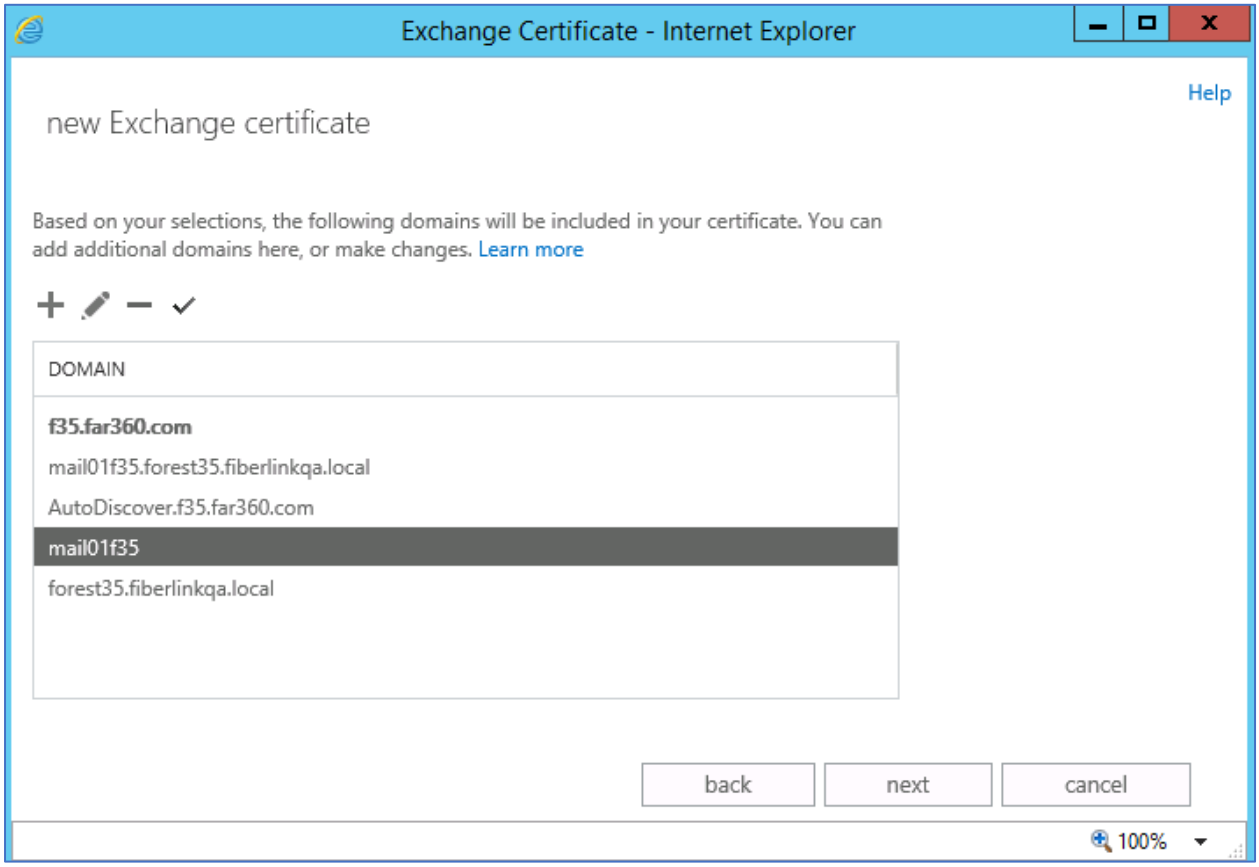



- Click the + sign to create a new certificate.
- Select Create a request for a certificate from a certification authority and click next.
- Enter a friendly name (anything) when prompted and click **next**.
- Make sure “request a wildcard cert” is unchecked, and click **next**.
- On the next screen, click **browse**, and select your exchange server.

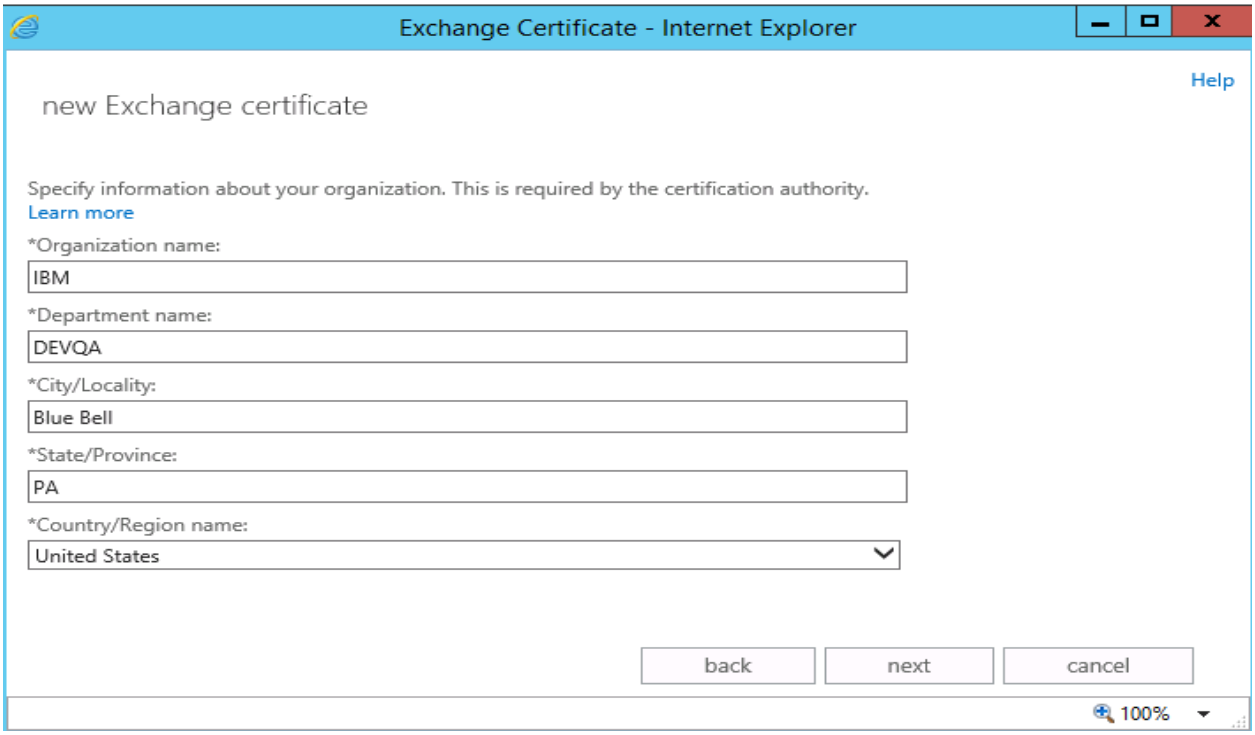
On this screen, you must make sure the URLS for the sites marked “INTRANET” are all set correctly to the internal URL of the mail server. The sites marked “EXTRANET” are optional, but can be set if you will be connecting devices externally.



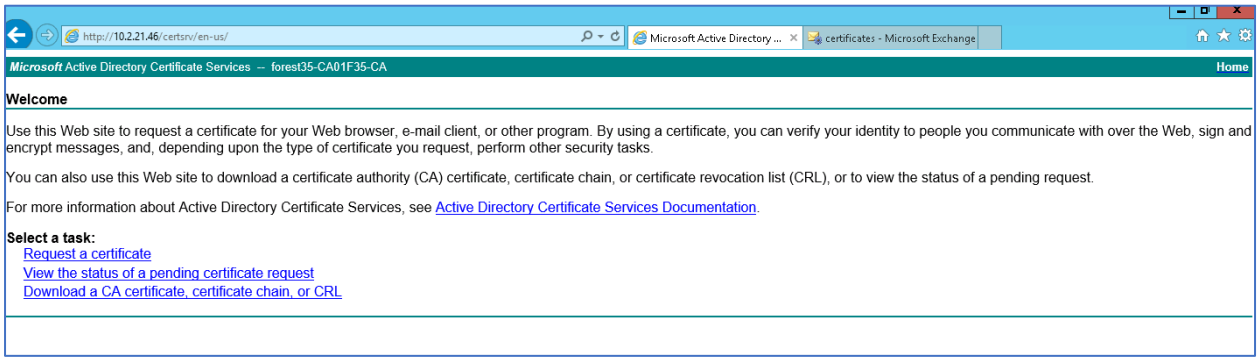

- On the next screen, verify that both the Fully Qualified Domain Name (FQDN) of the mail server, as well as the short name have been added to the domain list. If either is missing, add it manually.



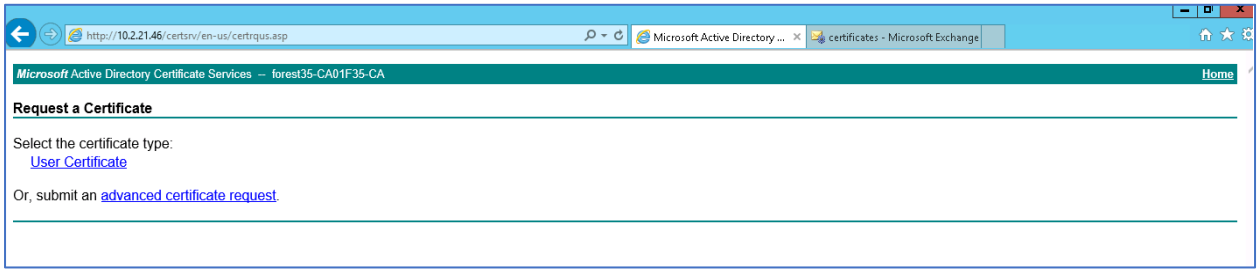

- On this screen, enter information about your organization that will appear in the certificate and click **next**.



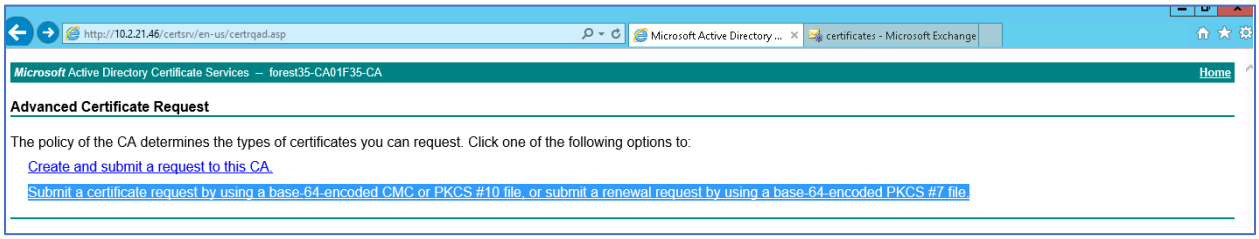

- On the next step, enter a UNC path to save the cert request and click finish. The file will then be saved and ready to submit to the CA server.
- Do not close the exchange admin center, as you will return here shortly.
- Open the self-service certificate portal for the CA you are using to generate the actual certificate. If you have installed the "Certificate Authority Web Enrollment" feature on the CA, the site will be something like http://<FQDNofinternalserver>/certsvr/en-us.
- From the introduction screen, select **Request a certificate.**



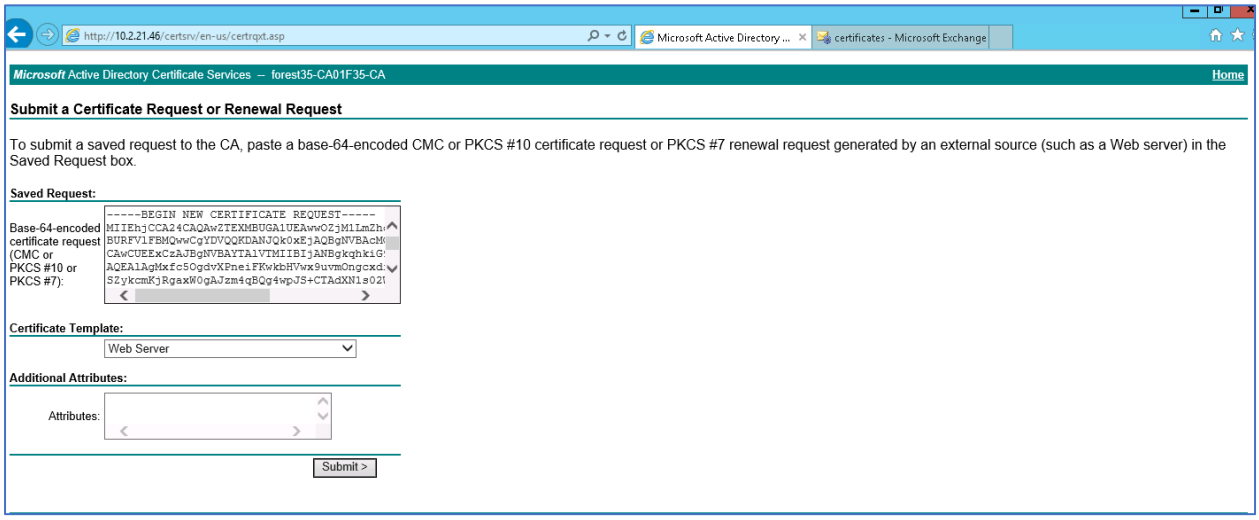

- Click **advanced certificate request**.



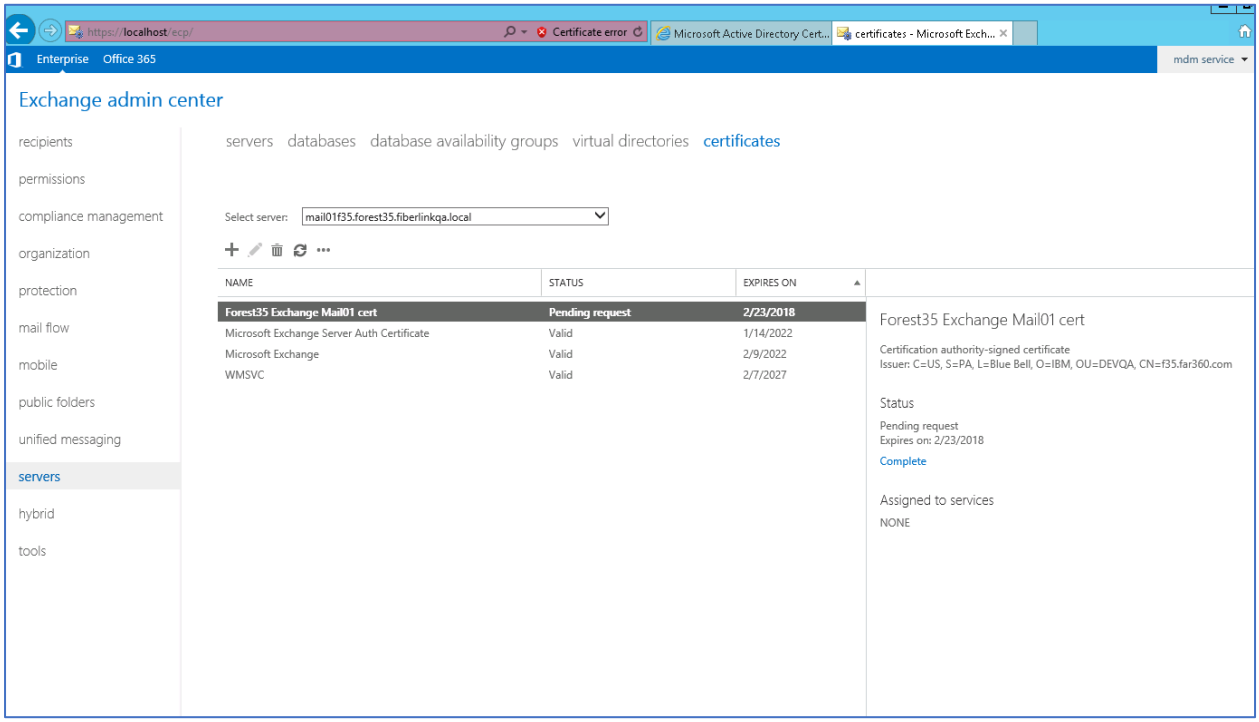

- Click **Submit a certificate request…** (the second option).



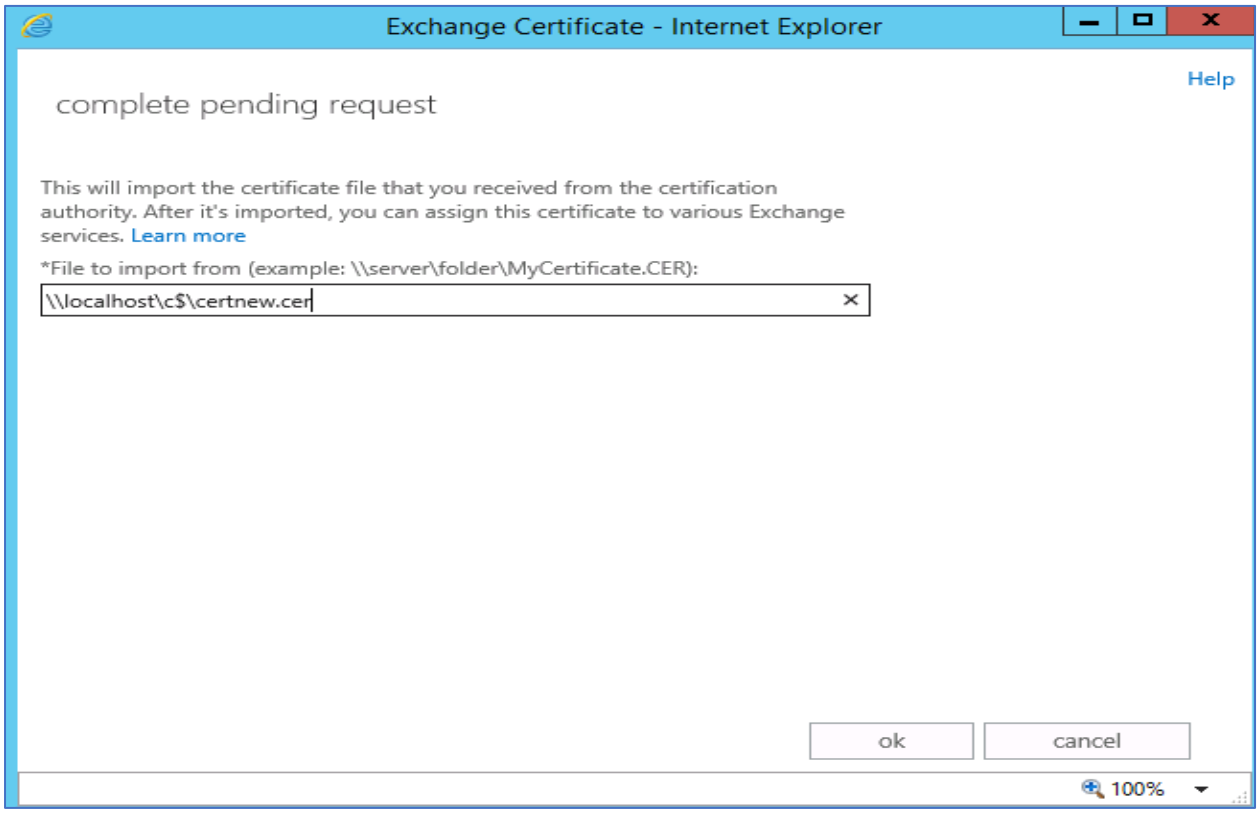

- In the template drop down box, select **web server**. Open the certificate request file you generated from the exchange server in a text editor, copy the contents, and paste them into the large text box at the top of the screen. Click **submit**.



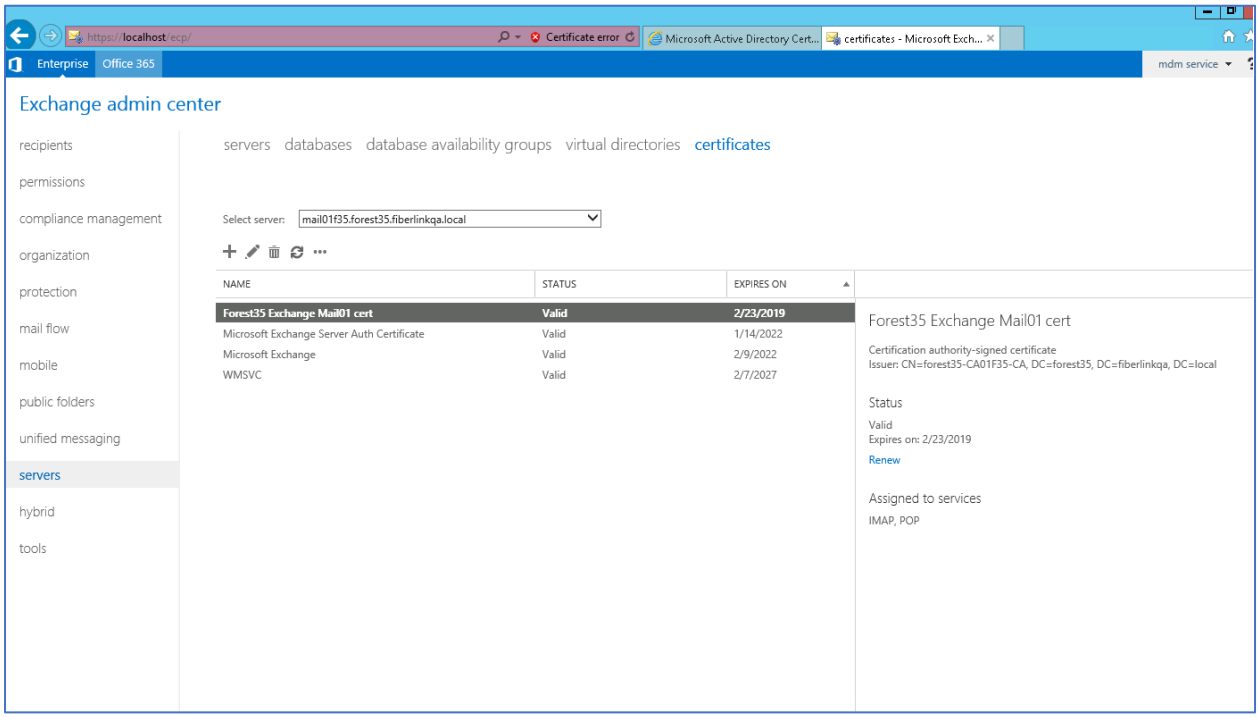

- Download the generated certificate file to use in the next steps.
- Back in the Exchange Admin Center, find the pending certificate request in the list, and select it. Then on the right, click the **complete** link.



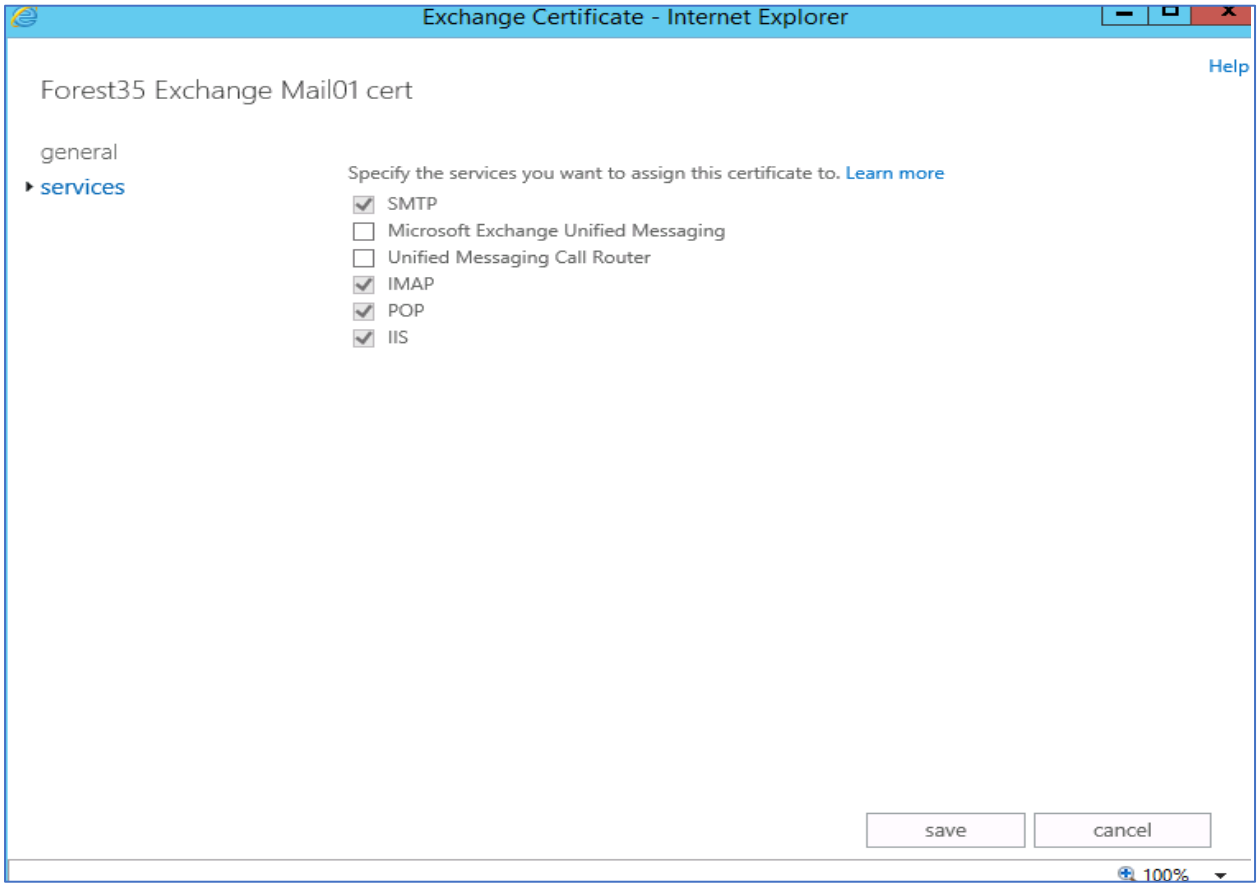

- Copy the cert file you downloaded previously to a UNC path accessible from the exchange server, enter the path to the file, and click **next**



- The cert should now show as valid in the list. Select the cert, click **edit**, and then click **services** on the left of the new window that opens



- Select the IIS and SMTP check boxes, click **save**, and acknowledge any warning prompts.



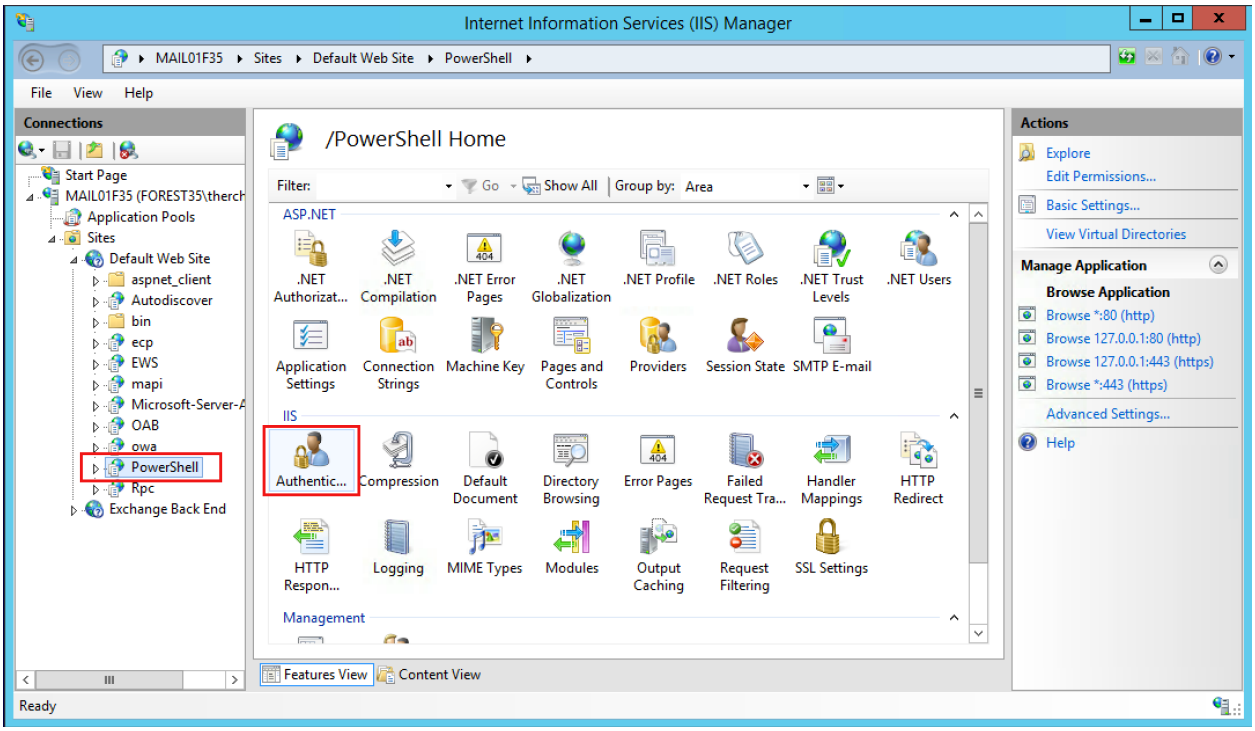

- As a final step, delete the **Microsoft Exchange** self-signed certificate from the list if it exists. This will make sure the new cert is the only one answering IIS requests.

The certificate is now installed and ready to use with exchange.

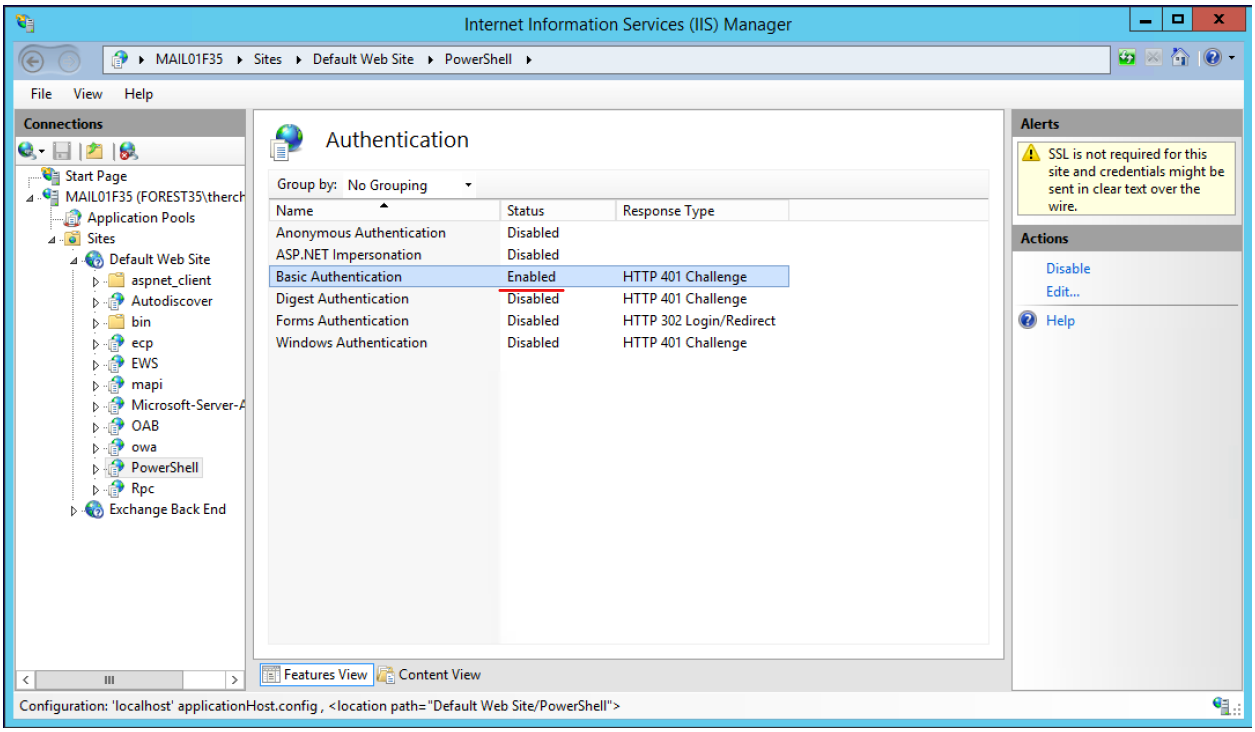
## 2.4 Enable WinRM for HTTPS

- Log in to the Exchange mail server.
- Open a command prompt as admin.
- Execute the following command: **winrm quickconfig -transport:https**.
- Open IIS on the Exchange mail server from the Control Panel (Control Panel > System and Security > Administrative Tools > Internet Information Services (IIS) Manager).

- Open Default Website > PowerShell.




- Double click authentication in the right pane.
- Enable basic authentication and save the setting.



## 2.5 TLS Server Certificates

The administrator is not required to generate and install TLS server certificates on the domain controller and Certificate Authority (CA) servers. When installing a new Certificate Authority, on a Windows Domain, and selecting the type Enterprise CA (not standalone CA), the process of configuring the Certificate authority will automatically generate certificates and assign to them to CA servers as well as the domain controllers.

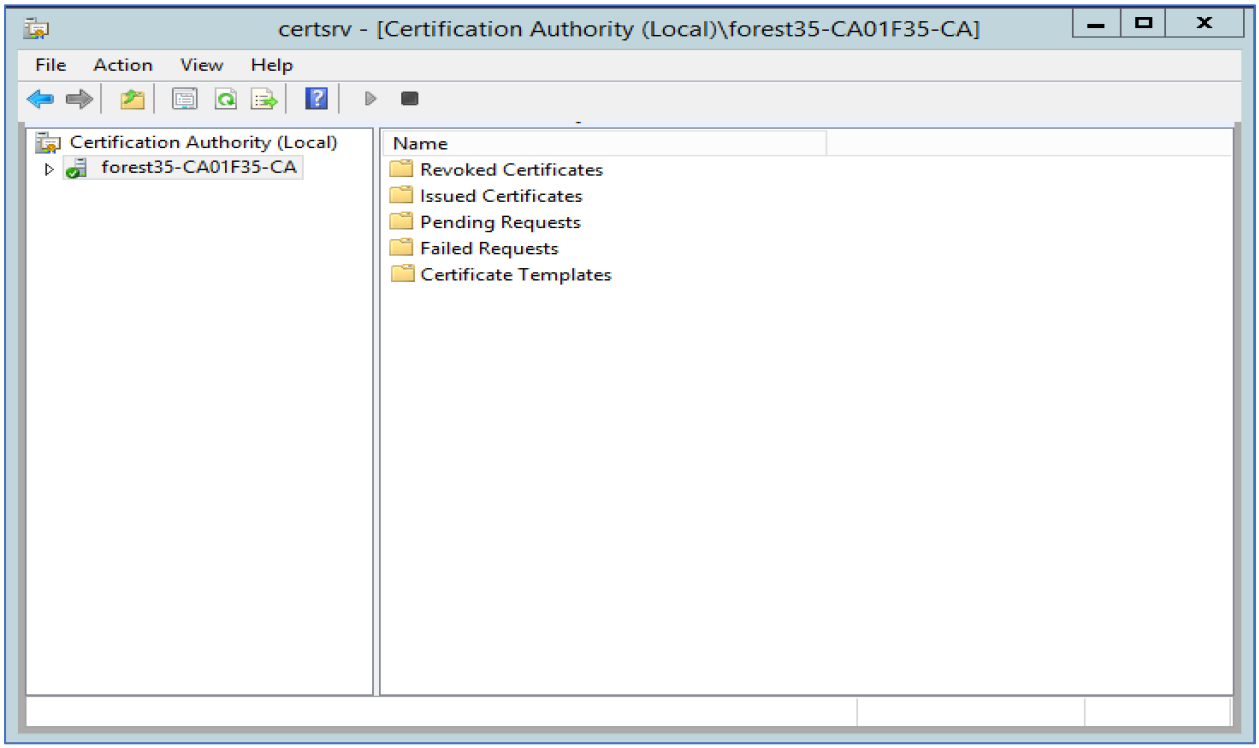
In the evaluated configuration, the Cloud Extender supports RSA certificates with key size of 2048 bits or greater, and signed with SHA-256 and SHA-384.

# 3 Certificate Revocation Support

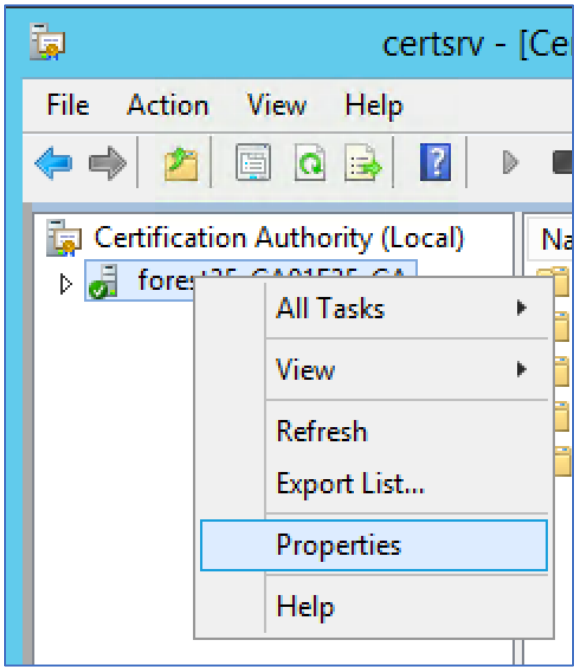
This section describes how to create certificates that support a Certificate Revocation List (CRL). When creating certificates used for HTTPS communications, they must contain a URL to a CRL so the Cloud Extender can verify the certificate has not been revoked. This is only for certificates used to communicate to on premise servers. For instance, Exchange Server or NDES server integration. The certificates must include a CRL URL. Cloud Extender will not connect to a server unless it can verify the certificate is not revoked.

Use the following steps to validate or create a HTTPS server certificate that contains a CRL URL.

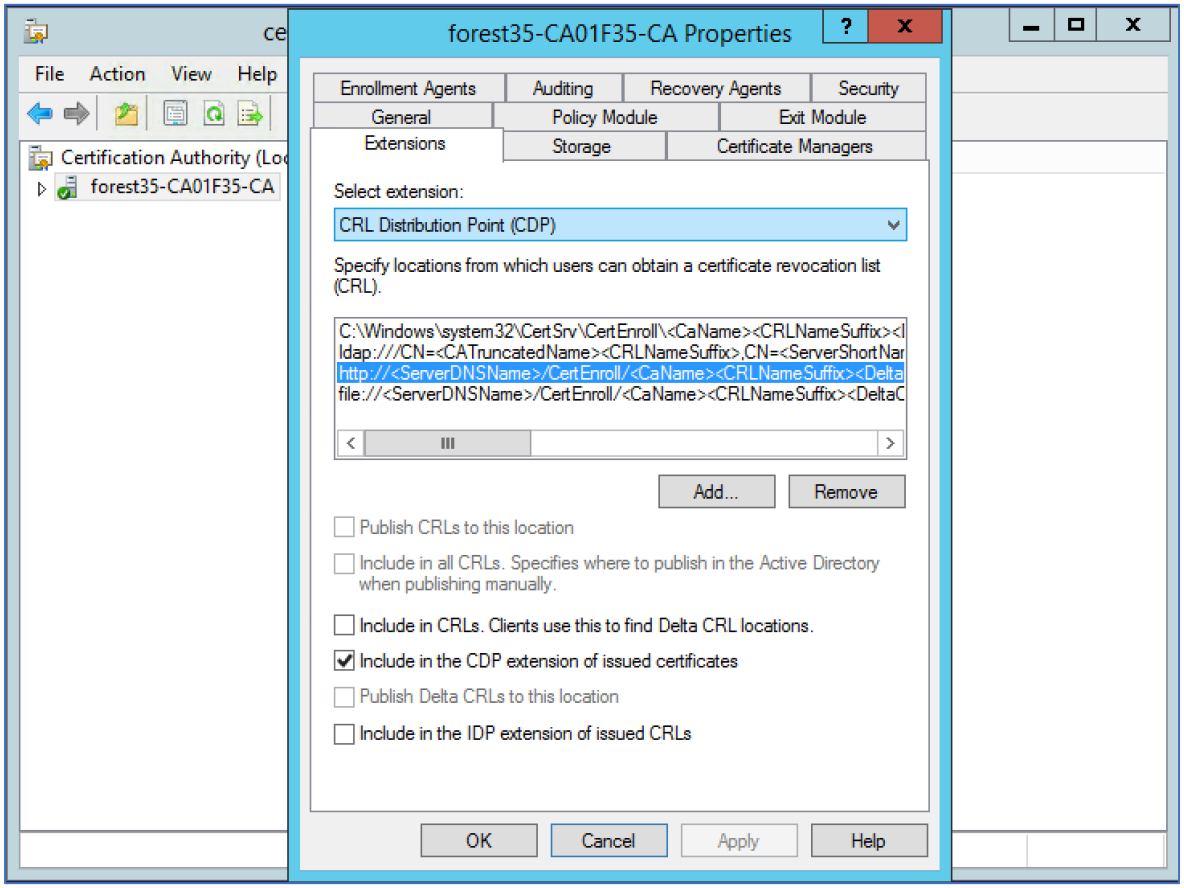
- Login, or RDP, into the CA server used for certificate management
- Start the Certification Authority application, (Administrative Tools > Certification Authority). For instance…



- Right click on the CA name and select properties




- Click on the Extensions tab.




- Select “CRL Distribution Point (CDP)” in the drop down.
- Find and select the proper HTTP entry in the list.
- Check “Include in the CDP extension of issued certificates”.
- Click OK/Apply to save this configuration.

# 4 Encrypt Cloud Extender Data

This section describes using Encrypted File System (EFS) to Protect Data at Rest.

When using EFS to encrypt your files only the account used to encrypt the files will be able to access the encrypted files. This means this account must be used to log in to the system to install, configure, and maintain the Cloud Extender. Other user accounts (even with administrative permissions) won't be able to access the encrypted files.

If the Cloud Extender needs to be uninstalled and later reinstalled, then **Step 3 and later** must be performed again. Any folders removed during the uninstall will not be re-encrypted during a reinstall.

## 4.1 Step 1: Create an Exchange Domain Admin Account

Create an Exchange domain admin account. This service account must be a local administrator on the Cloud Extender server. This account will be referred to as the **mdmservice** account for the remainder of this document. Add this user to the **Remote Desktop** group so it can RDP into the Cloud Extender server. See below for instructions on how to add the mdmservice to the Remote Desktop Group.

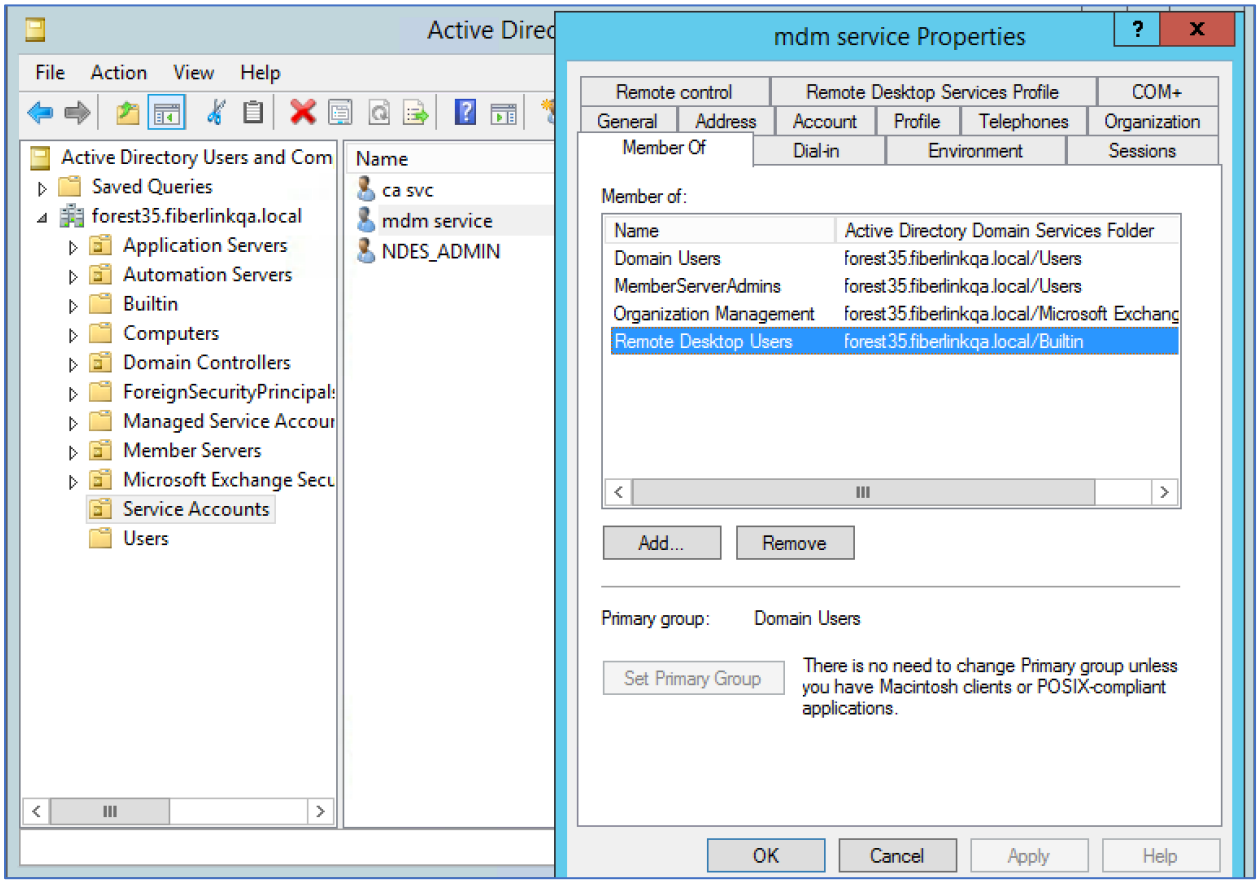
The **mdmservice** account is used to encrypt the **\ProgramData\MaaS360\ Cloud Extender** folder with EFS. Always RDP into the CE server as **mdmservice** to run the Config Tool, gather diagnostics, etc. Only **mdmservice** will be able to access the encrypted files after the following steps are completed.

### 4.1.1 Adding the Service Account to the Remote Desktop Group

To add an account, complete the following steps.

- Start the Control Panel and navigate to System and Security > Administrative Tools.
- Start "Active Directory Users and Computers".
- Navigate to the folder that contains the account. In the below example **mdmservice** is in Service Accounts. The Users folder is the other common place where the account may reside.
- Right click on the desired account and click on Properties.
- Navigate to the "Member Of" tab.
- Click on Add.
- In the "Enter the object names to select (examples): edit box type in "Remote Desktop Users" and click "Check Names".

- Click OK. See below for an example.

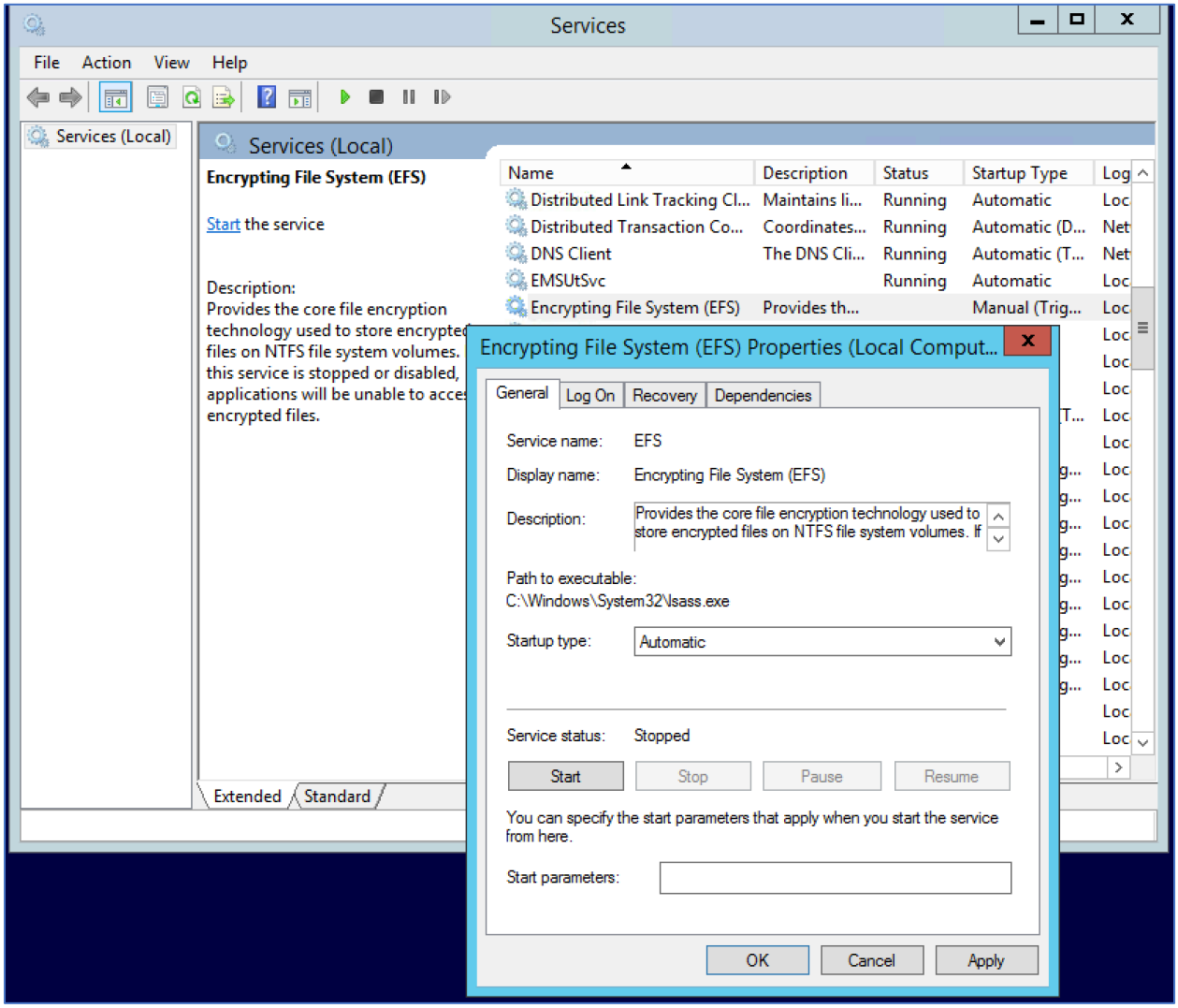



## 4.2 Step 2: Enable the EFS Service

To enable the EFS service, follow the instructions below:

- Type **Services** in the Start search box.
- In the new window that opens, find **Encrypting File System** in the list.
- Go to its **Properties** and click on **Start** and select the start-up type as **Automatic.** See below for an example.
- Save settings.

**Note:** You must be an administrator on the computer to perform this task. If you're not, then contact your system administrator.




## 4.3 Step 3: Install the Cloud Extender

Log in to the CE server as **mdmservice** and install the Cloud Extender. To obtain the NIAP certified Cloud Extender application, reach out to MaaS360 support team to gain access to https://ibm.box.com/s/5vrp23psd6hqn2lq4ypgmlrwst4axwko

Instructions on how to obtain the license key are documented in the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/concepts/ce_install_container.htm

Cloud Extender requires .NET framework version 4.6.1 or higher. Version 4.7.2 of the .NET framework is enabled by default on Windows Server 2019 Standard Version 1809. Users can check the version of .NET at the following link:

https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies#net-framework-472

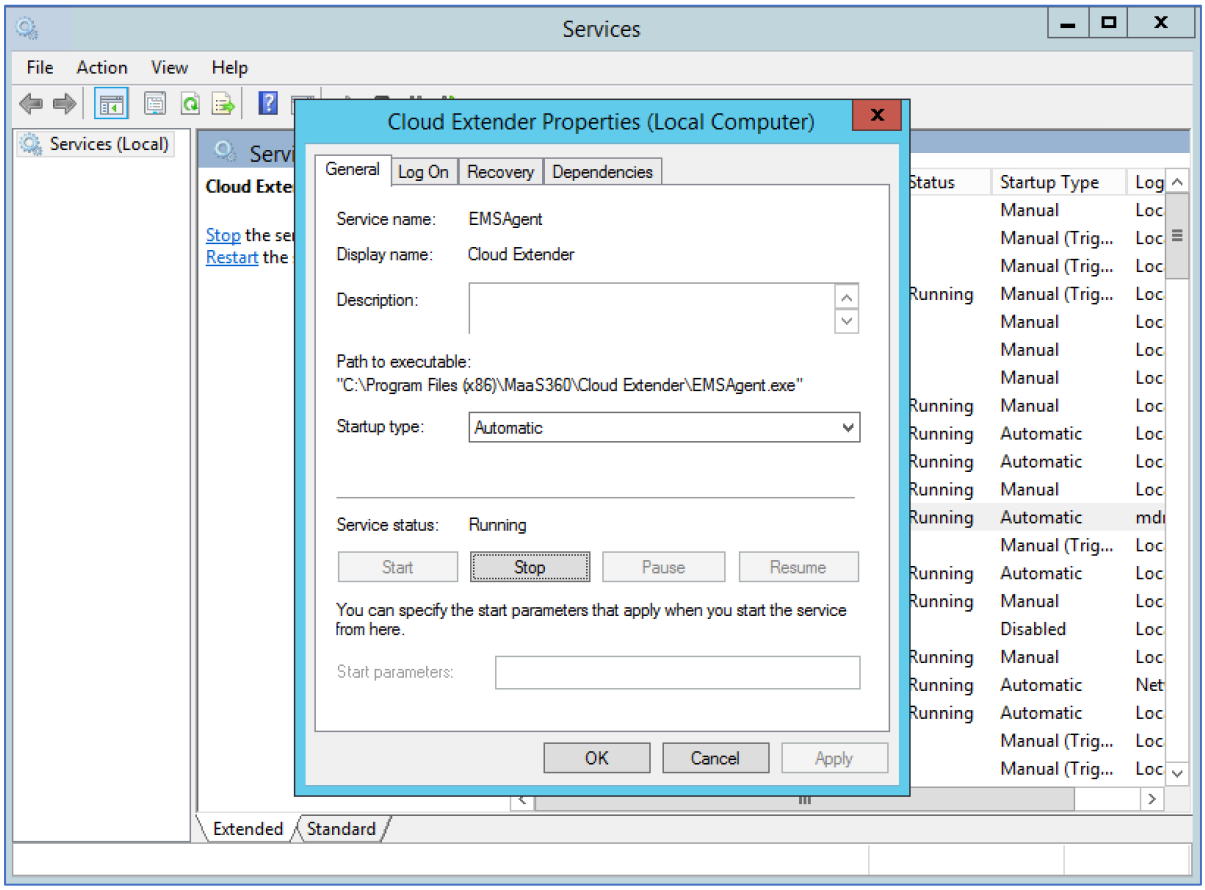
Users can determine the installed .NET version by checking that 461814 is present in the windows registry for the DWORD "Release" key found at:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET
Framework Setup\NDP\v4\Full\1033
```

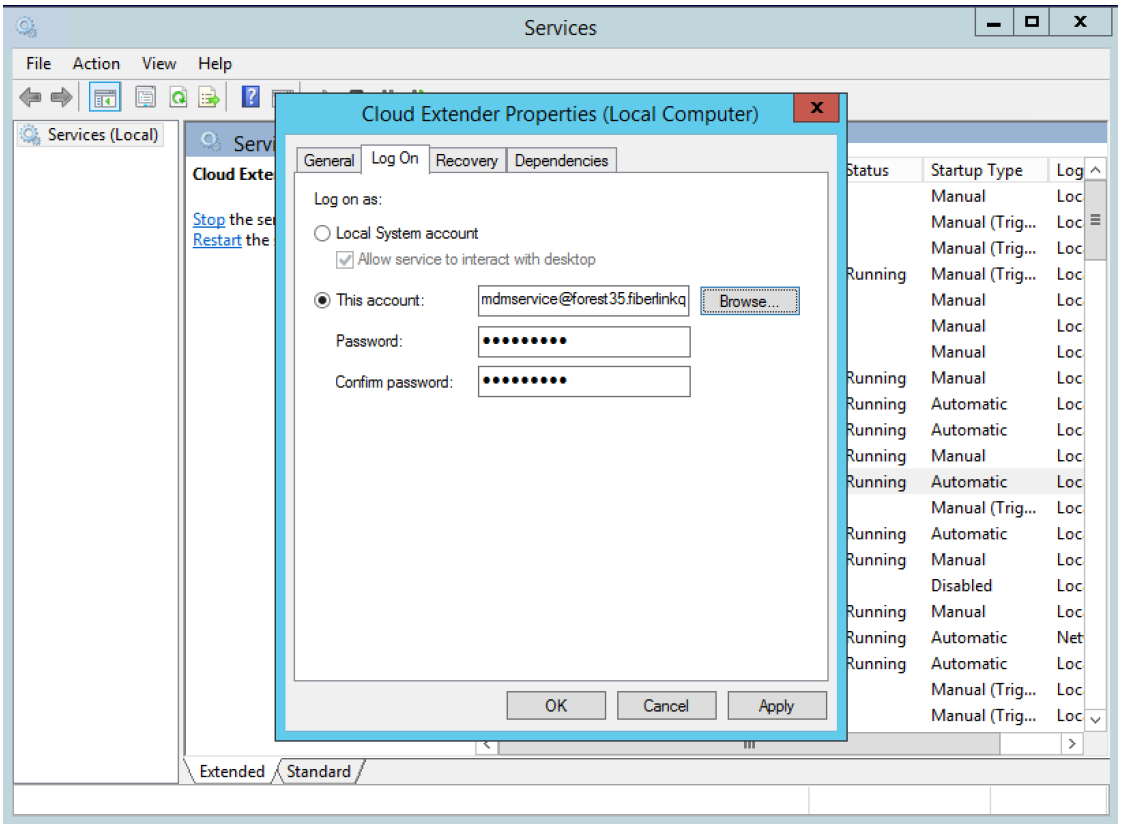
Download & extract CE_NIAP_Customer_Artifacts.zip from the box folder and install the Cloud Extender. Configuring the services will be done after the data folder is encrypted.

Configure the Cloud Extender services to run as the **mdmservice** account. Both the Cloud Extender (emsagent) and EMSUtSvc services must run as the **mdmservice** account. Complete the following steps.

- Bring up the service dialog from the Admin Tools dialog or type **Services** in the Start search box.
- Double click the **Cloud Extender** service from the list.
- The properties dialog is shown as follows.

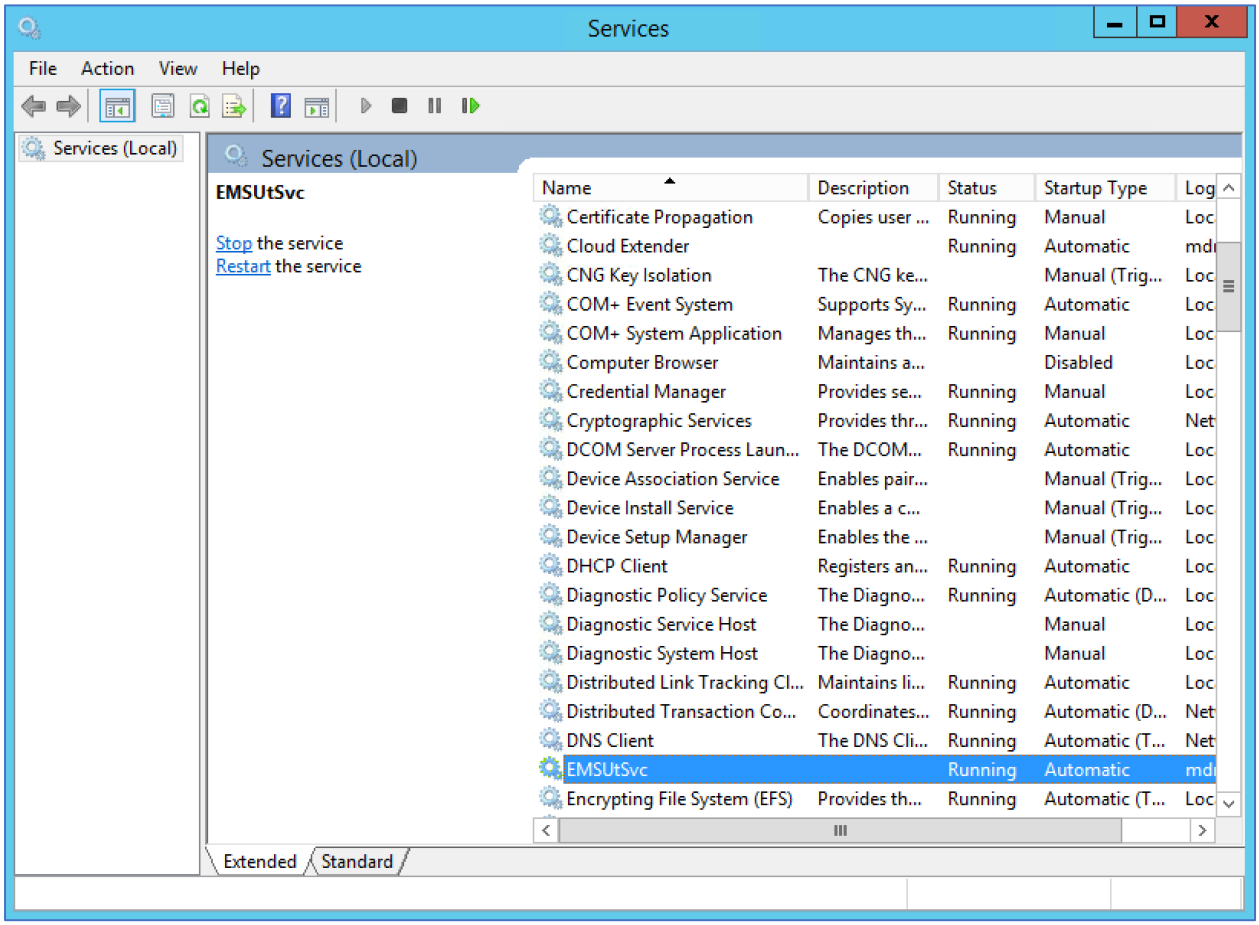


- Click on the **Log On** tab and enter the **mdmservice** credentials.




- Apply the changes, and then stop and start the service so it picks up the new credentials.

- Perform the same steps for the **EMSUtSvc** service.




## 4.4 Copying the modules

Before proceeding with the installation of the modules, wait 15 minutes after installing the Cloud Extender. This delay allows the Cloud Extender to check and install updates during the installation process, so once this step finishes, the proper modules that are part of the evaluated configuration can be copied in the following installation steps. Notice that automatic updates are disabled in the evaluated configuration, but this initial update is not affected by the **AutoUpgrade** registry entry added in section 2.2.

To copy the binaries to the Cloud extender installation path, follow the below steps.

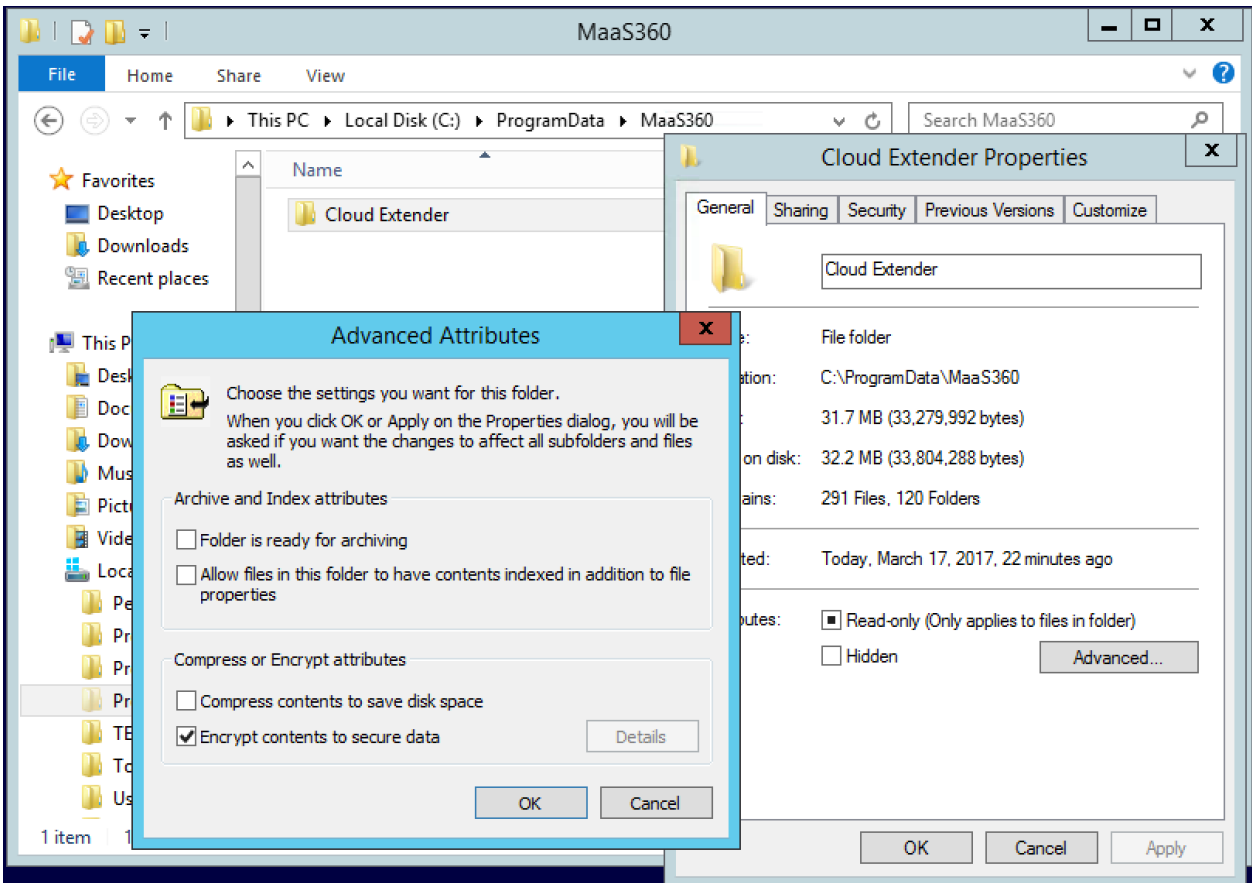
- Stop EMSUtSvc and EMSAgent service from Services
- Extract the zipped package from the box link and copy all the binaries under “Modules” folder to Cloud Extender installation directory “C:\Program Files (x86)\MaaS360\Cloud Extender\”.

- Start EMSUtSvc and EMSAgent service.

## 4.5 Step 4: Encrypt the Cloud Extender Data Folder

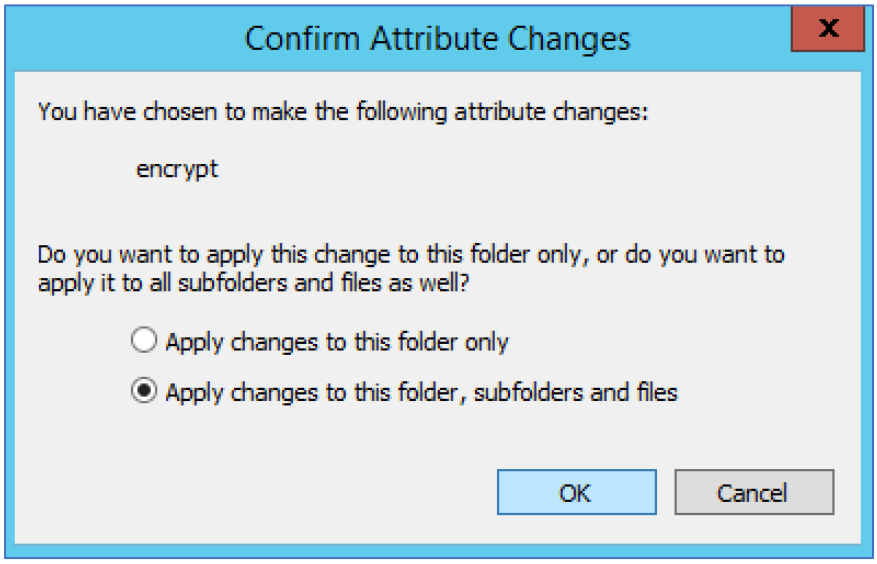
Complete the following steps to encrypt the Cloud Extender data.

- Using the **Services** dialog shown above, stop the **EMSUtSvc** and Cloud Extender (**emsagent**) services to close all files. Files cannot be in use during the encryption process.
- Bring up and navigate to: Control Panel > Folder Options > View tab.
- Under **Hidden files and folders** click **Show hidden files, folders, and drives**. Click **Apply** to allow File Manager to show hidden folders.
- Using File Manager, navigate to \ProgramData\MaaS360\Cloud Extender folder, right-click on it and go to **Properties.**
- On the **General** tab, click the **Advanced** button.
- Under **Compress or encrypt attributes**, check **Encrypt content to secure data**.




- Click **OK**.

- Select **Apply changes to this folder, subfolders, and files** and click **OK**.

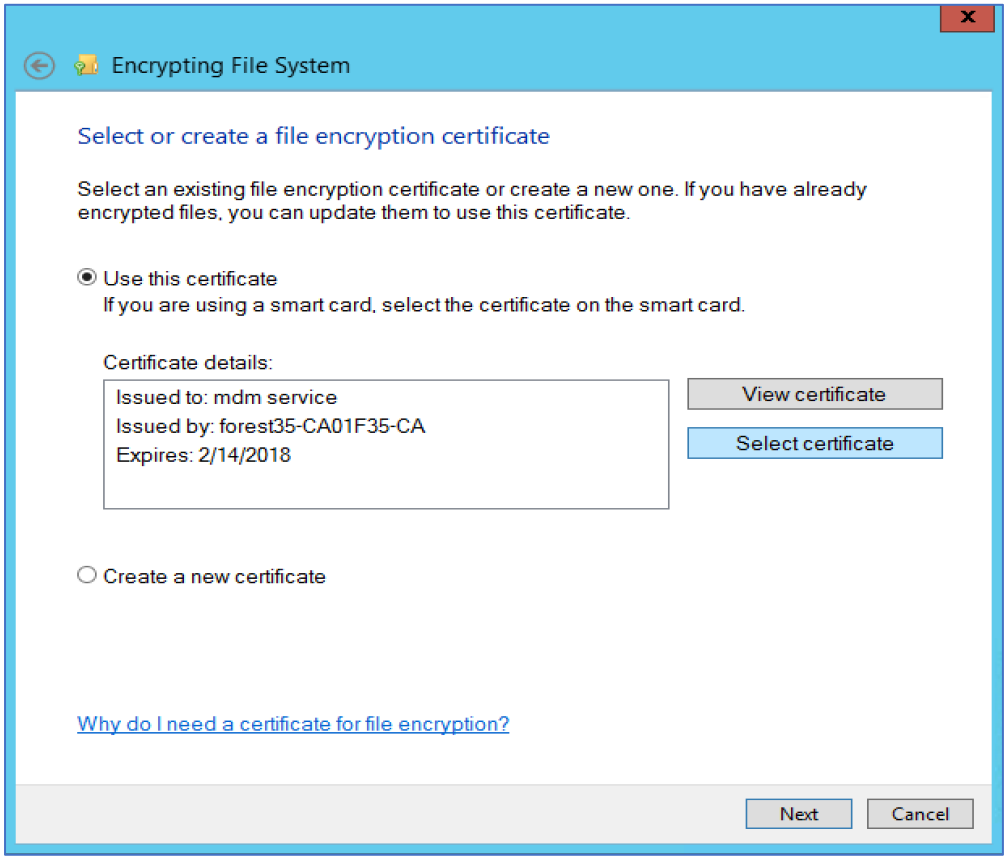


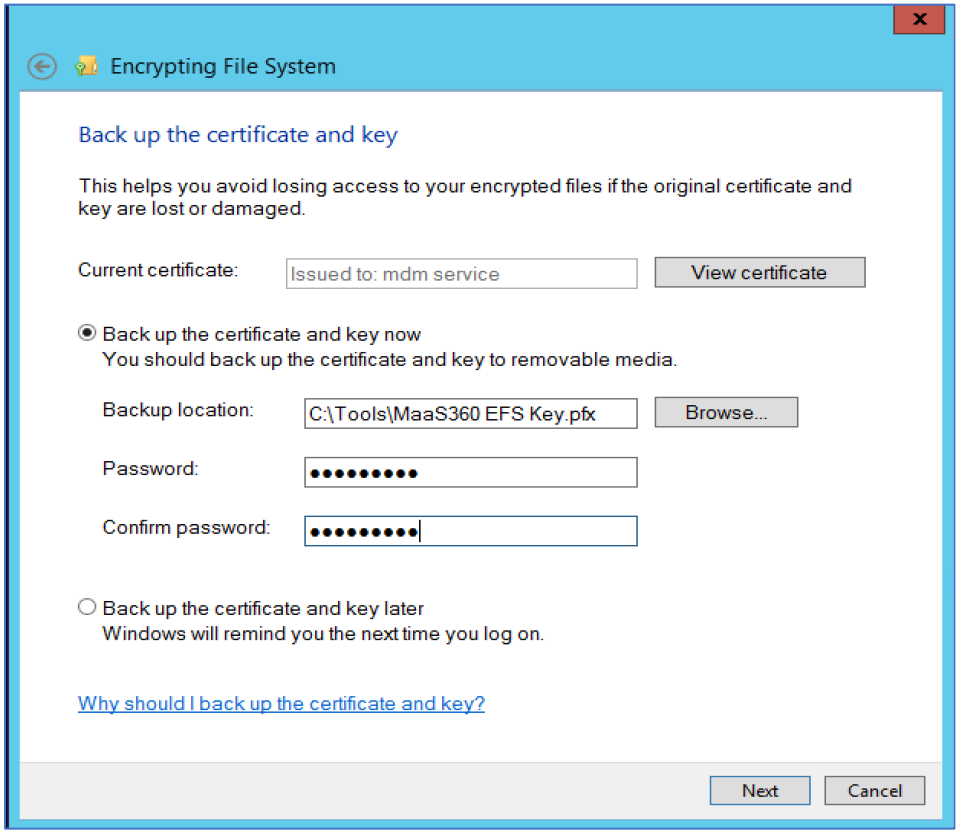

- Restart both services.

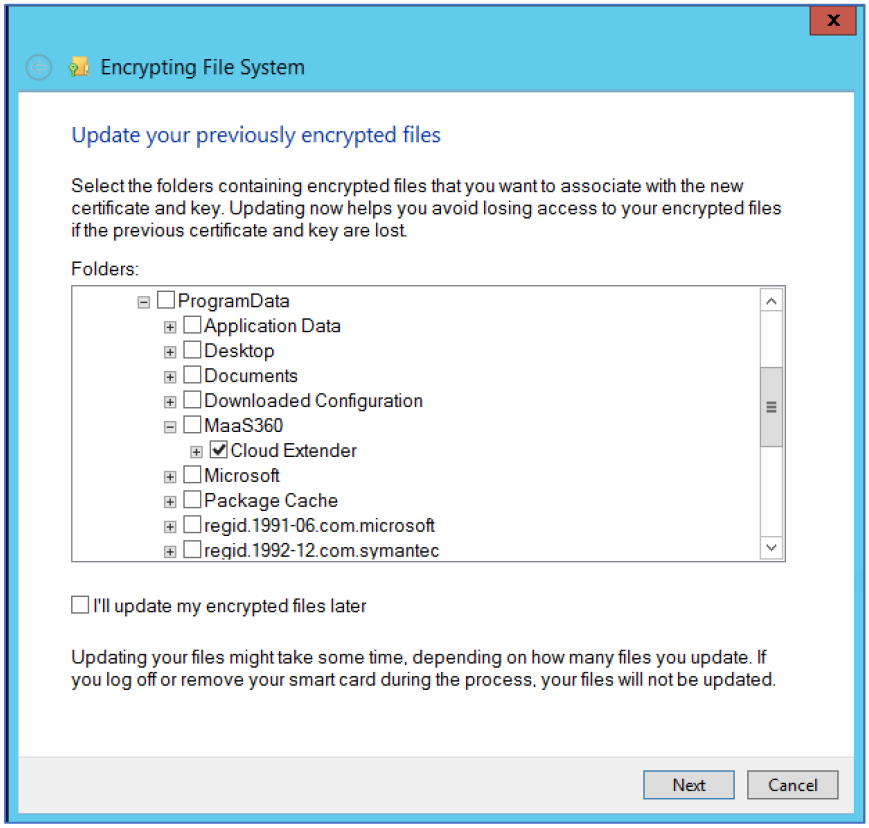
## 4.6 Step 5: Backup your Encryption Certificate with the Private Key

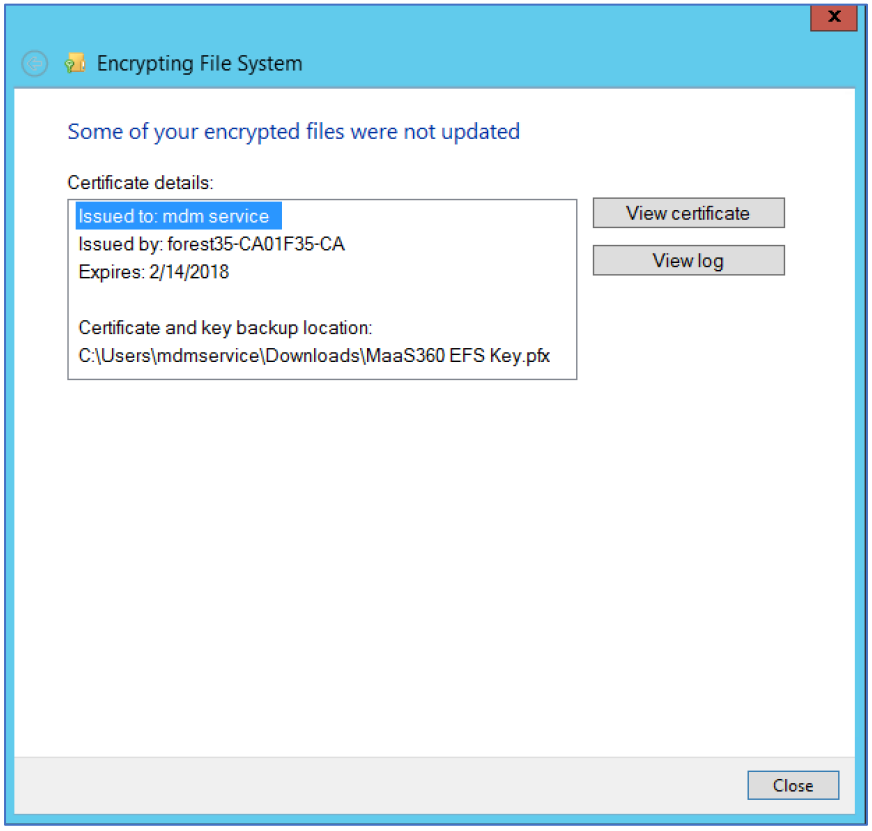
Since the data in the MaaS360 folder is encrypted with a certificate it is important to backup this certificate to an external device to keep it safe and separate. Use the **Manage File Encryption** wizard for this.

- Type **Encryption Certificates** in the search box from the Start menu to open **Manage** File Encryption wizard
- Follow the steps in this wizard. The mdm service certificate should be selected by default. Example screen shots are below.


Encrypting File System
Select or create a file encryption certificate
Select an existing file encryption certificate or create a new one. If you have already encrypted files, you can update them to use this certificate.
Use this certificate
If you are using a smart card, select the certificate on the smart card.
Certificate details:
Issued to: mdm service
Issued by: forest35-CA01F35-CA
Expires: 2/14/2018
View certificate
Select certificate
Create a new certificate
Why do I need a certificate for file encryption?
Next
Cancel


Encrypting File System
Back up the certificate and key
This helps you avoid losing access to your encrypted files if the original certificate and key are lost or damaged.
Current certificate:
Issued to: mdm service
View certificate
Back up the certificate and key now
You should back up the certificate and key to removable media.
Backup location:
C:\Tools\MaaS360 EFS Key.pfx
Browse...
Password:
Confirm password:
Back up the certificate and key later
Windows will remind you the next time you log on.
Why should I back up the certificate and key?
Next
Cancel

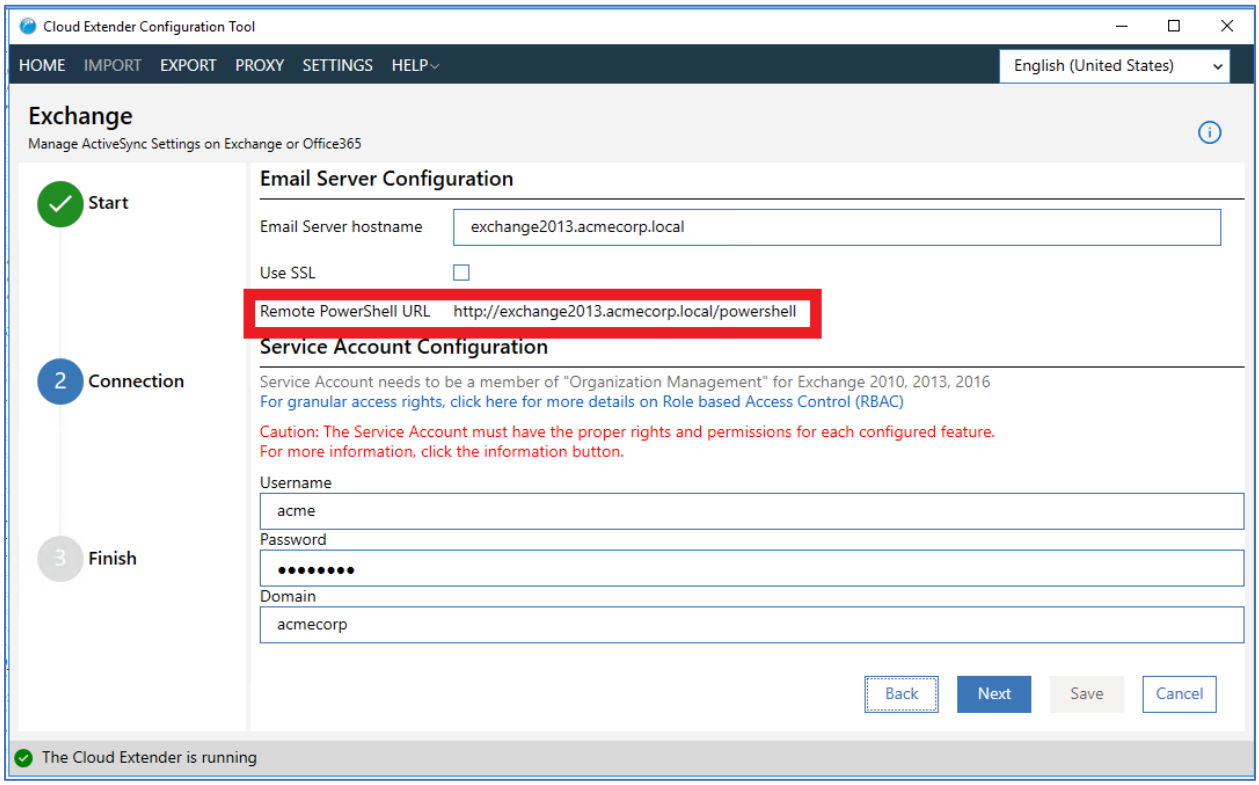

Encrypting File System
Update your previously encrypted files
Select the folders containing encrypted files that you want to associate with the new certificate and key. Updating now helps you avoid losing access to your encrypted files if the previous certificate and key are lost.
Folders:
ProgramData
Application Data
Desktop
Documents
Downloaded Configuration
MaaS360
Cloud Extender
Microsoft
Package Cache
regid.1991-06.com.microsoft
regid.1992-12.com.symantec
I'll update my encrypted files later
Updating your files might take some time, depending on how many files you update. If you log off or remove your smart card during the process, your files will not be updated.
Next
Cancel


Encrypting File System
Some of your encrypted files were not updated
Certificate details:
Issued to: mdm service
Issued by: forest35-CA01F35-CA
Expires: 2/14/2018
Certificate and key backup location:
C:\Users\mdmservice\Downloads\MaaS360 EFS Key.pfx
View certificate
View log
Close

# 5 Exchange URI and PKI Certificate Settings

## 5.1 Only use HTTPS in URIs

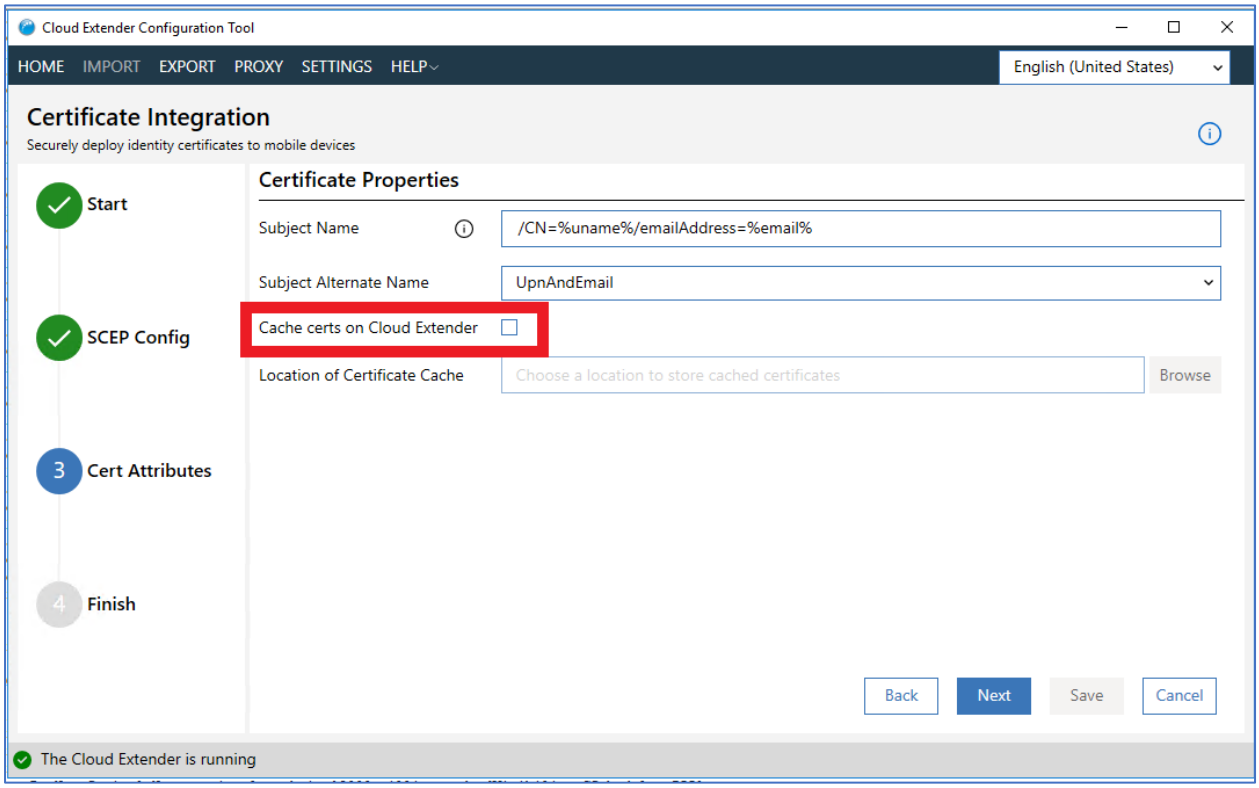
When configuring either Exchange ActiveSync or PKI Certificate templates (shown in the next section) the URL must have a HTTPS schema type in the URI. It is forbidden to use the FILE (file://) schema. Schemas other than HTTPS are not supported and could lead to a security vulnerability. There are cases where HTTP could be used instead of HTTPS, but this is forbidden in the evaluated configuration. HTTPS is mandatory and should always be used whenever there is a choice between HTTP and HTTPS.




## 5.2 Do Not Enable Certificate Caching

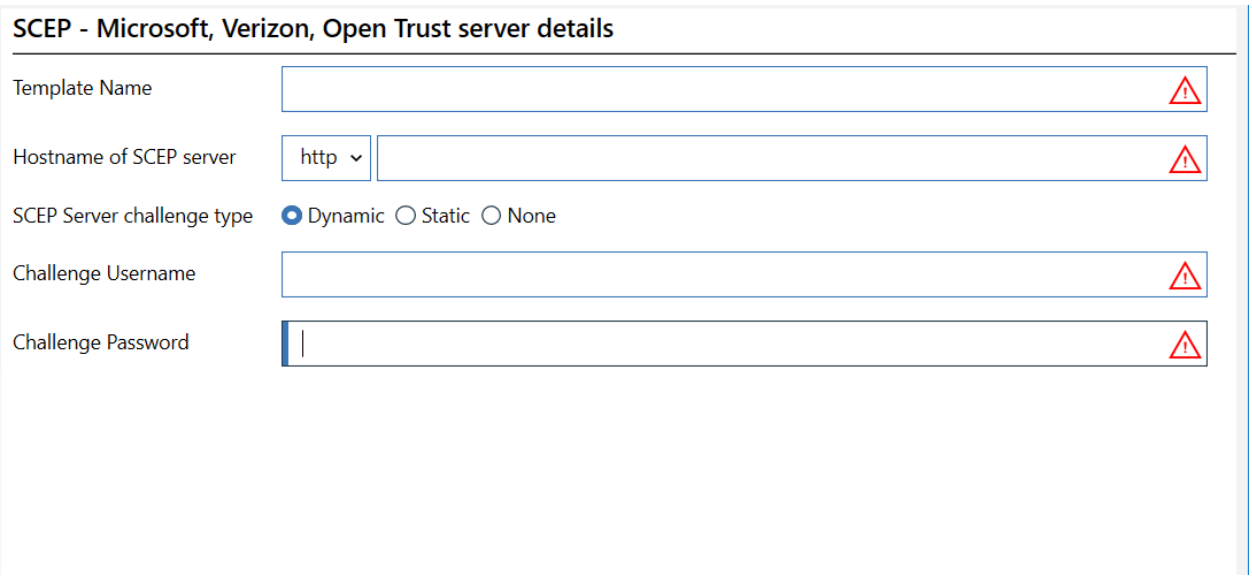
When creating a certificate template, to integrate to a Microsoft NDES server, it is important to have certificate caching disabled. Certificate caching must be disabled to adhere to the NIAP

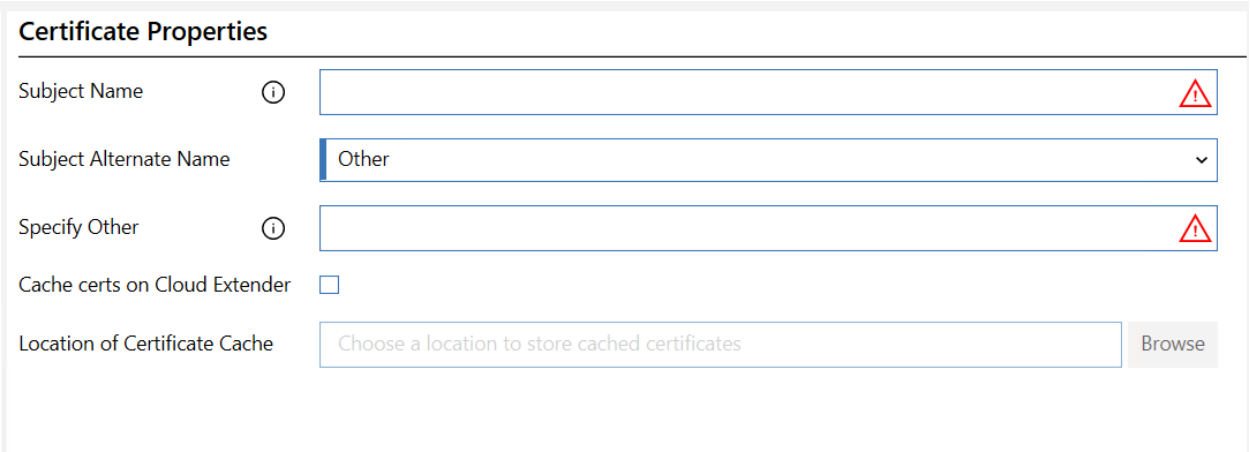
protection profile. By default, certificate caching is disabled. The screen below shows the option, in advanced mode, which must remain unchecked.




## 5.3 Microsoft NDES certificate template configuration

For creating a template, to integrate to a Microsoft NDES server, fields marked in red below are mandatory




Certificate Properties
Subject Name
Subject Alternate Name
Other
Specify Other
Cache certs on Cloud Extender
Location of Certificate Cache
Choose a location to store cached certificates
Browse

# 6 Cloud Extender supported OS, Updates, Versions and Use cases

## 6.1 Supported OS

Install the Cloud Extender on a physical or virtual machine with Windows Server 2019 by following the steps mentioned within this document.

## 6.2 How to Check for Updates

Checking for updates is performed using a command line tool called EMSAgentCLI.exe. This tool is located in the Cloud Extender program folder.

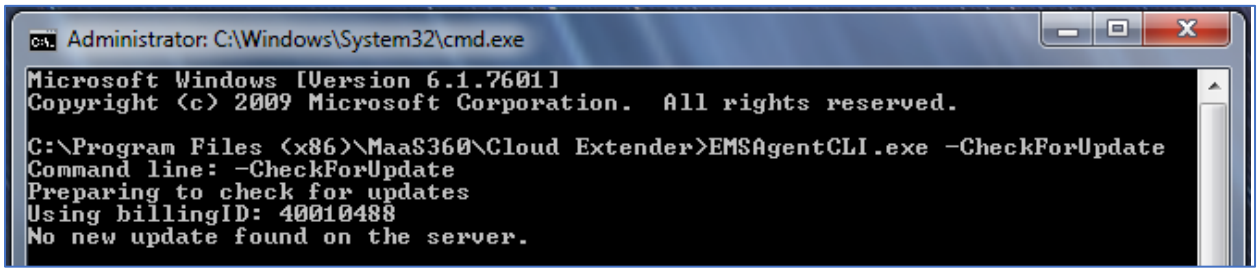
To run this command, open a command window and cd to where the Cloud extender is installed.

The default installation folder is: “C:\Program Files (x86)\MaaS360\Cloud Extender”.

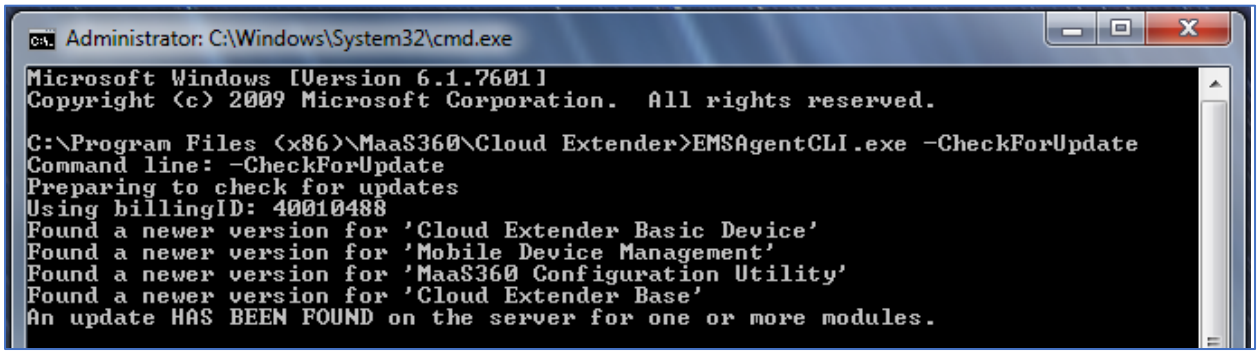
Type in the following command and hit enter.

```
EMSAgentCLI.exe -CheckForUpdate
```

If there are no available updates the following message is displayed.

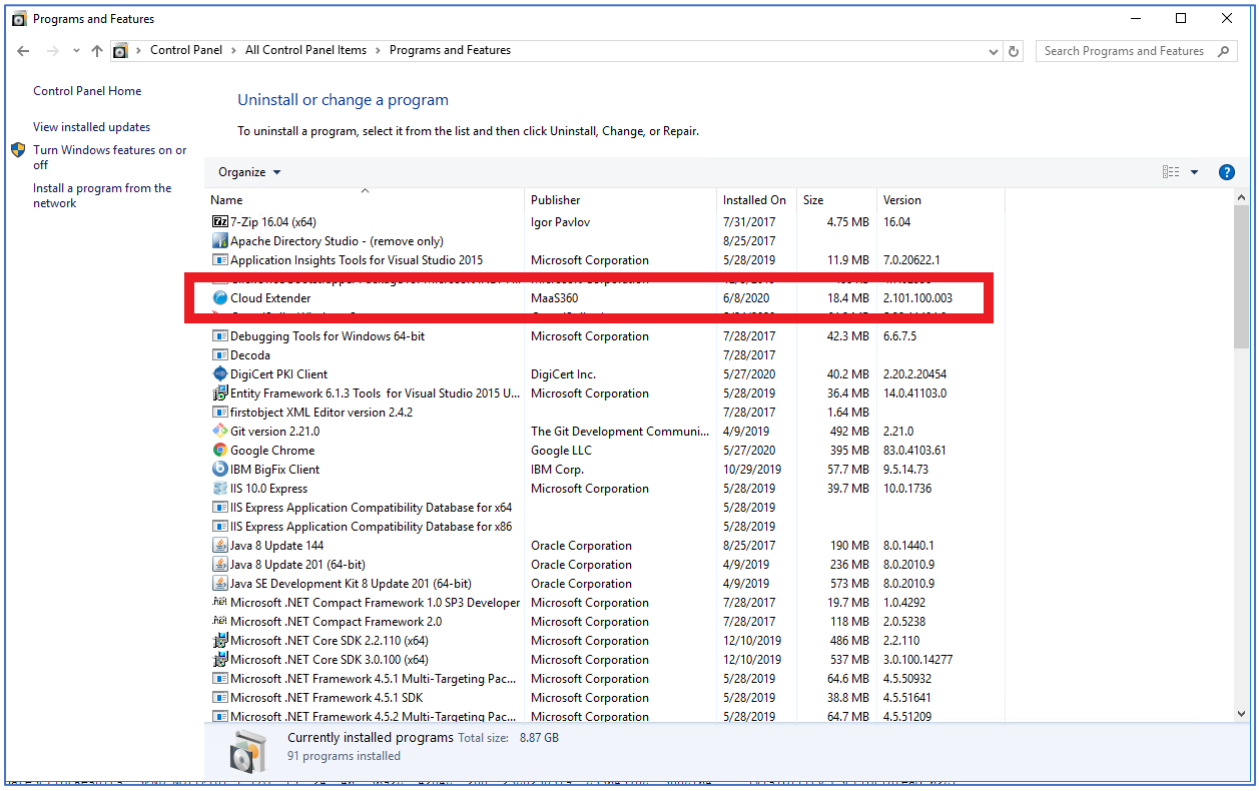



If there are available updates, then the following message is displayed.

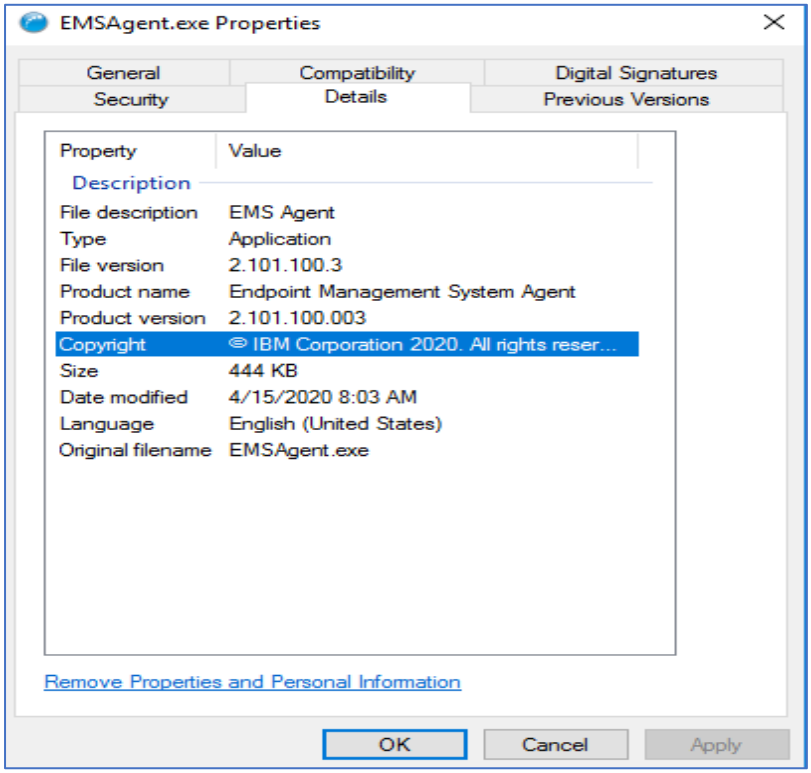


## 6.3 Cloud Extender Versioning

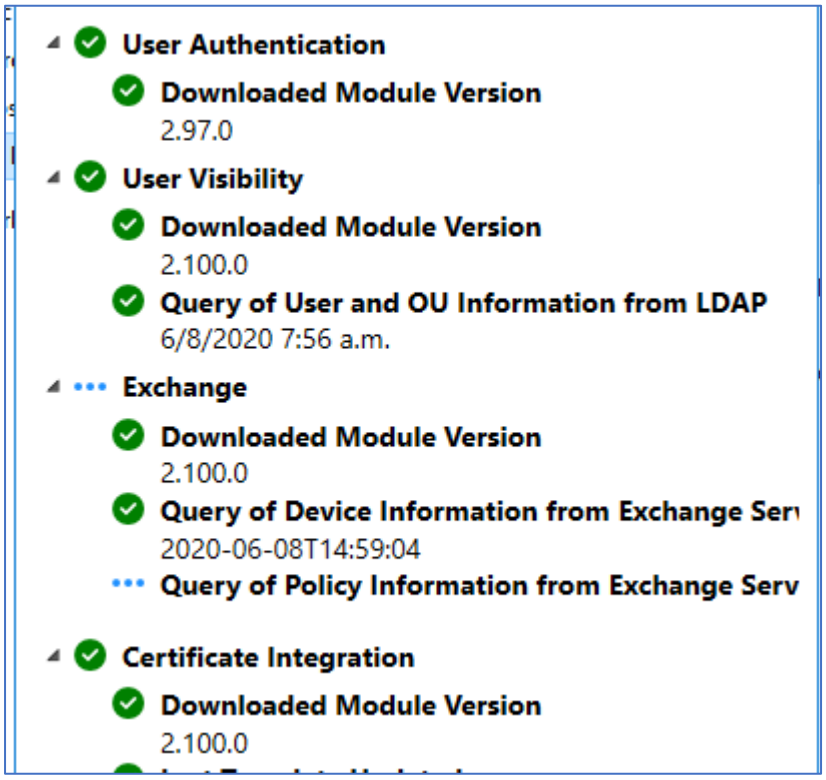
The Cloud Extender consists of an agent and a series of service modules. After the agent is installed the version of the agent is displayed on the Control Panel > Program and Features dialog as shown below.




The version can also be found by using the File Manager and navigating to the “C:\Program Files (x86)\MaaS360\Cloud Extender” folder. Right-click on the emsagent.exe file and select Properties. Select the Details tab as shown below to see the version.


EMSAgent.exe Properties
General
Compatibility
Digital Signatures
Security
Details
Previous Versions
Property
Value
Description
File description
EMS Agent
Type
Application
File version
2.101.100.3
Product name
Endpoint Management System Agent
Product version
2.101.100.003
Copyright
© IBM Corporation 2020. All rights reser...
Size
444 KB
Date modified
4/15/2020 8:03 AM
Language
English (United States)
Original filename
EMSAgent.exe
Remove Properties and Personal Information
OK
Cancel
Apply

The version of the modules is displayed in the Config Tool. Launch the Cloud Extender Configuration Tool and select “Next >” until you hit the screen below. Scroll down to see what modules are installed along with their versions.



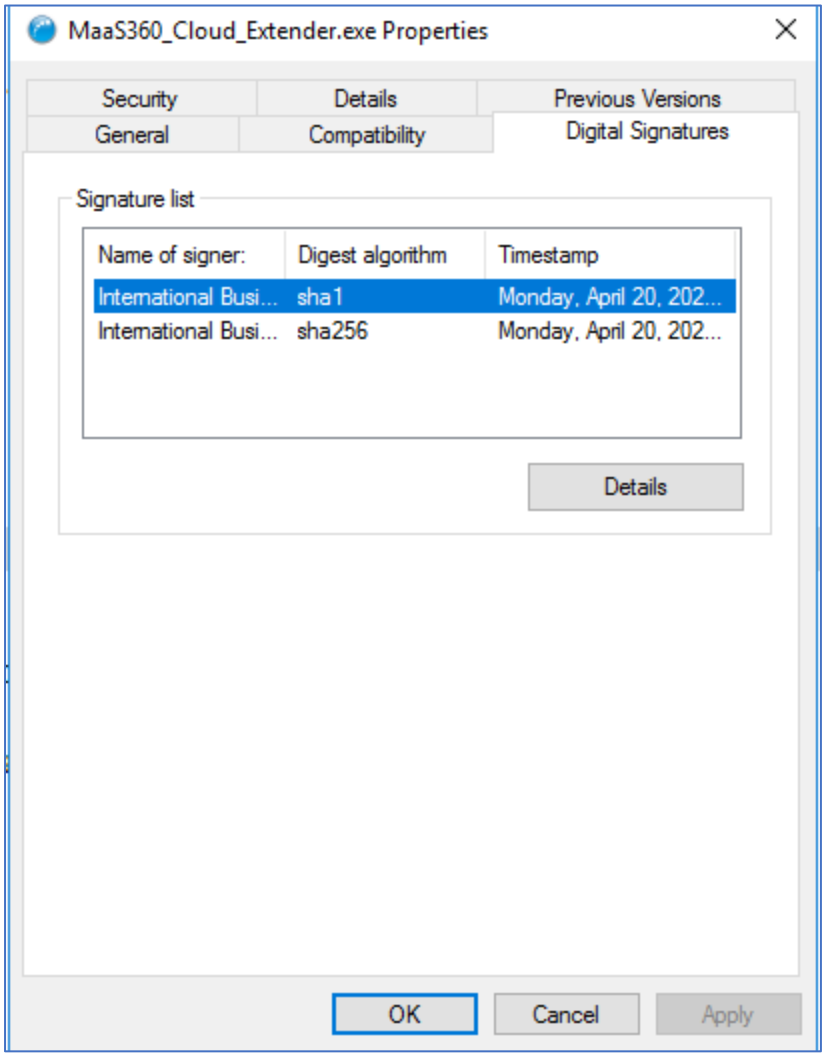

## 6.4 Cloud Extender Use cases

When the Cloud Extender software is installed, the Cloud Extender core connects to the MaaS360 Cloud to download the list of available services that are enabled in your MaaS360 Portal. By default, some modules are disabled in the MaaS360 Portal. You must enable below modules from Setup > Services in your MaaS360 Portal.

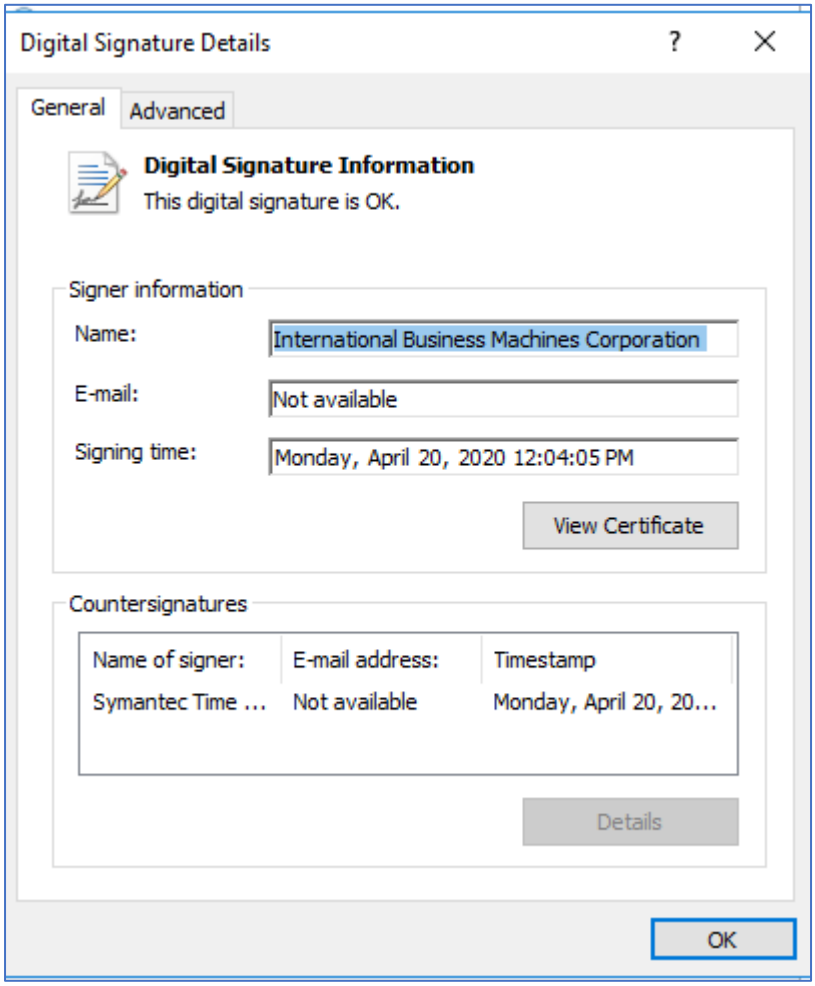
- Exchange and IBM® Traveller module
- Mobile Enterprise Gateway (MEG)
- MaaS360 VPN
- Email Notification

# 7 Verify Authenticity of the Install Package

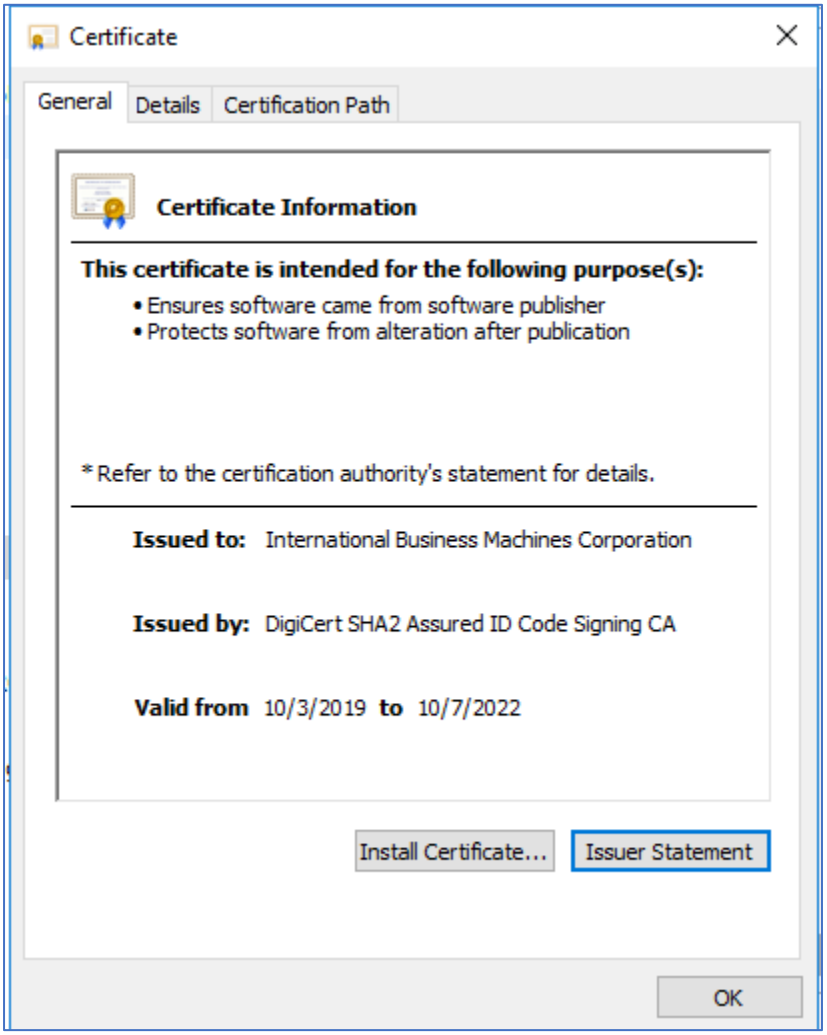
The Cloud Extender installation package is signed using a Symantec certificate issued to IBM. To view the Signing Certificate, used to sign the CE installer package, using File Manager right-click on the installer file (for instance, MaaS360_Cloud_Extender_2.102.000.???.exe) select Properties and choose the Digital Signatures tab. The following screen is displayed.




Select one of the signatures and click Details.




Click “View Certificate”.




You'll see that DigiCert, a trusted root authority, issued this code signing certificate to IBM.

# 8 Appendix A. Registry Settings to Make TLS 1.2 the System Default

## 8.1 A.1. Reg File to Enable TLS 1.2 and Disable TLS 1.1 and Lower

Copy the following lines into a file called Protocols.reg:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\Multi-Protocol Unified Hello]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\Multi-Protocol Unified Hello\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\Multi-Protocol Unified Hello\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\PCT 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\PCT 1.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\PCT 1.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 2.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 2.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 3.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 3.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\SSL 3.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.1\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.1\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.2]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.2\Server]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000
```

## 8.2 A.2. Reg File to Limit to Specific Ciphers

Copy the following lines into a file called CipherAvail.reg:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\
SSL\00010002]

@="NCRYPT_SCHANNEL_INTERFACE"

"Functions"=hex(7):54,00,4c,00,53,00,5f,00,45,00,43,00,44,00,48,00,45,00,5f,00,\

52,00,53,00,41,00,5f,00,57,00,49,00,54,00,48,00,5f,00,41,00,45,\

00,53,00,5f,00,31,00,32,00,38,00,5f,00,47,00,43,00,4d,00,5f,00,53,00,48,00,\

41,00,32,00,35,00,36,00,00,00,00,00
```

## 8.3 A.3. Reg File to Specify TLS Cipher Suites to Use for All TLS Connections

Copy the following lines into a file called CCCiphers.reg:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Fiberlink\V360]
"NIAP_SSL_Ciphers"="ECDHE-RSA-AES128-GCM-SHA256"
```

# 9 Appendix B. Cloud Extender Registry Settings for NIAP

## 9.1 B.1. Reg file to enable CE FIPS and NIAP modes and to turn off module updates

Copy the following lines into a file called NIAP=1_FIPS=3.reg:

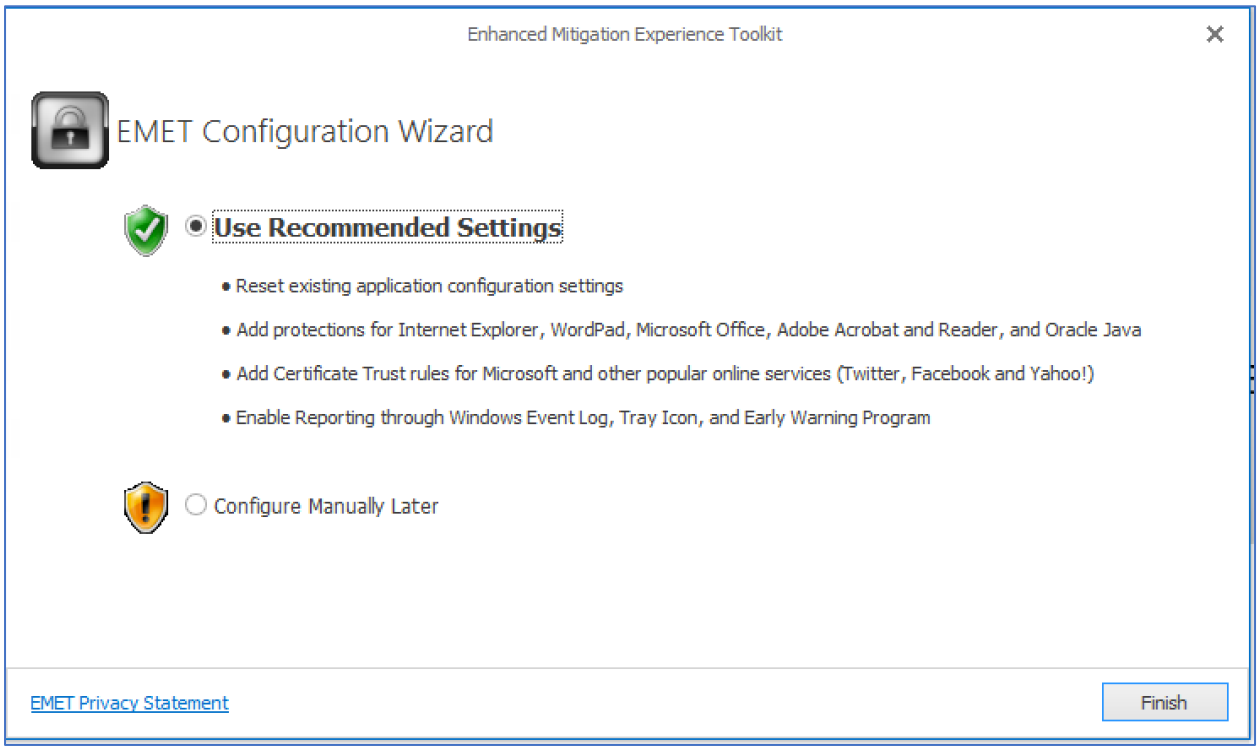
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360]
"NIAP"="1"
"AutoUpgrade"="N"
"FIPSComplianceMode"=dword:00000003
```

# 10 Appendix C. Configuring Cloud Extender with Microsoft's Enhanced Mitigation Experience Toolkit (EMET)

The latest version of EMET and the EMET User Guide can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=54264 and https://www.microsoft.com/en-us/download/details.aspx?id=54265

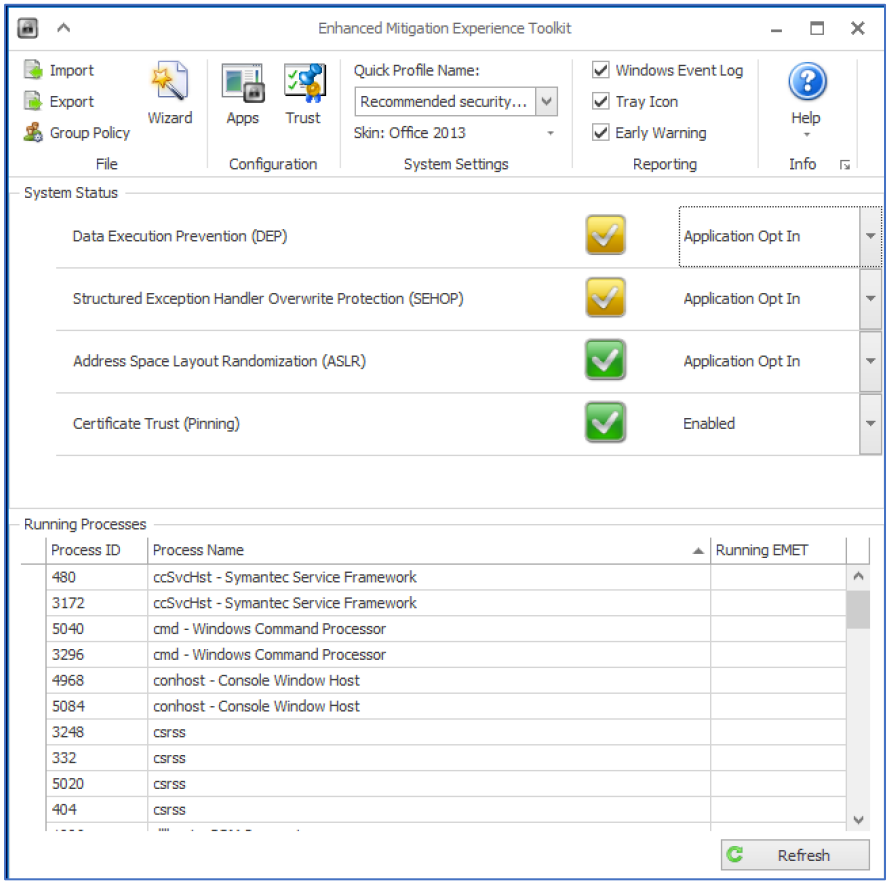
- Follow the steps on the above two links to download the EMET installer and user guide to the Cloud Extender server.
- Run the EMET Setup.msi to install the EMET 5.52 application.
- When prompted, select Use Recommended Settings.



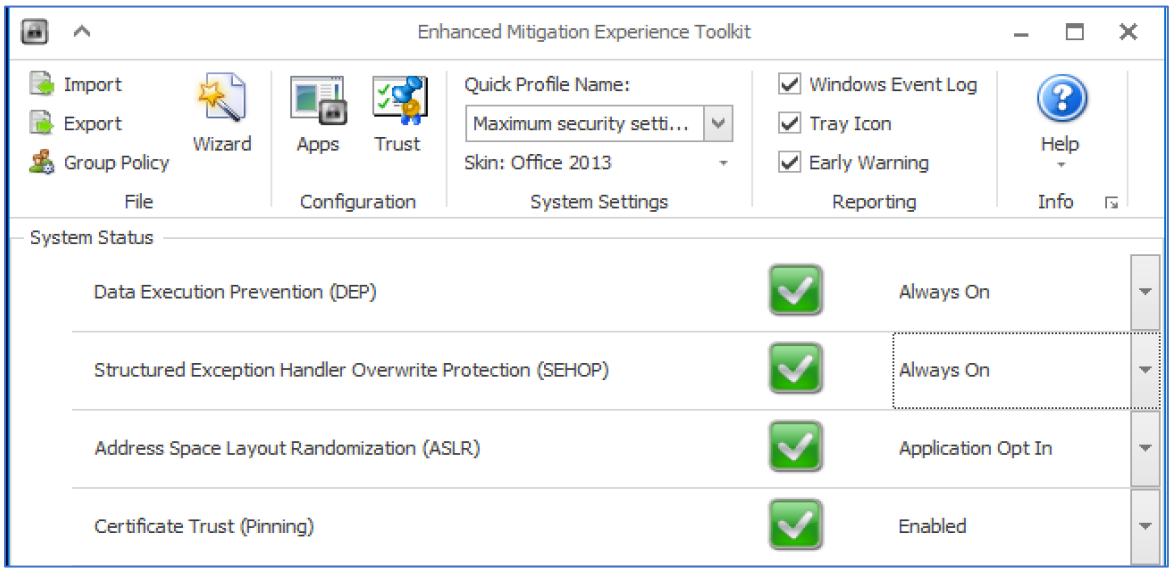

- Reboot the server after installing EMET.

Perform the steps below to set up EMET for the Cloud Extender.

- Start the EMET GUI application as shown below.

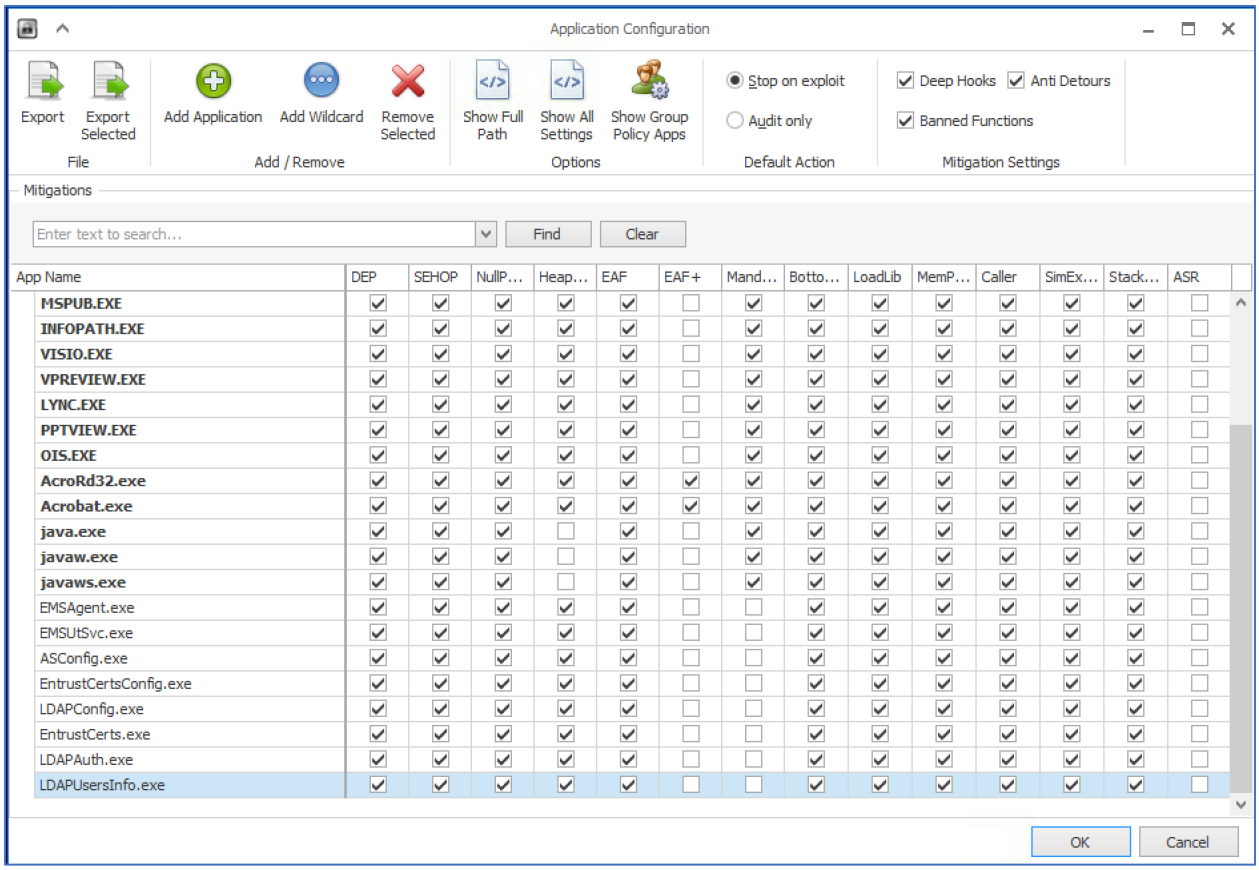



- Select the **Maximum security settings** profile to enable Data Execution Prevention (DEP) and Structured Exception Handler Overwrite Protection (SEHOP).




- Add the Cloud Extender apps by clicking the **Apps** icon and then the  Add Application icon

- Add the following applications from the C:\Program Files (x86)\MaaS360\Cloud Extender folder: EMSAgent.exe, EMSUtSvc.exe, ASconfig.exe, EntrustCerts.exe, EntrustCertsConfig.exe, LDAPAuth.exe, LDAPConfig.exe, LDAPUserInfo.exe
- After adding uncheck the "Mandatory Address Space Layout Randomization" column. Leaving this checked will keep the Cloud Extender from running.




- After selecting **OK**, the **EMSAgent** and **EMSUtSvc** services need to be restarted
- This may cause the **emsagent** process to use 100% CPU for extended periods of time