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	Ir	troduction	. 4
	1.1	Intended Audience	4
	1.2	Evaluated Versions	4
	1.3	Cryptographic Acknowledgment	5
	1.4	Security Objectives and Assumptions	5
	1	4 1 Platform	5
	1	4.2 Proper User	5
	1	4.3 Proper Oser	5
	1		
	1.5	Managing Updates and Known Vulnerabilities	5
	1.6	TOE Security Functionality	6
	1	6.1 Cryptographic Support	6
	1	6.2 User Data Protection	6
	1	6.3 Identification and Authentication	7
	1	6.4 Security Management	7
	1	6.5 Privacy	7
	1	6.6 Protection of the TSF	7
	1	6.7 Trusted Path/Channels	7
	1.7	Excluded Functionality	7
	_		
2	Р	otect Cloud Extender Communications When Using HTTPS	. 9
2	Р 2.1	rotect Cloud Extender Communications When Using HTTPS Make TLS 1.2 the System Default on Windows Server 2019	. 9 9
2	Р 2.1 2.2	rotect Cloud Extender Communications When Using HTTPS Make TLS 1.2 the System Default on Windows Server 2019 Enable FIPS and NIAP Modes and disable module updates	. 9 9 11
2	Р 2.1 2.2 2.3	rotect Cloud Extender Communications When Using HTTPS Make TLS 1.2 the System Default on Windows Server 2019 Enable FIPS and NIAP Modes and disable module updates Exchange Server Certificate	. 9 9 11 12
2	P 2.1 2.2 2.3 2.4	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS	. 9 9 11 12 19
2	P 2.1 2.2 2.3 2.4 2.5	Potect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates	• 9 9 11 12 19 21
2	P 2.1 2.2 2.3 2.4 2.5 C	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates	. 9 9 11 12 19 21 22
3	P 2.1 2.2 2.3 2.4 2.5 C E	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates ertificate Revocation Support	 .9 9 11 12 19 21 22 25
2 3 4	P 2.1 2.2 2.3 2.4 2.5 C E	Protect Cloud Extender Communications When Using HTTPS	. 9 9 11 12 19 21 22 22 25
2 3 4	P 2.1 2.2 2.3 2.4 2.5 C E 4.1	rotect Cloud Extender Communications When Using HTTPS	. 9 9 11 12 19 21 22 25 25
2 3 4	P 2.1 2.2 2.3 2.4 2.5 C E 4.1 4	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates ertificate Revocation Support Step 1: Create an Exchange Domain Admin Account 1.1 Adding the Service Account to the Remote Desktop Group	. 9 9 11 12 19 21 22 25 25 25
3	P 2.1 2.2 2.3 2.4 2.5 C E 4.1 4 4.2	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate . Enable WinRM for HTTPS. TLS Server Certificates . ertificate Revocation Support https://doi.org/11.00000000000000000000000000000000000	 .9 9 11 12 19 21 22 25 25 25 26
3	P 2.1 2.2 2.3 2.4 2.5 C E 4.1 4 4.2 4.3	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates ertificate Revocation Support Step 1: Create an Exchange Domain Admin Account	 .9 9 11 12 19 21 22 25 25 25 26 27
3	P 2.1 2.2 2.3 2.4 2.5 C E 4.1 4 4.2 4.3 4.4	rotect Cloud Extender Communications When Using HTTPS. Make TLS 1.2 the System Default on Windows Server 2019. Enable FIPS and NIAP Modes and disable module updates. Exchange Server Certificate Enable WinRM for HTTPS. TLS Server Certificates ertificate Revocation Support. https://www.communications.com/ Step 1: Create an Exchange Domain Admin Account 1.1 Adding the Service Account to the Remote Desktop Group Step 2: Enable the EFS Service Step 3: Install the Cloud Extender	. 9 9 11 12 19 21 22 25 25 25 26 27 30
3	P 2.1 2.2 2.3 2.4 2.5 C E 4.1 4 4.2 4.3 4.4 4.5	rotect Cloud Extender Communications When Using HTTPS	.9 9 11 12 19 21 22 25 25 25 25 26 27 30 31

5	Ex	change URI and PKI Certificate Settings
	5.1	Only use HTTPS in URIs
	5.2	Do Not Enable Certificate Caching35
	5.3	Microsoft NDES certificate template configuration
6	Cle	oud Extender supported OS, Updates, Versions and Use cases
	6.1	Supported OS
	6.2	How to Check for Updates
	6.3	Cloud Extender Versioning
	6.4	Cloud Extender Use cases
7	Ve	rify Authenticity of the Install Package42
8	Ap	pendix A. Registry Settings to Make TLS 1.2 the System Default45
	8.1	A.1. Reg File to Enable TLS 1.2 and Disable TLS 1.1 and Lower45
	8.2	A.2. Reg File to Limit to Specific Ciphers
	8.3	A.3. Reg File to Specify TLS Cipher Suites to Use for All TLS Connections
9	8.3 Ap	A.3. Reg File to Specify TLS Cipher Suites to Use for All TLS Connections
9	8.3 Ar 9.1	A.3. Reg File to Specify TLS Cipher Suites to Use for All TLS Connections

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 (<u>https://m1.maas360.com/tryMDM/SK_MDM_C</u>) 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\Configura tion\Local\SSL\00010002. Only the following cipher is enabled:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

📸 Registry Editor — 🗆 🗙							
File Edit View Favorites Help							
BGFX ^	Name	Туре	Data				
BitlockerStatus	(Default)	REG_SZ	NCRYPT_SCHANNEL_INTERFACE				
	ab EccCurves	REG_MULTI_SZ	curve25519 NistP256 NistP384				
Class	ab Functions	REG_MULTI_SZ	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256				
CoDeviceInstallers							
COM Name Arbiter							
> . CommonGlobUserSettings							
> . Compatibility							
> - ComputerName							
> ContentIndex							
> CrashControl							
Cryptography							
y local							
> - Default							
SSL							
ECCParameters							
> Ngc							
> Providers							
DeviceContainers							
DeviceGuard							
S DevOuerv Y							
< >							
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002							

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:



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.

🛚 Registry Editor							
File Edit View Favorites Help	ile Edit View Favorites Help						
File Edit View Favorites Help P HARDWARE P P SAM SECURITY SOFTWARE P 7-Zip P Classes P Classes P OBEC Policies Software P OBEC Software Software P Classes Software Software P OBC Software Software Software P Clients Software Software Software P Software Software Software Software P Software Software Software Software P Software Software Software <td>Name</td> <td>Type REG_SZ REG_SZ REG_DWORD REG_SZ</td> <td>Data (value not set) N 0x00000003 (3) 1</td> <td></td>	Name	Type REG_SZ REG_SZ REG_DWORD REG_SZ	Data (value not set) N 0x00000003 (3) 1				
Loniputer\nkt1_LoCAt_iviAcInive\soft i viAkte\viowvid2lvode\riberink\visov							

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

← 🕘 🔩 https://localhost/ecp/		🔎 👻 😵 Certificate error 🖒 🔙 o	ertificates - Microsoft Exch ×	
Enterprise Office 365				mdm service 🔻 ? 🕇
Exchange admin cer	iter			
recipients	servers databases database av	ailability groups virtual directorie	es certificates	
permissions				
compliance management	Select server: mail01f35.forest35.fiberlinkqa.l	ocal 🗸		
organization	+∥亩ೞ…			
protection	NAME	STATUS	EXPIRES ON	A
mail flow	Microsoft Exchange Server Auth Certificate Microsoft Exchange	Valid Valid	1/14/2022 2/9/2022	Microsoft Exchange Server Auth Certificate
mobile	WMSVC	Valid	2/7/2027	Self-signed certificate Issuer: CN=Microsoft Exchange Server Auth Certificate
public folders				Status
unified messaging				Valid Expires on: 1/14/2022
servers				Renew
hybrid				Assigned to services
tools				
	Would you like to store your password for loca	Ihost? More info		Yes Not for this site ×
= 占 🛛 🚞) 🛍 🏈			▲ 📴 😳 😘 1:46 PM 2/23/2017

- 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.

Exchange Certifica	te - Internet Explorer		_ _ X
new Exchange certificate			Help
Specify the domains you want to be included in your certificate	. Learn more		
ACCESS A	DOMAIN		
Exchange ActiveSync (when accessed from the Internet)	f35.far360.com	~	
Exchange ActiveSync (when accessed from the intranet)	mail01f35.forest35.fib		
Autodiscover (when accessed from the Internet)	AutoDiscover.f35.far3		
Autodiscover (when accessed from the intranet)	mail01f35.forest35.fib		
POP	mail01f35		
IMAP	mail01f35		
Outlook Anywhere	<not specified=""></not>	×	
	back	next	cancel
			🔍 100% 🛛 👻

• 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.

Exchange Certificate - Internet Explorer	_ _ ×
new Exchange certificate	Help
Based on your selections, the following domains will be included in your certificate. You can add additional domains here, or make changes. Learn more	
DOMAIN	
f35.far360.com	
mail01f35.forest35.fiberlinkqa.local	
AutoDiscover.f35.far360.com	
mail01f35	
forest35.fiberlinkqa.local	
back	next cancel
	🔍 100% 🔻 🔡

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

Exchange Certificate - Internet Exchange	xplorer – – ×
new Exchange certificate	Help
Specify information about your organization. This is required by the certification Learn more	authority.
*Organization name:	
IBM	
*Department name:	
DEVQA	
*City/Locality:	
Blue Bell	
*State/Province:	
PA	
*Country/Region name:	
United States	~
back	next cancel
	🕄 100% 👻 📑

- 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.**

C 🗇 🧭 http://10.2.21.46/certsrv/en-us/	5 - Q	🥖 Microsoft Active Directory ×	👒 certificates - Microsoft Exchange	L= □ × A ★ Ø
Microsoft Active Directory Certificate Services forest35-CA01F35-CA				Home
Welcome				
Use this Web site to request a certificate for your Web browser, e-mail client, or other pro encrypt messages, and, depending upon the type of certificate you request, perform othe	gram. By us er security ta:	sing a certificate, you can ver sks.	rify your identity to people you	u communicate with over the Web, sign and
You can also use this Web site to download a certificate authority (CA) certificate, certific	ate chain, or	r certificate revocation list (C	RL), or to view the status of a	pending request.
For more information about Active Directory Certificate Services, see Active Directory Ce	rtificate Serv	vices Documentation.		
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>				

• Click advanced certificate request.

P ▼ C 🥖 Microsoft Active Directory × 😼 certificates - Microsoft Exchange	□ <mark>▲</mark> ħ ★ భ
	Home
	오 -

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

E 🕑 🍘 http://10.2.21.46/certsrv/en-us/certrqad.asp	P ▼ C Ø Microsoft Active Directory × 端 certificates - Microsoft Exchange	<u> </u>
Microsoft Active Directory Certificate Services - forest35-CA01F35-CA		Home
Advanced Certificate Request		
The policy of the CA determines the types of certificates you can request. Click one of the	following options to:	
Submit a certificate request to unis CA.	mit a renewal request by using a base-64-encoded PKCS #7 file.	

• 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**.

🗲 😔 🙋 http:	//10.2.21.46/certsrv/en-us/certrqxt.asp	🔎 🕆 🖒 🏉 Microsoft Active Directory 🗙 🛁 certificates - Microsoft Exchange	🕆 🛧 (
Microsoft Active	Microsoft Active Directory Certificate Services – forest35-CA01F35-CA Home						
Submit a Certi	ficate Request or Renewal Request						
To submit a sa Saved Request	ved request to the CA, paste a base-64-encoded CN t box.	IC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour	ce (such as a Web server) in the				
Saved Request:							
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	BEGIN NEW CERTIFICATE REQUEST MIIEbjCCA24CAQAvZTEXMBUGAUEAwwoZjMIImZh.^ BURVJFRWQCQTVOQKONHQKOEjAGBQWNDAAM CAWCUERCCAJBQNVBAYTAJVTMIIBIJANBgkqhkiG' AQAEllAgtkrCSQdvXPaiEfkwhHVxsQumoqcxd, SZykcmKjRgaxW0gAJzm4gBQg4wpJS+CTAdXN1s021						
Certificate Temple	ate:						
	Web Server 🗸						
Additional Attribu	ites:						
Attributes:	< >> >						
	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.

A https://localhost/e	co/	Ø - 😫 Certificate error Ĉ 🖉 №	dicrosoft Active Directory Cert 🖂	certificates - Microsoft Evch
Enterprise Office 365			-	ndm service 🔻
Exchange admin c	enter			
recipients	servers databases database availa	oility groups virtual directorie	es certificates	
permissions				
compliance management	Select server: mail01f35.forest35.fiberlinkqa.local	~		
organization	+/=:0			
protection	NAME	STATUS	EXPIRES ON	A
mail flow	Forest35 Exchange Mail01 cert Microsoft Exchange Server Auth Certificate	Pending request Valid	2/23/2018 1/14/2022	Forest35 Exchange Mail01 cert
mobile	Microsoft Exchange WMSVC	Valid Valid	2/9/2022 2/7/2027	Certification authority-signed certificate Issuer: C=US, S=PA, L=Blue Bell, O=IBM, OU=DEVQA, CN=f35.far360.com
public folders				Status
unified messaging				Pending request Expires on: 2/23/2018
servers				Complete
hybrid				Assigned to services
tools				NONE

• 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**

Exchange Certificate - Internet Explorer	
complete pending request	Help
This will import the certificate file that you received from the certification authority. After it's imported, you can assign this certificate to various Exchange services. Learn more	
*File to import from (example: \\server\folder\MyCertificate.CER):	
\\localhost\c\$\certnew.cer ×	
ok cancel	
€, 10	00%

• 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

				_ 0
+ ttps://localhost/ecp	o/	,♀ ∽ 😵 Certificate error ♂ 🄏	🗿 Microsoft Active Directory Cert 🔤 c	ertificates - Microsoft Exch × 👘 🛠
Enterprise Office 365				mdm service 🔻
Exchange admin ce	enter			
recipients	servers databases database availa	bility groups virtual directo	ries certificates	
permissions				
compliance management	Select server: mail01f35.forest35.fiberlinkqa.local	~		
organization	+ 🖍 🖮 😋 …			
protection	NAME	STATUS	EXPIRES ON	
mail flow	Forest35 Exchange Mail01 cert Microsoft Exchange Server Auth Certificate	Valid Valid	2/23/2019 1/14/2022	Forest35 Exchange Mail01 cert
mobile	Microsoft Exchange	Valid	2/9/2022	Certification authority-signed certificate
mobile	WMSVC	Valid	2/7/2027	isach creitorsiss cientiss cir, belloresiss, bellochnikau, belloca
public folders				Status
unified messaging				Valid Expires on: 2/23/2019
servers				Renew
hybrid				Assigned to services
				IMAP, POP
toois				

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

Exchange Certificate - Internet Explorer	
Forest35 Exchange Mail01 cert	Help
general ▶ services Specify the services you want to assign this certificate to. Learn more SMTP Microsoft Exchange Unified Messaging Unified Messaging Call Router MAP POP IIS	
save	cancel

• 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...

📮 certsrv -	[Certification Authority (Local)\forest35-CA	.01F35-CA]	_ 🗆 🗙
File Action View Help			
🗢 🔿 🖄 🖾 🧟 🛃 🕨			
Certification Authority (Local)	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates		

• Right click on the CA name and select properties



• Click on the Extensions tab.

📮 ce	forest35-CA01F35-	CA Properties 2	<u>x</u> <u>- </u> x
File Action View Help	Enrollment Agents Auditing General Policy Modu Extensions Storage Select extension: CRL Distribution Point (CDP) Specify locations from which users can of (CRL). C:\Windows\system32\CettSrv\CettEnroll/ <crt Idap:///CN=<catruncatedname>/CettEnroll/<crt file://<serverdnsname>/CettEnroll/<crt file://<serverdnsname>/CettEnroll/<crt include in all CRLs. Specifies where to when publishing manually. Include in CRLs. Clients use this to fine Velocities in the CDP extension of issued Publish Delta CRLs to this location Include in the IDP extension of issued</crt </serverdnsname></crt </serverdnsname></crt </catruncatedname></crt 	Recovery Agents Si e Exit Modu Certificate Manag tain a certificate revocation III< <caname><crlnames< td=""> NameSuffix>,CN=<serversi< td=""> aName><crlnamesuffix> Name><crlnamesuffix> Add Remultion publish in the Active Direct Delta CRL locations. certificates CRLs</crlnamesuffix></crlnamesuffix></serversi<></crlnames<></caname>	isecurity ule gers in list Suffix><1 ShortNar >CDelta <delta Cove ctory</delta
	Cancel	Арріу	

- 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.

Active Direc		mdm serv	vice Prop	perties	? ×
File Action View Help Active Directory Users and Com Saved Queries Application Servers Automation Servers Automation Servers Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accounts Service Accounts Viers Notes	Remote control General Address Member Of	Remote I Account Dial-in Acti fore ns fore gement fore sers fore UII Remove Uomain Users you have applicatio	Desktop Se Profile Env ve Director st 35 fiberlin st 35 fiberlin st 35 fiberlin st 35 fiberlin	change Primary (COM+ Organization Sessions es Folder soft Exchang
1	0	К	Cancel	Apply	Help

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.

х - | Services File View Help Action 🔲 🙆 📑 🚺 **I** 🎑 Services (Local) Services (Local) Name Description Status Startup Type Encrypting File System (EFS) Log ^ Distributed Link Tracking Cl... Maintains li... Running Automatic Loc Start the service 🕵 Distributed Transaction Co... Coordinates... Net Running Automatic (D... 🔍 DNS Client The DNS Cli... Running Automatic (T... Net Carl EMSUtSvc Running Automatic Loc Description: Manual (Trig... 🔍 Encrypting File System (EFS) 🛛 Provides th... Provides the core file encryption Loc technology used to store encrypte = Loc x Encrypting File System (EFS) Properties (Local Comput.. files on NTFS file system volumes. Loc this service is stopped or disabled, Loc applications will be unable to acce General Log On Recovery Dependencies Π... encrypted files. Loc FES Service name: Loc Loc Display name: Encrypting File System (EFS) Loc q, Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If ~ Description: Loc а. U Loc Loc Path to executable: C:\Windows\System32\Isass.exe Loc Loc Startup type: Automatic v Loc g Loc Loc Stopped Service status: Loc > Stop Resume Start Pause Extended (Standard) You can specify the start parameters that apply when you start the service from here Start parameters οк Cancel Apply

MaaS360 Cloud Extender Common Criteria Guide

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 <u>https://ibm.box.com/s/5vrp23psd6hqn2lq4ypgmlrwst4axwko</u>

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

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-anddependencies#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.

9		Services		_ □	x
File Action View	Help				
) 🗟 🛛	Cloud Extender Properties (Local Computer)	I		
Services (Local)	Servi Cloud Exte	General Log On Recovery Dependencies Service name: EMSAgent	Status	Startup Type Manual Manual (Trig	Log ^ Loc Loc ≡
	Restart the	Display name: Cloud Extender Description:	Running	Manual (Trig Manual (Trig Manual	Loc Loc Loc
		Path to executable: "C:\Program Files (x86)\MaaS360\Cloud Extender\EMSAgent.exe" Startup type: Automatic V	Running Running	Manual Manual Manual Automatic	Loc Loc Loc Loc
		Service status: Burning	Running Running Running	Automatic Manual Automatic	Loc Loc mdi
		Start Stop Pause Resume You can specify the start parameters that apply when you start the service from bace Start Start	Running Running	Manual (Trig Automatic Manual Disabled	Loc Loc Loc
		Start parameters:	Running Running Running	Manual Automatic Automatic	Loc Net Loc
		OK Cancel Apply		Manual (Trig Manual (Trig	Loc Loc v
	Extended (Standard /			

Q.	Services		_ □	x
File Action View Help				
File Action View Help File Action View Help File Services (Local) Cloud Externation Stop the services (Local)	Cloud Extender Properties (Local Computer) General Log On Recovery Dependencies Log on as: Local System account Allow service to interact with desktop This account: Mamservice@forest35.fiberlinka Browse Password: Confirm password:	Status Running Running Running Running	Startup Type Manual Manual (Trig Manual (Trig Manual (Trig Manual Manual Manual Manual Automatic Automatic	Log ^ Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc
		Running Running	Manual Automatic	Loc
			Manual (Trig	Loc
		Running	Automatic	Loc
		Running	Manual	Loc
			Disabled	Loc
		Running	Manual	Loc
		Running	Automatic	Net
		Running	Automatic	Loc
	OK Cancel Apply		Manual (Trig Manual (Trig	
		-		>
Extended	(Standard /			

• 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.

Q.		Services			_ □	x
File Action View	Help					
	i 🗟 🔽 🖬 🕨 🔲 II 🕪					
🎑 Services (Local)	Services (Local)					
	EMSUtSvc	Name 🔺	Description	Status	Startup Type	Log ^
		🥋 Certificate Propagation	Copies user	Running	Manual	Loc
	Stop the service	鵒 Cloud Extender		Running	Automatic	mdi
	Restart the service	🎑 CNG Key Isolation	The CNG ke		Manual (Trig	Loc _
		🎎 COM+ Event System	Supports Sy	Running	Automatic	Loc
		🍓 COM+ System Application	Manages th	Running	Manual	Loc
		鵒 Computer Browser	Maintains a		Disabled	Loc
		🎑 Credential Manager	Provides se	Running	Manual	Loc
		鵒 Cryptographic Services	Provides thr	Running	Automatic	Net
		🔍 DCOM Server Process Laun	The DCOM	Running	Automatic	Loc
		🔍 Device Association Service	Enables pair		Manual (Trig	Loc
		🎑 Device Install Service	Enables a c		Manual (Trig	Loc
		🎑 Device Setup Manager	Enables the		Manual (Trig	Loc
		🔍 DHCP Client	Registers an	Running	Automatic	Loc
		🎑 Diagnostic Policy Service	The Diagno	Running	Automatic (D	Loc
		🎑 Diagnostic Service Host	The Diagno		Manual	Loc
		鵒 Diagnostic System Host	The Diagno		Manual	Loc
		🔍 Distributed Link Tracking Cl	Maintains li	Running	Automatic	Loc
		鵒 Distributed Transaction Co	Coordinates	Running	Automatic (D	Net
		🎑 DNS Client	The DNS Cli	Running	Automatic (T	Net
		EMSUtSvc		Running	Automatic	mdi
		🤹 Encrypting File System (EFS)	Provides th	Running	Automatic (T	Loc 🗸
	<u> </u>	<	III			>
	Extended Standard					

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, rightclick 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**.

Confirm Attribute Changes					
You have chosen to make the following attribute changes:					
encrypt					
Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?					
\odot Apply changes to this folder, subfolders and files					
OK Cancel					

• 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.

Г

📀 🕺 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 sma Certificate details: 	art card.					
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	ancel

	x
💿 🕺 Encrypting File System	
Update your previously encrypted files	
Select the folders containing encrypted files that you want to as certificate and key. Updating now helps you avoid losing acce if the previous certificate and key are lost	ssociate with the new ess to your encrypted files
Folders:	
ProgramData Application Data	^
	=
■ MaaS360	
	~
I'll undate my encrypted files later	
Updating your files might take some time, depending on how r	nany files you update. If files will not be updated.
	nico un norbe apadica.
	Next Cancel
	X
💿 🕺 Encrypting File System	X
Some of your encrypted files were not updated	X
 Encrypting File System Some of your encrypted files were not updated Certificate details: 	X
 Encrypting File System Some of your encrypted files were not updated Certificate details: Issued to: mdm service 	X View certificate
 Encrypting File System Some of your encrypted files were not updated Certificate details: Issued to: mdm service Issued by: forest35-CA01F35-CA 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
 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 	X View certificate View log
I compare of pour 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	X View certificate View log

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.

Cloud Extender Configuration To	ol	- 🗆 X
HOME IMPORT EXPORT P	ROXY SETTINGS HELP~	English (United States) 🗸 🗸
Exchange Manage ActiveSync Settings on Exc	hange or Office365	(i)
	Email Server Configuration	
Start	Email Server hostname exchange2013.acmecorp.local	
	Use SSL	
	Remote PowerShell URL http://exchange2013.acmecorp.local/powershell	
	Service Account Configuration	
2 Connection	Service Account needs to be a member of "Organization Management" for Exchange 2010, 2013, 20 For granular access rights, click here for more details on Role based Access Control (RBAC)	16
	Caution: The Service Account must have the proper rights and permissions for each configured feat For more information, click the information button.	ure.
	Username	
	acme	
Binish		
	Domain	
	acmecorp	
	Back	Next Save Cancel
The Cloud Extender is running	ng	

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.

Cloud Extender Configuration To	ol			- 🗆 X
HOME IMPORT EXPORT P	roxy settings help~			English (United States) 🛛 🗸
Certificate Integration	ON to mobile devices			(i)
Chart	Certificate Properties			
Start	Subject Name (i)	/CN=%uname%/emailAddress=%email%		
	Subject Alternate Name	UpnAndEmail		~
SCEP Config	Cache certs on Cloud Extender			
	Location of Certificate Cache	Choose a location to store cached certificates		Browse
3 Cert Attributes				
4 Finish				
			Back Nex	t Save Cancel
The Cloud Extender is runnir	ng			

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

SCEP - Microsoft, Veri	zon, Open Trust server details
Template Name	
Hostname of SCEP server	http 🗸
SCEP Server challenge type	O Dynamic ○ Static ○ None
Challenge Username	
Challenge Password	

Certificate Propertie	s		
Subject Name	i		\wedge
Subject Alternate Name		Other	~
Specify Other	i		\wedge
Cache certs on Cloud Exter	nder		
Location of Certificate Cach	he	Choose a location to store cached certificates Browners	owse

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.

Programs and Features							- 🗆	×
← → × ↑ 🖬 > Control 🛙	Panel > All Control Panel Items > Programs and Features				~	ර් Search Program	is and Features	م ر
Control Panel Home View installed updates	Uninstall or change a program	click Uninstall Change of Renair						
Turn Windows features on or	to dimistan a program, select it norther as and their	click onlinistall, change, or hepall.						
off	Organize 🔻							?
Install a program from the network	Name	Publisher	Installed On	Size	Version			^
	2 7-Zip 16.04 (x64)	Igor Pavlov	7/31/2017	4.75 MB	16.04			
	Apache Directory Studio - (remove only) Application Insights Tools for Visual Studio 2015	Microsoft Corporation	8/25/2017 5/28/2019	11.9 MB	7.0.20622.1			
	Cloud Extender	MaaS360	6/8/2020	18.4 MB	2.101.100.003			
	Debugging Tools for Windows 64-bit	Microsoft Corporation	7/28/2017	42.3 MB	6.6.7.5			
	Decoda	P1 10 11	7/28/2017	10.01.00	2 22 2 22 45 4			
	DigiCert PKI Client	DigiCert Inc.	5/2//2020	40.2 MB	2.20.2.20454			
	Bentity Framework 6.1.3 Tools for Visual Studio 2015 U	Microsoft Corporation	5/28/2019	30.4 MB	14.0.41103.0			
	Cityrenian 2.21.0	The Cit Development Communi	//28/2017	1.04 MB	2.21.0			
	Canada Change	The Git Development Communi	4/9/2019	492 MB	2.21.0			
	Google Chrome	BNA Com	5/27/2020	595 IVIB	0.5.14.72			
		Misrosoft Corneration	5/29/2019	20.7 MP	9.3.14.75			
	III Toto Express	Microsoft Corporation	5/20/2019	59.7 IVID	10.0.1750			
	IIS Express Application Compatibility Database for x86		5/29/2019					
	A Java 8 Undate 144	Oracle Corporation	8/25/2017	190 MB	8 0 1440 1			
	A Java 8 Undate 201 (64-bit)	Oracle Corporation	4/9/2019	236 MB	8.0.2010.9			
	A Java SE Development Kit 8 Undate 201 (64-bit)	Oracle Corporation	4/9/2019	573 MB	8.0.2010.9			
	Microsoft .NET Compact Framework 1.0 SP3 Developer	Microsoft Corporation	7/28/2017	19.7 MB	1.0.4292			
	.ñël Microsoft .NET Compact Framework 2.0	Microsoft Corporation	7/28/2017	118 MB	2.0.5238			
	Wicrosoft .NET Core SDK 2.2.110 (x64)	Microsoft Corporation	12/10/2019	486 MB	2.2.110			
	Microsoft .NET Core SDK 3.0.100 (x64)	Microsoft Corporation	12/10/2019	537 MB	3.0.100.14277			
	Microsoft .NET Framework 4.5.1 Multi-Targeting Pac	Microsoft Corporation	5/28/2019	64.6 MB	4.5.50932			
	Microsoft .NET Framework 4.5.1 SDK	Microsoft Corporation	5/28/2019	38.8 MB	4.5.51641			
	Microsoft .NET Framework 4.5.2 Multi-Targeting Pac	Microsoft Corporation	5/28/2019	64.7 MB	4.5.51209			~
	Currently installed programs Total size: 8 91 programs installed	3.87 GB						

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.

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

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 rightclick 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.

laaS360_Cloud_Ext	tender.exe Propertie	25
Security	Details	Previous Versions
General	Compatibility	Digital Signatures
ignature list		
Name of signer:	Digest algorithm	Timestamp
International Busi	. sha1	Monday, April 20, 202
International Busi	. sha256	Monday, April 20, 202
		Details

Select one of the signatures and click Details.

Digital Signature Deta	ils	?	×
General Advanced			
Digital Sig This digital	gnature Information signature is OK.	1	
Signer information			
Name:	International Busine	ss Machines Corporation	
E-mail:	Not available		
Signing time:	Monday, April 20, 2	020 12:04:05 PM	
		View Certificate	
Countersignatures			
Name of signer:	E-mail address:	Timestamp	
Symantec Time	Not available	Monday, April 20, 20	
		Details	
		C	Ж

Click "View Certificate".

🐖 Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for • Ensures software came from • Protects software from altera	the following purpose(s): software publisher ation after publication
* Refer to the certification authority Issued to: International Bus	's statement for details.
Issued by: DigiCert SHA2 As	ssured ID Code Signing CA
Valid from 10/3/2019 to 1	10/7/2022
Install	Certificate Issuer Statement
	ОК

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:0000000
"DisabledByDefault"=dword:0000001
[HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\Multi-Protocol Unified Hello\Server]
"Enabled"=dword:0000000
"DisabledByDefault"=dword:0000001
[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:0000000
"DisabledByDefault"=dword:0000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\PCT 1.0\Server]
"Enabled"=dword:0000000
"DisabledByDefault"=dword:0000001
```

```
[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:0000001
```

```
[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:fffffff
"DisabledByDefault"=dword:0000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCH
ANNEL\Protocols\TLS 1.2\Server]
"Enabled"=dword:fffffff
"DisabledByDefault"=dword:0000000
```

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 <u>https://www.microsoft.com/en-us/download/details.aspx?id=54264</u> and <u>https://www.microsoft.com/en-us/download/details.aspx?id=54265</u>

- 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.

Enhanced Mitigation Experience Toolkit	×
EMET Configuration Wizard	
Use Recommended Settings	
 Reset existing application configuration settings 	
Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java	
 Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!) 	
• Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program	
Configure Manually Later	
EMET Privacy Statement Finish	ı

• 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.

a ^	Er	hanced Mitigation Experience Toolkit		- 0	×	
 Import Export Group Policy 	Wizard Apps Trust	Quick Profile Name: Recommended security ¥ Skin: Office 2013 * System Settings	 Windows Even Tray Icon Early Warning Reporting 	it Log Help		
Svetem Statue	Comgaradon	System Settings	Reporting	1110	131	
Data Exec	ution Prevention (DEP)		Арр	lication Opt In	-	
Structured	Exception Handler Overwrite	Protection (SEHOP)		plication Opt In		
Address S	plication Opt In					
Certificate Trust (Pinning) Enab					-	
Running Processe	s				1 1	
Process ID	Process ID Process Name					
480	ccsvcHst - Symantec Servic		_			
51/2	ccsvcHst - Symantec Servic	reconner			- 11	
3296	cmd - Windows Command P					
4968	conhost - Console Window					
5084	conhost - Console Window					
3248	CSrSS					
332	csrss					
5020	csrss					
404	CSFSS		_			
					v	
				C Refresh		

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

a ^	Enhanced Mitigation Experience Toolkit						
import	Apps Trust	Quick Profile Name: Maximum security setti V Skin: Office 2013 · System Settings	 Windows Event Log Tray Icon Early Warning Reporting 	ent Log 👔 ng Help			
– System Status Data Execution Prev		•					
Structured Exceptio	n Handler Overwrite	Always On	Always On				
Address Space Layo	out Randomization <mark>(</mark> A	Application	Application Opt In				
Certificate Trust (Pinning) Enabled							

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

(A

- 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.

Image: Depict Sepert Image: De	■ ^				Applica	ation Con	figuration	(-		×
Export Add Application Add Wildard Remove Selected Show Full Setting Show Full Setting Show Full Policy Application Audd rolly E Banned Functions File Add / Remove Options Default Action Mitgation Settings Mitgation Settings Mitgations Entry Image			<			Ś	2	• Stop	on exploit		Deep Ho	ooks 🗸	Anti Detour	s		
File Add / Remove Options Default Action Mitgation Settings Mitgations Enter text to search Image: Construction of the search Image: Construction of the search App Name DEP SEHOP Null* Heap EAF EAF+ Mad Botto LoadLb MemP Caller SmEX ASR MSPUB.EXE V	Export Export Add Application Add Wile Selected	dcard Rer Sele	nove	Show Full Path	Show Full Show All Show Group			○ A <u>u</u> dit	○ Audit only			5				
Milgations App Name DEP SEHOP NullP Heap EAF EAF+ Mand Botto Loadlib MemP Caler SinEx Stack ASR MSPUB.EXE V <	File Add / Remo	ve			Option	ns		Defau	ult Action		Mitig	ation Set	tings			
Enter text to search V Find Clear App Name DEP SEHOP NullP Heap EAF EAF + Mand Botto Loadub MemP Caler SimEx Stack ASR MSPUB.EXE V	Mitigations															
Enter text to search Find Clear App Name DEP SEHOP NullP Heap EAF EAF+ Mand Botto LoadLib MemP Caller SimEx Stadk ASR MSPUB.EXE U																
Ap Name DEP SEHOP NullP Heap EAF EAF Mand Botto Load.lb MemP Caller SineX ASA INFOPATH.EXE V	Enter text to search			~	Find	Clea	ar									
MSPUBLEXE V	App Name	DEP	SEHOP	NullP	Heap	EAF	EAF+	Mand	Botto	LoadLib	MemP	Caller	SimEx	Stack	ASR	
INFORMALEXE V <td< td=""><td>MSPUB.FXF</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>A</td></td<>	MSPUB.FXF															A
VISIO.EXE V	INFOPATH.EXE															1
VPREVIEW_EXE V <t< td=""><td>VISIO.EXE</td><td></td><td></td><td></td><td>~</td><td></td><td></td><td>~</td><td>×</td><td>~</td><td>~</td><td>~</td><td></td><td>~</td><td></td><td>1</td></t<>	VISIO.EXE				~			~	×	~	~	~		~		1
LYNCEXE Y </td <td>VPREVIEW.EXE</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td></td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td></td> <td>~</td> <td></td> <td>1</td>	VPREVIEW.EXE	~	~	~	~	~		~	~	~	~	~		~		1
PPTVIEW.EXE V <td< td=""><td>LYNC.EXE</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td></td><td></td><td>~</td><td>~</td><td>~</td><td></td><td>~</td><td></td><td></td><td>1</td></td<>	LYNC.EXE	~	~	~	~	~			~	~	~		~			1
OTS.EXE V </td <td>PPTVIEW.EXE</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td></td> <td></td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td>~</td> <td></td> <td>1</td>	PPTVIEW.EXE	~	~	~	~	~			~	~	~	~	~	~		1
AcroRd32.exe ✓ <t< td=""><td>OIS.EXE</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td></td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td></td><td>1</td></t<>	OIS.EXE	~	~	~	~	~		~	~	~	~	~	~	~		1
Acrobat.exe ✓ <td< td=""><td>AcroRd32.exe</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td></td><td>1</td></td<>	AcroRd32.exe	~	~	~	~	~	~	~	~	~	~	~	~	~		1
java.exe ✓<	Acrobat.exe	~	~	~	~	~	~	~	~	~	~	~	~	~]
javaw.exe ✓	java.exe	~	~	~		~		~	~	~	~	~	~	\checkmark]
javaws.exe ✓	javaw.exe	~	~	~		~		~	~	~	~	~	~	~]
EMSAgent.exe ✓ <t< td=""><td>javaws.exe</td><td>~</td><td>~</td><td>~</td><td></td><td>~</td><td></td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td>~</td><td></td><td>j</td></t<>	javaws.exe	~	~	~		~		~	~	~	~	~	~	~		j
EMSULSvc.exe Image: style="text-align: center;">Image: style="text-align: center;"/>Image: style="text-align: center;"/>Image: style="text-align:	EMSAgent.exe	~	~	~	~	~			~	~	~	~	~	~		1
ASConfig.exe Image: Config.exe Image:	EMSUtSvc, exe	~	~	~	~	~			~	~	~	~	~	~		1
EntrustCertsConfig.exe Image: Config.exe <	ASConfig.exe	~	~	~	~	~			~	~	~	~	~	~]
LDAPConfig.exe Image: Config.exe Image	EntrustCertsConfig.exe	~	~	~	~	~			~	~	~	~	~	\checkmark]
EntrustCerts.exe Image: Constraint of the system Image: Consthe system Image: Constraint o	LDAPConfig.exe	\checkmark	\checkmark	~	~	~			~	~	~	\checkmark	~	\checkmark]
LDAPAuth.exe Image: Constraint of the state	EntrustCerts.exe	~	\checkmark	~	~	~			~	~	~	\checkmark	~	\checkmark]
LDAPUsersInfo.exe	LDAPAuth.exe	~	~	~	~	~			~	~	~	~	~	\checkmark]
	LDAPUsersInfo.exe	~	~	~	\checkmark	~			~	~	~	\checkmark	\checkmark	~		

- 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