MaaS360 Cloud Extender

Admin Guide

Abstract

Guide to Setup the Cloud Extender to Meet NIAP Common Criteria Requirements

Version 1.0, 20 July 2022

Table of Contents

1 Cloud Extender Admin Guide

About the Cloud Extender

The IBM® MaaS360® Cloud Extender™ is a lightweight agent that enhances device management capabilities by integrating with on-premises systems within your environment, such as email, corporate directories, certificate authorities, and application and content servers.

Installing the Cloud Extender

Information about installing the Cloud Extender software.

Configuring Settings for the Cloud Extender Modules

Information about configuring settings for the Cloud Extender modules.

2 About the Cloud Extender

The IBM® MaaS360® Cloud Extender™ is a lightweight agent that enhances device management capabilities by integrating with on-premises systems within your environment, such as email, corporate directories, certificate authorities, and application and content servers.
The Cloud Extender requires minimum resources, easily traverses proxy environments, and provides secure messaging and data transfer between the MaaS360 platform and your on-premises systems.

Cloud Extender Use Cases

The Cloud Extender provides various combinations of use cases for a mobile device program, based on integration requirements, the size of the environment, and High Availability (HA) requirements.

Cloud Extender Architecture

The Cloud Extender is a small Windows application that you install behind the firewall with network access to the appropriate internal systems.

Parent topic: Cloud Extender Admin Guide

3 Cloud Extender Use Cases

The Cloud Extender™ provides various combinations of use cases for a mobile device program, based on integration requirements, the size of the environment, and High Availability (HA) requirements.
The following Cloud Extender use cases are the most common scenarios for a mobile device program:

1. Enrolling mobile devices with Corporate Active Directory credentials (User Authentication module)
2. Limiting enrollments to certain user groups (User Authentication module)
3. Creating policies for a specific Active Directory (AD) / LDAP groups (User Visibility module)
4. Discovering active devices connected in your email environment by using ActiveSync (Exchange and IBM® Traveler module)
5. Blocking new ActiveSync devices that are not enrolled in MaaS360® (Exchange and IBM Traveler module)
6. Creating identity certificates with an internal certificate authority (CA) and distributing those certificates to devices for authentication with Wi-Fi, VPN, Exchange module, IBM Traveler module, F5/Load Balancer pass-through, and SMIME
7. Allowing access to internal corporate resources, such as SharePoint, Windows file shares, or intranet sites (Mobile Enterprise Gateway (MEG) module)

Parent topic: [About the Cloud Extender]

4 Cloud Extender Architecture

The Cloud Extender™ is a small Windows application that you install behind the firewall with network access to the appropriate internal systems.

4.1 How the Cloud Extender Works

The Cloud Extender makes an outbound connection to the IBM® MaaS360® Cloud or On-Premises instance over port 443. The MaaS360 Cloud and the Cloud Extender both use the Extensible Messaging and Presence Protocol (XMPP) protocol to maintain the connection for real-time actions.

The Cloud Extender includes a Configuration Tool that you use to configure proxy settings either manually, PAC, or automatically. The Cloud Extender also accepts credentials to traverse through authenticated proxies. When you configure proxy settings, the Cloud Extender connects to the MaaS360 Cloud to establish two-way communication between theMaaS360 Cloud and the Cloud Extender - from the MaaS360 Cloud to the Cloud Extender and action responses back from the Cloud Extender to the MaaS360 Cloud.

The Cloud Extender uses a modular architecture with multiple services (like Exchange Integration, User Visibility, User Authentication). You enable the corresponding service (or module) on the Cloud Extender for integration and configuration. If a new feature is enabled, the related module and the associated configuration elements are automatically updated for all Cloud Extender instances. All updates are automatic unless otherwise configured. The modular architecture provides mechanisms for module versioning and the limited release of modules to support pre-production testing.

4.2 Resilience and Scalability

You can install multiple instances of the Cloud Extender to provide scale and resilience. The MaaS360 Cloud acknowledges all Cloud Extender instances for a specific customer and uses those instances to maximize performance and reliability.

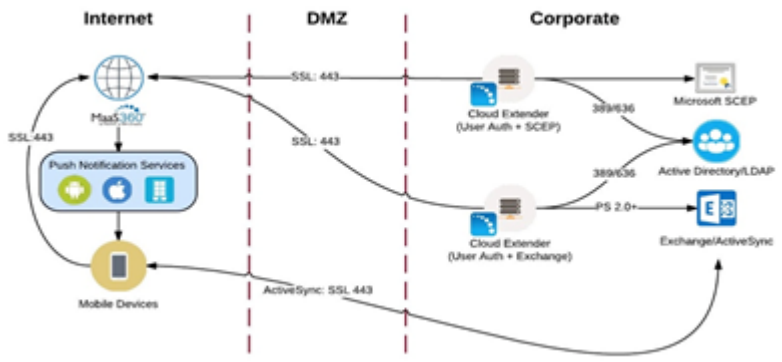
The Cloud Extender provides self-monitoring and usage statistics to the MaaS360 Cloud to facilitate viewing, monitoring, and alerting on Cloud Extender activity.

4.3 MaaS360 Real-Time Notification Services

Using the outbound connection from the customer premises to MaaS360 facilitated by the Cloud Extender, MaaS360 administrators can send commands to the appropriate systems to achieve a specific result. Since the Cloud Extender does not require an inbound connection, you can place the Cloud Extender on the internal network.

For example, the MaaS360 administrator issues a Block command for a specific device to block that device from syncing email. The MaaS360 Portal issues an action response through an explicit device action or an automated compliance rule. This command is sent to the appropriate customer Cloud Extender instance in real-time, the Cloud Extender issues the appropriate command, and then reports back the action status (Success/Failure/Pending) to the MaaS360 Cloud.

The following diagram illustrates an example of a typical small/medium sized business Cloud Extender implementation that incorporates LDAP Authentication in High Availability, Exchange Integration for ActiveSync device discovery, and Certificate Authority Integration for issuing Identity Certificates.



4.4 The Cloud Extender Modules

A Cloud Extender module is a package of scripts and actions that integrate with one component of your on-premises infrastructure and provides full integration service with that component. You can enable multiple Cloud Extender modules to integrate with various on-premises components.

The MaaS360 Cloud platform provides extra management capabilities based on the type of modules that are enabled on the Cloud Extender and configured to integrate with your environment. You can enable these modules with each other, but make sure that you have enough system resources available to use those modules.

The Cloud Extender includes the following modules:

Table 1. Cloud Extender modules

Module Name	Module Description
Exchange Integration Module	The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices, and uploads that device information to the MaaS360 Cloud. The Exchange Integration module automatically quarantines devices, allows only MaaS360 enrolled devices, carries out actions (such as Approve, Block, or Remove device from the Mailbox) sent from MaaS360 and applies ActiveSync device policies. This module supports MS Exchange 2007, 2010, 2013, 2016, Office 365, and BPOS-D.
Email Notification Module	The Email Notification module sends a notification alert to all iOS devices for new email messages if you are using Secure Mail as the email client. Due to iOS architecture, the OS can suspend third-party apps when the user is not actively using the app. For the Secure Mail app, this OS restriction results in users not being notified when new mails are received. The Email Notification module allows the Cloud Extender to

	directly subscribe to these notifications with Exchange, and then notifies the device with the APNS notification alert, which bypasses the OS limitation.
IBM Traveler Integration Module	The IBM Traveler Integration module interacts with information received from IBM Traveler and IBM SmartCloud® about ActiveSync-connected devices, and uploads device information to the MaaS360 Cloud. The IBM Traveler module automatically quarantines devices that are connected to your mail infrastructure (selected versions) and facilitates actions that are sent from the MaaS360 Portal.
User Authentication Module	The User Authentication module interacts with Active Directory and LDAP directories to provide user authentication service for various MaaS360 functions, such as self-service device enrollment with corporate credentials, MaaS360 Portal login, and user management portal. The Cloud Extender supports integration with LDAP implementations, including Active Directory, Domino® LDAP, Oracle LDAP, Novell eDirectory LDAP, and OpenLDAP.
User Visibility Module	The User Visibility module uses the corporate directory groups to allow for the assignment and distribution of policies, apps, and content to mobile devices. These groups are imported by the MaaS360 Administrator to control administrator access to manage a subset of devices. LDAP filters are used to limit the groups and organizations

	imported. Devices are managed based on corporate directory structure.
Certificate Integration Module	The Certificate Integration module facilitates the automatic provisioning, distribution, and renewal of digital identity certificates to managed mobile devices by using existing Microsoft CA, Symantec CA, or Entrust Admin Services and Identity Guard. You can also use these identity certificates for user or device authentication for corporate Wi-Fi, VPN, or email (both native and MaaS360 Secure Mobile Mail) solutions.
Blackberry Enterprise Server Module	The BlackBerry Enterprise Server (BES) module uses the BES 5.0 Administrator APIs to provide complete visibility and control of BlackBerry devices connected to your BES 5.0 environment. **Note:** For BlackBerry 10 device management, use the Exchange Integration module.
Mobile Enterprise Gateway Module	The Mobile Enterprise Gateway (MEG) module provides gateway and relay functions by providing secure mobile application access to behind-the-firewall information and resources such as SharePoint, internal websites, Windows file shares, and IBM Connections. The Mobile Enterprise Gateway (MEG) module provides a more efficient and targeted approach than traditional VPNs.

Parent topic: [About the Cloud Extender]

5 Installing the Cloud Extender

Information about installing the Cloud Extender™ software.

Minimum Requirements for the Cloud Extender

The Cloud Extender is a scalable piece of software that can increase the depth of view into your network environment and allows high availability in managing your mobile device program.

Scaling the Cloud Extender

MaaS360® provides a scaling tool that you use to determine the number of Cloud Extenders that you need to install in your environment.

Downloading the License Key and the Cloud Extender Software

Before you can install the Cloud Extender software, you must obtain the license key and the software from the MaaS360 Portal.

Installing the Cloud Extender Software

The MaaS360 Cloud Extender installation package installs the core software.

Configuring the Cloud Extender

The Cloud Extender software requires access to the MaaS360 Cloud to connect and to implement services. If you installed your Cloud Extender in a proxy environment, use the Cloud Extender Configuration Tool to configure the Cloud Extender.

Parent topic: Cloud Extender Admin Guide

5.1 Minimum Requirements for the Cloud Extender

The Cloud Extender™ is a scalable piece of software that can increase the depth of view into your network environment and allows high availability in managing your mobile device program.

5.1.1 Software Requirements

Install the Cloud Extender on a physical or virtual machine with Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, or 2008.

Note: Cloud Extender does not support the Server Core installation option for Windows Server 2016, 2012 R2, 2012, 2008 R2, or 2008. Only Full Server Installation, Server Graphical Shell, or Server with a Desktop Experience installation options are supported.

Before you install the Cloud Extender, make sure that the following requirements are met:

Component	Minimum Requirement
Physical or Virtual Machine	Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, or 2008
Other Software	.NET Framework 4.6.1 or higher must be installed
Memory	2 GB 4 GB for Mobile Enterprise Gateway
Processor	Dual Core CPU: 2.8 Gigahertz
Disk	4 GB free space

For resource sizing, see the sections for each module.

5.2 Networking

The Cloud Extender makes an outbound connection to the MaaS360® Cloud or MaaS360 On-Premises installation. The following tables outline the outbound connection requirements for each instance of MaaS360 Cloud and MaaS360 On-Premises.

If you are using the Cloud Extender on the MaaS360 Cloud, you can locate your instance of the MaaS360 Portal from the following areas:

- The first digit of your Billing ID (at the bottom of the MaaS360 Portal after you log in)
- The login URL that corresponds with the URLs in the following tables

The following table provides the connection requirements from the MaaS360 Portal to the Cloud Extender cloud instance:

Table 2. Location of MaaS360 Portal from cloud/outbound connection requirements

M1 (portal.fiberlink.com)	M2 (m2.maas360.com)	M3 (m3.maas360.com)	M4 (m4.maas360.com)
services.fiberlink.com:443 208.76.128.153 208.76.130.181	services.m2.maas360.com:443 88.205.104.145 217.112.145.234	services.m3.maas360.com:443 208.76.133.30 50.204.34.212	services.m4.maas360.com:443 119.81.110.141 119.81.173.174
mpns.maas360.com:443 208.76.128.168 208.76.131.110	mpns.m2.maas360.com:443 88.205.104.154 217.112.145.235	mpns.m3.maas360.com:443 208.76.133.28 50.204.34.211	mpns.m4.maas360.com:443 119.81.110.140 119.81.173.173
internettest.fiberlink.com:80 208.76.128.58 208.76.130.58	internettest.fiberlink.com:80 208.76.128.58 208.76.130.58	internettest.fiberlink.com:80 208.76.128.58 208.76.130.58	internettest.fiberlink.com:80 208.76.128.58 208.76.130.58
maascentral.maas360.com:443	maascentral.maas360.com:443	maascentral.maas360.com:443	maascentral.maas360.com:443

maas-central-01.maas360.com:443 208.76.128.150 208.76.130.120	maas-central-02.maas360.com:443 208.76.128.150 208.76.130.120	maas-central-03.maas360.com:443 208.76.128.150 208.76.130.120	maas-central-04.maas360.com:443 208.76.128.150 208.76.130.120
upload.fiberlink.com:443 72.21.0.0/16	upload.fiberlink.com:443 72.21.0.0/16	upload.fiberlink.com:443 72.21.0.0/16	upload.fiberlink.com:443 72.21.0.0/16
dl.maas360.com (no IP range)	dl.m2.maas360.com (no IP range)	dl.m3.maas360.com (no IP range)	dl.m4.maas360.com (no IP range)

The following table provides the URL locations for the MaaS360 Portal from the Cloud Extender on-premises instance:

Table 3. URL locations of MaaS360 Portal from on-premises instance

MaaS360 Portal URL	Port or IP Range
Services VM URL	443
Enroll VM URL	443
upload.fiberlink.com:80	72.21.0.0/16

For Cloud Extender updates:
The Cloud Extender requires access to the MaaS360 Content Delivery service provided by `dl.XX.maas360.com`, which does not require a specific IP range.
In addition to these networking requirements, the Cloud Extender needs outbound connections open to the Cloud Extender modules. For example, if you enable User Authentication for LDAP, the respective LDAP ports need to be accessible from the Cloud Extender server.
Optionally, you can open outbound connections to `upload.fiberlink.com` that allows IBM® Support to remotely collect logs from all installations of the Cloud Extender.

However, if this host name is blocked, you must manually collect the Cloud Extender logs by following these steps:

1. Log in to the Cloud Extender Server.
2. From the `C:\Program Files(x86)\MaaS360\Cloud Extender` folder, click `DiagnosticCmd.exe`. A compressed version of the logs is saved to your desktop.
3. Upload the `*.zip` file to `ftp://ftp.fiberlink.com` and provide the file name of the `*.zip` file to IBM Support.

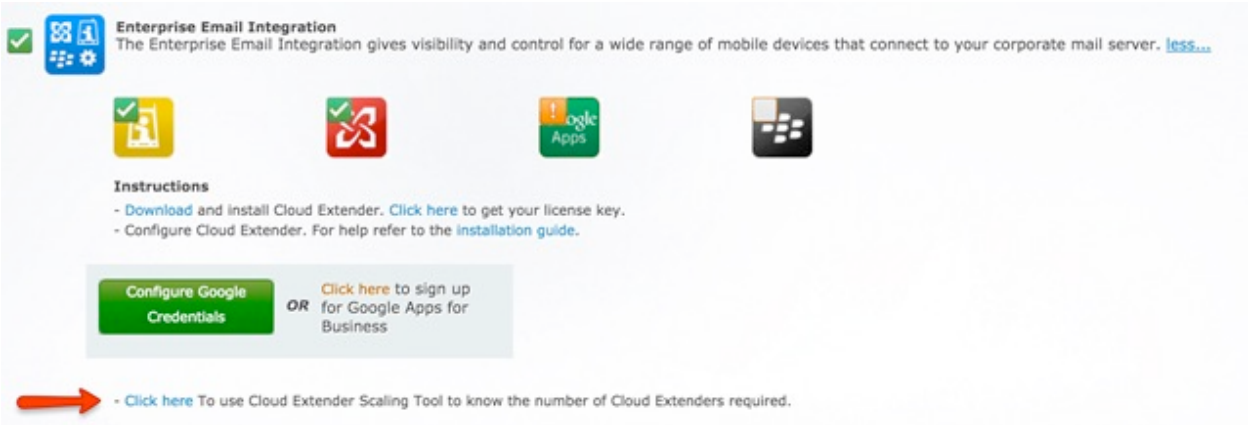
Parent topic: [Installing the Cloud Extender]

6 Scaling the Cloud Extender

MaaS360® provides a scaling tool that you use to determine the number of Cloud Extenders that you need to install in your environment.
The Cloud Extender™ Scaling Tool uses the size of your environment, plus a list of integrated services that you need, as inputs and outputs for installation requirements.

Follow these steps to download the Cloud Extender Scaling Tool:

1. From the MaaS360 Portal Home page, select **Setup** > **Services** > **Enterprise Email Integration**. The Enterprise Email Integration window is displayed.



2. The scaling tool uses Excel macros. When you open the scaling tool, make sure that these macros are enabled. The scaling tool prompts you for sizing details about each corporate server that requires Cloud Extender integration:

Integration with Corporate Servers		
	Device Management	
1	Estimated number of devices that will be enrolled into MaaS360	400
	Mail Server Integration for Email Access Control	
1	Do you want to integrate MaaS360 with your Mail server to allow secure access to emails only from Managed and Compliance devices	Yes
2	Select which of the following Mail servers do you use in your organization (Select multiple if you have a mixed environment)	
	Exchange 2007	
	Exchange 2010	
	Exchange 2013	
	Office 365	Yes
	BPOS-Dedicated	
	Note Traveler 8.x	
	Note Traveler 9.x	
	IBM SmartCloud	
	Google Apps for Business	
	Others, please specify	
3	Estimated number of Mailboxes in each Mail server (Specfy values for each Server Type in case of a mixed environment)	
	Exchange 2007	
	Exchange 2010	
	Exchange 2013	
	Office 365	450
	BPOS-Dedicated	
	Note Traveler 8.x	
	Note Traveler 9.x	
	IBM SmartCloud	
	Google Apps for Business	
	Others, please specify	
	Total Mailboxes	450
4	Estimated number of Devices (already syncing or planned to sync)	
	Exchange 2007	
	Exchange 2010	
	Exchange 2013	
	Office 365	400
	BPOS-Dedicated	

	User Directory integration (AD/LDAP)	
1	Do you want to integrate with your User Directory for authenticating users prior to enrollment	Yes
2	Do you want to integrate with your User Directory for User & Groups information for Group based policy assignment & app/doc distribution	Yes
3	Estimated number of Users in your User Directory (Specify only those users who will be uploaded to MaaS360)	600
	Certificate Integration (Microsoft SCEP, Entrust, Symantec Verisign Online CA)	
1	Do you want to integrate with your Certificate Server for Authentication certificates for Email, Wi-Fi or VPN	Yes
	Mobile Enterprise Gateway	
1	Do you want to allow your devices to access Intranet servers (Intranet website/web apps, SharePoint or Network Fileshare)	Yes
		Generate Recommended Setup

3. Click **Generate Recommended Setup** to generate setup requirements for your environment. The output displays the following information:
    a. The total number of Cloud Extenders that are required for your environment
    b. The number of Cloud Extenders that share certain services
    c. The number of Cloud Extenders that you must configure with dedicated services.
    d. The list of services for each Cloud Extender.

6.1 General Guidelines for Scaling

Follow these general guidelines for scaling the Cloud Extender:

1. The User Authentication, Certificate Integration, and the Mobile Enterprise Gateway (MEG) services also run in High Availability (HA) mode. You can configure multiple Cloud Extenders for these services.
2. The Exchange Integration and the IBM® Traveler Integration services run on multiple Cloud Extenders, but the scope of each Cloud Extender instance must be restricted to an exclusive subset of the mail environment.

3. The Exchange Integration for Real-time Mail Notifications (Email Notification) service must use a dedicated Cloud Extender. However, you cannot enable other Cloud Extender services on the same Cloud Extender instance that runs the Exchange Integration for Real-time Mail Notifications (Email Notification) service. Multiple Cloud Extenders can run the Exchange Integration for Real-time Mail Notifications (Email Notification) service.
4. The Mobile Enterprise Gateway (MEG) service must use a dedicated Cloud Extender. However, you cannot enable other Cloud Extender services on the same Cloud Extender instance that runs the Mobile Enterprise Gateway (MEG) service. Multiple Cloud Extenders can run the Mobile Enterprise Gateway (MEG) service.

Parent topic: Installing the Cloud Extender

6.2 Downloading the License Key and the Cloud Extender Software

Before you can install the Cloud Extender™ software, you must obtain the license key and the software from the MaaS360® Portal.

Procedure

1. Log in to the MaaS360 Portal with your administrator credentials.
2. Select **Setup** > **Services**. For each service that you want to integrate, enable the services that need to operate with a Cloud Extender.
   a. Enterprise Email Integration: Exchange, IBM® Traveler, and BlackBerry
   b. Enterprise Server
   c. Enterprise Gateway
3. Locate the **Enterprise Email Integration** or **Mobile Enterprise Gateway** service and click **More**.
4. Click **Download** to locate the Cloud Extender application.
5. Select **Click Here** to send the license key to your administrator email address.
6. Start the MaaS360 Cloud Extender installation package.
   Note: Choose to download the Cloud Extender from the MaaS360 Portal even if you have a previous copy of the software to make sure that you are installing the most recent version of the product.

Parent topic: Installing the Cloud Extender

6.3 Installing the Cloud Extender software

The MaaS360® Cloud Extender™ installation package installs the core software.

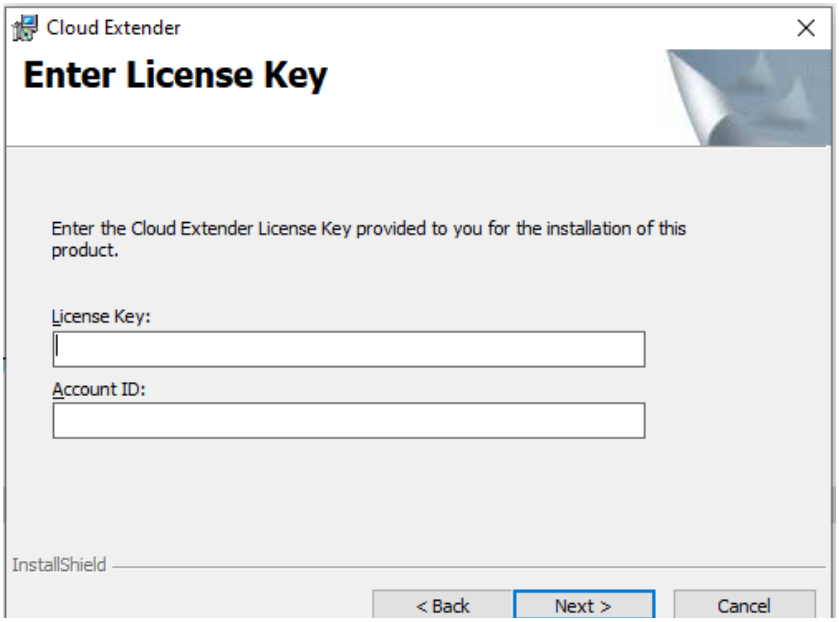
6.3.1 About This Task

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 these modules from **Setup** > **Services** in your MaaS360 Portal.

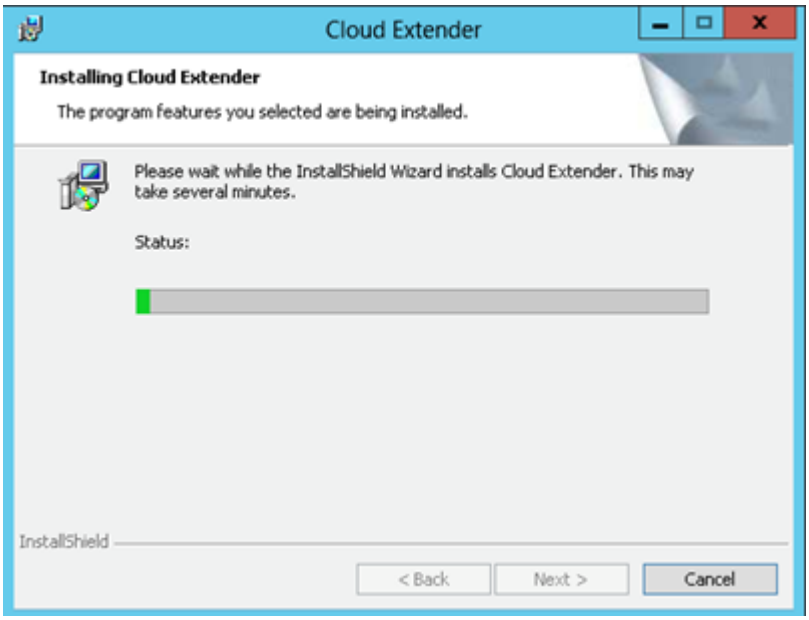
6.3.2 Procedure

1. Double-click the **MaaS360 Cloud Extender Install** icon
2. Click **Next** to advance to the Install Location screen
3. Choose your destination folder and click **Next**

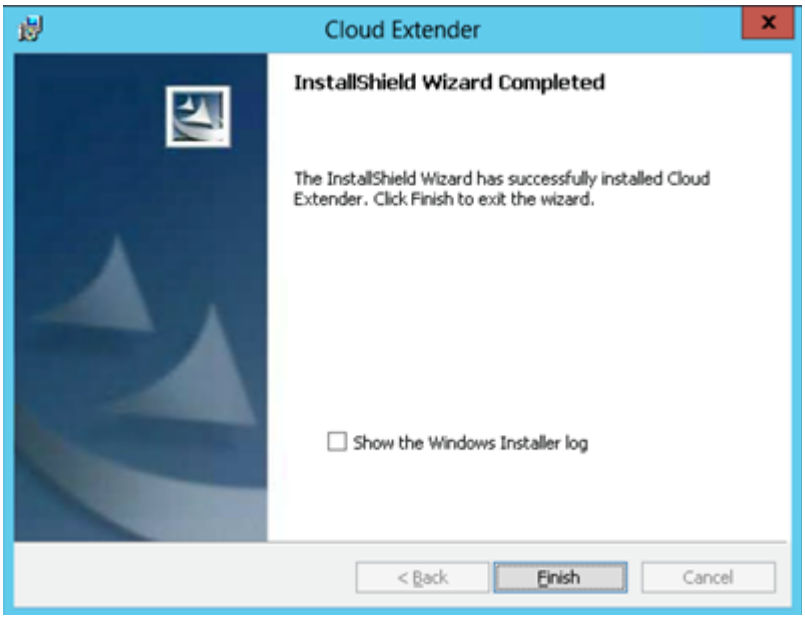
4. Type or paste the license key number and account id that you received in the Welcome email message, and then click **Next**



5. Click **Install**, and then click **Next** to continue the installation



6. When prompted, click **Finish** to start the Cloud Extender Configuration Tool



Note: After you install the Cloud Extender, the software starts automatically. If the Cloud Extender does not start automatically, you can start the software from the **Start** menu or directly from `%Program Files(x86)%\MaaS360\Cloud Extender\ASConfig.exe`.

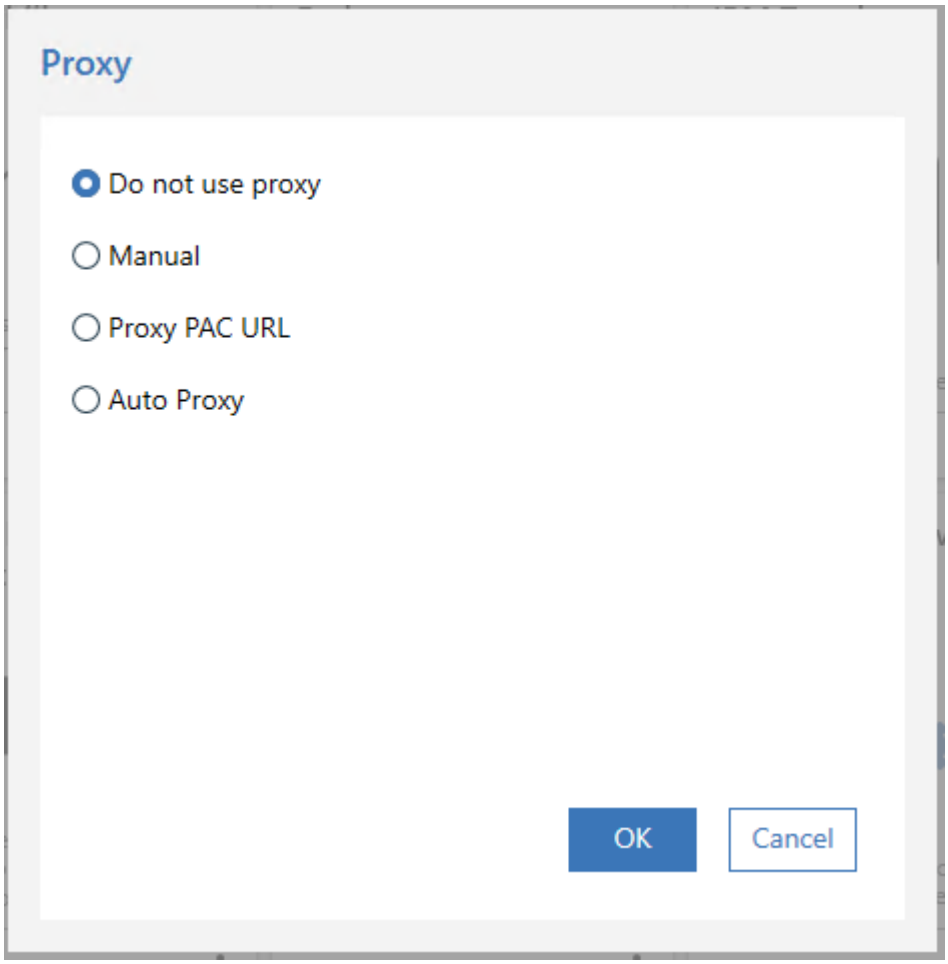
Parent topic: [Installing the Cloud Extender]

6.4 Configuring the Cloud Extender

The Cloud Extender™ software requires access to the MaaS360® Cloud to connect and to implement services. If you installed your Cloud Extender in a proxy environment, use the Cloud Extender Configuration Tool to configure the Cloud Extender.

6.4.1 Procedure

1. Select the mode for Internet access.
    a. For manual proxy configuration, the Cloud Extender supports Direct, PAC, or Auto Proxy. You can also set credentials for proxy authentication.
    b. Click the PROXY menu of the main menu in Config Tool
    c. If you do not need a proxy to access the Internet, enable the **Do not use proxy** option.



If Internet connectivity is not successful, you will be prompted with an error.

Option	Description
Do not use proxy	If the Cloud Extender is not installed in a proxy environment, select this option to establish a direct connection between the Cloud Extender and the MaaS360 Cloud
Manual	Provide a static proxy address and proxy port for your proxy server
Proxy PAC URL	Provide the URL of the proxy PAC file hosted in your environment
Auto Proxy	Automatically search for the Proxy PAC file from your DNS or DHCP server
Use Proxy Authentication	If your proxy requires authentication, select this option and provide the service account credentials (user name, domain, and password) to authenticate against your proxy

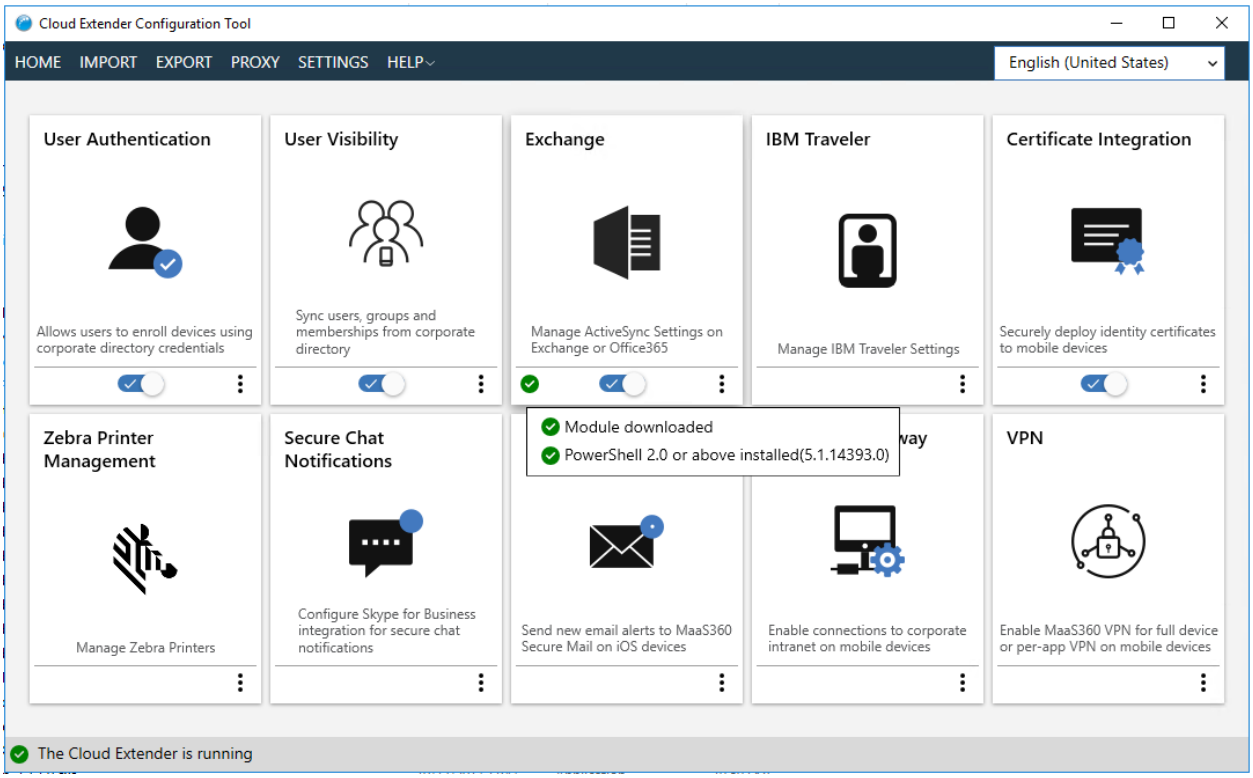
Note: To prevent Antivirus/scanning software from quarantining the Cloud Extender executable and other configuration files, make sure that the Cloud Extender directories are allowed in the exclusion list.

2. Select the module you wish to configure from the available module tiles.

Note: For more information about each service/module, see Configuring Setting for the Cloud Extender Modules.

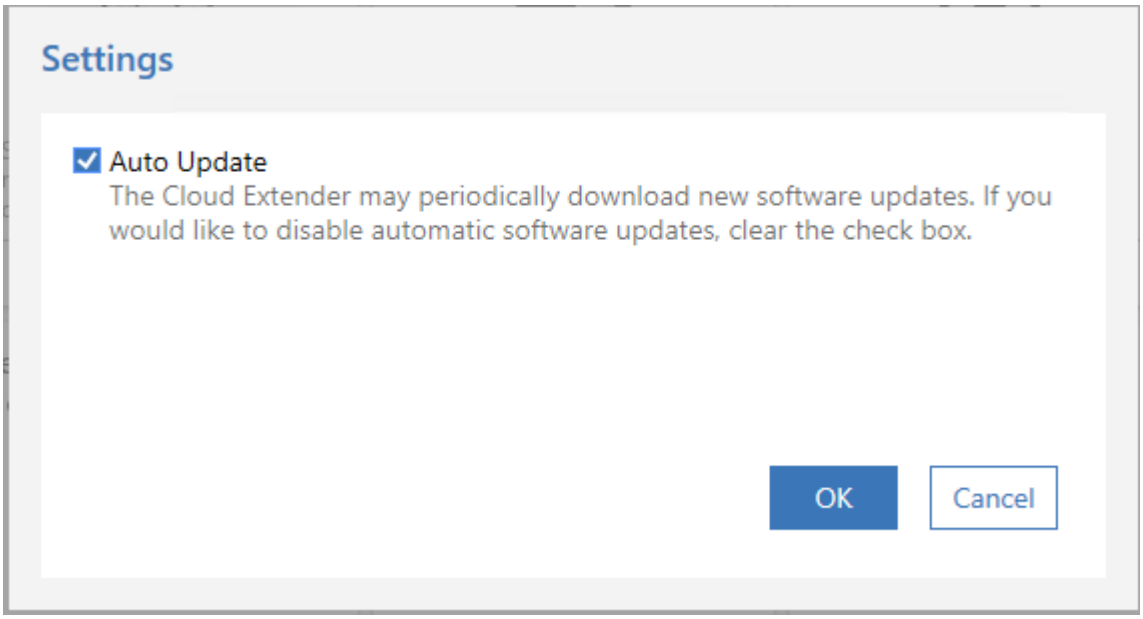
Important: If you are missing a module, contact IBM® Support or send an email to `ops@fiberlink.com` with your question.

3. Verify that each module you wish to configure meets any prerequisites. Module prerequisite status can be viewed by hovering your mouse over the module tile and then hovering over the green checkmark or red X in the lower left of the tile:



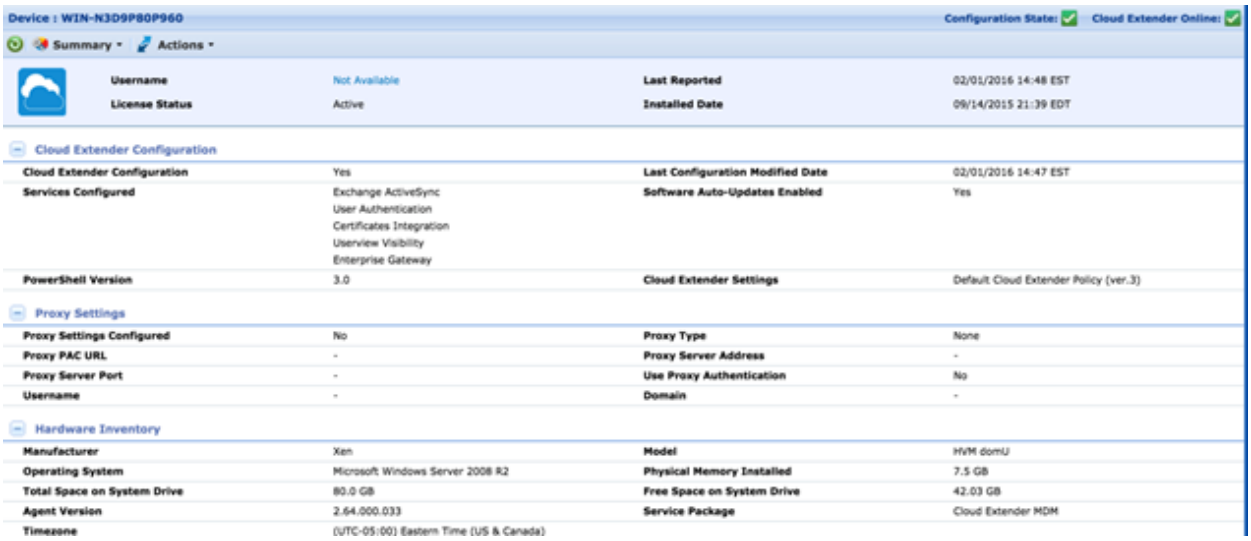
Note: you can view the status of modules any time by selecting **Status** from the **HELP** menu.

4. Configure automatic update by clicking the **SETTINGS** menu. Automatic updates are enabled by default. You may disable automatic updates by unchecking the checkbox and click **OK**:



With Automatic Updates enabled, the Cloud Extender will download the most recent modules available for installation. With Automatic Updates disabled, modules will still be downloaded when the Cloud Extender first runs, but updates will need to be enabled to receive future module upgrades.

5. Once you have completed module configuration, the Cloud Extender collects data and uploads that data to the MaaS360 Portal.
   You can check this process by logging in to the MaaS360 Portal with your portal URL and selecting **Setup** > **Manage Cloud Extenders** workflow. The Cloud Extender in the MaaS360 Portal shows connection status and the configured services. However, depending on the speed of your installation and the number and the size of enabled modules, you might see a slight delay with updated status information.



Device : WIN-N3D9P80P960 | Configuration State: | Cloud Extender Online:

Summary | Actions

Username	Not Available	Last Reported	02/01/2016 14:48 EST
License Status	Active	Installed Date	09/14/2015 21:39 EDT

Cloud Extender Configuration

Cloud Extender Configuration	Yes	Last Configuration Modified Date	02/01/2016 14:47 EST
Services Configured	Exchange ActiveSync User Authentication Certificates Integration Userview Visibility Enterprise Gateway	Software Auto-Updates Enabled	Yes
PowerShell Version	3.0	Cloud Extender Settings	Default Cloud Extender Policy (ver.3)

Proxy Settings

Proxy Settings Configured	No	Proxy Type	None
Proxy PAC URL	-	Proxy Server Address	-
Proxy Server Port	-	Use Proxy Authentication	No
Username	-	Domain	-

Hardware Inventory

Manufacturer	Xen	Model	HVM domU
Operating System	Microsoft Windows Server 2008 R2	Physical Memory Installed	7.5 GB
Total Space on System Drive	80.0 GB	Free Space on System Drive	42.03 GB
Agent Version	2.64.000.033	Service Package	Cloud Extender MDM
Timezone	(UTC-05:00) Eastern Time (US & Canada)		

Parent topic: [Installing the Cloud Extender]

6.5 Configuring Settings for the Cloud Extender Modules

Information about configuring settings for the Cloud Extender™ modules.

User Authentication Module

The User Authentication module integrates with your Active Directory (AD) or LDAP environment to authenticate users by using various workflows within MaaS360®. With this module, your users can reuse corporate credentials without having to generate and manage a new set of credentials.

User Visibility Module

The User Visibility module manages mobile devices based on corporate directory structure. With this module, administrators can manage user devices that belong to specific groups, and target apps, policies, and content to user devices that are members of a specific directory group.

Exchange (On-Premises and Cloud) Integration Module

The Cloud Extender integrates with Exchange servers and provides complete visibility to all ActiveSync devices that are connected to the mail system.

IBM Traveler Integration Module

The Cloud Extender integrates with IBM® Traveler and IBM SmartCloud® environments to provide complete visibility to all ActiveSync devices connected to the mail system.

Certificate Integration Module

The Certificate Integration module allows users to use their existing Certificate Authority (CA) and auto-provision device and user certificates to enrolled devices. Certificates are used for email, Wi-Fi, VPN, or Secure Mail authentication.

Exchange Integration for Real-Time Mail Notifications Module

MaaS360 uses the Exchange Integration for Real-time Mail Notifications module to support real-time email notifications for iOS and Windows Phone devices.

Mobile Enterprise Gateway (MEG) Module

IBM MaaS360 Mobile Enterprise Gateway (MEG) provides simple, seamless, and secure access to behind-the-firewall information resources for mobile users beyond implementing a new VPN-like technology.

MaaS360 VPN Module

The MaaS360 VPN module is a VPN solution that allows users to access their corporate network from an iOS or an Android device.

Parent topic: Cloud Extender Admin Guide

7 User Authentication Module

The User Authentication module integrates with your Active Directory (AD) or LDAP environment to authenticate users by using various workflows within MaaS360®. With this module, your users can reuse corporate credentials without having to generate and manage a new set of credentials. The Cloud Extender™ facilitates AD/LDAP authentication for the following scenarios:

1. Mobile device self-service enrollment into MaaS360
2. User portal access to manage devices
3. When authentication is required before accessing secured applications and documents
4. When a workplace PIN is reset by the user
5. MaaS360 administrator authentication for portal access
6. Signing into shared devices

The Cloud Extender receives the credentials securely from the MaaS360 Cloud (client originated) and validates those credentials against your directory server. The credential information is passed from the client through theMaaS360 Cloud to your Cloud Extender, but the information is not stored locally.

7.1 Modes of Operation

The Cloud Extender integrates with the corporate directory by using the following modes:

1. Active Directory Mode: This mode is specific to Microsoft Active Directory environments. The Cloud Extender runs as a service account and runs PowerShell commands to authenticate any user in your directory. If you have multiple trusting forests or domains in your environment, some additional configuration is required. In this mode, the Cloud Extender can authenticate users in the entire scope of your directory.
2. LDAP Mode: This mode is used for any corporate directory. The Cloud Extender offers standard LDAP templates to integrate with Domino® LDAP, Oracle LDAP, Novell eDirectory, and OpenLDAP. In addition to these standard LDAPs, use this mode to configure against any customized LDAP. The Cloud Extender also provides a template to help you configure Microsoft Active Directory in LDAP mode.

To determine which implementation mode to use for your environment, consider these guidelines:

1. If you are not using Microsoft Active directory (AD), use LDAP mode.
2. If you are using Microsoft Active directory (AD), the following table provides LDAP options for your environment:

Table 4. Determining which LDAP implementation mode to use for your environment

Scenario	**Active Directory Mode**	**LDAP Mode**
Ability to limit authentication scope to a certain OU, subtree, or group		✓
Requirement that the Cloud Extender needs to be part of your domain	✓	
Ability to support trusted forest/domain authentication	✓	✓
Ability to support untrusted forest/domain authentication		✓
Ability to customize attributes that are read from AD during the user authentication process		✓
Support for User Custom Attributes (1)		✓
Ability to customize user and group filters for optimized user authentication performance		✓
Support for High Availability (HA)	✓	✓
Ease of configuration	Easy	Medium
Implementation technology	.NET Libraries	LDAP Libraries
Configured along with User Visibility on the same Cloud Extender (2)	✓	✓
Time to authenticate	Limited to .NET Libraries	Typically faster than AD

In most situations, the LDAP mode of authentication is the implementation of choice even in Microsoft Active Directory environments with

consideration to the advantages listed in the table and easy adaptability to future requirements.

7.2 Requirements and Scaling

The User Authentication module for LDAP or Active Directory does not have scaling limits. However, the following specifications are the minimum requirements that are needed by a server to incorporate scaling. Increase these limits for better server functions and usability.
In large environments, deploy separate instances of the Cloud Extender to service Corporate Directory Integration and to provide predicable performance of all functions. You can deploy as many instances of the Cloud Extender as needed. However, enable at least two User Authentication modules on two instances of the Cloud Extender for redundancy.

Table 5. Scaling requirements for the User Authentication module

Item	Minimum Requirement
Scaling (for both Active Directory and LDAP implementations)	**CPU**: 2 Cores **Memory**: 2 GB to 8 GB **Storage**: 50 GB **Scaling**: One Cloud Extender for 10,000 devices and one Cloud Extender for High Availability (HA) Supports installation on multiple instances of the Cloud Extender Install on a dedicated Cloud Extender or enabled on Cloud Extender with the User Visibility, Certificate Authority Integration, Exchange Integration, or IBM® Traveler Integration services enabled. For accurate scaling of your environment, see the Cloud Extender scaling document at

	Setup > **Services** > **Enterprise Email Integration**.
Network Traffic	Authentication request/response = 1 KB per request
Active Directory	Hardware specs meet minimum Requirements PowerShell 3.0+ installed Windows operating system is joined to the domain Service Account Domain User Password does not Expire Non-interactive account Local Administrator on the Cloud Extender server
LDAP	Hardware specs meet minimum Requirements Service Account Username and password to bind to LDAP server Password does not expire Non-interactive account

User Authentication Service Configuration
Follow these steps to configure the User Authentication service for the Cloud Extender.

Basic Configuration: Active Directory Mode
Follow these steps to configure basic Active Directory mode settings for user authentication.

Advanced Configuration: Active Directory Mode Cross-Forest and Domain Authentication

Follow these steps to configure advanced Active Directory mode settings if you implemented the Cloud Extender in Active Directory mode, you are working in a multi-forest/multi-domain environment, and the forest and domains have a trust (minimum of one-way trust from the Cloud Extender domain).

Basic Configuration: LDAP Mode

Follow these steps to configure basic LDAP mode settings for user authentication.

Advanced Configuration: LDAP Mode

The values for Advanced LDAP configuration mode are populated with default configuration settings based on the LDAP server type that you selected. Use this option if you need to edit these values for your environment.

Enabling Health Check Alerts for User Authentication

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender module.

Troubleshooting Issues with User Authentication

Troubleshooting issues with authenticating users for the Cloud Extender.

Parent topic: Configuring Settings for the Cloud Extender Modules

1 User Custom Attributes is a feature in MaaS360 where you define your own attribute and use this attribute in various configuration workflows. For example: You define a User Custom Attribute that is called `Employee Serial Number` and use this value in MaaS360 policies for device configuration, application configuration, or a part of Identity Certificates. This attribute can be read directly from your directory by using the LDAP configuration.

2 Consider whether to configure the User Visibility service along with the User Authentication service for your Cloud Extender. If so, then the mode of configuration for both these services is either Active Directory or LDAP.

For example, User Authentication as AD and User Visibility as LDAP on the same Cloud Extender is not possible. If you require this combination, you must use separate instances of the Cloud Extender.

7.3 User Authentication Service Configuration

Follow these steps to configure the User Authentication service for the Cloud Extender™.

Procedure

Open the Cloud Extender Configuration Tool and select the **User Authentication** tile.

Select **Active Directory**.

Choose the mode of authentication that you want to configure. For Active Directory, select **Allow any user in directory**, for LDAP select **Allow users only in specific groups and organizational units (OU) t**hen click **Next**.

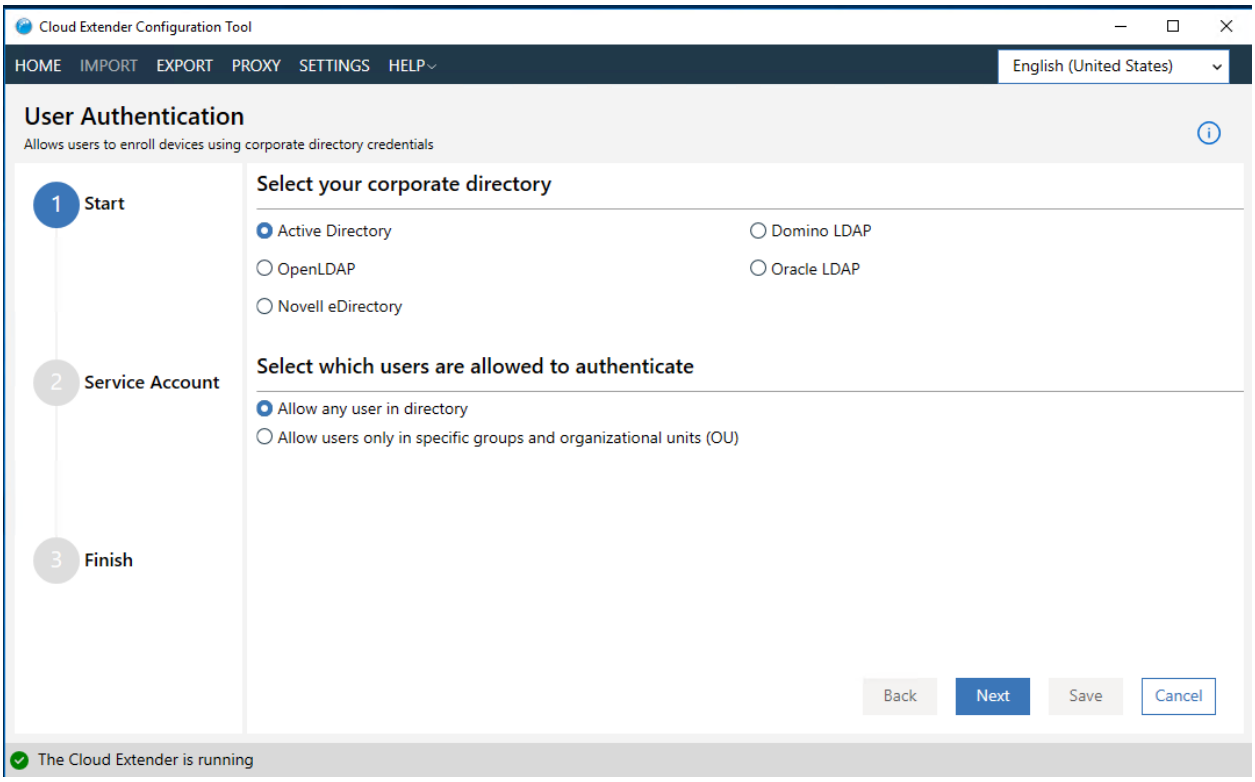
Parent topic: User Authentication Module

7.4 Active Directory Mode Configuration

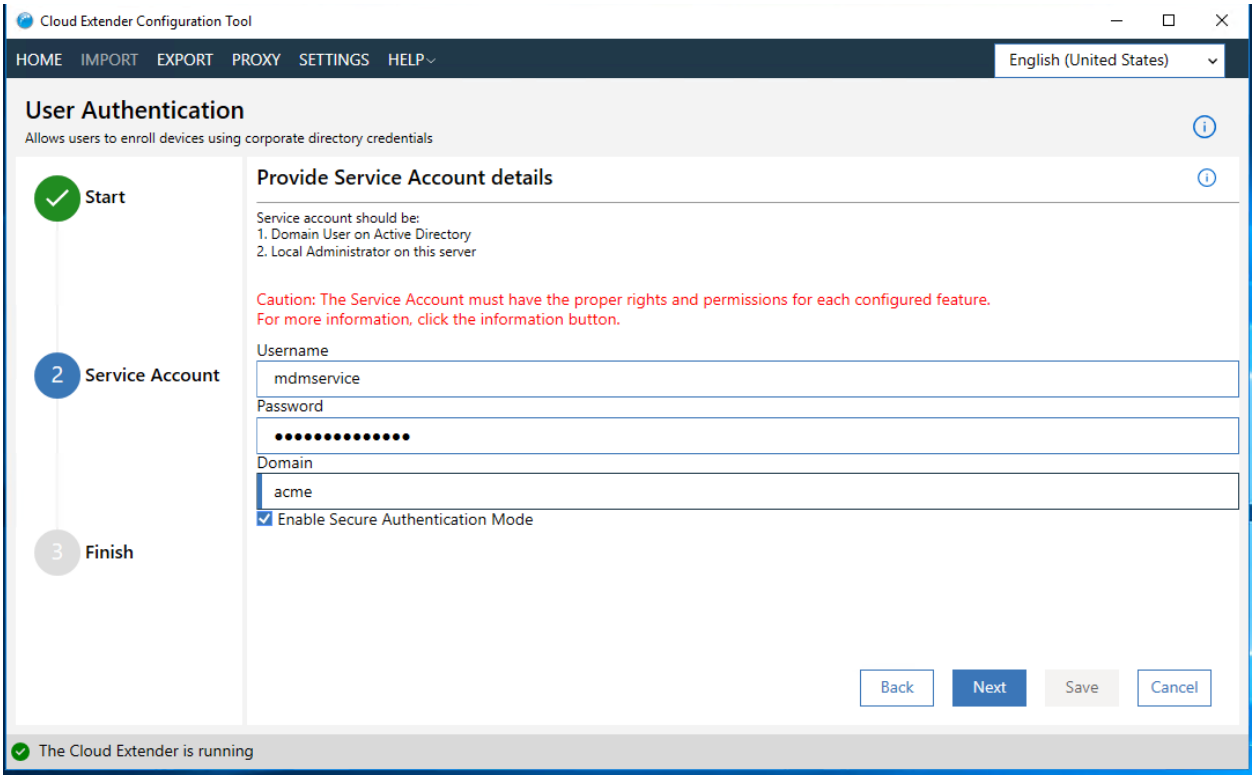
Follow these steps to configure basic Active Directory mode settings for user authentication.

7.4.1 Procedure

1. Select Active Directory mode

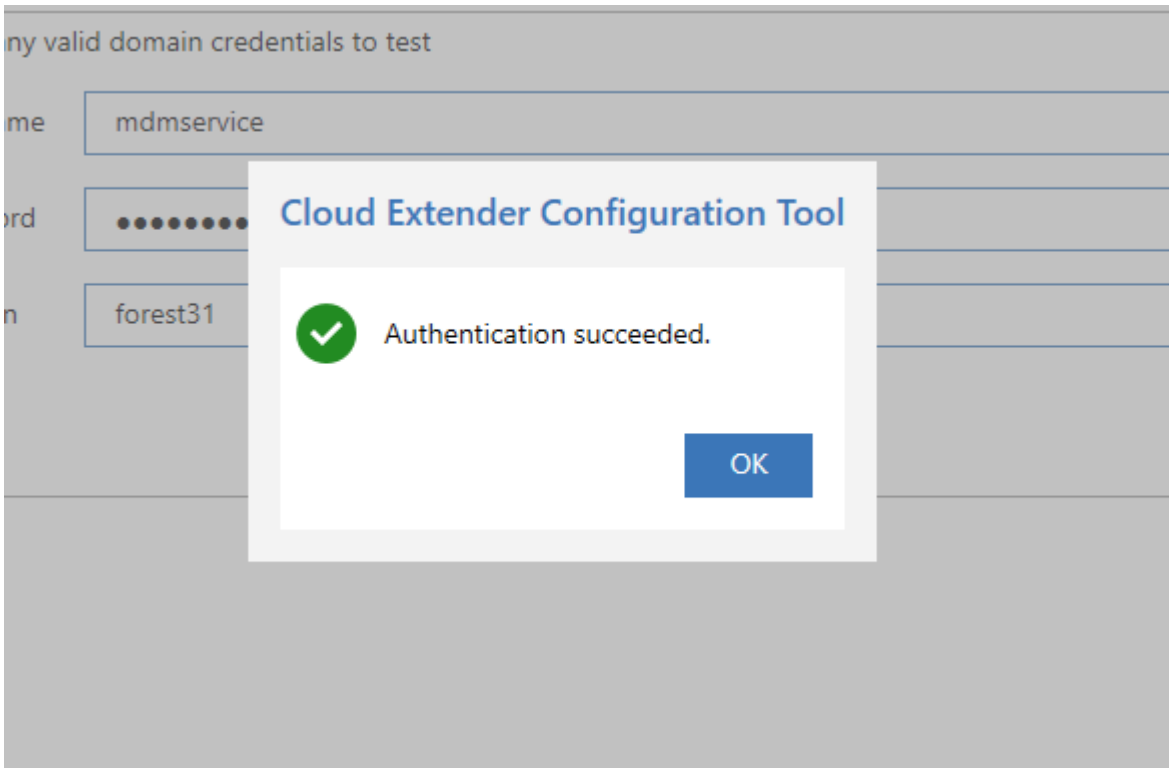


2. Complete the service account configuration:



Option	Description
Username	The service account username must be a local administrator on the Cloud Extender™ server.
Password	The service account password must not expire. If your corporate policy requires you to change the service account password on a periodic basis, make sure that you update the password from the Cloud Extender Configuration Tool.
Domain	The domain of the service account.
Enable Secure Authentication Mode	Enable this option if your environment is configured for secure authentication.

3. Click **Next**
4. To run a test authentication, enter a valid username, password and domain then click the **Test** button.



5. Click the **Save** button to complete configuration.

Parent topic: [User Authentication Module]

7.5 Active Directory Mode Configuration for Cross-Forest and Domain Authentication

Follow these steps to configure advanced Active Directory mode settings if you implemented the Cloud Extender™ in Active Directory mode, you are working in a multi-forest/multi-domain environment, and the forest and domains have a trust (minimum of one-way trust from the Cloud Extender domain).

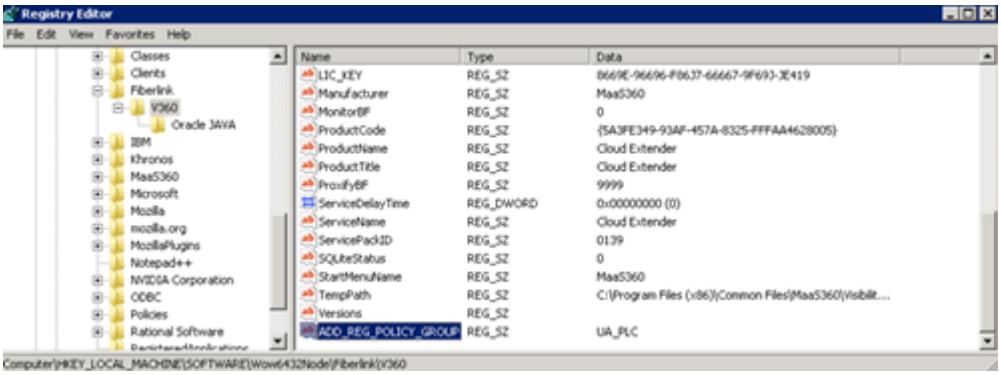
7.5.1 About This Task

You must configure extra settings for the Cloud Extender to authenticate users in other forests and domains. Your domain must be trusted. If you have multiple forests, you must have at least one-way trust from the domain of the Cloud Extender server to other target domains. You must modify or add registry keys manually for theCloud Extender to support multi-domain/forest authentication because these keys exist and must be overwritten.

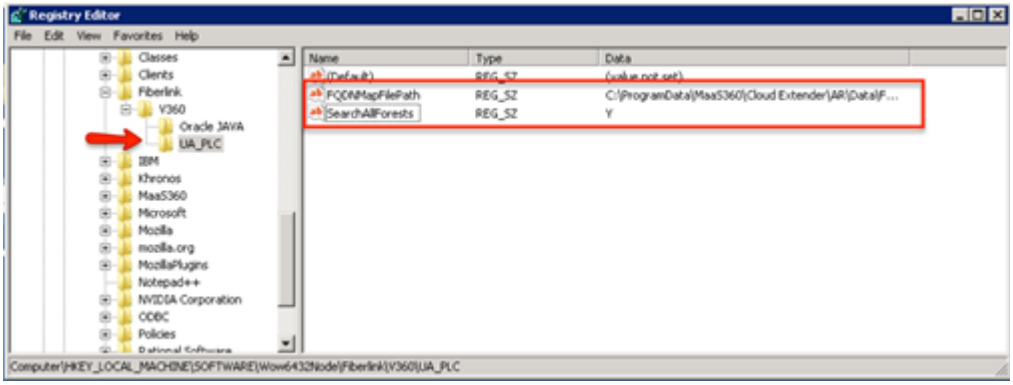
7.5.2 Procedure

Configure the Cloud Extender in multi-domain mode by setting a registry key as follows:

1. Open the Registry Editor (`regedit.exe`) on the Cloud Extender server.
2. From `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360`, create a value in the V360 key:
   a. `"ADD_REG_POLICY_GROUP"="UA_PLC”`.
   Note: If the `ADD_REG_POLICY_GROUP` key exists, you must append `UA_PLC` to the list separated by a semicolon (;).



3. Create a key under the V360 key named `UA_PLC`.
   a. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\UA_PLC`
4. Create two new string values under `UA_PLC`:
   a. `"FQDNMapFilePath"="C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data\FQDNMap.txt""SearchAllForests"="Y"`



5. Create a mapping of all your trusted domains in new text file called `FQDNMap.txt` by using any plain text editor. This mapping file is a text file that contains one entry per line of text for each domain in the environment. Each line entry in the file looks like the following example, with the short domain to the left of the `=` (equals) sign and the `FQDN` to the right of the `=` (equals) sign: `shortDomainName=FQDN` and `FQDN=FQDN` (make sure to map both combinations).

   For example: You have three domains: `everest` and `mckinley` under `f01.example.local` root and another domain `k2` under the `example.local` forest. Your domain mapping file looks like the following example:

   everest=everest.f01.example.local

mckinley=mckinley.f01.example.local
k2=k2.example.local
everest.f01.example.local=everest.f01.example.local
mckinley.f01.example.local=mckinley.f01.example.local
k2.example.local=k2.example.local

NOTE: each line in the file must end with either a `<CRLF>` (DOS line ending convention) or a `<LF>` (UNIX line ending convention.)

6. Save the file as `FQDNMap.txt`.
7. Copy the FQDN Map File `FQDNMap.txt` to the folder: `C:\ProgramData\MaaS360\Cloud Extender\AR\Data\`.
8. Restart the Cloud Extender service.
9. Test authentication again on all domains to make sure that the configuration is complete.

Parent topic: [User Authentication Module]

7.6 LDAP Mode Configuration

Follow these steps to configure basic LDAP mode settings for user authentication.

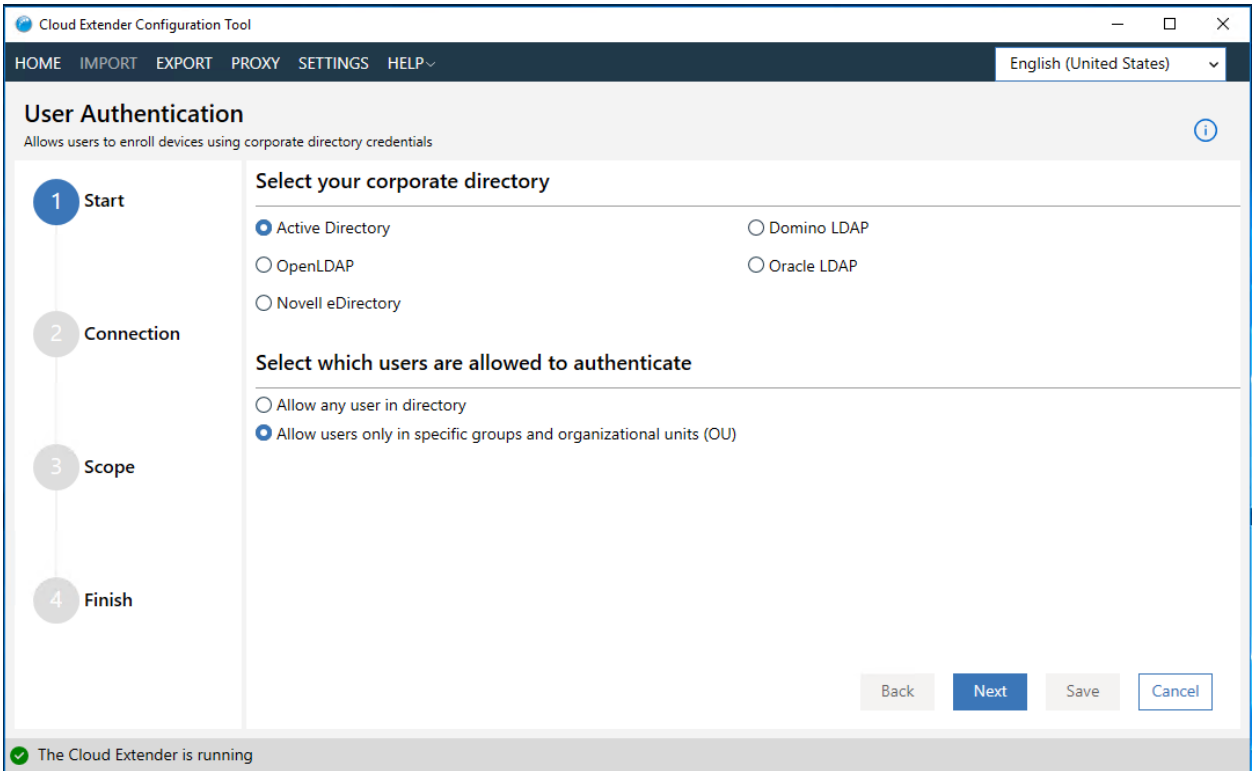
7.6.1 Before You Begin

Make sure that you can connect to your LDAP server through telnet or any other mechanism before you set up the Cloud Extender™.

7.6.2 Procedure

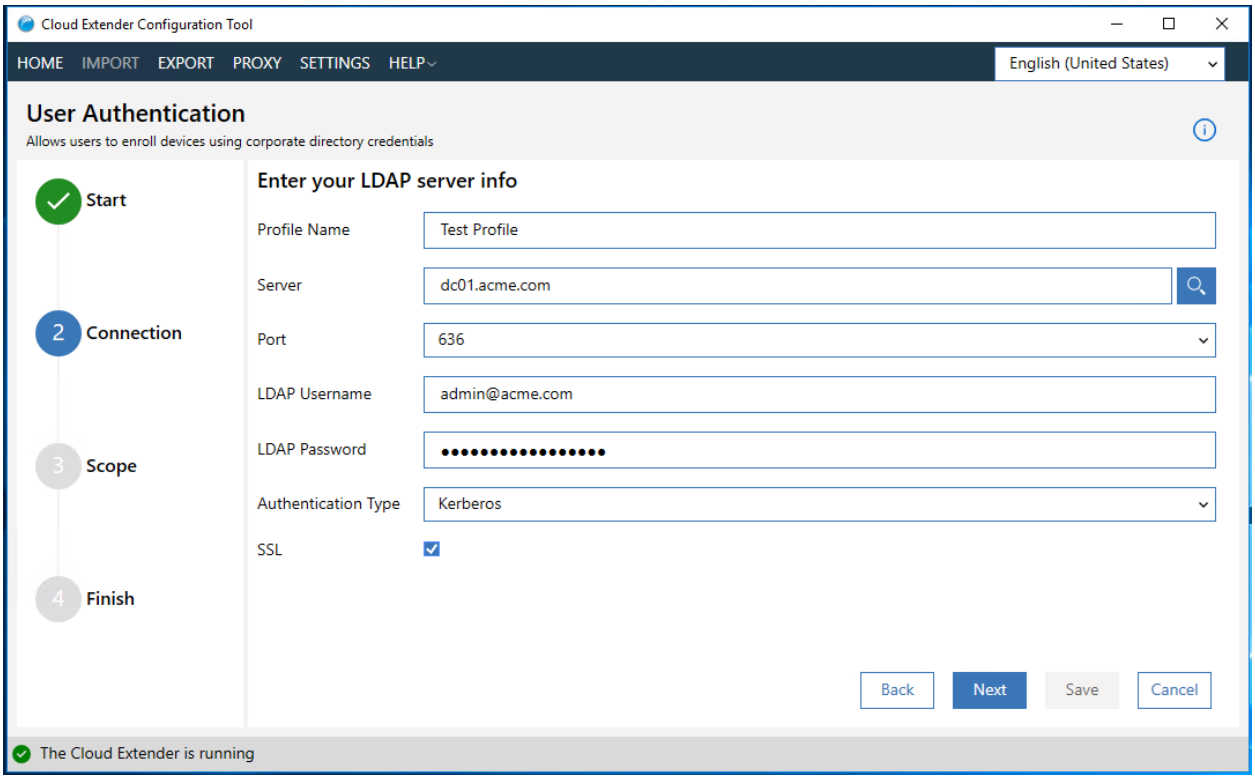
Configure your LDAP setup by using the following options:

1. Select the User Authentication tile from Config Tool Modern
2. Select **Active Directory** and **Allow users only in specific groups and organizational units (OU)**



3. Click **Next**
4. Fill in the following fields:

Parameter	Description
Profile Name	The name of your authentication profile. The Cloud Extender for LDAP authentication supports multiple authentication profiles for crossforest/cross-domain authentication.
Server	The host name of your LDAP server. The Cloud Extender supports multiple LDAP servers when they are mirroring LDAP servers. Click on the magnifying glass icon to search for available LDAP servers.
Port	The port of your LDAP server.
LDAP Username	The admin username of your service account. This account is used to bind to LDAP to authenticate other users. Some implementations of LDAP accept the bind username in a standard format like `user@company.com`, while other LDAP implementations might require a Distinguished Name (DN) of the user. The following list provides an example of the DN format: `uid=username,c=us,ou=subdom ain,dc=company,dc=com`
LDAP Password	Password for the given LDAP username
Authentication Type	Authentication type for your LDAP installation. You can choose from: Kerberos NTLM Basic Digest
SSL	If your LDAP configuration supports SSL connections, you can check this box to enable secure connections



5. Click **Next**
6. Fill in the following fields:

Parameter	Description

Search Attribute	The name of the LDAP field that identifies the user in your directory. The name varies between the LDAP types and you can use only one attribute.
	The following list includes common user search attributes:
	
	Active Directory:
	`samAccountName`
	`(DOMAIN\username)email`
	`(user@company.com)`
	`userPrincipalName`
	`(user@domain.company.com)`
	
	OpenLDAP:
	`mail`
	`(user@company.com)uid`

	(user) Novell: eDirectorymail (user@company.com)cn (user) Oracle LDAP: loginid (user)mail (user@company.com)uid (user) IBM Domino LDAP: cn (user)mail (user@company.com)uid (user)
User Search Base	The search base for users is the root location in your directory from where all users are searched. The Cloud Extender discovers any user under the hierarchy. Enter the Distinguished Name (DN) of the Organization Unit (OU) that has users.
Group Search Base (optional)	The search base for groups is the location on your directory that includes all defined user groups. This option is similar to the **LDAP Search base for Users** option. The Cloud Extender uses this attribute to discover all groups from this root location.

Note: When configuring search bases, the four icons are available for the following purposes:

- Plus – manually add search base to the list
- Minus – remove the currently highlighted search bases from the list
- Edit – edit the currently highlighted search base
- Search – clicking this icon will trigger Config Tool to scan your LDAP directory and display all contents where you can choose your search base from the display

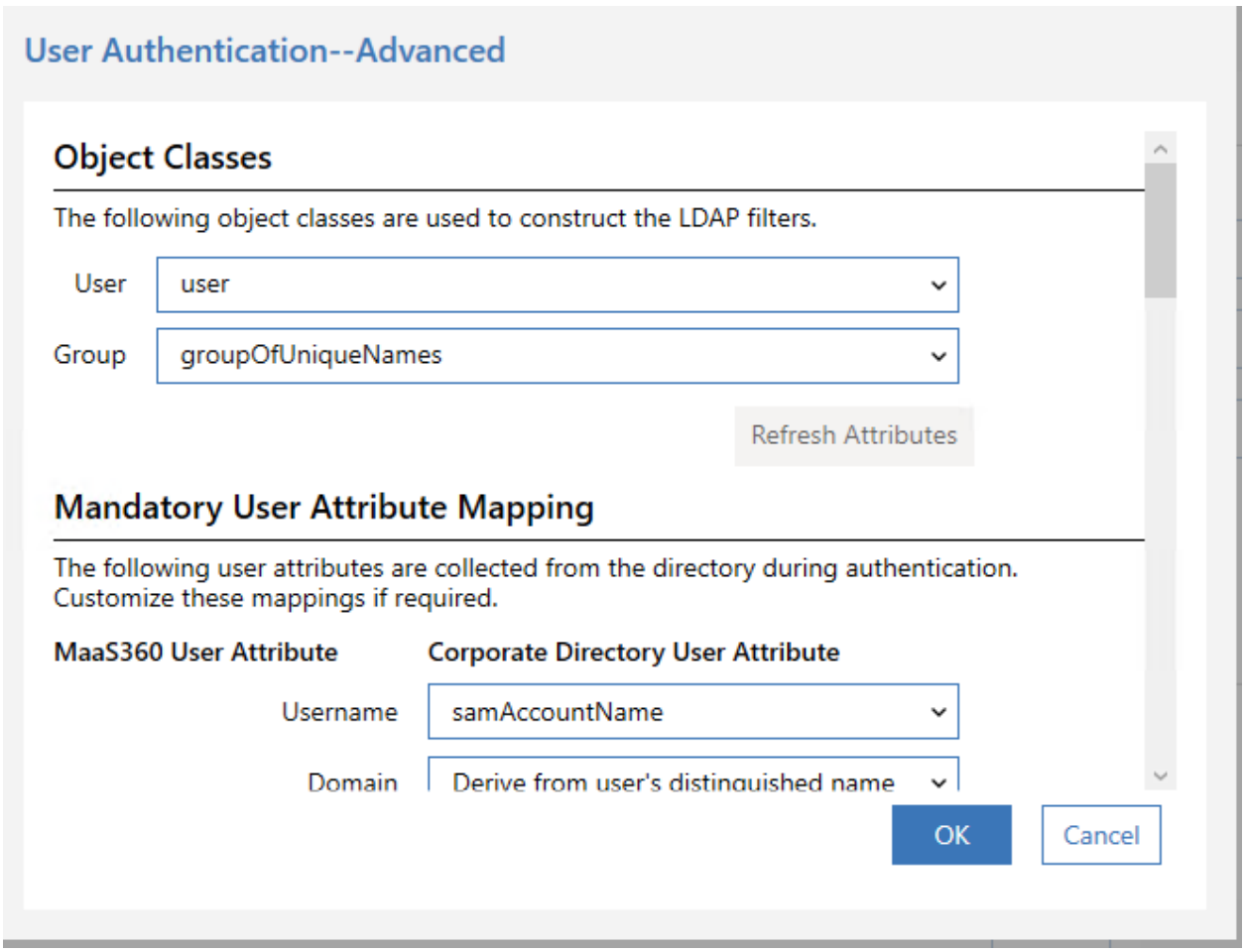
7. Click **Next**
    a. If a failure message is displayed, check LDAP connectivity from the Cloud Extender server, port, credentials, and authentication type.
8. To run a test authentication, enter a valid user name, password and domain then click the **Test** button
    a. If successful, you will be presented with a dialog box showing some of the attributes of the test user
9. Click the Save button

If you wish to add more User Authentication profiles, click on the User Authentication tile again and click **Add New Profile** button.

Parent topic: [User Authentication Module]

7.7 LDAP Mode Advanced Configuration

On the final view of the LDAP User Authentication configuration, you can click the **Advanced** button to make further modifications to your LDAP configuration.



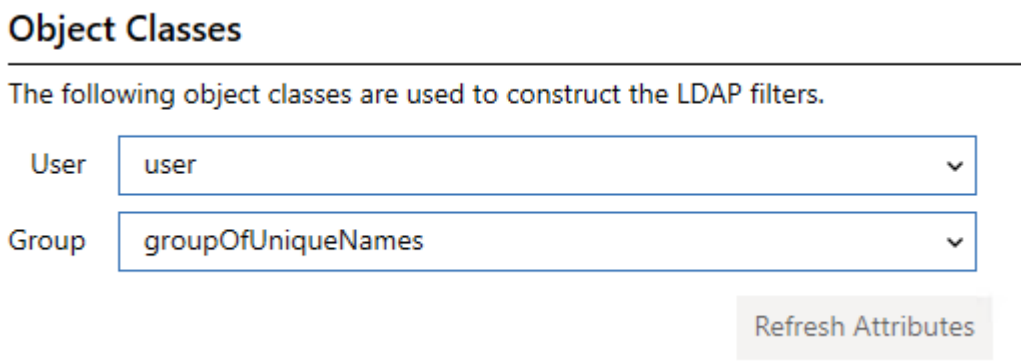
The values in this advanced view are populated with default configuration settings based on the LDAP server type that you selected. Use this option if you need to edit these values for your environment. Use Advanced LDAP configuration with the following scenarios:

1. If you are using OpenLDAP, you must configure how the Cloud Extender™ looks for users and groups.
2. Must read specific attributes of users during the authentication process.
3. Must map user properties on MaaS360® to specific fields in your LDAP.

4. Must support user custom attributes.

The advanced view will allow you to modify the following configuration values:

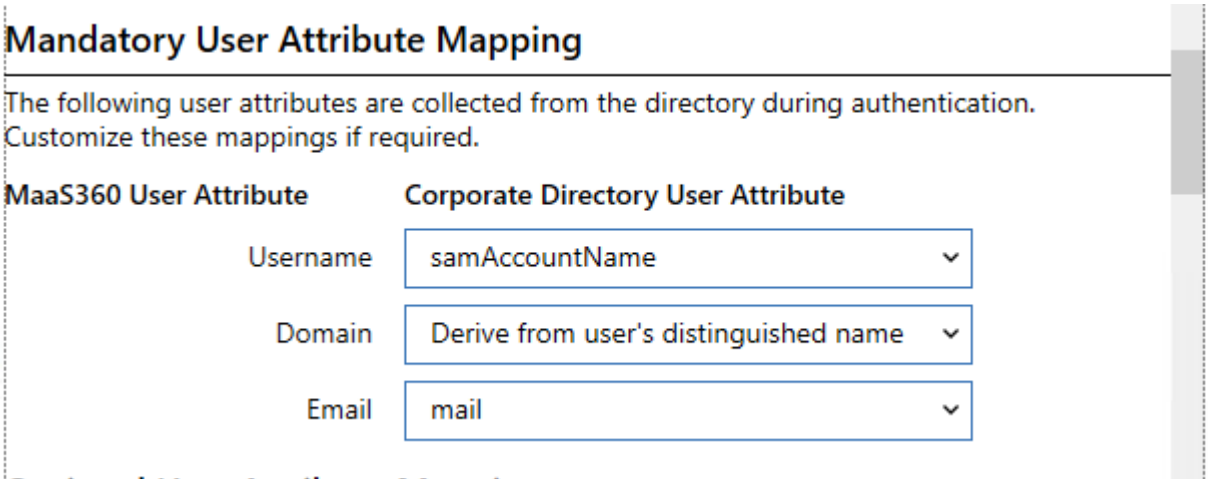
1. **Object Classes Configuration**
   LDAP Object Classes define a type of object in LDAP. Every user and every user group on LDAP uses a specific Object Class. With the Object Class, you can list all objects that have that Object Class. After you set up a User Authentication profile, select the Object Class of your users and groups from the options provided in the list boxes shown below:



Object Class	Description
User	The object class that identifies the type of all your users. The Cloud Extender uses the Basic mode configuration and queries your LDAP for all possible Object Classes for users and lists. If the Object Class for your users is not automatically discovered or is not featured on the select list, type the `Object Class` for users.
Group	The object class that identifies the type of all your user groups

2. **Mandatory User Attributes Configuration**
   During the authentication process, the Cloud Extender reads certain attributes of the user from your directory that it requires for other

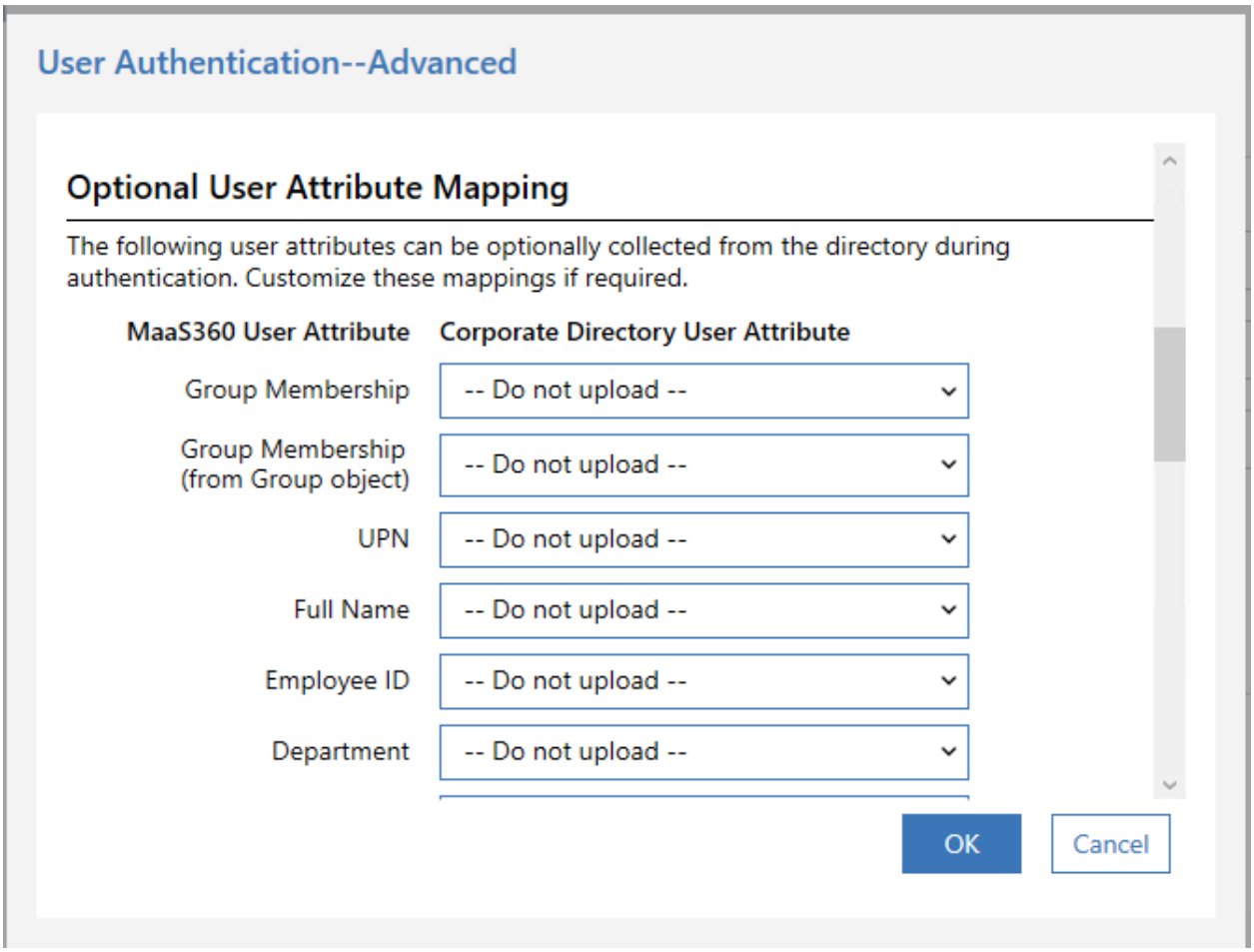
configuration aspects after a device is enrolled in the MaaS360 Portal.



Attribute	Description
User name	The Cloud Extender uses the **User Search Attribute Name** to search for the user in LDAP. This user is the user who is trying to enroll the device. You can pick the same attribute here. If you need to represent users by a different attribute in MaaS360 (for example, by email address), select a different attribute. **Note:** This attribute is part of the *%username%* variable in MaaS360. Use this variable in MaaS360 policies to configure email on mobile devices. This variable converts to the user name for the user's email configuration.
Domain	The domain of the user. You use the domain to configure email on the mobile device. You can map the domain field to a specific attribute on your directory or derive the domain from the user's Distinguished Name (DN).

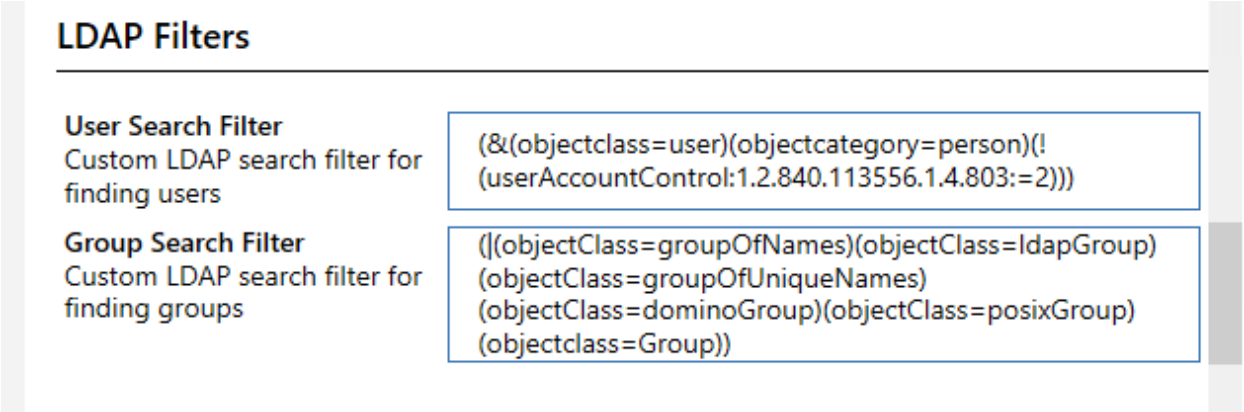
	The following list provides an example of the DN format: `uid=username,c=us,ou=subdomain,dc=company,dc=com` From the example, if your domain is set to **Derive from DN**, the domain is `company.com`.
Email	The email address of the user. Use this address to configure email on the device.

3. **Optional User Attribute Mapping**
   In addition to Mandatory User Attributes, the Cloud Extender module for User Authentication reads optional user attributes during the authentication process. These values are uploaded to the MaaS360 Portal and are used later for grouping devices or as configuration parameters. The User Principal Name (UPN) is a common field that is read during authentication. The following window provides a standard list of user attributes on MaaS360 that can be mapped to the user's attribute on your directory.



Note: This mapping is typically more relevant for User Visibility configuration. The User Visibility module reads these attributes periodically and updates the MaaS360 console with changes on an ongoing basis. The User Authentication module reads these attributes just one time during the user authentication process.

4. **LDAP Filters**
   Use this option to filter the list of users that the Cloud Extender discovers, such as filtering only by active users or by users that belong to specific departments. Use the standard LDAP filter queries to further optimize your user searches.



7.7.1 Next Steps

The MaaS360 Portal offers the Cloud Extender Scaling Tool at **Setup** > **Services** > **Enterprise Email Integration**. Enter the number of users/devices that you plan to enroll for MaaS360 and determine how many Cloud Extenders you might need to support this scale.

Install the specified number of Cloud Extenders in a High Availability (HA) environment. To install the Cloud Extender for User Authentication in an HA environment, implement the same steps on all Cloud Extenders that have the User Authentication module enabled (including any new Cloud Extenders that are added in the future).

The Cloud Extender also offers an **Export Configurations** option that you use to export all details from one Cloud Extender to import those details to another Cloud Extender.

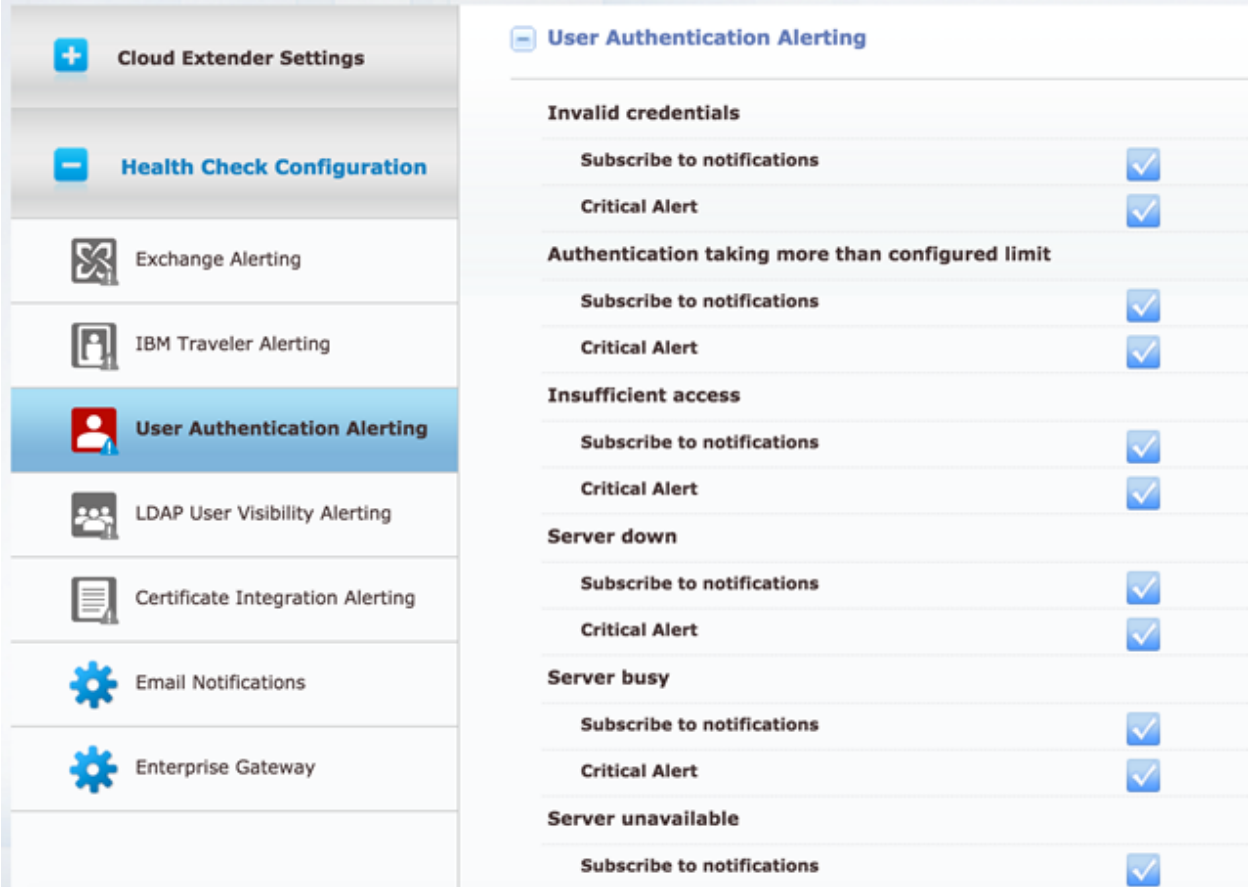
Parent topic: [User Authentication Module]

7.8 Enabling Health Check Alerts for User Authentication

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ module.

7.8.1 Procedure

1. From theMaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.
2. Select **Health Check Configuration** > **User Authentication Alerting**. The User Authentication Alerting list is displayed.



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a

description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
Invalid credentials	The service account credentials are expired or invalid. The Cloud Extender cannot connect to the configured LDAP server because the server is unreachable or the service account credentials are invalid.	Verify that LDAP is operational. Check for recent firewall or proxy changes that might block access to the LDAP server. Check whether the bind administrator credentials are valid and not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the credentials. Check whether any intrusion detection software in your network might be locking the bind administrator account. If the account is locked, add the account to the allow list to prevent the intrusion detection software from locking the account. If this issue continues, collect logs from the Cloud Extender, and then contact IBM® Support for further assistance.
Authentication taking more	The User	Verify that scanning software is not

than configured limit	Authentication service is taking more time to complete than the configured limit.	scanning the Cloud Extender services and causing a delay during the authentication process. If you are using LDAP mode, verify that the search base for users is not that wide. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to limit the scope of the search base and use filters for Users and Groups to optimize search performance. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Insufficient access	Insufficient permissions on the LDAP bind administrator account is causing an insufficient access error response from the LDAP server for certain LDAP operations.	Verify that the LDAP bind administrator account uses the necessary permissions to execute Bind, Query, and Filter operations on LDAP. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind

		administrator account. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server down	The authentication LDAP server is down. The Cloud Extender cannot connect to the directory server because the directory server is down or the Cloud Extender configuration is invalid.	Verify that the configured LDAP server is reachable from the Cloud Extender server. Use the Cloud Extender reachability test to confirm that the LDAP server is reachable from the Cloud Extender server. Check whether the bind administrator account is still active and the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind administrator account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server busy	The authentication LDAP server is busy. The Cloud Extender cannot process the client request because the LDAP server is busy.	Check whether the LDAP server is low on system resources. Check whether other applications are also using LDAP resources during this time period.

		Review the LDAP server performance and contact internal or vendor teams for assistance with resolving this issue.
Server unavailable	The authentication LDAP server is unavailable. The Cloud Extender cannot process the LDAP bind request with the configured bind administrator credentials because the LDAP server might be unavailable.	Verify that the configured LDAP server is reachable from the Cloud Extender server. Use the Cloud Extender reachability test to confirm that the LDAP server is reachable from the Cloud Extender server. Check whether the bind administrator account is still active and the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind administrator account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

7.8.2 Troubleshooting Issues with User Authentication

Troubleshooting issues with authenticating users for the Cloud Extender™.

1. **Authentication or reachability errors during setup**

When you set up the Cloud Extender for user authentication, debug errors by accessing the following log:
`C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data`.

Review the `LDAPAuthTest_Debug.log` and `LDAPReachability_Debug.log` to view the error messages.

2. **Users cannot authenticate when they enroll devices**
   The MaaS360® logs are called `EMSAgent` logs with an appended date and time and are located at
   `C:\%ProgramData%\MaaS360\Cloud Extender\logs`.

   Old logs are compressed in the `gzip` format. The most recent `EMSAgent` log is 0 kb in size, but open the file to display the data.

   To find the authentication success or failure, search for:
   `LDAP-AUTH`, **`AuthStatus: Success`**, or **`AuthStatus: Failure`**.
3. **High Availability – Determine which Cloud Extender is used for Authentication**
   When multiple instances of the Cloud Extender are used for User Authentication High Availability, MaaS360 uses a round-robin style authentication to equally balance requests to all the Cloud Extenders. However, you might not easily locate the Cloud Extender that is used for authentication.
   To locate the Cloud Extender that is used to debug authentication issues, log in to the MaaS360 Portal, access the **Devices** > **Actions & Events** workflow. If you do not see the authentication record that you want to view, search for the record by using the workflow in the Action History section.
   When you locate the record, you can view which Cloud Extender is used for authentication. The first column provides the Computer Name and the third column provides the device ID. To debug the issue, log in to the Cloud Extender server and obtain the EMS agent logs to look for failures by using the `LDAP-AUTH` search string.

Parent topic: [User Authentication Module]

8 User Visibility Module

The User Visibility module manages mobile devices based on corporate directory structure. With this module, administrators can manage user devices that belong to specific groups, and target apps, policies, and content to user devices that are members of a specific directory group.
The User Visibility module integrates with your Active Directory (AD) or LDAP environment to discover users, groups, and their membership associations from the corporate directory. The User Visibility module collects information about these directory objects and uploads that information to the MaaS360® Cloud. The module uses the user and group information to assign and distribute policies, apps, and docs, including administrative role-based access.
The Cloud Extender™ facilitates AD/LDAP visibility in the following ways:

1. Discovery of User Objects from the directory within a specific scope (no sensitive information collected)
2. Discovery of User Groups from the directory within a specific scope
3. On-demand discovery of members of specific groups. Use customized configuration options to limit data that is exported from the directory and from within a specific scope instead of exporting the entire directory.
4. Map attributes that are read from the corporate directory for the user object for specific use cases.

When the User Visibility module is configured correctly, the administrator can view all users and groups from the corporate directory within the MaaS360 Portal. The MaaS360 platform allows the administrators to import these User Groups into MaaS360 to trigger a discovery of users within that specific group.
The User Visibility module runs on a schedule and uploads data (users, groups, user attributes, and group memberships) in increments (changes from the last upload) every four hours and also uploads the full scope of data once a month. The MaaS360 Portal constantly updates any changes to user attributes or any changes or deletions to group membership.

8.1 Modes of Operation

The Cloud Extender integrates with the corporate directory by using the following modes:

1. Active Directory Mode: This mode is specific to Microsoft Active Directory environments. The Cloud Extender runs as a service account and runs scripts to discover users and groups within your directory. If you have multiple trusting forests or resource forests in your environment, some additional configuration is required.
2. LDAP Mode: This mode is used for any corporate directory. The Cloud Extender offers standard LDAP templates to integrate with Domino® LDAP, Oracle LDAP, Novell eDirectory, and OpenLDAP. In addition to these standard LDAPs, use this mode to configure against any customized LDAP. The Cloud Extender also provides a template to help you configure Microsoft Active Directory in LDAP mode.

To determine which implementation mode to use for your environment, consider these guidelines:

If you are not using Microsoft Active directory (AD), use LDAP mode.
If you are using Microsoft Active directory (AD), the following table provides LDAP options for your environment:

Table 1. Determining which LDAP implementation mode to use for your environment

Scenario	**Active Directory Mode**	**LDAP Mode**
Ability to limit authentication scope to a certain OU, subtree, or group		✓
Requirement that the Cloud Extender needs to be part of your domain	✓	
Ability to support trusted forest/domain visibility	✓	✓
Ability to support untrusted forest/domain visibility	Requires a separate instance of the Cloud Extender for	Requires a separate instance of the Cloud Extender for

	each untrusted forest	each untrusted forest
Ability to customize attributes that are read from AD		✓
Support for User Custom Attributes		✓
Ability to customize user and group filters for optimized user search performance		✓
Support for High Availability		
East of configuration	Easy	Medium
Implementation technology	.NET libraries	LDAP libraries
Configured along with User Authentication on the same Cloud Extender	✓	✓

In most situations, the LDAP mode of user visibility is the implementation of choice even in Microsoft Active Directory environments with consideration to the advantages listed in the table and easy adaptability to future requirements.

8.2 Requirements and Scaling

The User Visibility module requires one instance of the Cloud Extender for LDAP or Active Directory, which scales up to 100,000 users. If your directory scope for the Cloud Extender is greater than 100,000 users, you must implement additional instances of the Cloud Extender.
The following table provides hardware requirements for the User Visibility module:

Table 2. Hardware requirements for the User Visibility module

Item	Minimum Requirement
Hardware Component	CPU: 2 cores Memory: 2 GB to 8 GB

	Storage: 50 GB Scaling: One Cloud Extender for 100,000 users. Supports installation on multiple instances of the Cloud Extender but does not support High Availability. Each Cloud Extender that implements User Visibility must have an exclusive scope and must not overlap with other instances of the Cloud Extender that implement User Visibility. Install on a dedicated Cloud Extender or enabled on Cloud Extender with User Authentication or Certificate Authority Integration services enabled. For accurate scaling of your environment, see the Cloud Extender scaling document at **Setup** > **Services** > **Enterprise** **Email Integration**.
Network Traffic	Traffic exchange between the Cloud Extender and LDAP/AD: First-time upload data usage: 0.5 MB Steady state data usage per month: 90 MB Traffic exchange between the Cloud Extender and MaaS360: First-time upload data usage: 0.15 MB Steady state data usage per month: 0.87 MB Test metrics (usage based on 1,000 users): Data upload frequency Incremental data uploads frequency = 4 hours Full data uploads frequency = 1 Week

	Incremental data uploads (uploads only changes from last successful upload) Every incremental query, one percent of users with attribute Changes Average data packet size per user: 0.5 KB Average ratio of encryption and compression of data upload to MaaS360 = 70 percent
Active Directory	Hardware specs meet minimum Requirements PowerShell 3.0+ installed Windows operating system is joined to the domain Service Account Domain User Password does not Expire Non-interactive account Local Administrator on the Cloud Extender server
LDAP	Hardware specs meet minimum Requirements Service Account Username and password to bind to LDAP server Password does not expire Non-interactive account

User Visibility Service Configuration

Follow these steps to configure the User Visibility service for the Cloud Extender.

Basic Configuration: Active Directory Mode

Follow these steps to configure basic Active Directory mode settings that discover all users, groups, and memberships from the entire directory.

Advanced Configuration: Active Directory Mode Trusted Cross-Forest Visibility

The Advanced configuration mode extends the functions of the Cloud Extender Basic configuration mode to discover all users, groups, and relationships from all domains in the same forest or other forests where the service account is provisioned.

Basic Configuration: LDAP Mode

Follow these steps to configure basic LDAP mode settings for user visibility.

Advanced Configuration: LDAP Mode

The values for Advanced LDAP configuration mode are populated with default configuration settings based on the LDAP server type that you selected. Use this option if you need to edit these values for your environment.

Enabling Health Check Alerts for User Visibility

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender User Visibility module.

Troubleshooting Issues with User Visibility

Troubleshooting issues with reaching users from the Cloud Extender.

Parent topic: Configuring Settings for the Cloud Extender Modules

1 User Custom Attributes is a feature in MaaS360 where you define your own attribute and use this attribute in various configuration workflows. For example: You define a User Custom Attribute that is called `Employee Serial Number` and use this value in MaaS360 policies for device configuration, application configuration, or a part of Identity Certificates. This attribute can be read directly from your directory by using the LDAP configuration.

2 Consider whether to configure the User Visibility service along with the User Authentication service for your Cloud Extender. If so, then the mode of configuration for both these services is either Active Directory or LDAP.

For example, User Authentication as AD and User Visibility as LDAP on the same Cloud Extender is not possible. If you require this combination, you must use separate instances of the Cloud Extender.

8.3 User Visibility Service Configuration

Follow these steps to configure the User Visibility service for the Cloud Extender™.

8.3.1 Procedure

1. Open the Cloud Extender Configuration Tool and select the **User Visibility** tile
2. Select the appropriate corporate directory type

NOTE: If you have configured the same Cloud Extender with the User Authentication module, you must use the same authentication mode for the User Visibility module.
If you need to implement User Visibility and User Authentication in different modes, use separate instances of the Cloud Extender.

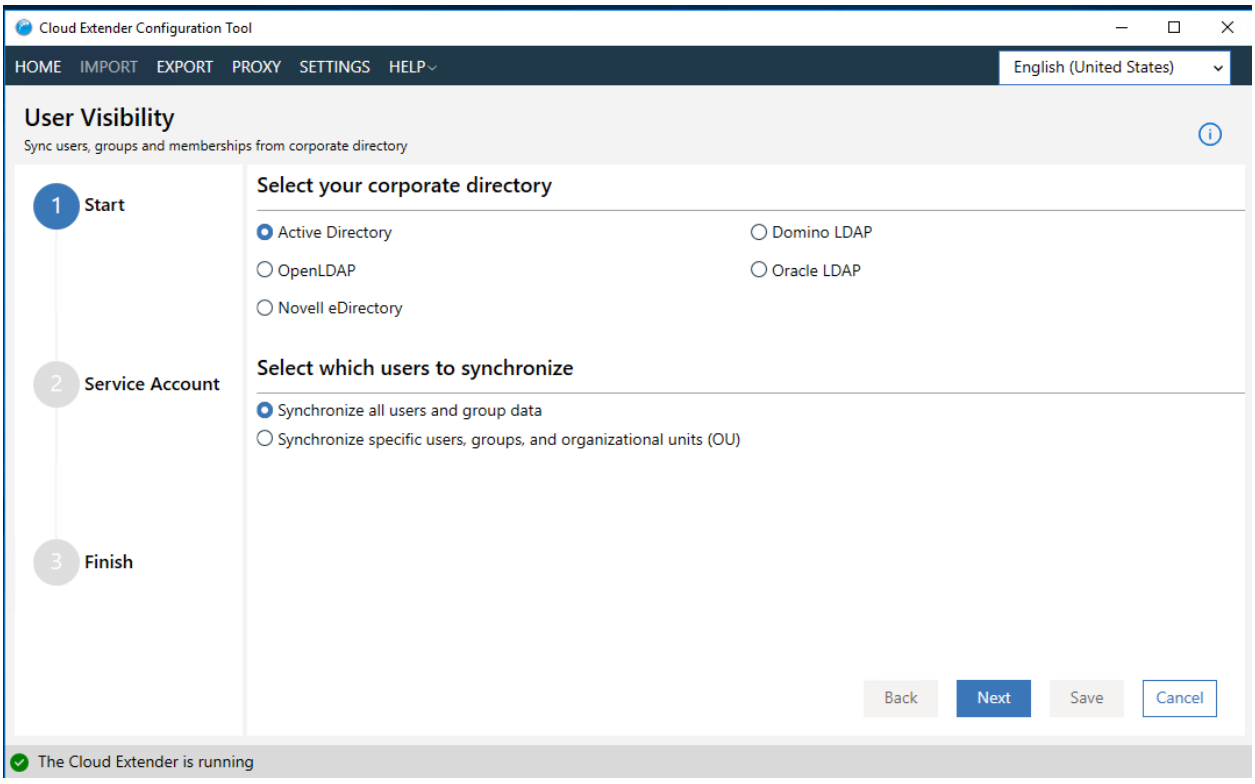
Parent topic: User Visibility Module

8.4 Active Directory Mode Configuration

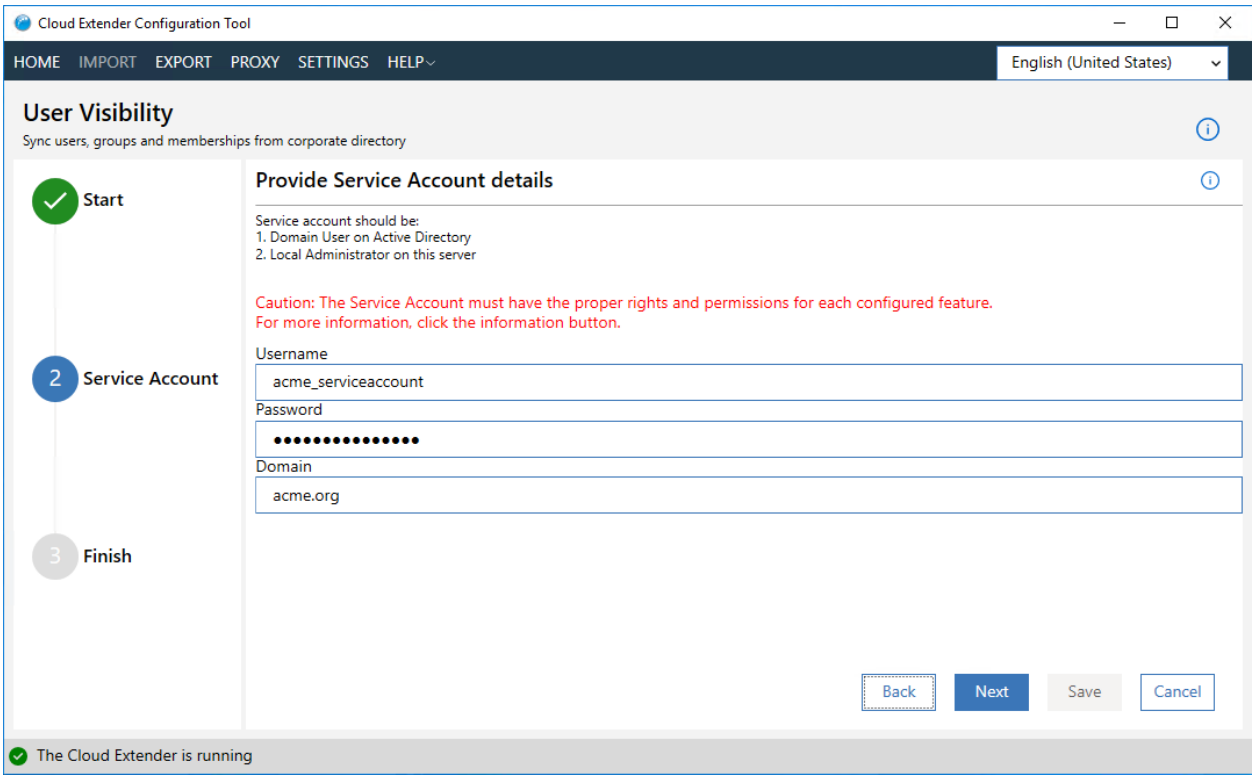
Follow these steps to configure basic Active Directory mode settings that discover all users, groups, and memberships from the entire directory.

8.4.1 Procedure

1. Make sure your system meets all prerequisites
    a. Hover your mouse over the User Visibility tile, then hover over the green check mark or red X that appears in the lower left corner of the tile
2. Select the User Visibility corporate directory type as **Active Directory**
3. Select **Synchronize all users and group data**



4. Click **Next**
5. Complete Service Account configuration



Parameter	Description
Username	The service account username must be a local administrator on the Cloud Extender server.
Password	The service account password must not expire. If your corporate policy requires you to change the service account password on a periodic basis, make sure that you update the password from the Cloud Extender Configuration Tool.
Domain	The domain of the service account.

6. To run a reachability test, click the **Test Reachability** button.
7. If successful, you will be presented with reachability results including the number of OUs found and the number of users found.
8. Click the **Save** button

Parent topic: User Visibility Module

8.5 Active Directory Mode Trusted Cross-Forest Visibility Configuration

The User Visibility module allow for discovery of all users, groups, and relationships from all domains in the same forest or other forests where the service account is provisioned. You can use this functionality for the following scenarios:

1. Trusted multi-forest environment: The service account discovers users and groups from other domains in a trusted forest.
2. Restricting Active Directory integration to the current domain: The Cloud Extender in Active Directory mode discovers all users, groups, and relationships from all domains in the same forest. Use this option when you must restrict this scope to specific domains. However, LDAP mode is a better option for this scenario.
3. Cross-forest group membership support: A user is a member of one group in a forest (for example, `Forest1`), and also a member of another group in a forest (for example, `Forest2`).

Trusted Multi-Forest Environment

Use this option if your environment contains more than one forest and there is at least one-way trust from one forest (where the Cloud Extender is installed) to the other forest.

Restrict Active Directory Integration to the Current Domain

The User Visibility module usually retrieves data from the entire Active Directory, but the module is flexible enough to retrieve data only from the current domain based on a policy value or by using a registry key setting.

Cross-Forest Group Membership Support in Active Directory Environments

The User Visibility module supports a user who is a member of one group and is also a member of another group. The Cloud Extender can detect this type of membership and map the user to the right group, and then import those groups into MaaS360®.

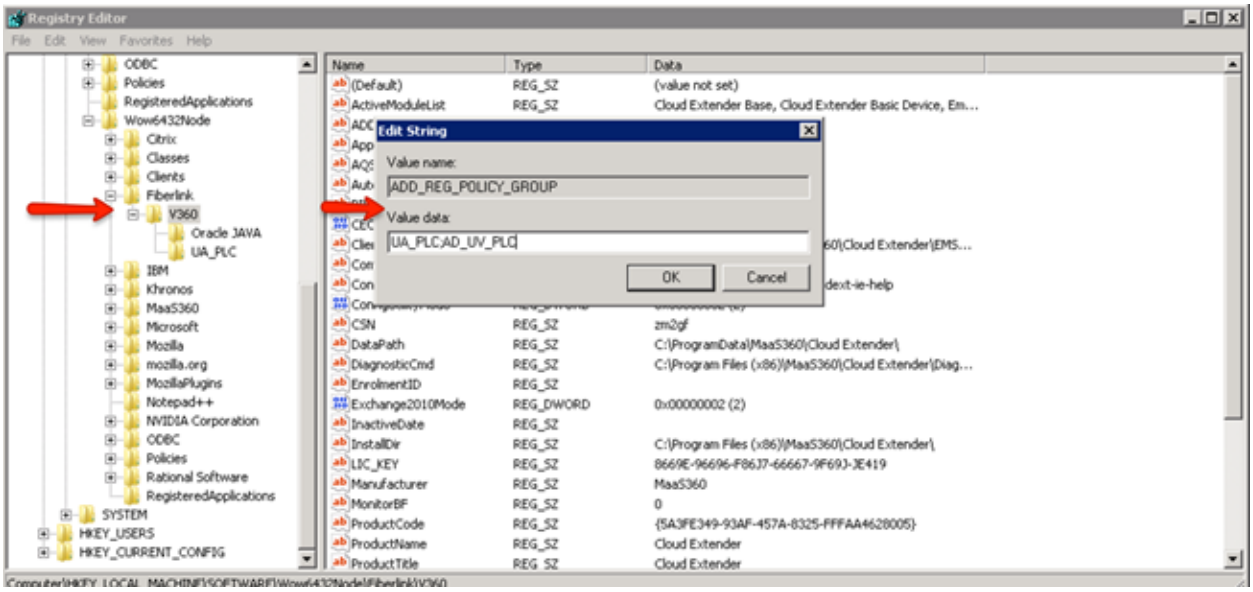
Parent topic: User Visibility Module.

8.6 Trusted Multi-Forest Environment

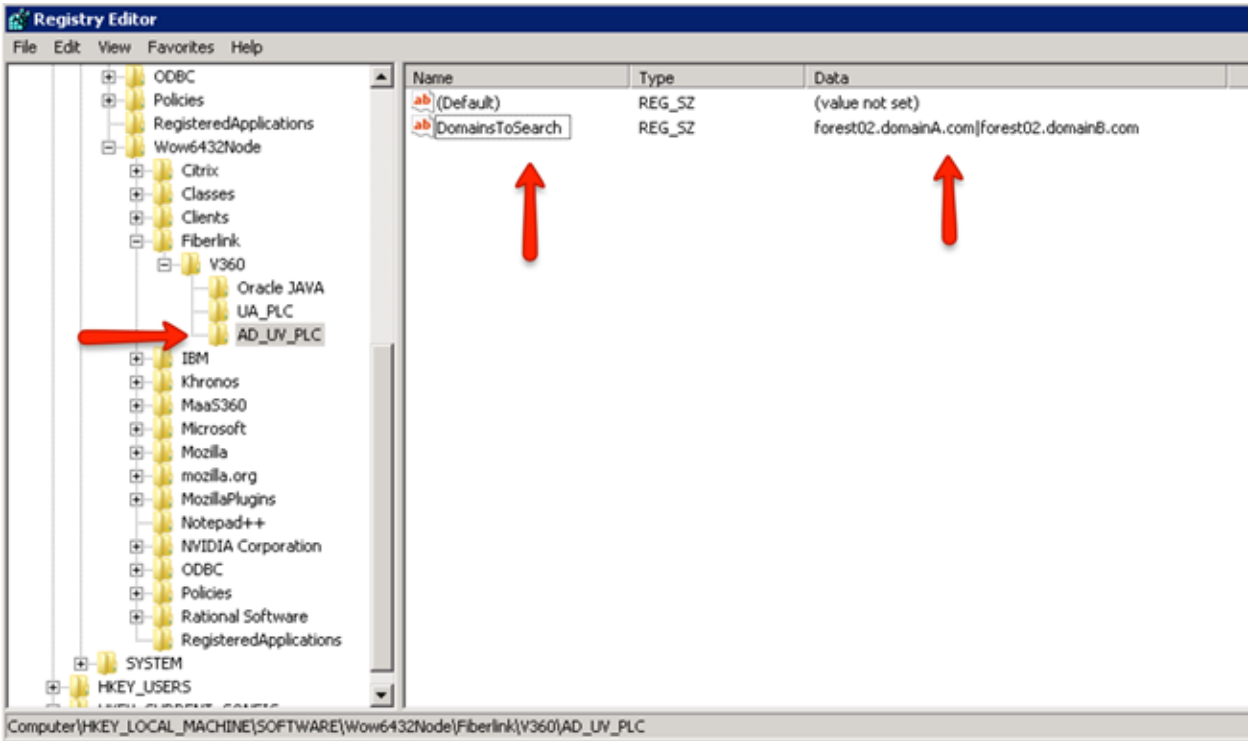
Use this option if your environment contains more than one forest and there is at least one-way trust from one forest (where the Cloud Extender™ is installed) to the other forest.

8.6.1 Procedure

1. Open the Registry Editor (`regedit.exe`) on the Cloud Extender server.
2. From `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360`, create a value in the V360 key: `"ADD_REG_POLICY_GROUP"="AD_UV_PLC”`.
   Note: If the `ADD_REG_POLICY_GROUP` key exists, you must append `AD_UV_PLC` to the list separated by a semicolon (;).



3. Create a key under the V360 key named `AD_UV_PLC`.
4. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\AD_UV_PLC`



5. Create a string value under `AD_UV_PLC` called `DomainsToSearch`. The value of this data is a pipe-separated list of domains from a trusting forest.

6. Restart the Cloud Extender service from the Windows Services console for the configuration to take effect.

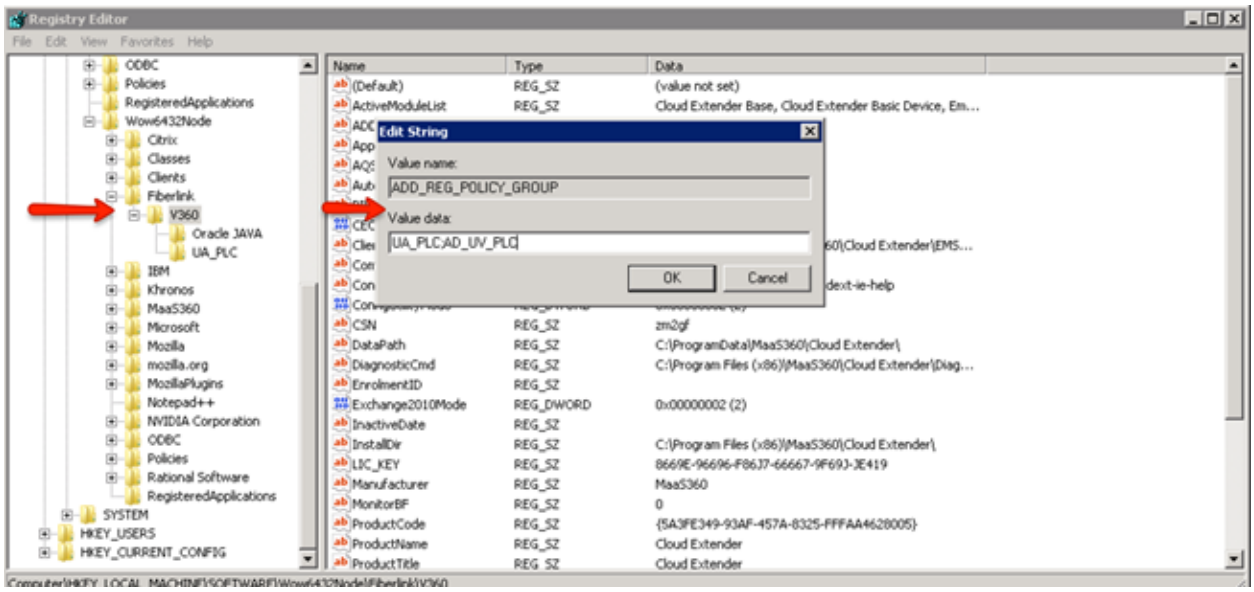
Parent topic: [Advanced Configuration: Active Directory Mode Trusted Cross-Forest Visibility]

8.7 Restrict Active Directory Integration to the Current Domain

The User Visibility module usually retrieves data from the entire Active Directory, but the module is flexible enough to retrieve data only from the current domain based on a policy value or by using a registry key setting.

8.7.1 Procedure

1. Open the Registry Editor (`regedit.exe`) on the Cloud Extender™ server.
2. From `KEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360`, create a value in the V360 key: `"ADD_REG_POLICY_GROUP"="AD_UV_PLC”`.
   Note: If the `ADD_REG_POLICY_GROUP` key exists, you must append `AD_UV_PLC` to the list separated by a semicolon (;).
3. Create a string value under `AD_UV_PLC` called `CurrentDomainUsersOnly`, and set the value to `Yes`.



4. Restart the Cloud Extender service from the Windows Services console for the configuration to take effect.

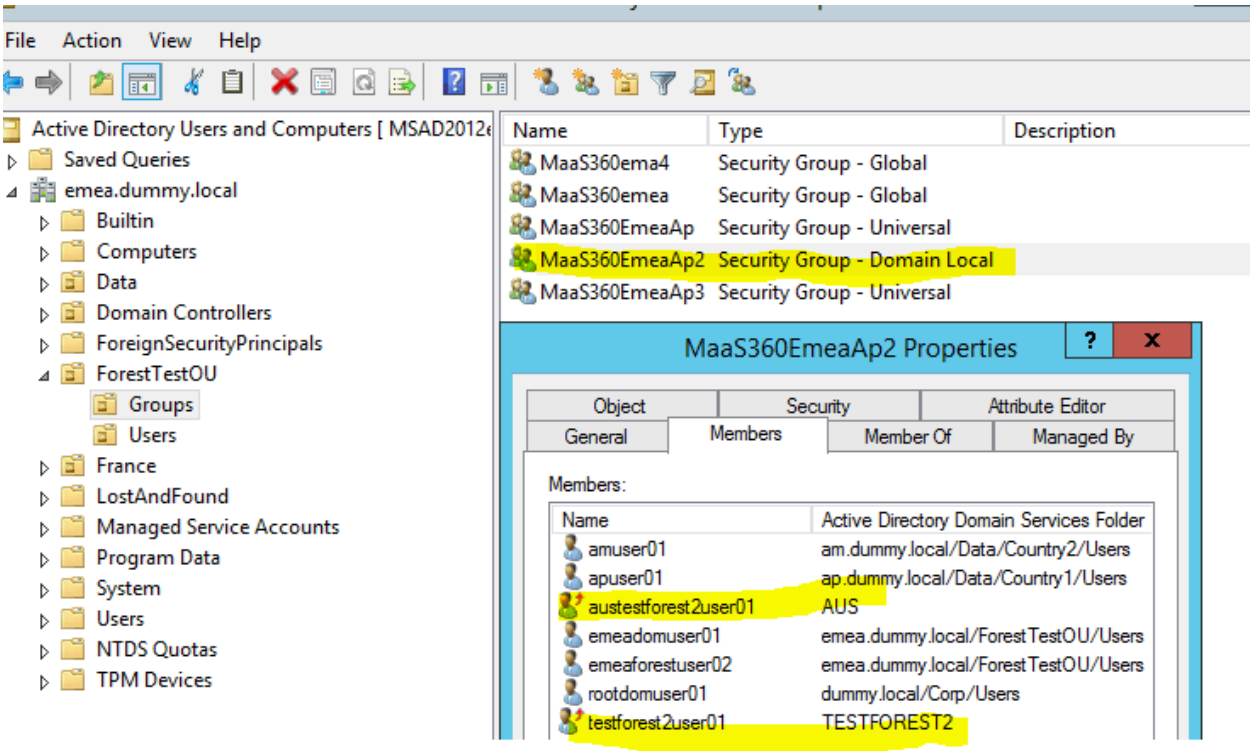
Parent topic: [Advanced Configuration: Active Directory Mode Trusted Cross-Forest Visibility]

8.8 Cross-Forest Group Membership Support in Active Directory Environments

The User Visibility module supports a user who is a member of one group and is also a member of another group. The Cloud Extender™ can detect this type of membership and map the user to the right group, and then import those groups into MaaS360®.
Note: This feature is supported only in Active Directory mode.

The following example uses a group that is named `MaaS360EmeaAp2` that has most members in the local domain and forest (`dummy.local`), but has two users on foreign trusted domains (`AUS` and `TESTFOREST2`).

member	CN=apuser01,OU=Users,OU=Country1,OU=Data,DC=ap,DC=dummy,DC=local
member	CN=amuser01,OU=Users,OU=Country2,OU=Data,DC=am,DC=dummy,DC=local
member	CN=emeauser03,OU=Users,OU=Country1,OU=Data,DC=emea,DC=dummy,DC=local
member	CN=emeaforestuser02,OU=Users,OU=ForestTestOU,DC=emea,DC=dummy,DC=local
member	CN=rootdomuser01,OU=Users,OU=Corp,DC=dummy,DC=local
member	CN=emeadomuser01,OU=Users,OU=ForestTestOU,DC=emea,DC=dummy,DC=local
member	CN=S-1-5-21-4036306258-3547744107-2837512241-1108,CN=ForeignSecurityPrincipals,DC=...
member	CN=S-1-5-21-250142341-237385165-2322164573-1108,CN=ForeignSecurityPrincipals,DC=em...



Parent topic: [Advanced Configuration: Active Directory Mode Trusted Cross-Forest Visibility]

8.9 LDAP Mode Configuration

Follow these steps to configure basic LDAP mode settings for user visibility.

8.9.1 Before you begin

Make sure that you can connect to your LDAP server through telnet or any other mechanism before you set up the Cloud Extender™.

8.9.2 Procedure

1. Click on the User Visibility tile from the Config Tool home screen
2. Select the appropriate Corporate Directory type from the presented options
    a. If you select Active Directory, select **Synchronize specific users, groups, and organizational units (OU)**
3. Click the **Next** button
4. Fill in the following parameters:

Parameter	Description
LDAP Server	The host name and the port of your LDAP server. The Cloud Extender supports multiple LDAP servers if the servers are mirroring LDAP servers.
Username	The admin username of your service account. This account is used to bind to LDAP to authenticate other users. Some implementations of LDAP accept the bind username in a standard format like `user@company.com`, while other LDAP implementations might require a Distinguished Name (DN) of the user. The following provides an example of the DN format: `uid=username,c=us,ou=subdom`

	`ain,dc=company,dc=com`
Password	The admin password of your service account.
Authentication Type	Choose authentication type from available options: Kerberos NTLM Basic Digest
SSL	Check this box if your system is configured for secure (SSL) LDAP connections.

5. Click the **Next** button
6. Fill in the following parameters:

Parameter	Description
Search Roots for Users	The search base for users is the root location in your directory from where all users are searched. The Cloud Extender discovers any user under the hierarchy. Enter the Distinguished Name (DN) of the Organization Unit (OU) that has users.
Search Roots for Groups	The search base for groups is the location on your directory that includes all defined user groups. This option is similar to the **LDAP Search base for Users** option. The Cloud Extender uses this attribute to discover all groups from this root location.
Filter by Groups (Optional)	Enter any groups you want to filter out of all searches.

7. Click the **Next** button
8. To run a reachability test, click the **Test Reachability** button.
    a. If successful, you will be presented with search results including the number of OUs and users found during the reachability test

Parent topic: [User Visibility Module]

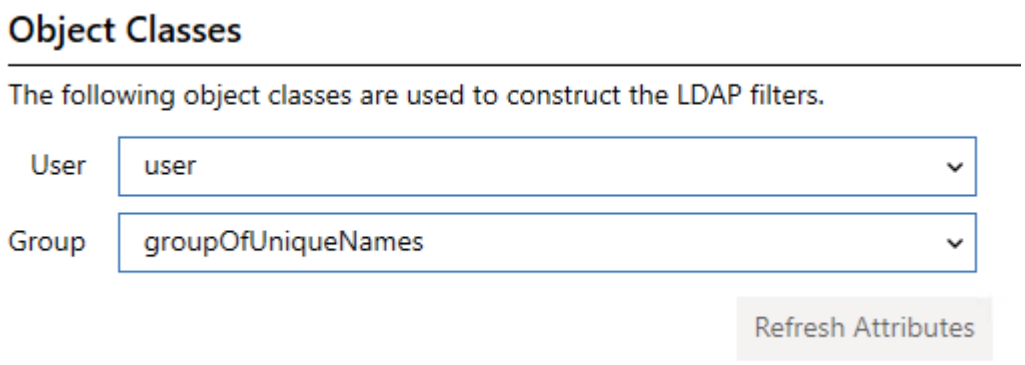
8.10 LDAP Mode Advanced Configuration:

Click the Advanced button for access to advanced configuration settings. Use Advanced LDAP configuration with the following scenarios:

1. If you are using OpenLDAP, you must configure how the Cloud Extender™ looks for users, groups, Organizational Units (OU), and domains.
2. Must map user properties on MaaS360® to specific fields in your LDAP.
3. Must support user custom attributes.

8.10.1 Object Classes Configuration

LDAP Object Classes define a type of object in LDAP. Every user and every user group on LDAP uses a specific Object Class. With the Object Class, you can list all objects that have that Object Class. After you set up a User Authentication profile, select the Object Class of your users and groups from the options provided in the list boxes shown below:

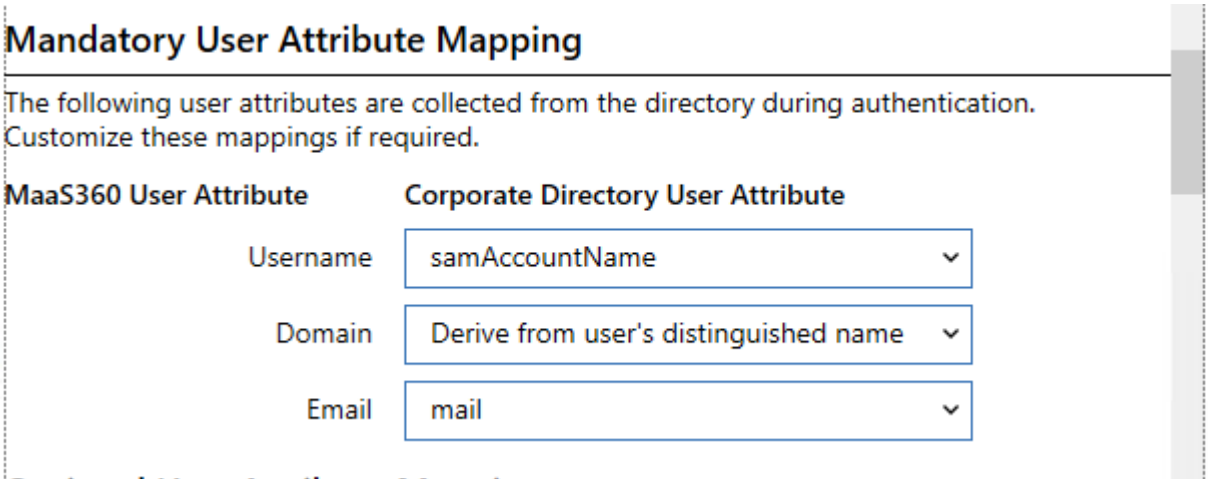


Object Class	Description
User	The object class that identifies the type of all your users. The Cloud Extender uses the Basic mode configuration and queries your LDAP for all possible Object Classes for users and lists. If the Object Class for your users is not automatically discovered or is not featured on

	the select list, type the `Object Class` for users.
Group	The object class that identifies the type of all your user groups

8.10.2 Mandatory User Attributes Configuration

During the authentication process, the Cloud Extender reads certain attributes of the user from your directory that it requires for other configuration aspects after a device is enrolled in the MaaS360 Portal.

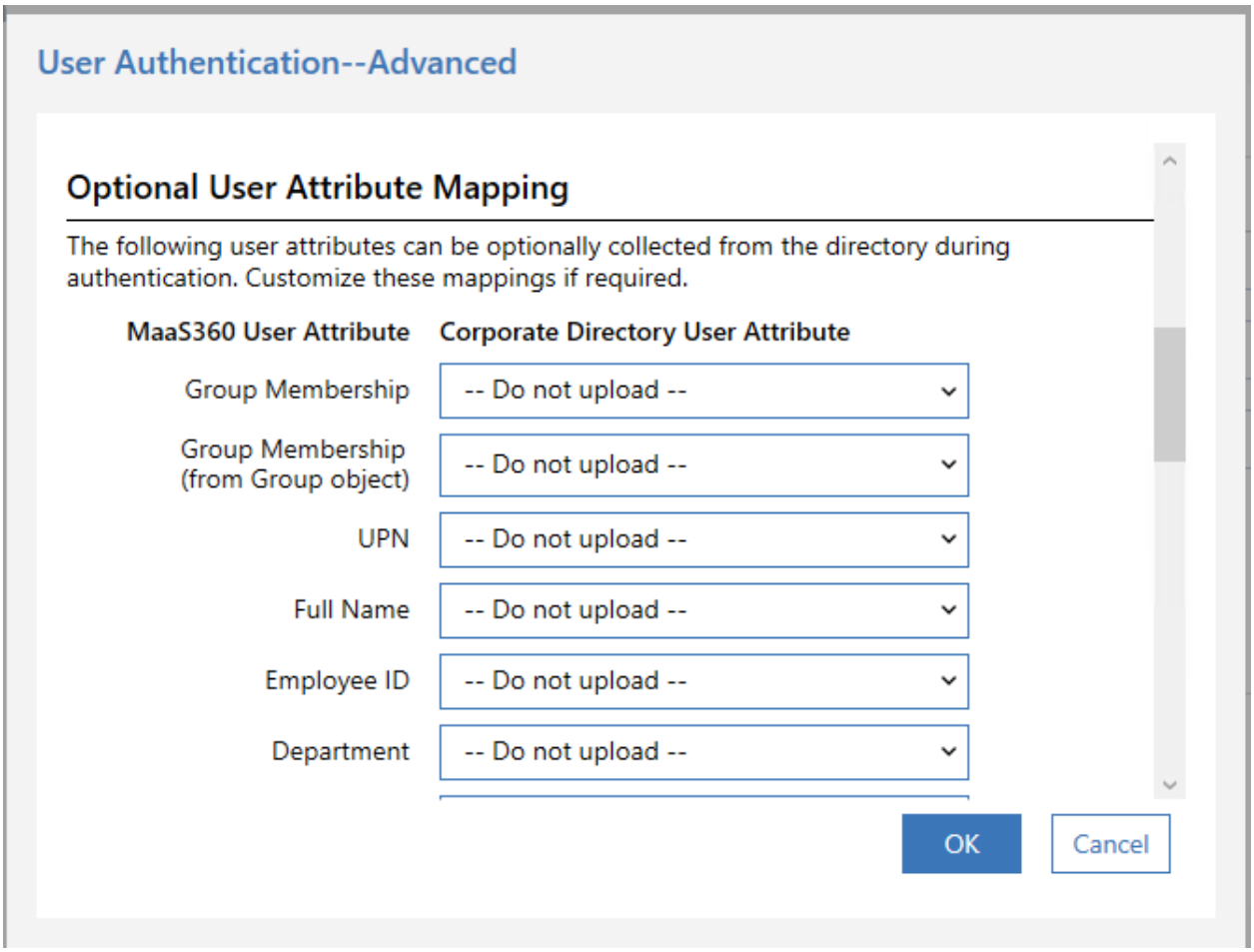


Attribute	Description
User name	The Cloud Extender uses the **User Search Attribute Name** to search for the user in LDAP. This user is the user who is trying to enroll the device. You can pick the same attribute here. If you need to represent users by a different attribute in MaaS360 (for example, by email address), select a different attribute. **Note:** This attribute is part of the *%username%* variable in MaaS360. Use this variable in MaaS360 policies to configure email on mobile devices. This variable converts to the user name for the user's email configuration.

Domain	The domain of the user. You use the domain to configure email on the mobile device. You can map the domain field to a specific attribute on your directory or derive the domain from the user's Distinguished Name (DN). The following list provides an example of the DN format: `uid=username,c=us,ou=subdomain,dc=company,dc=com` From the example, if your domain is set to **Derive from DN**, the domain is `company.com`.
Email	The email address of the user. Use this address to configure email on the device.

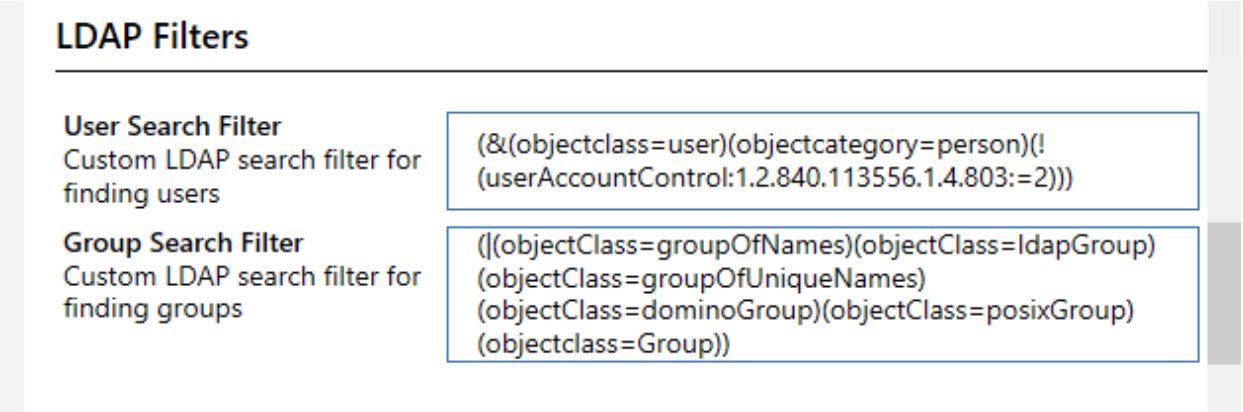
8.10.3 Optional User Attribute Mapping

In addition to Mandatory User Attributes, the Cloud Extender module for User Authentication reads optional user attributes during the authentication process. These values are uploaded to the MaaS360 Portal and are used later for grouping devices or as configuration parameters. The User Principal Name (UPN) is a common field that is read during authentication. The following window provides a standard list of user attributes on MaaS360 that can be mapped to the user's attribute on your directory.



8.10.4 LDAP Filters

Use this option to filter the list of users that the Cloud Extender discovers, such as filtering only by active users or by users that belong to specific departments. Use the standard LDAP filter queries to further optimize your user searches.



Click the **Save** button to complete User Visibility configuration.

8.10.5 LDAP Configuration for Cross-Forest Visibility

Unlike the User Authentication module, the User Visibility module does not support multiple profiles for LDAP configuration. If your environment requires cross-forest visibility while the Cloud Extender is configured in LDAP mode, configure separate instances of the Cloud Extender for each forest (trusting or non-trusting).

8.10.6 Next steps

The MaaS360 Portal offers the Cloud Extender Scaling Tool at **Setup** > **Services** > **Enterprise Email Integration**. Input the number of users/devices that you plan to enroll for MaaS360 and determine how many Cloud Extenders you might need to support this scale.
Install the specified number of Cloud Extenders and configure each instance with a unique and non-overlapping search base for finding users and groups. The User Visibility module does not support High Availability (HA). You can set up redundant instances of the Cloud Extender if the primary instance of the Cloud Extender fails.

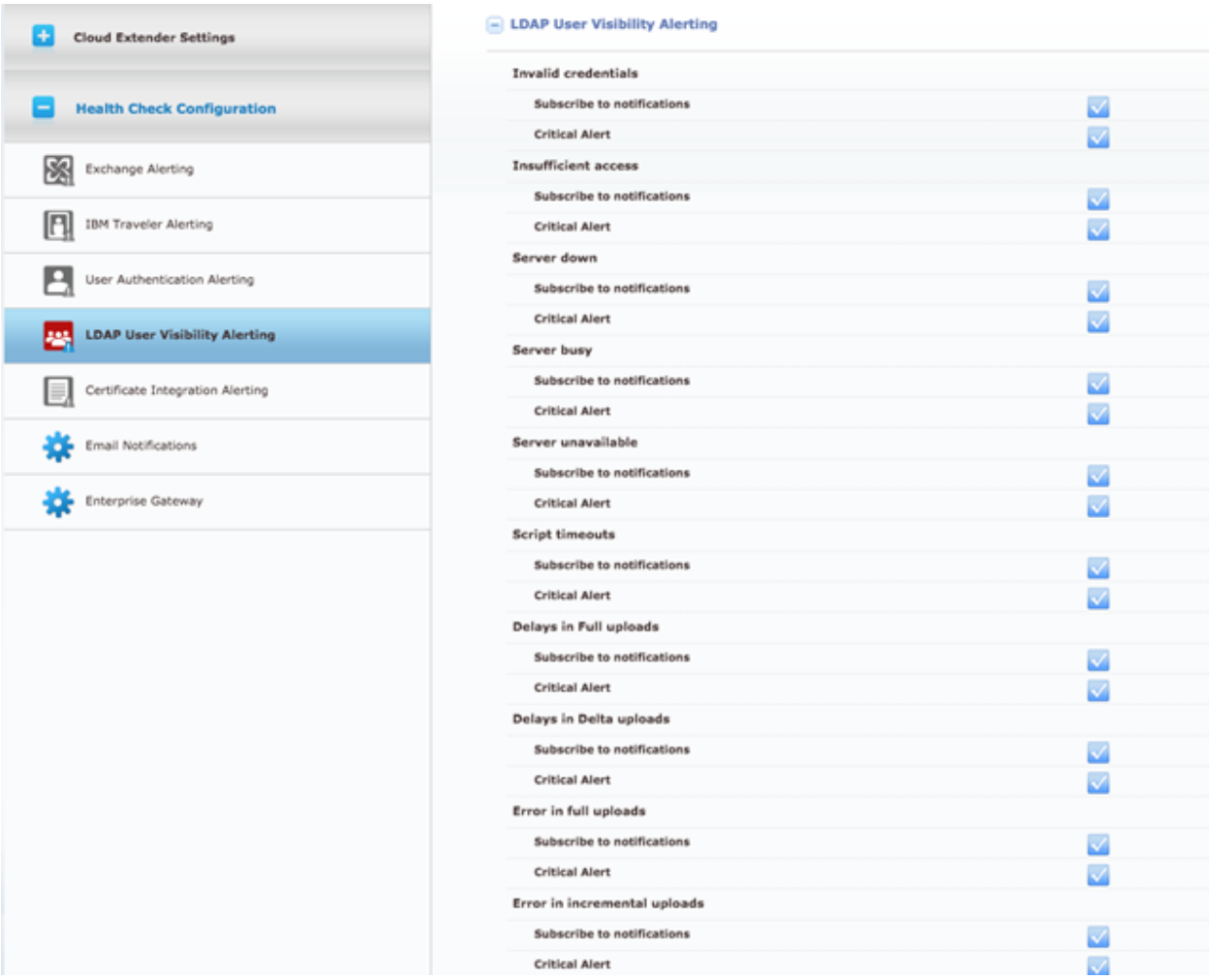
Parent topic: User Visibility Module

8.11 Enabling Health Check Alerts for User Visibility

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ User Visibility module.

8.11.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.
2. Select **Health Check Configuration** > **LDAP User Visibility Alerting**. The LDAP User Visibility Alerting list is displayed.
   Note: This list also displays alerts for User Visibility for Active Directory.



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**.

The following table provides a description of each alert and the steps you take to remediate the alert:

Alert	Alert Description	Remediation Steps
Invalid credentials	The service account credentials are expired or invalid. The Cloud Extender cannot connect to the configured LDAP server because the server is unreachable or the service account credentials are invalid.	Verify that LDAP is operational. Check for recent firewall or proxy changes that might block access to the LDAP server. Check whether the bind administrator credentials are valid and not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the credentials. Check whether any intrusion detection software in your network might be locking the bind administrator account. If the account is locked, add the account to the allow list to prevent the intrusion detection software from locking the account. If this issue continues, collect logs from the Cloud Extender, and then contact IBM®

		Support for further assistance.
Insufficient access	Insufficient permissions on the LDAP bind administrator account is causing an insufficient access error response from the LDAP server for certain LDAP operations	Verify that the LDAP bind administrator account uses the necessary permissions to execute Bind, Query, and Filter operations on LDAP. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind administrator account. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server down	The authentication LDAP server is down. The Cloud Extender cannot connect to the directory server because the directory server is down or the Cloud Extender configuration is invalid.	Verify that the configured LDAP server is reachable from the Cloud Extender server. Use the Cloud Extender reachability test to confirm that the LDAP server is reachable from the Cloud Extender server. Check whether the bind administrator account is still active and the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind administrator account credentials.

		If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server busy	The authentication LDAP server is busy. The Cloud Extender cannot process the client request because the LDAP server is busy.	Check whether the LDAP server is low on system resources. Check whether other applications are also using LDAP resources during this time period. Review the LDAP server performance and contact internal or vendor teams for assistance with resolving this issue
Server unavailable	The authentication LDAP server is unavailable. The Cloud Extender cannot process the LDAP bind request with the configured bind administrator credentials because the LDAP server might be unavailable.	Verify that the configured LDAP server is reachable from the Cloud Extender server. Use the Cloud Extender reachability test to confirm that the LDAP server is reachable from the Cloud Extender server. Check whether the bind administrator account is still active and the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the bind administrator account credentials.

		If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Script timeouts	The User and Group discovery script from LDAP is taking more time to complete than the configured threshold. The MaaS360 Portal might not be using the latest User and Group information from your LDAP directory. The User and Group discovery scripts time out due to the following issues: Too many users and groups that are configured in the Cloud Extender scope. The Cloud Extender is trying to reach remote LDAP servers or domain controllers that are slowing down the script.	Follow these steps to remediate this alert: Use the Cloud Extender Scaling Tool to determine whether you require multiple Cloud Extenders for your environment and if your current scale meets the criteria. From the MaaS360 Portal Home page, select **Setup** > **Services** > **Enterprise Email Integration** to download the tool. If you are using LDAP mode, verify that the search base for users is not that wide. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to limit the scope of the search base and use filters for Users and Groups to optimize search performance. If this issue continues, collect logs from the Cloud Extender, and

		then contact IBM Support for guidance on correct scaling or recommendations on how to increase the timeout settings.
Delays in full uploads	An error occurred during a full sync from your LDAP directory. The last successful and complete upload from the server occurred more than a day ago from the scheduled upload date. The server is either unreachable or the service account is invalid. The scheduled full sync of Users and Groups from your LDAP directory did not complete within the expected time frame.	Verify that the Cloud Extender that is configured for User Visibility is operational. Check whether the bind administrator account is still active and the password is not expired. Check whether your LDAP server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** and run a **Test** action on the Cloud Extender that is configured for User Visibility. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **User Visibility Refresh** to refresh the User Visibility data. Wait 1 hour to confirm that the issue is resolved.

		If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Delays in delta uploads	The last successful incremental upload from the LDAP server is more than 8 hours from the scheduled upload date. The server is unreachable, or the service account is invalid. The scheduled incremental sync of Users and Groups from your LDAP server did not complete within the expected time frame.	Verify that the Cloud Extender that is configured for User Visibility is operational. Check whether the bind administrator account is still active and the password is not expired. Check whether your LDAP server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** and run a **Test** action on the Cloud Extender that is configured for User Visibility. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **User Visibility Refresh** to refresh the User Visibility data. Wait 1 hour to confirm that the issue is

		resolved. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Error in full uploads	The Cloud Extender cannot upload all User and Group information from the LDAP server due to critical errors during the sync.	Verify that LDAP is operational. Check for recent firewall or proxy changes that might block access to the LDAP server. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Error in incremental uploads	The Cloud Extender cannot upload new or changed User and Group information from the LDAP server due to critical errors during the sync.	Verify that LDAP is operational. Check for recent firewall or proxy changes that might block access to the LDAP server. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [User Visibility Module]

8.12 Troubleshooting Issues with User Visibility

Troubleshooting issues with reaching users from the Cloud Extender™.

8.12.1 Why can't I view user or group information in MaaS360®?

Use the Cloud Extender Configuration Tool to confirm whether you can reach the LDAP/AD server. Make sure that targeted Organizational Units (OU) contain user or groups in that Organizational Unit and not two levels deep.

8.12.2 Why aren't the Organizational Units (OU) under my system containers displayed in MaaS360?

The User Visibility module does not retrieve data from system containers. System containers are built-in objects, so they are excluded during data collection.

8.12.3 Why does the User Visibility module query too often, and is this affecting my LDAP/AD resources?

If a customer contains many users, groups, and organizational units (OU), then pulling this information every four hours might burden servers. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**, and then change the policy to run scripts once every 24 hours.

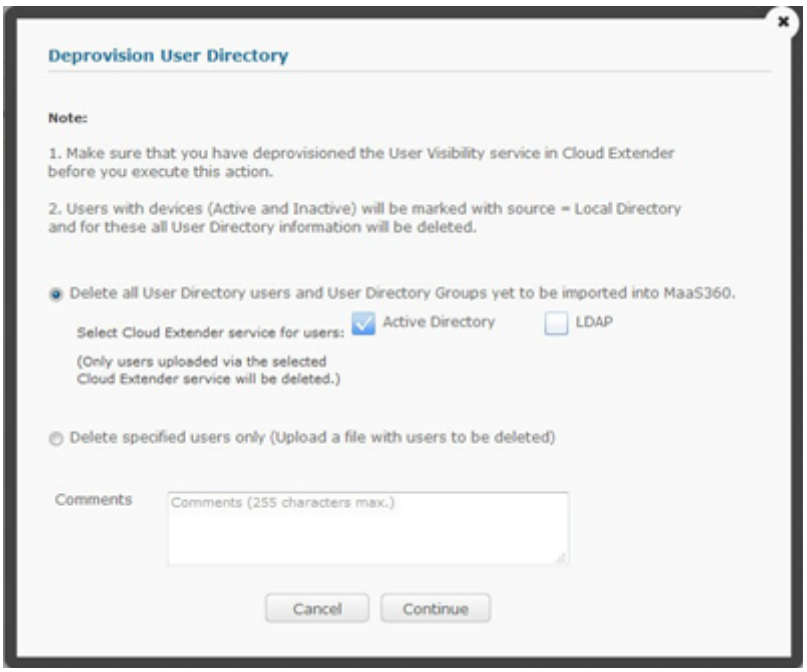
8.12.4 When I turned on User Visibility, every user in the Corporate Directory was imported?

When a customer configures the User Visibility module, they might set up the Cloud Extender to point to Active Directory, which imports all users to MaaS360. Since this result is not the intended result, you must purge old user records in the MaaS360 workflow.
You can either purge all users or upload a CSV file to purge users.

To purge all users, follow these steps:

1. Go to **Users** > **Directory**.
2. Click **More**, and then select **Deprovision User Directory**.

3. Follow the prompts on the window to either remove all users from the AD or LDAP or to upload a file that removes users.



4. Click **Continue**. A confirmation message is displayed after you type your password.
   a. If you upload the file, the number of users that you want to remove is also displayed.
   b. The admin receives an email when the job is complete.

c. The job to remove the users runs at midnight GMT (SaaS and On-Premises).

Parent topic: User Visibility Module

9 Exchange (On-Premises and Cloud) Integration Module

The Cloud Extender™ integrates with Exchange servers and provides complete visibility to all ActiveSync devices that are connected to the mail system. With the Exchange integration, the Cloud Extender functions in the following ways:

1. Queries the Exchange server by using Microsoft PowerShell commands to discover devices and ActiveSync policies.
2. Uploads the device list and policy configurations to the MaaS360® Portal for reporting and management functions.
3. Supports all ActiveSync device actions such as approve, block, or remove a device from the mailbox and wipes devices that are initiated by the MaaS360 Portal, either through administrative action or automated rules.
4. Supports ActiveSync policy assignments to connected devices.
5. Enables Auto-Quarantine to prevent new devices from connecting to Exchange servers. Since existing ActiveSync devices are approved, existing connections are not affected by the quarantine process.
6. Supports pre-approval of Secure Mail connections and approval of connections from enrolled devices.
7. Supports granular integration against specific mailbox servers and domains.
8. Supports automated cleanup of old ActiveSync connections from the environment.

Important: The Cloud Extender integration with Exchange does not affect the flow of email traffic because the Cloud Extender is not an email proxy. The Cloud Extender instance does not sit between email and devices. This integration provides visibility only to your Exchange environment where you can manage devices. If the Cloud Extender is unavailable, users can continue to send and receive email messages.

9.1 Supported Versions of Exchange

The Cloud Extender integrates with both the on-premises and cloud versions of Exchange. The Cloud Extender supports the following versions of Exchange:

1. On-Premises: Exchange 2007, 2010, 2013, or 2016
2. Cloud: BPOS-dedicated (BPOS-shared not supported) and Office 365

Note: For integration with Exchange 2007, the Cloud Extender uses the Exchange Management Console and local PowerShell. For Exchange 2010 and later, and for all cloud versions of Exchange, the Cloud Extender uses Remote PowerShell for integration.

9.2 Requirements and Scaling

The MaaS360 Portal offers a Cloud Extender Scaling Tool at **Setup** > **Services** > **Enterprise Email Integration**. Enter the number of mailboxes and devices that you plan to enroll for MaaS360 and determine how many Cloud Extenders you might need to support integration with Exchange.

Consider the following guidelines for scaling the Exchange integration:

1. Gather times for device data does not exceed 60 minutes and averages 25 – 40 minutes for 5,000 devices. Current and average gather times are available on the Cloud Extender Status page in the MaaS360 Portal.
2. To determine the number of Cloud Extender instances that you need for your environment, divide the potential number of ActiveSync connected devices by 5,000 and the number of Mailboxes by 10,000 and use the higher of the two values.
3. To minimize latency, regional Cloud Extenders might be more appropriate to use.

Table 1. Scaling requirements for the Exchange Integration module

Item	Requirement
Exchange 2007, 2010, 2013,	Mailboxes: less than 10,000 mailboxes Devices: less than 5,000 devices

2016, and BPOS-D (for less than 10,000 mailboxes)	CPU: 2 cores Memory: 8 GB
Exchange 2007, 2010, 2013, 2016, and BPOS-D (for more than 10,000 mailboxes)	Mailboxes: more than 10,000 mailboxes Devices: more than 5,000 devices CPU: Use more Cloud Extenders Memory: N/A Scaling: Supports installation on multiple instances of the Cloud Extender, but does not support High Availability (HA). Each Cloud Extender that implements Exchange Integration must have an exclusive scope and must not overlap with other instances of the Cloud Extender that implement Exchange Integration. Install on a dedicated Cloud Extender or enabled on Cloud Extender with the User Authentication service enabled. For accurate scaling of your environment, see the Cloud Extender scaling document at **Setup** > **Services** > **Enterprise Email Integration**.
Office 365 using Remote PowerShell	Mailboxes: All / Devices: All CPU: 2 cores Memory: 8 GB Scaling: Office 365 supports only one instance of the Cloud Extender. Requires multiple service accounts for load distribution for more than 500 mailboxes. For accurate scaling of your environment, see the Cloud

	Extender scaling document at **Setup** > **Services** > **Enterprise Email Integration**.
Network traffic	Traffic exchange between the Cloud Extender and the Exchange server: First-time upload data usage: 3.35 MB Steady state data usage per month: 8872.75 MB Traffic exchange between the Cloud Extender and MaaS360: First-time upload data usage: 1 MB Steady state data usage per month: 95.75 MB Test metrics (usage based on 1,000 devices): Incremental data uploads frequency = 15 minutes Heartbeat frequency = 1 hour Full data uploads frequency = 1 week with environment Change Every incremental query, 1 percent of devices have attribute changes Average data packet size per device: 3 KB Average data packet size for heartbeat: 0.3 KB Average data packet size for policy = 50 KB (assuming 10 policies) Average ratio of encryption and compression of data upload to MaaS360 = 70 percent

9.3 Exchange Integration Requirements

The Exchange Integration module requires the following versions and service accounts:

Table 2. Version and service account requirements for the Exchange Integration module

Item	Requirement
Version	Exchange Server 2007, 2010, 2013, or 2016Office 365 and BPOS-Dedicated
Service Account	Domain User Local Administrator access on the Cloud Extender server
Service Account Exchange Permissions	2007: Member of Exchange Organization Administrator Security group 2010/2013/2016/BPOS-D: Member of Organization Management security group Office 365: Global Administrator rights
Role-based Access Control (RBAC)	If your organization supports Organization Management or Global Administrator accounts, create RBAC accounts based on specific access rights. Supports Exchange 2010 and later, and Office 365 See About Exchange Role-Based Access Control (RBAC) for detailed information.
Office 365 Only	Requires multiple service accounts configured on the Cloud Extender Follow these guidelines: One Global Administrator account per 500 mailboxes for device discovery. Two dedicated Global Administrator accounts:

	One account reserved for gathering mailbox data and another account reserved for MaaS360 Portal actions. For example: If you have 2,000 mailboxes, you need four service accounts for device discovery and two dedicated service accounts for a total of six required accounts. See About Office 365 Budgets for detailed information.
Exchange 2007 Only	Requires Exchange Management Tools installed on the same server as the Cloud Extender. The version of the Exchange Management Tool must match the service pack version of the Exchange server.
PowerShell	PowerShell 3.0+

About Exchange Role-Based Access Control (RBAC)

To implement the Cloud Extender correctly for integration with Exchange, the Cloud Extender service account must have Organization Administrator (2007), Organization Management (2010, 2013, 2016), and Global Administrator (Office 365) rights (the highest-level roles available for the Exchange domain).

About Exchange Organization Administrators (Exchange 2007)

With Exchange 2007, you cannot grant a subset of rights associated with a role group to a particular user account. To access rights for the Exchange Organization Administrator, the user account must have access to all rights associated with that role.

About Office 365 Budgets

Office365 Wave15 uses an access budget policy to limit the resources that are available to a client on the Office 365 server, which causes some of the functions of the Cloud Extender, such as device discovery, to fail.

Basic Mode: Exchange Integration

Follow these steps to configure basic settings for the Cloud Extender to integrate with Exchange.

Advanced Mode: Exchange Integration

Follow these steps to configure advanced settings for the Cloud Extender to integrate with Exchange.

Cloud Extender Settings in the MaaS360 Portal

Use the following procedures to enable the Cloud Extender features, Auto-Quarantine (AQ) and Auto-Cleanup, to integrate with Exchange.

Enabling Health Check Alerts for Exchange Integration

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender Exchange Integration module.

High Availability (HA) Mode for Exchange Integration

Information about support for High Availability (HA) mode for Cloud Extender integration with Exchange.

Parent topic: Configuring Settings for the Cloud Extender Modules

9.4 About Exchange Role-Based Access Control (RBAC)

To implement the Cloud Extender™ correctly for integration with Exchange, the Cloud Extender service account must have Organization Administrator (2007), Organization Management (2010, 2013, 2016), and Global Administrator (Office 365) rights (the highest-level roles available for the Exchange domain).
The Organization Administrator, Organization Management, and Global Administrator roles might contain additional access rights that are not required by the Cloud Extender. You can restrict the Cloud Extender from accessing these additional rights. Microsoft provides the role-based access control (RBAC) feature to address this issue.

For Exchange 2010 and later, use RBAC to create a custom role group within the Active Directory that is limited to the requirements of the Cloud Extender service. You can assign this role to the Cloud Extender service account instead of using Organization Administrator rights to allow the Cloud Extender to function correctly. RBAC applies to Exchange 2010 and later.

9.4.1 Requirements

You can create a custom role group in either Exchange 2010, 2013, 2016, or Office 365. To create a custom role group, follow these steps:

1. Identify the rights that are needed for the role. The Cloud Extender uses the following PowerShell commands to communicate with the Exchange server:

Table 1. PowerShell commands used by the Cloud Extender

PowerShell Command	Description
Get-PSSnapin	Determines the available PowerShell Snapins for Exchange ActiveSync
Add-PSSnapin	Add the available Exchange ActiveSync Snapin

Get-CASMailbox	Gathers a list of mailboxes and displays mailbox attributes
Set-CASMailbox	Changes settings on user mailboxes
Get-ActiveSyncDeviceStatistics	Gathers a list of devices and displays device attributes
Get-MobileDeviceStatistics	Exchange 2013 or Office 365 Wave 15 version of Get-ActiveSyncDeviceStatistics
Get-ActiveSyncMailboxPolicy	Gathers a list of policies and displays policy attributes
Get-MobileDeviceMailboxPolicy	Exchange 2013 or Office 365 Wave 15 version of Get-ActiveSyncMailboxPolicy
New-ActiveSyncMailboxPolicy	Create a mailbox policy
New-MobileDeviceMailboxPolicy	Exchange 2013 or Office 365 Wave 15 version of New-ActiveSyncMailboxPolicy
Remove-ActiveSyncMailboxPolicy	Removes a mailbox policy
Remove-MobileDeviceMailboxPolicy	Exchange 2013 or Office 365 Wave 15 version of Remove-ActiveSyncMailboxPolicy
Set-ActiveSyncMailboxPolicy	Associates a policy with a user's mailbox
Set-MobileDeviceMailboxPolicy	Exchange 2013 or Office 365 Wave 15 version of Set-ActiveSyncMailboxPolicy
Clear-ActiveSyncDevice	Wipes a device or cancels a wipe request
Clear-MobileDevice	Exchange 2013 or Office 365 Wave 15 version of Clear-ActiveSyncDevice
Remove-ActiveSyncDevice	Removes a device association with a mailbox
Remove-MobileDevice	Exchange 2013 or Office 365 Wave 15 version of Remove-MobileDevice
Get-ActiveSyncOrganizationSettings	Exchange 2010, 2013, Office 365: Determines Auto-Quarantine state

Set-ActiveSyncOrganizationSettings	Exchange 2010, 2013, Office 365: Sets a new Auto-Quarantine default access level
Get-ExchangeServer	Retrieves a list of Exchange servers and reports the server role and version
Get-Recipient	Counts the number of mailboxes

2. Create a role group that combines all the new custom roles. Assign this final role group to the Cloud Extender service account.

9.4.2 Base Roles

Use one of the following five base roles as a template for creating custom roles:

1. Organization Client Access
2. Mail-Recipients
3. View-Only Configuration
4. Recipient Policies
5. User Options

When combined, these five role groups contain access to all the required PowerShell commands for Cloud Extender to function. However, the best approach is to create a new custom role that encompasses all access rights to the PowerShell commands that are used by the Cloud Extender.

Parent topic: [Exchange (On-Premises and Cloud) Integration Module]

9.5 About Exchange Organization Administrators (Exchange 2007)

With Exchange 2007, you cannot grant a subset of rights associated with a role group to a particular user account. To access rights for the Exchange Organization Administrator, the user account must have access to all rights associated with that role.
Microsoft provides the following four pre-defined access role groups to delegate these rights:

Role Group	Description
Administrators	The highest access group, which grants full rights over the Exchange organization.
Exchange Recipient Administrators	Grants full access mailbox level rights for assigned users but restricts access to organization level settings.
Exchange View-Only Administrators	Grants full view (read-only) access at both the organization and the recipient levels.
Exchange Servers Administrators	Grants full access rights at the Exchange server level but restricts access to read-only at an organization level.

Parent topic: Exchange (On-Premises and Cloud) Integration Module

9.6 About Office 365 Budgets

Office365 Wave15 uses an access budget policy to limit the resources that are available to a client on the Office 365 server, which causes some of the functions of the Cloud Extender™, such as device discovery, to fail.
To work with service accounts in Office 365 that reach the maximum allocated budget, the enhanced Cloud Extender module for Office 365 works with multiple service accounts as follows:

1. A dedicated service account gathers all mailboxes that are associated with ActiveSync devices.
2. Multiple service accounts (scaled according to guidelines) work on selected portions of the mailbox list to discover devices.
3. Any service account that reaches the maximum allocated budget cannot participate in the device discovery process until the account is unlocked.
4. A dedicated service account handles real-time actions from the MaaS360® Portal against Office 365.

For better performance, configure multiple service accounts in the Cloud Extender for Office 365 integration and increase the budgets on these service accounts to higher limits.

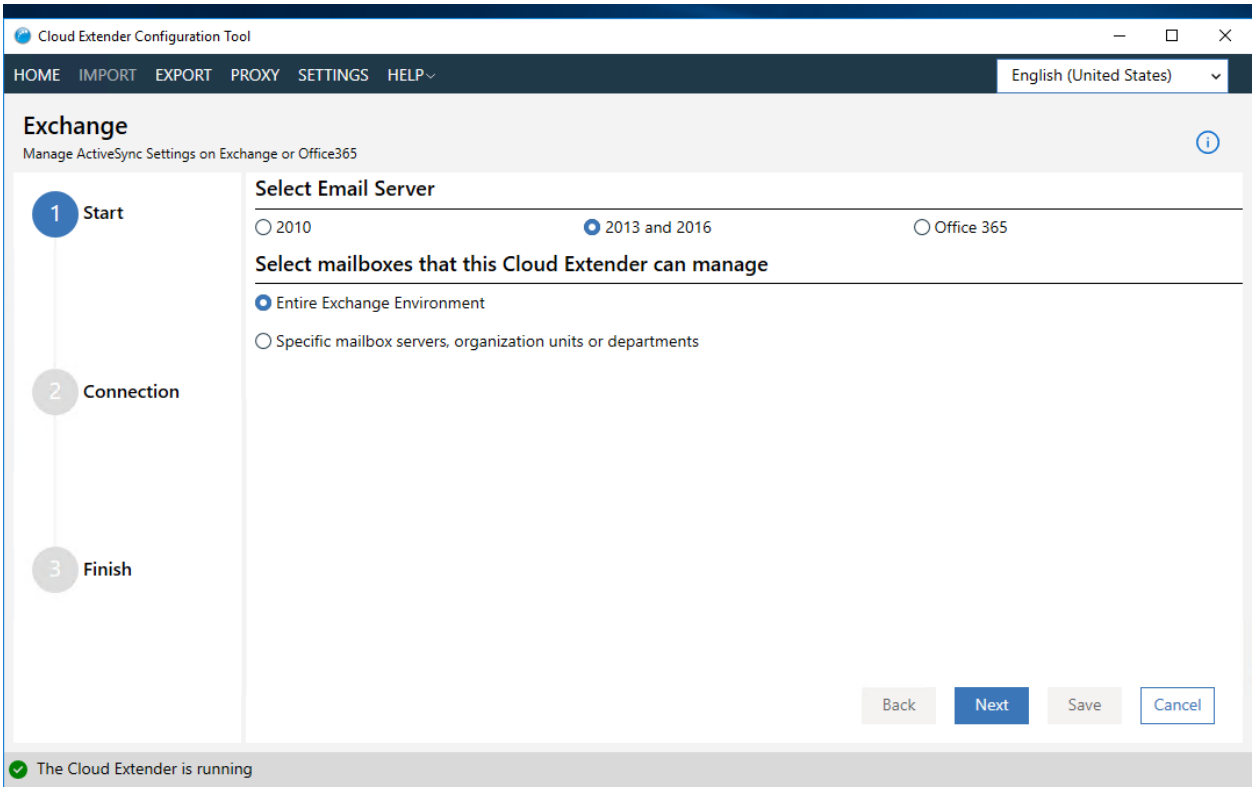
Parent topic: Exchange (On-Premises and Cloud) Integration Module

9.7 Exchange Integration Configuration

Follow these steps to configure basic settings for the Cloud Extender™ to integrate with Exchange.

9.7.1 Procedure

1. Open the Cloud Extender Configuration Tool and verify all prerequisites are met.
    a. Hover your mouse over the **Exchange** tile and then hover over the green checkmark or red X in the lower left corner.
2. Select the **Exchange** tile.
3. Select the version of Exchange that you are using and click the **Next** button.



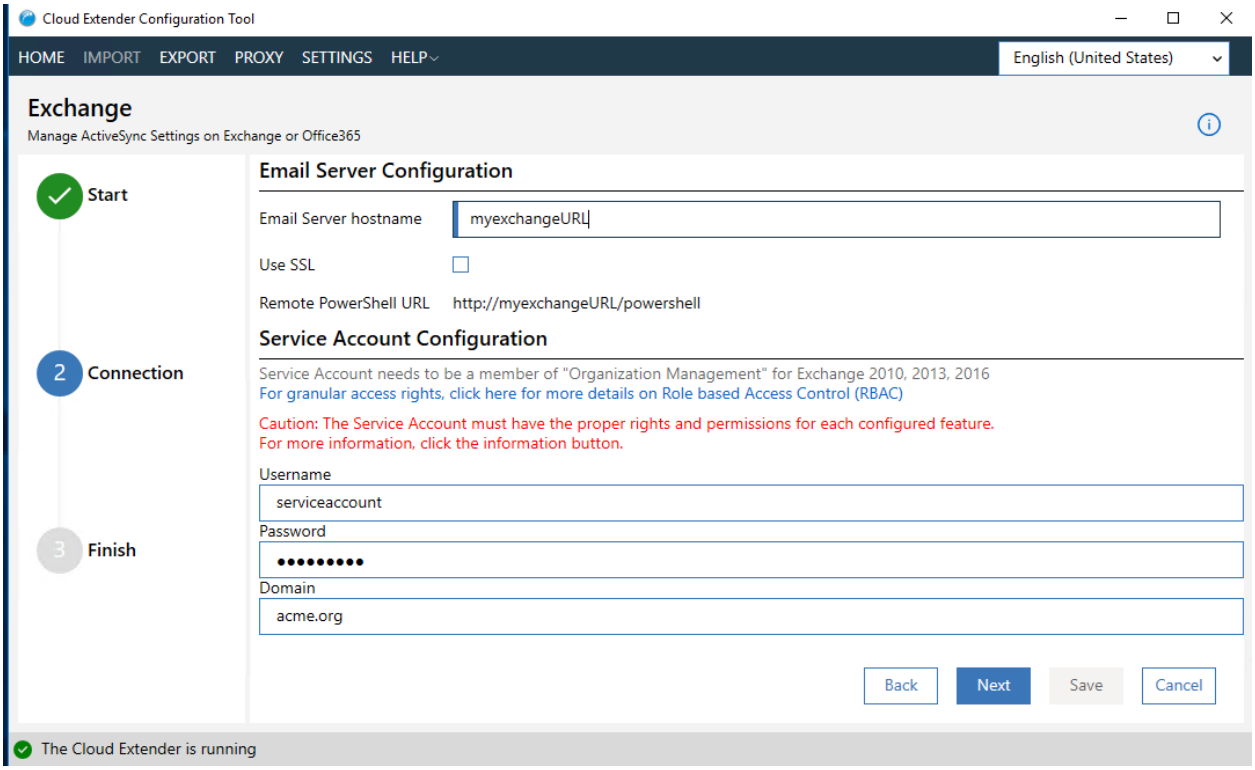
4. Configure the following settings based on server type:
    a. If you are using Exchange On-Premises (20101, 2013, 2016), supply the Exchange server URL and service account credentials.

Parameter	Description
Exchange server URL	For Exchange 2010, 2013, and 2016 integration, the Cloud Extender uses Remote PowerShell. Use the following formats to configure your Remote PowerShell URL from the Cloud Extender Configuration Tool: The Remote PowerShell URL format: `https://<CAS-Serverhostname>/powershell` Cloud Extender does not support a load-balanced CAS (Client Access Server) array. The Cloud Extender must point to PowerShell on a specific CAS server. If you use RBAC roles for the service account, the Cloud Extender Configuration Tool does not display a warning that permissions are not validated. This behavior is expected and does not affect the configuration process.
Username, password, domain	The credentials for the service account. The service account must be a local administrator on the Cloud Extender server and must have necessary rights on Exchange for integration: either standard rights or RBAC rights.

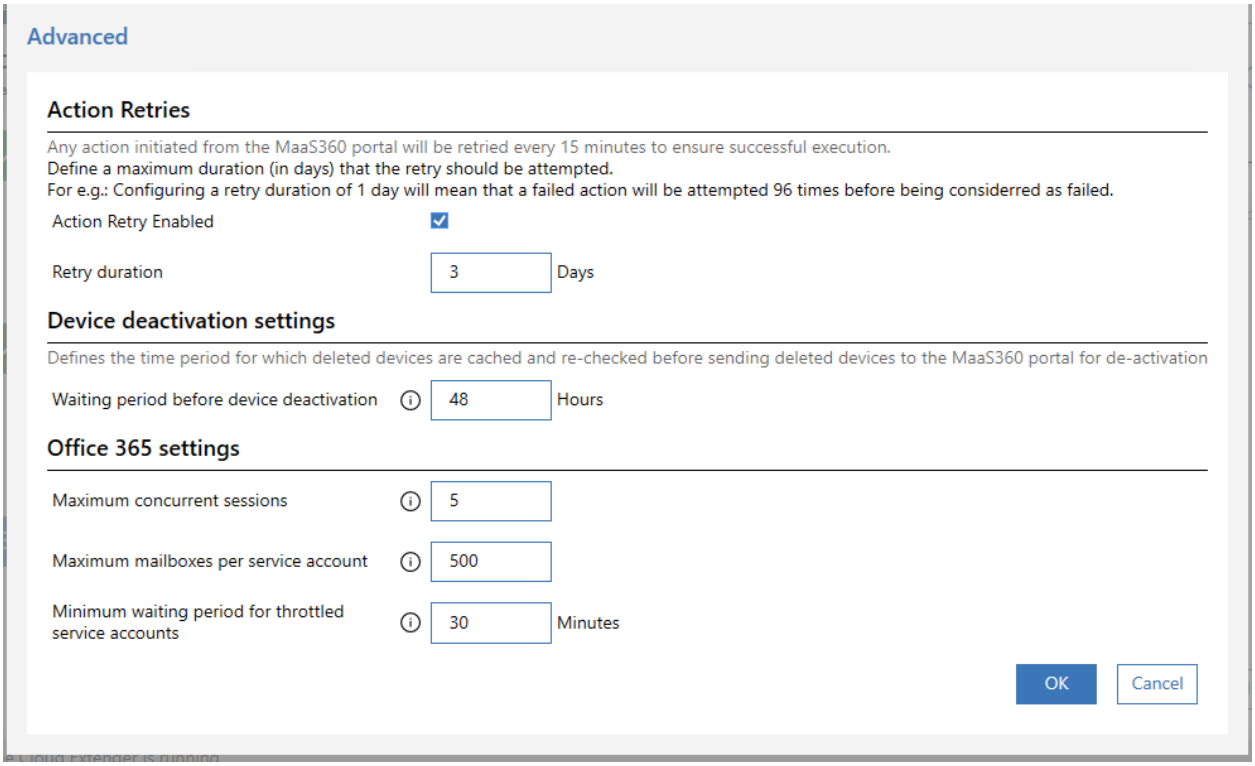
b. If you are using Office 365, configure the Office 365 PowerShell URL and the required service accounts.

Parameter	Description
Office 365 Server URL	The Cloud Extender automatically fills the Office 365 PowerShell URL as `https://ps.outlook.com/powershell`. Make sure that the Cloud Extender can connect outbound to this URL from the Cloud Extender network.
Office 365 Accounts	Click the (+) plus sign to add the number of service accounts based on the guidelines for your environment.
Use IE Proxy Settings	If the outbound connection from the Cloud Extender network to the Office 365 PowerShell URL must use the internal proxy, complete the following steps: Open the Internet Explorer (IE) or Edge browser on the Cloud Extender server in **`SYSTEM`** context or **`Service Account`** context. **Note:** Opening IE/Edge from the **Start** menu starts the browser as the logged in administrator and not in **`SYSTEM`** context. To switch to **`SYSTEM`** context, use `psexec` from SysInternals or press **Shift** and click **IE**, and then run the browser as the **`SYSTEM`** user. Select **Tools** > **Internet Options** > **Connections Tab** > **LAN Settings**. Configure proxy settings for the internal proxy, and then apply the settings. The Cloud Extender Configuration Tool uses this proxy setting to establish a remote PowerShell session to

	Office 365. The proxy settings on the first page of the Cloud Extender Configuration Tool do not apply to Office 365 connections.
Validate All Accounts	Click this button to have the Cloud Extender run validation checks against Office 365 from each configured service account. The Cloud Extender checks for connectivity, validity of credentials, and permissions for each configured service account, including any accounts with issues. Make sure that all service accounts are functional.



5. Click the **Next** button
6. Configure Advanced settings
    a. Review the current values in the Advanced settings and make modifications if required.



Parent topic: [Exchange (On-Premises and Cloud) Integration Module]

9.8 Advanced Exchange Integration Features

Restricting the Scope of the Cloud Extender

Use this setting if you want the Cloud Extender to discover devices only from a subset of mailbox servers, domains, or an OU list in the Exchange environment.

Multiple Cloud Extenders for Exchange Integration

Information about using multiple instances of the Cloud Extender for integration with Exchange.

Master Cloud Extender in Multi-Cloud Extender Environments

The MaaS360® Portal and the Cloud Extender are designed to designate one Cloud Extender as the master Cloud Extender and additional Cloud Extenders as non-master Cloud Extenders.

Advanced Office 365 Integration Options

Information about configuring advanced settings for the Cloud Extender to integrate with Office 365.

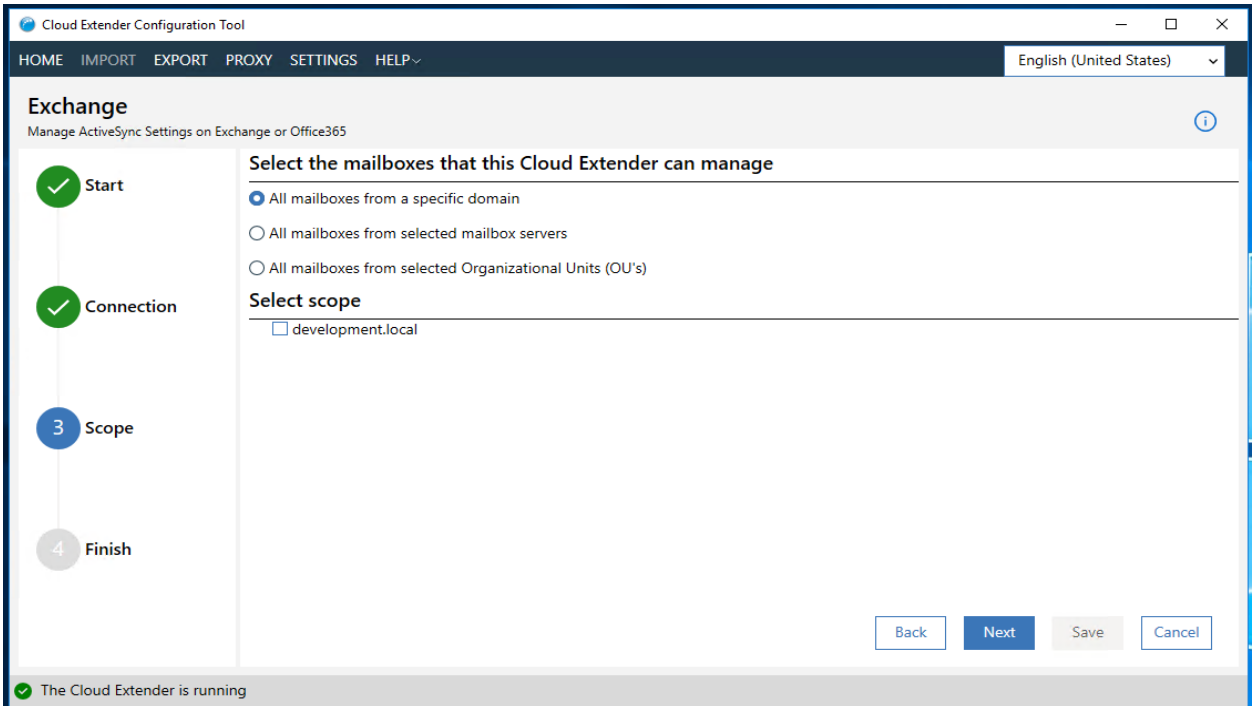
Action retry Settings for Failed Actions on Devices (Exchange/Office 365)

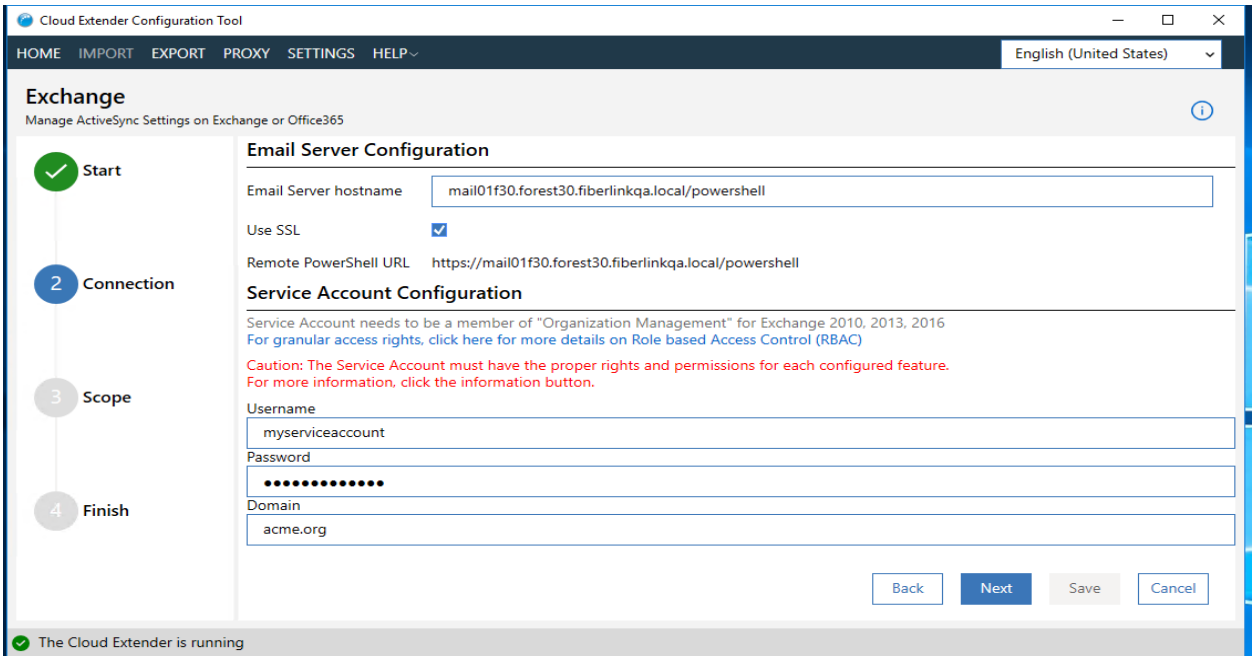
Information about configuring Action Retry settings for actions that failed on devices against Exchange or Office 365.

Parent topic: Exchange (On-Premises and Cloud) Integration Module

9.9 Restricting the Scope of the Cloud Extender

Use this setting if you want the Cloud Extender™ to discover devices only from a subset of mailbox servers, domains, or an OU list in the Exchange environment.





Note: If you require multiple Cloud Extenders for your Exchange environment, see Multiple Cloud Extenders for Exchange Integration for detailed information.

Parent topic: Advanced Mode: Exchange Integration

9.10 Multiple Cloud Extenders for Exchange Integration

Information about using multiple instances of the Cloud Extender™ for integration with Exchange.

Use multiple instances of the Cloud Extender for the following scenarios:

1. In a large Exchange environment, you require multiple Cloud Extenders to discover devices from a subset of mailbox environments. Use regional Cloud Extenders to work against regional mailbox servers.

   Example: An environment contains 8000 mailboxes in North America, 5000 mailboxes in Europe, and 6000 mailboxes in Asia. All regions use Exchange 2013. In this scenario, use three Cloud Extenders, one Cloud Extender for each region.
2. You are using multiple versions of Exchange and need to integrate with all the versions of Exchange that you are using.

   Example: You are migrating from an Exchange 2010 mail environment to an Office 365 mail environment. You have 500 mailboxes on the Exchange 2010 environment and 9500 mailboxes on the Office 365 environment. In this scenario, use two Cloud Extenders, one Cloud Extender for Exchange 2010 and one Cloud Extender for Office 365 with multiple service accounts.

Use the Cloud Extender Scaling Tool at **Setup** > **Services** > **Enterprise Email Integration** to determine the number of Cloud Extenders that you require for your environment. The scaling tool completes the device discovery script within 30 minutes. Depending on your environment, regional Cloud Extenders might be required to avoid latency issues.

9.11 Multiple Cloud Extender Support for Office 365 Integration in Large Environments

If your Office 365 environment uses several mailboxes that contain over 10,000 devices, one Cloud Extender might take a significant amount of time to scan the environment from a device discovery standpoint, even if you configured several service accounts. The amount of time to scan the environment is even more critical if you enabled Auto-Quarantine on Office 365 and you must quickly discover new devices. Office 365 also imposes throttling limitations on PowerShell commands that can increase scan times in large environments.

To introduce parallel processing and reduce delays, MaaS360® now supports installing multiple Cloud Extenders against Office 365. The following list explains how the integration works with multiple Cloud Extenders:

1. The first Cloud Extender that is installed against Office 365 is the master Cloud Extender.
2. The master Cloud Extender receives a list of all mailboxes and the devices in those mailboxes. This list is named the master mailbox list.
3. Any additional Cloud Extender that is installed against Office 365 assumes a non-master role.
4. The master Cloud Extender splits the master mailbox list into equal portions based on the total number of Cloud Extenders.
5. Each Cloud Extender receives its own list and works only with those mailboxes for device discovery and actions.
6. If the master Cloud Extender is offline, one of the non-master Cloud Extenders automatically assumes the master Cloud Extender status (within 24 hours). The master Cloud Extender is responsible for enabling Auto-Quarantine in the environment. An action in the MaaS360 Portal forces which non-master Cloud Extender becomes the new master Cloud Extender.

When the administrator configures the Cloud Extenders for Office 365 integration, the administrator must also configure unique service accounts for each Cloud Extender.
All the service accounts that are used across the Cloud Extender setups can communicate in parallel with Office 365, adding to the concurrent sessions currently running as part of the existing Cloud Extender setup.

However, the tenant budget remains the same and setting up multiple Cloud Extenders does not alter this budget. You still set the total number of service accounts and concurrent sessions that are used according to the environmental restrictions to make sure that throttling errors do not occur.
Note: Multiple Cloud Extenders for Office 365 function only when there are at least three or more service accounts that are configured on each of the Cloud Extenders.

Parent topic: [Advanced Mode: Exchange Integration]

9.12 Master Cloud Extender in Multi-Cloud Extender Environments

The MaaS360® Portal and the Cloud Extender™ are designed to designate one Cloud Extender as the master Cloud Extender and additional Cloud Extenders as non-master Cloud Extenders.
When you set up multiple Cloud Extenders for your environment, consider the following things:

1. The master Cloud Extender is responsible for enabling Auto-Quarantine (AQ). For any MaaS360 Portal account, you can have only one master Cloud Extender for Exchange integration. All other Cloud Extenders for Exchange Integration must be marked as non-master.
2. The option to set master status for Cloud Extender is not available in Basic configuration mode. When you configure the Cloud Extender in Basic configuration mode, that Cloud Extender assumes master status.
3. When you configure the Cloud Extender for Office 365, that Cloud Extender assumes master status. If you require additional Cloud Extenders to integrate with other versions of Exchange, mark those additional Cloud Extenders as non-master. In mixed environments, the environment that the master Cloud Extender is pointing to enables Auto-Quarantine (AQ).
   Example: In scenarios where you configured one Cloud Extender for Office 365 (master) and one Cloud Extender for Exchange 2010 (non-master), enable Auto-Quarantine (AQ) only on Office 365.

9.13 Configuring Multiple Cloud Extenders

To configure multiple instances of Cloud Extender, follow these steps:

1. Follow steps 1 - 3 from the procedure in Exchange Integration Configuration
2. After you run the reachability tests, click **Next**. The Restrict devices import window is displayed.
3. Select **No** to restrict import, and then click **Next**. The Configure Exchange ActiveSync Integration window is displayed.
4. Configure the following options:

Option	Description
Enable Exchange ActiveSync Integration on multiple Cloud Extenders for distributed Processing	Select **Yes** if you use multiple Cloud Extenders for Exchange Integration.
Select the mailbox servers that this Cloud Extender will manage	If **Enable Exchange ActiveSync Integration on multiple Cloud Extenders for distributed processing** is set to **Yes**, the Cloud Extender Configuration Tool discovers and then lists all mailbox servers in the environment. Select the required mailbox servers from the list.
Configure this Cloud Extender to manage policies and Auto-Quarantine settings	Select **Yes** to set the Cloud Extender as the master. See Multiple Cloud Extenders for Exchange Integration to determine the appropriate value for this Cloud Extender.

Parent topic: Advanced Mode: Exchange Integration

9.14 Advanced Office 365 Integration Options

Information about configuring advanced settings for the Cloud Extender™ to integrate with Office 365.
Configure the following options to integrate the Cloud Extender with Office 365:

Option	Description
Waiting period for device deregistration (hours)	If a device is removed directly from the Exchange server, the Cloud Extender detects this removal. However, the device is not removed immediately from MaaS360®. The Cloud Extender maintains the deleted devices in a cache on the Cloud Extender for 48 hours before the Cloud Extender signals the MaaS360 Portal to remove the devices. The default setting is 48 hours. Depending on your environment, you can adjust this setting. This setting applies to all versions of Exchange, not just Office 365.
Maximum concurrent PowerShell scripts	The maximum number of concurrent PowerShell scripts that you can run on the Cloud Extender for Office 365 device discovery. The default is five scripts. Increase this value, if you experience timeouts.
Maximum mailboxes queried per configured account	The default is 500 mailboxes for each service account. You can adjust this number if want a service account to query more mailboxes for device discovery. **Note:** Increasing this limit delays the script.
Throttled account recover	When a service account reaches

time (minutes)	its maximum budget, the service account must wait before the budget limit is lifted, and it can make further calls to Office 365. Based on testing, recovery time is typically 30 minutes. The Cloud Extender waits for 30 minutes before reusing the service account after the account is throttled. If certain accounts are throttled more frequently, increase the recovery time.

Parent topic: [Advanced Mode: Exchange Integration]

9.15 Action Retry Settings for Failed Actions on Devices (Exchange/Office 365)

Information about configuring Action Retry settings for actions that failed on devices against Exchange or Office 365.
The Cloud Extender™ supports the following actions for retry:

Action	Description
Approve Device	Syncs email on the device
Block Device	Blocks the device from syncing email on the device
Remove Device	Removes the device from the mailbox
Wipe Device	Issues a factory reset wipe on the device
Change Policy	Changes the ActiveSync policy that is associated with the device

[[Configuration Screenshots]]

Option	Description
Action Retry Enabled	Select this option to retry actions that previously failed on devices against Exchange or Office 365.
Retry Time Limit (Hours)	The maximum number of times the failed actions are retried before the action ultimately fails. Enter the number of hours (168 hours or 7 days) to retry the action. You can configure this setting during any server outage or maintenance window. By default, the retry action runs every 15 minutes. If the action succeeds, the Cloud Extender notifies the MaaS360® Portal about the successful attempt. If the action fails, the next retry occurs during the next iteration for the specified

	time limit. The Cloud Extender attempts a retry under the following conditions: Connection failures where the Cloud Extender cannot reach the server or cannot authenticate due to invalid credentials. Office 365 throttling lockouts PowerShell timeouts

9.16 Action Retry Settings Available from the MaaS360 Portal

The Action Retry framework is now available from the MaaS360 Portal. If the MaaS360 Portal is unable to successfully send an action to the Cloud Extender, the MaaS360 Portal retries the action until the action is successful (up to a maximum of 3 days). The following actions are supported for retries from the MaaS360 Portal:

Action	Description
Approve	Sends an approve action to Exchange that allows users to sync email. If you Exchange environment uses Auto-Quarantine and rules to automatically approve enrolled and compliant devices, this action is critical because the user needs access to email. The retry logic makes sure that the approve actions are always sent down to the Cloud Extenders.
Block	Sends a block action to Exchange to block users from syncing email. This action is sent if the device is out of compliance and compliance rules are configured to block the email sync. If the Cloud Extender is not reachable, the action is retried.
Remove	Sends an action to remove a device from the mailbox. This action is sent to clean up activity where a device is not reporting and needs to be cleaned up in time for accurate license reporting.

Parent topic: Advanced Mode: Exchange Integration

9.17 Cloud Extender Settings in the MaaS360® Portal

Use the following procedures to enable the Cloud Extender™ features, Auto-Quarantine (AQ) and Auto-Cleanup, to integrate with Exchange.

Enabling Auto-Quarantine (AQ) for Exchange

Follow these steps to enable the Cloud Extender Auto-Quarantine (AQ) feature for integration with Exchange.

Enabling Auto-Removal with Exchange

Follow these steps to remove old ActiveSync connections based on when the devices reported back to Exchange.

Parent topic: Exchange (On-Premises and Cloud) Integration Module

9.18 Enabling Auto-Quarantine (AQ) for Exchange

Follow these steps to enable the Cloud Extender™ Auto-Quarantine (AQ) feature for integration with Exchange.

9.18.1 About This Task

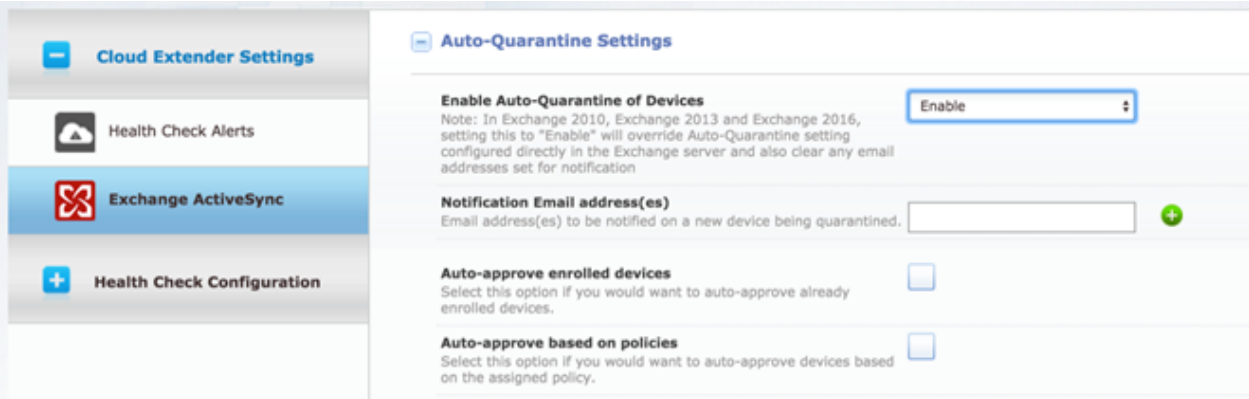
The Auto-Quarantine (AQ) feature for the Exchange Integration module provides the following benefits:

1. Prevents new devices from connecting to your Exchange server with ActiveSync
2. Automatically approves devices that are enrolled in MaaS360® Automatically approves devices that receive email settings only from MaaS360
3. Automatically approves Secure Mail records

Note: When you enable Auto-Quarantine (AQ) in the Cloud Extender policies, the Cloud Extender automatically approves existing ActiveSync devices and then enables Auto-Quarantine (AQ). Only new devices are blocked. Existing ActiveSync devices are not affected. However, if you enable Auto-Quarantine (AQ) directly on Exchange, instead of using MaaS360, existing ActiveSync devices are blocked.

9.18.2 Procedure

1. Log in to the MaaS360 Portal with Administrator credentials.
2. Select **Setup** > **Cloud Extender Settings**, and then click **Edit**.
3. Configure policies in the Exchange ActiveSync section.



Option	Description
Enable Auto-Quarantine of Device	Use the default setting, where the Cloud Extender uses the Auto-Quarantine (AQ) setting that is configured on the Exchange server or enable or disable Auto-Quarantine (AQ).
Notification Email Address(es)	A comma-separated list of email addresses that are notified when a new device is quarantined.
Auto-Approve Enrolled Devices	Automatically approves email connections from devices that are enrolled in MaaS360. The device is briefly quarantined before enrollment is confirmed.
Auto-Approve Based on Policies	Automatically approves email connections from enrolled devices when the email configuration is pushed from MaaS360. This setting requires that you configure MDM / Persona policies to push email configuration to devices. This setting blocks connections from the device if the user manually configures email on email clients. Only MDM pushed email configuration is approved.

4. Click **Save & Publish**. The Secure Mail records are automatically approved regardless of whether Auto-Quarantine (AQ) is enabled from the MaaS360 Portal or enabled directly on Exchange.

MaaS360 merge process for mobile device records
Information about configuring the Cloud Extender policies for auto-approvals (enrolled or based on policy).

Parent topic: Cloud Extender Settings in the MaaS360 Portal

9.19 MaaS360 Merge Process for Mobile Device Records

Information about configuring the Cloud Extender™ policies for auto-approvals (enrolled or based on policy).

9.19.1 Device Sources

A device has two sources: one source from the enrolled record and one source from the Cloud Extender discovery process.

1. When a device enrolls in MaaS360®, a device record is formed on the device. The device identifier for this record is the serial number or device ID from each platform.
2. When the user configures email on the same device, the email client registers to Exchange again with a device identifier. The Cloud Extender discovers this device connection within the mail infrastructure and imports the device information in MaaS360.

MaaS360 merges these two records into one record:

1. If the serial number or device ID of the ActiveSync managed device exactly matches the enrolled device, then the two records merge as one record for the device.
2. If the device IDs do not match, for example if you are using Android devices where the native or third-party email clients use their own device IDs to register with Exchange, there might be issues with the merge process. MaaS360 uses platform and manufacturer attributes from the two records to determine whether it can match the records. If MaaS360 can successfully match the two records, it merges the two records into one record.
3. If MaaS360 cannot merge records, it displays potential match candidates on the user interface for administrators to log in and manually merge records. Access this workflow from **Devices** > **Exceptions**.

9.19.2 Workflow

The auto-approval feature follows this workflow:

1. A device enrolls in MaaS360.

2. The user either configures email manually on the device or pushes the email configuration from the MDM. The user completes the email setup.
3. If Auto-Quarantine (AQ) is enabled, the email record is quarantined. The user is blocked from receiving email. The only exception is if the user set up email through the Secure Mail client. MaaS360 approves the email record because it recognizes and pre-approves the device ID that the Secure Mail client uses.
4. The Cloud Extender scripts run and discover the new quarantined device. Depending on the number of Cloud Extenders that are configured and how long the discovery process takes, this process might take 15 minutes to a couple of hours.
5. When the ActiveSync managed device is discovered, the MaaS360 platform runs the merge logic, and merges devices from the two sources. The merge logic runs every 15 minutes.
6. The MaaS360 platform issues a device approval action to the Cloud Extender that approves the quarantined device on Exchange.
7. The user starts to receive email.

9.19.3 Caveats

Consider the following issues with the auto-approval feature:

1. If the user is not using Secure Mail client, the email connection is quarantined on the first connection.
2. It might take 30 minutes to a couple of hours for email messages to flow.
3. On certain devices when a merge is not completed, the email record remains blocked until the admin manually merges potential candidates.

Parent topic: [Enabling Auto-Quarantine (AQ) for Exchange]

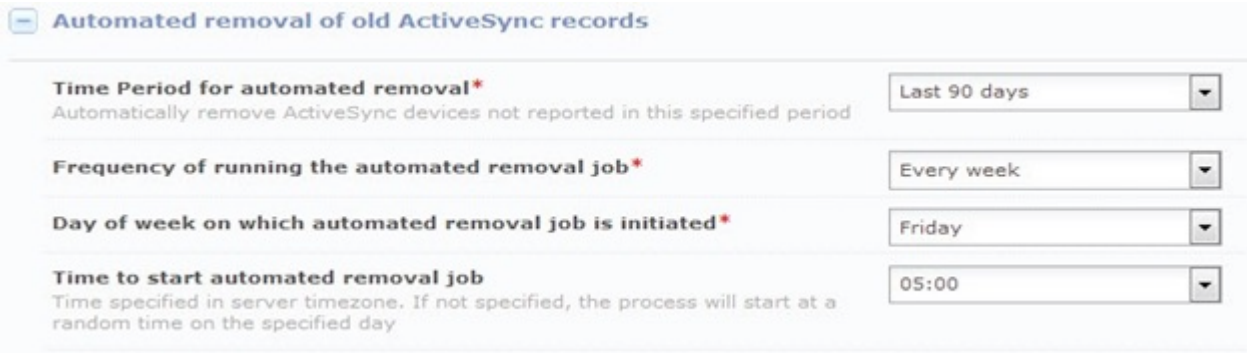
9.20 Enabling Auto-Removal with Exchange

Follow these steps to remove old ActiveSync connections based on when the devices reported back to Exchange.

9.20.1 About This Task

In most Exchange environments, old ActiveSync connections remain associated to user mailboxes and are often not removed. Use the Cloud Extender™ policies to automatically and periodically clean up old ActiveSync connections based on when these devices reported back to Exchange. The Cloud Extender runs scripts to clean up your Exchange environment.

Note: Enable **Auto-Removal** before you enable **Auto-Quarantine** or apply compliance rules to enforce enrollment.



9.20.2 Procedure

1. Log in to the MaaS360® Portal as the administrator.
2. Select **Setup** > **Cloud Extender Settings**.
3. Select **Exchange ActiveSync**, and then click **Edit**.
4. Select the **Enabled Automated removal of old ActiveSync records** check box.
5. Configure the following options:

Options	Description
Time Period for Automated Removal	Automatically removes ActiveSync devices from mailboxes that do not report in the last (x) days:

	Last 30 days Last 60 days Last 90 days (most common) Last 180 days
Frequency of Running the Automated Removal Job	Defines how often the Cloud Extender runs cleanup scripts: Every week (most common) Every alternative week Every fourth week
Day of Week on Which Automated Removal Job is Initiated	Select any day of the week.
Time to Start Automated Removal Job	Hour in GMT +0 time (hh:mm)

6. To view the last time the automated removal command ran on the server, select **Setup** > **Cloud Extenders** > **Select your Cloud Extender** with Exchange Integration implemented.
7. C. Click **Summary** > **Exchange ActiveSync**. From the Automated Removal Settings section, view the last time the Cloud Extender ran the removal command and how many devices were deleted.

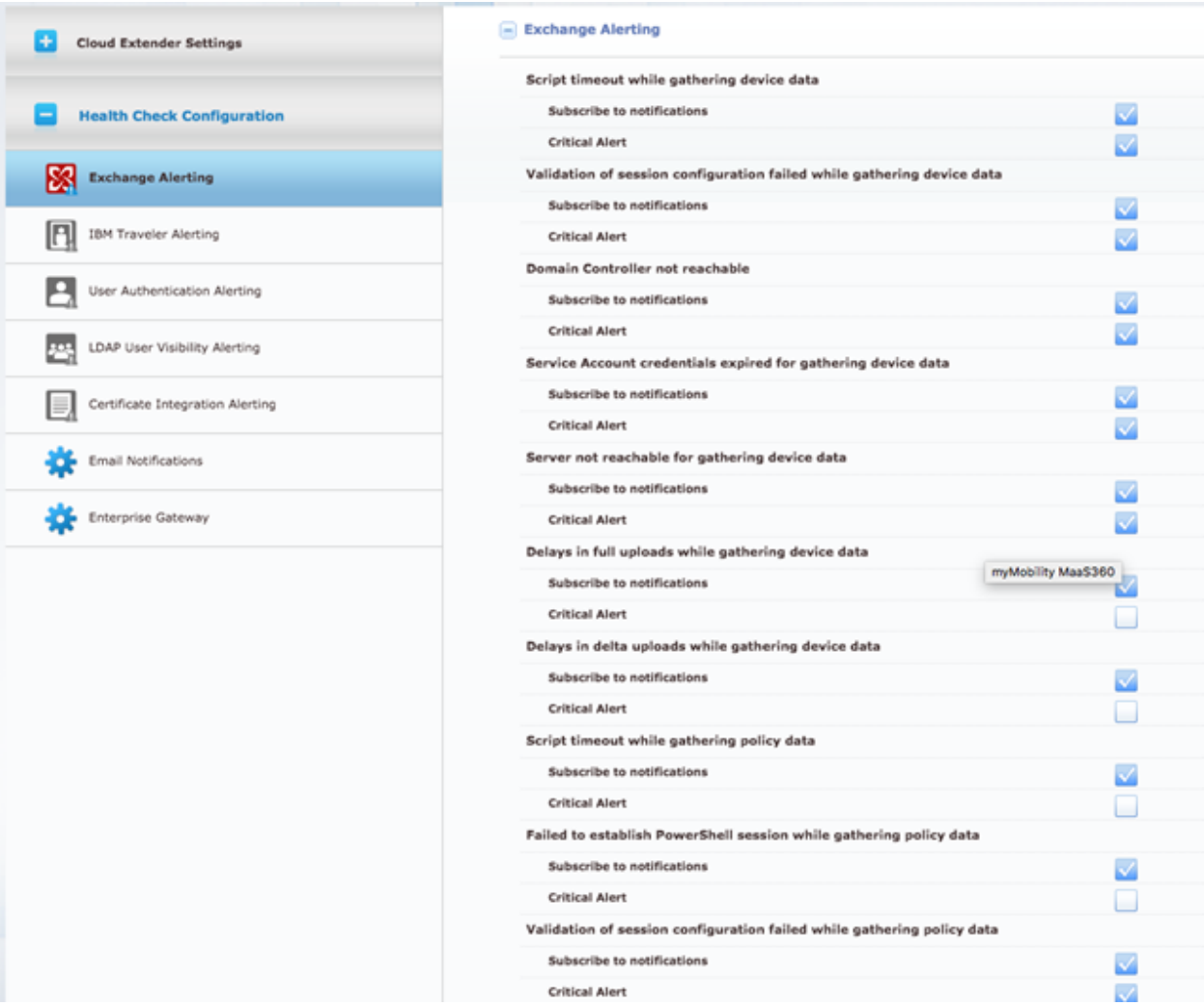
Parent topic: [Cloud Extender Settings in the MaaS360 Portal]

9.21 Enabling Health Check Alerts for Exchange Integration

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ Exchange Integration module.

9.21.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.
2. Select **Health Check Configuration** > **Exchange Alerting**. The Exchange Alerting list is displayed.



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
Script timeout while gathering device data	The device discovery script is taking more time to complete than the configured threshold. The MaaS360 Portal might not contain the most recent device information from Exchange.	The device discovery script times out due to the following issues: Too many mailboxes and devices in your Exchange environment. The Cloud Extender is trying to reach remote mailbox servers that are slowing down the script. Follow these steps to remediate this alert: Use the Cloud Extender Scaling Tool to determine whether you require multiple Cloud Extenders for your environment and whether your current scale meets the criteria. From the MaaS360 Portal Home page, select **Setup** > **Services** > **Enterprise Email Integration** to download the scaling tool.

		If this issue continues, collect logs from the Cloud Extender, and then contact IBM® Support for guidance on correct scaling or recommendations on how to increase the timeout settings.
Validation of session configuration failed while gathering device data	The Cloud Extender did not establish a PowerShell session because the validation of the Exchange PowerShell session configuration failed.	The PowerShell session validation typically fails when the service account does not use the required permissions. Verify that the service account uses the correct permissions from the prerequisites. If you are using RBAC roles, verify that all access rights are correctly provisioned to the service account. For more information, see About Exchange Role-Based Access Control (RBAC). From the Cloud Extender Configuration Tool in the MaaS360 Portal, update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

Domain Controller not reachable	The Cloud Extender cannot connect to the Exchange server because the domain controller or global catalog is unreachable.	Verify that the Exchange server URL that is listed in the Cloud Extender Configuration Tool is still valid. Verify that domain controllers, global catalog servers, and the Exchange servers are operational and reachable from the Cloud Extender server (check for recent proxy or firewall changes). If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Service Account credentials expired for gathering device data	The Cloud Extender cannot connect to the Exchange server to gather device data because the service account credentials are expired or invalid.	Verify that the configured Remote PowerShell URL is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, use the Test Reachability workflow to confirm. Check whether the configured service account is still active and that the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal

		to update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server not reachable for gathering device data	The Cloud Extender cannot connect to the Exchange server because the Exchange server is unreachable or the PowerShell URL settings are incorrect.	A remote PowerShell session cannot be established. Verify that the specified Exchange server URL is still valid and reachable. Verify that the remote PowerShell URL is pointing to a specific CAS server, not a load-balanced CAS array. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Delays in full uploads for gathering device data	The last successful and complete upload of device details from the server occurred more than a day ago from the scheduled	The scheduled full discovery and sync of mobile devices from your Exchange mail environment did not

	upload date. The server is unreachable or the service account is invalid.	complete within the expected time frame. Verify that the Cloud Extender that is configured for Exchange Integration is operational. Check whether the service account is still active and the password is not expired. Check whether the Remote PowerShell URL for the Exchange or Office 365 server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Test for Exchange** to run a **Test** action on the Cloud Extender that is configured for Exchange Integration. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Refresh Data (Exchange ActiveSync)** to refresh the Exchange data. Wait 1 hour to confirm that the issue is

		resolved. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Delays in delta uploads while gathering device data	The last successful incremental upload of device details from the server is more than 8 hours from the scheduled upload date. The server is unreachable or the service account is invalid.	The scheduled Incremental discovery and sync of mobile devices from your Exchange mail environment did not complete within the expected time frame. Verify that the Cloud Extender that is configured for Exchange Integration is operational. Check whether the service account is still active and the password is not expired. Check whether the Remote PowerShell URL for the Exchange or Office 365 server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Test for Exchange** to run a **Test** action on the Cloud Extender that

		is configured for Exchange Integration. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Refresh Data (Exchange ActiveSync)** to refresh the Exchange data. Wait 1 hour to confirm that the issue is resolved. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Script timeout while gathering policy data	The Exchange policy discovery script is taking more time to complete than the configured threshold. The MaaS360 Portal might not contain the most recent list of policies from Exchange.	The policy discovery script times out due to the following issues: Too many policies that are defined in your Exchange environment. The Cloud Extender is trying to reach remote Exchange servers that are slowing down the script. Follow these steps to remediate this alert: Use the Cloud Extender Scaling Tool to determine whether you require multiple

		Cloud Extenders for your environment and whether your current scale meets the criteria. From the MaaS360 Portal Home page, select **Setup** > **Services** > **Enterprise Email Integration** to download the scaling tool. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for guidance on correct scaling or recommendations on how to increase the timeout settings.
Failed to establish PowerShell session while gathering policy data	The Cloud Extender failed to establish a PowerShell session with Exchange servers during Exchange policy discovery.	The Cloud Extender uses a remote PowerShell session to communicate with the Exchange servers. A PowerShell session cannot be established. Verify that the specified Exchange server URL is still valid and reachable. Verify that the remote PowerShell URL is pointing to a specific CAS server, not a load-balanced CAS array. Check for recent firewall or proxy changes that might

		block access from the Cloud Extender server to the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Validation of session configuration failed while gathering policy data	The validation of the Exchange PowerShell session configuration failed during Exchange policy discovery.	The PowerShell session validation typically fails when the service account does not use the required permissions. Verify that the service account uses the correct permissions from the prerequisites. If you are using RBAC roles, verify that all access rights are correctly provisioned to the service account. For more information, see About Exchange Role-Based Access Control (RBAC). From the Cloud Extender Configuration Tool in the MaaS360 Portal, update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

Office 365 account throttled while gathering policy data	The Office 365 service account(s) reached the maximum allocated budget. Certain service accounts exceeded the maximum PowerShell usage budget and cannot execute data collection scripts. The MaaS360 Portal might not contain the most recent device information from Exchange.	The Office 365 throttling budget for certain service accounts is preventing the Cloud Extender from refreshing device or policy data. Verify that the correct number of service accounts are configured on the Cloud Extender based on scaling requirements. Configure more service accounts as needed. Adjust the Advanced configuration on the Cloud Extender for the number of mailboxes for each service account and the maximum concurrent PowerShell sessions based on the Office 365 throttling budgets that are configured on your tenant. Contact Microsoft Support to increase the throttling budget and concurrency. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

Service Account credentials expired for gathering policy data	The Cloud Extender cannot connect to the Exchange server to gather policy data because the service account credentials are expired or invalid.	Verify that the configured Remote PowerShell URL is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, use the Test Reachability workflow to confirm. Check whether the configured service account is still active and that the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server not reachable while gathering policy data	The Cloud Extender cannot connect to the Exchange server because the Exchange server is unreachable or the PowerShell URL settings are incorrect.	A remote PowerShell session cannot be established. Verify that the specified Exchange server URL is still valid and reachable. Verify that the remote PowerShell URL is pointing to a specific CAS server, not a load-balanced CAS array. Check for

		recent firewall or proxy changes that might block access from the Cloud Extender server to the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Delays in full uploads while gathering policy data	The last successful and complete upload of policy details from the server occurred more than a day ago from the scheduled upload date. The server is unreachable or the service account is invalid.	The scheduled full discovery and sync of mobile devices from your Exchange mail environment did not complete within the expected time frame. Verify that the Cloud Extender that is configured for Exchange Integration is operational. Check whether the service account is still active and the password is not expired. Check whether the Remote PowerShell URL for the Exchange or Office 365 server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Test for Exchange** to run a

		Test action on the Cloud Extender that is configured for Exchange Integration. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Refresh Data (Exchange ActiveSync)** to refresh the Exchange data. Wait 1 hour to confirm that the issue is resolved. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Delays in delta uploads while gathering policy data	The last successful incremental upload of policy details from the server is more than 8 hours from the scheduled upload date. The server is unreachable or the service account is invalid.	The scheduled Incremental discovery and sync of mobile devices from your Exchange mail environment did not complete within the expected time frame. Verify that the Cloud Extender that is configured for Exchange Integration is operational. Check whether the service account is still active and the password is not expired. Check

		whether the Remote PowerShell URL for the Exchange or Office 365 server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Test for Exchange** to run a **Test** action on the Cloud Extender that is configured for Exchange Integration. From the Cloud Extender Configuration Tool in the MaaS360 Portal, select **Setup** > **Cloud Extender** > **Actions** > **Refresh Data (Exchange ActiveSync)** to refresh the Exchange data. Wait 1 hour to confirm that the issue is resolved. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Failed to establish PowerShell session while gathering device data	The Cloud Extender failed to establish a PowerShell session to Exchange servers	The Cloud Extender uses a remote PowerShell session to communicate with

	while it gathered details from devices.	Exchange servers. A PowerShell session cannot be established. Verify that the specified Exchange server URL is still valid and reachable. Verify that the remote PowerShell URL is pointing to a specific CAS server, not a load-balanced CAS array. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Office 365 account throttled while gathering device data	The Office 365 service account(s) reached the maximum allocated budget. Certain service accounts exceeded the maximum PowerShell usage budget and cannot execute data collection scripts. The MaaS360 Portal might not use the most recent device information from Exchange.	The Office 365 throttling budget for certain service accounts is preventing the Cloud Extender from refreshing device or policy data. Verify that the correct number of service accounts are configured on the Cloud Extender based on scaling requirements.

		Configure more service accounts as needed. Adjust the Advanced configuration on the Cloud Extender for the number of mailboxes for each service account and the maximum concurrent PowerShell sessions based on the Office 365 throttling budgets that are configured on your tenant. Contact Microsoft Support to increase the throttling budget and concurrency. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Error in full uploads	The Cloud Extender cannot upload all device and policy information from Exchange due to critical errors during the sync.	Verify that the Exchange environment is operational. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to Exchange or the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then

		contact IBM Support for further assistance.
Error in incremental uploads	The Cloud Extender cannot upload new or changed device and policy information from Exchange due to critical errors during the sync.	Verify that the Exchange environment is operational. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to Exchange or the remote PowerShell URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [Exchange (On-Premises and Cloud) Integration Module]

9.22 High Availability (HA) Mode for Exchange Integration

Information about support for High Availability (HA) mode for Cloud Extender™ integration with Exchange.
The Cloud Extender for Exchange Integration does not support High Availability (HA) mode. You can set up backup Cloud Extenders in advance. If a Cloud Extender fails, use one of the backup Cloud Extenders.

Parent topic: Exchange (On-Premises and Cloud) Integration Module

10 IBM Traveler Integration Module

The Cloud Extender™ integrates with IBM® Traveler and IBM SmartCloud® environments to provide complete visibility to all ActiveSync devices connected to the mail system.
With IBM Traveler and IBM SmartCloud integration, the Cloud Extender functions in the following ways:

1. Queries the mail server by using APIs to discover ActiveSync devices.
2. Uploads the device list to the MaaS360® Portal for reporting and management functions.
3. Supports all ActiveSync device actions such as approve, block, or remove a device from the mailbox and wipes devices that are initiated by the MaaS360 Portal, either through administrative action or automated rules.
4. Enables Auto-Quarantine (AQ) to prevent new devices from connecting to IBM Traveler servers or IBM SmartCloud environments. Since existing ActiveSync devices are approved, existing connections are not affected by the quarantine process. Auto-Quarantine is supported on IBM Traveler 9+ and IBM SmartCloud.
5. Supports approval of Secure Mail connections, native connections from enrolled devices, and connections to the IBM Verse™ email client.

Important: The Cloud Extender integration with IBM Traveler and IBM SmartCloud does not affect the flow of email traffic because the Cloud Extender is not an email proxy. The Cloud Extender instance does not sit between email and devices. This integration provides visibility only to your email environment where you can manage devices. If the Cloud Extender is unavailable, users can continue to send and
receive email.

10.1 Supported Versions of IBM Traveler

The Cloud Extender integrates with both the on-premises and cloud versions of IBM Traveler. The Cloud Extender supports the following versions of IBM Traveler:

1. On-Premises: Lotus Notes® 8.5.2+
2. Cloud: IBM SmartCloud

10.2 Requirements and Scaling

The MaaS360 Portal offers a Cloud Extender Scaling Tool at **Setup** > **Services** > **Enterprise Email Integration**. Enter the number of mailboxes and devices that you plan to enroll for MaaS360 and determine how many Cloud Extenders you might need to support integration with IBM Traveler.

Consider the following guidelines for scaling the IBM Traveler integration:

1. Gather times for device data does not exceed 60 minutes and averages 25 – 40 minutes for 5,000 devices. Current and average gather times are available on the Cloud Extender Status page in the MaaS360 Portal.
2. To determine the number of Cloud Extender instances that you need for your environment, divide the potential number of ActiveSync connected devices by 5,000 and the number of Mailboxes by 10,000 and use the higher of the two values.
3. To minimize latency, regional Cloud Extenders might be more appropriate to use.

Table 1. Scaling requirements for IBM Traveler integration module

Item	Requirement
IBM Traveler (less than 10,000 mailboxes)	Mailboxes: less than 10,000 Devices: less than 5,000 devices CPU: 2 cores Memory: 8 GB
IBM Traveler (more than 10,000 mailboxes)	Mailboxes: more than 10,000 Devices: more than 5,000 CPU: Use more Cloud Extenders Memory: N/A
IBM SmartCloud	Mailboxes: All

	Devices: All CPU: 2 cores Memory: 8 GB Scaling: Supports only one instance of the Cloud Extender for each URL. For accurate scaling of your environment, see the Cloud Extender scaling document at **Setup** > **Services** > **Enterprise Email Integration**.

Module Requirements:

1. IBM SmartCloud Notes® or Lotus® Domino® 8.5.2 or later
2. For IBM Traveler integration: The Cloud Extender must be installed on a computer installed with the Lotus Notes client.
3. For IBM SmartCloud: Network access from the Cloud Extender server to the IBM SmartCloud URL.
4. .NET 3.5 or higher

Permission Requirements:

1. For Lotus Notes 8.5.2+: A Domino account and credentials with sufficient rights for the Domino/Traveler Admin. You must have at least an access level of Server Remote Admin Manager with delete access to `Traveler.nsf`.
2. For IBM SmartCloud: Account with Administrator rights in the IBM SmartCloud environment.

IBM Traveler Integration

Follow these steps to configure basic settings for the Cloud Extender to integrate with IBM Traveler.

Enabling Auto-Quarantine (AQ) for IBM Traveler or IBM SmartCloud

Follow these steps to enable the Cloud Extender Auto-Quarantine (AQ) integration with IBM Traveler or IBM SmartCloud.

Enabling Health Check Alerts for IBM Traveler Integration
Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender IBM Traveler Integration module.

High Availability (HA) Mode for IBM Traveler Integration
Information about support for High Availability (HA) mode for Cloud Extender integration with IBM Traveler or IBM SmartCloud.

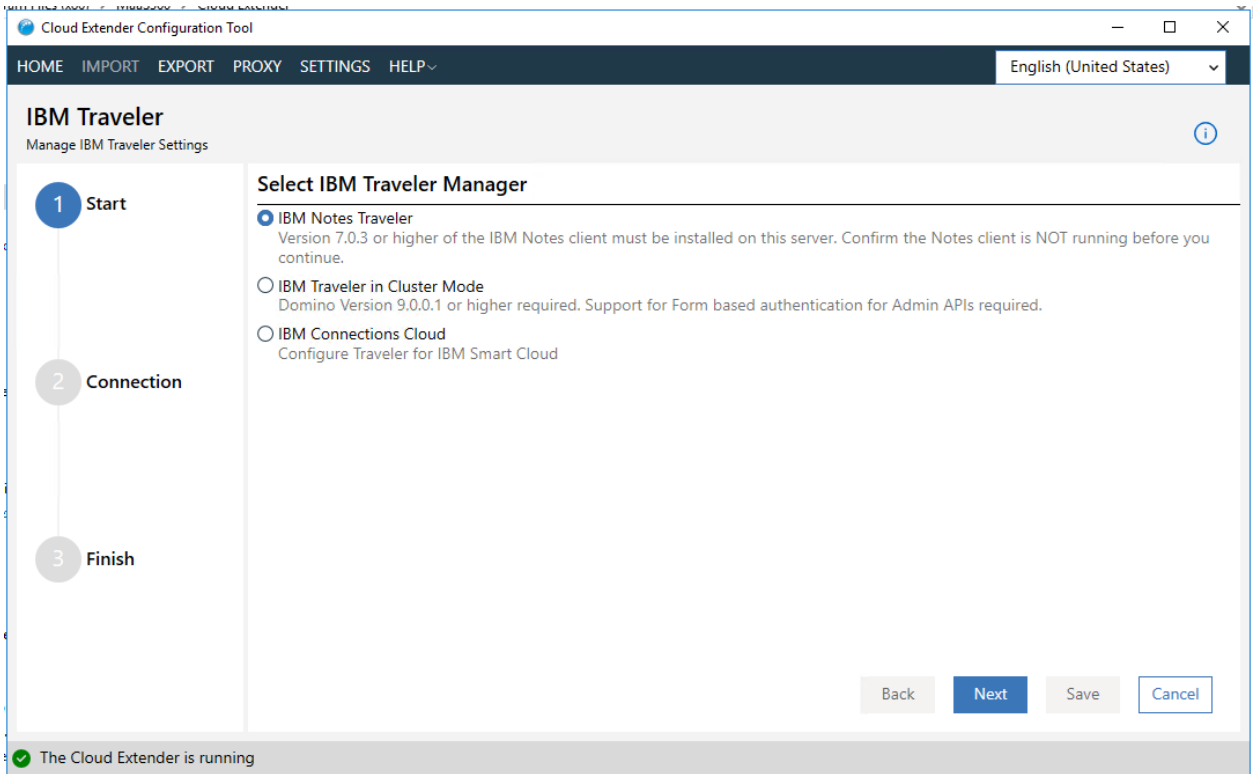
Parent topic: Configuring Settings for the Cloud Extender Modules

10.3 IBM Traveler Integration

Follow these steps to configure basic settings for the Cloud Extender™ to integrate with IBM® Traveler.

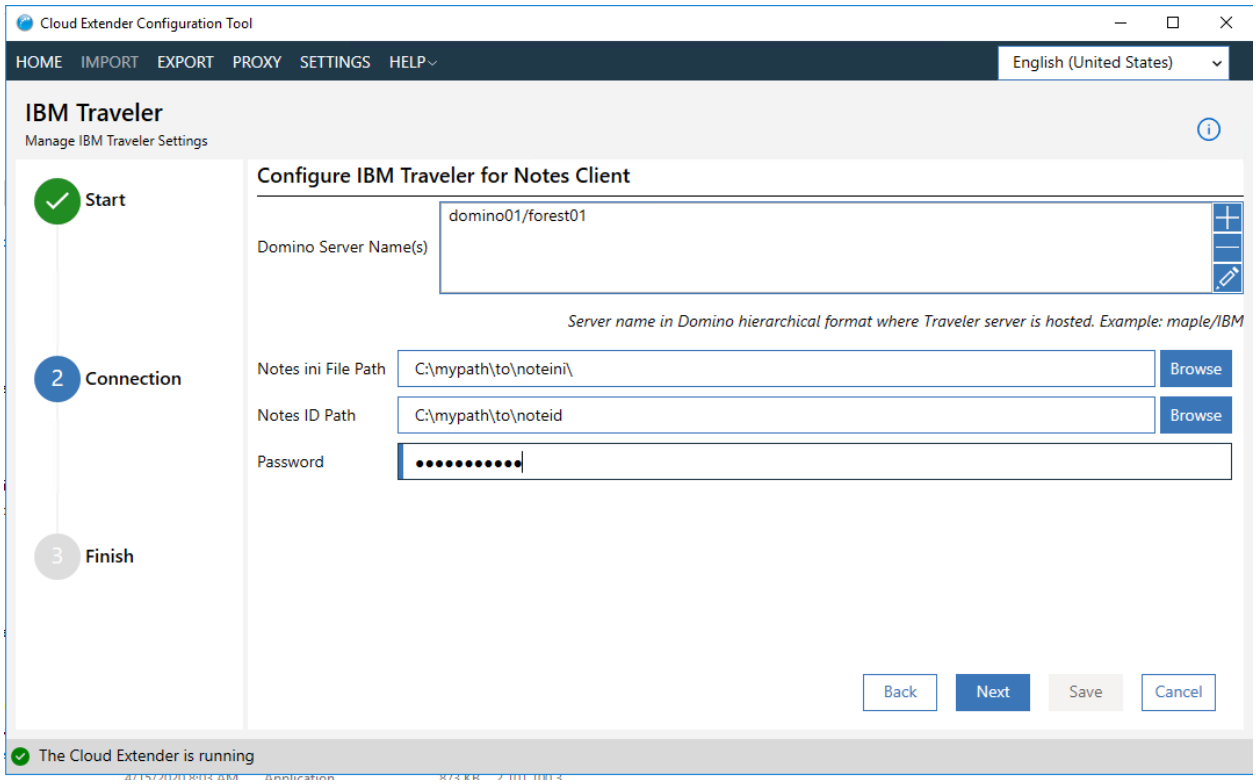
10.3.1 Procedure

1. Verify all required prerequisites have been met
    a. Hover mouse over the **IBM Traveler** tile the hover over the green checkmark or red X for prerequisite information
2. Open the Cloud Extender Configuration Tool and select **IBM Traveler** tile.
3. Select the integration server type that you use for IBM Traveler integration:

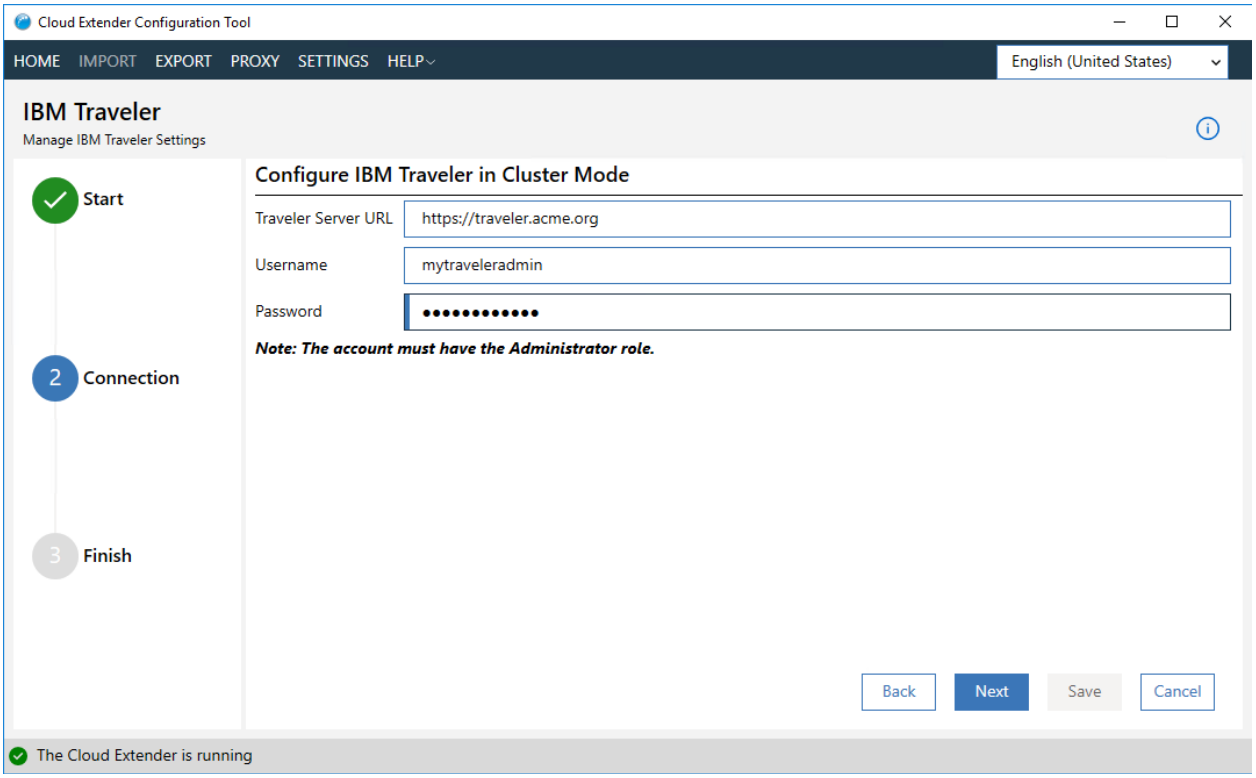


    a. IBM Notes Traveler
        a. Integrates with a single instance of the IBM Traveler server
    b. IBM Traveler in Cluster Mode
        a. Supports Domino® Version 9.0.0.1.
    c. IBM Connections Cloud
        a. IBM Connections™ Cloud: IBM SmartCloud® integration

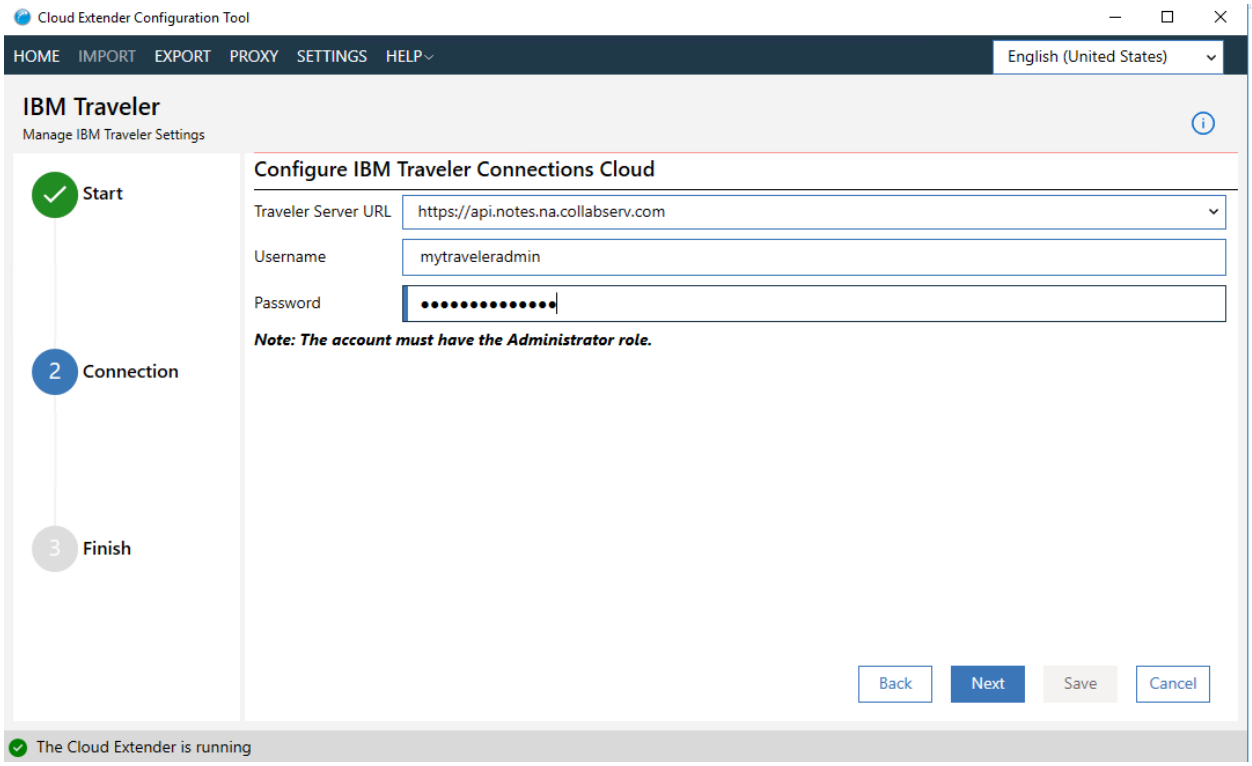
4. Click **Next** button
5. If you are using IBM Notes Traveler mode, complete the following steps:
    a. Stop the Notes® client before you continue with this procedure.
    b. Add your Domino server name(s) in the server list box
    c. Locate the path of your `Notes.ini` file and enter this path into the **Notes ini File Path** field
    d. Locate the Notes ID for your Notes administrator and enter the file path into the **Notes ID Path** field
    e. Enter the Notes administrator password into the **Password** field
    f. Click the **Next** button



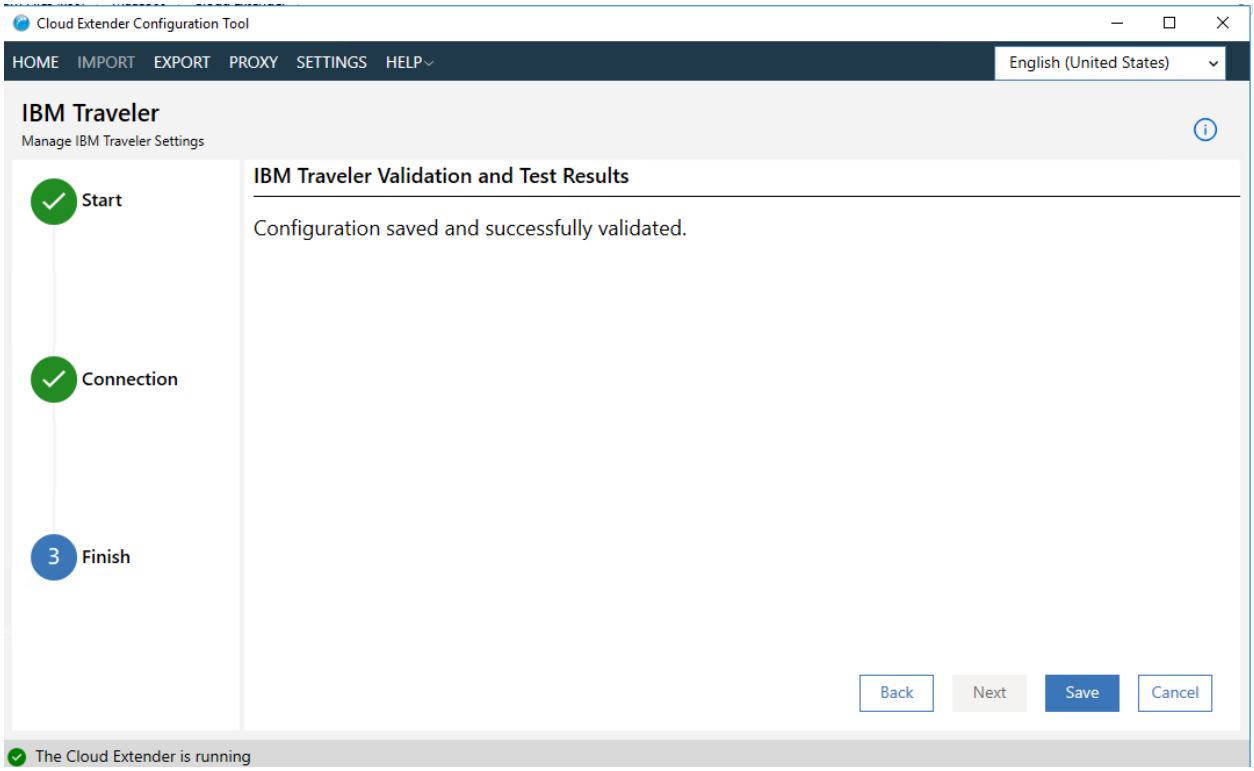
6. If you are using IBM Traveler in Cluster Mode, complete the following steps:
    a. Enter your Traveler server URL into the **Traveler Server URL** field
    b. Enter the username used to administer devices into the **Username** field
    c. Enter the password for the given username in the **Password** field
    d. Click the **Next** button



7. If your are using IBM Connections Cloud mode, complete the following steps:
    a. Select your Traveler Server URL from the available options
    b. Enter the username used to administer devices into the **Username** field
    c. Enter the password for the given username in the **Password** field
    d. Click the **Next** button



8. Click Save to complete the setup



Note: Depending on the size of your environment, devices start importing into your MaaS360® Portal in a few hours. View the Cloud Extender logs in real-time for status updates.

Parent topic: [IBM Traveler Integration Module]

10.4 Enabling Auto-Quarantine (AQ) for IBM Traveler or IBM SmartCloud

Follow these steps to enable the Cloud Extender™ Auto-Quarantine (AQ) feature for integration with IBM® Traveler or IBM SmartCloud®.

10.4.1 About This Task

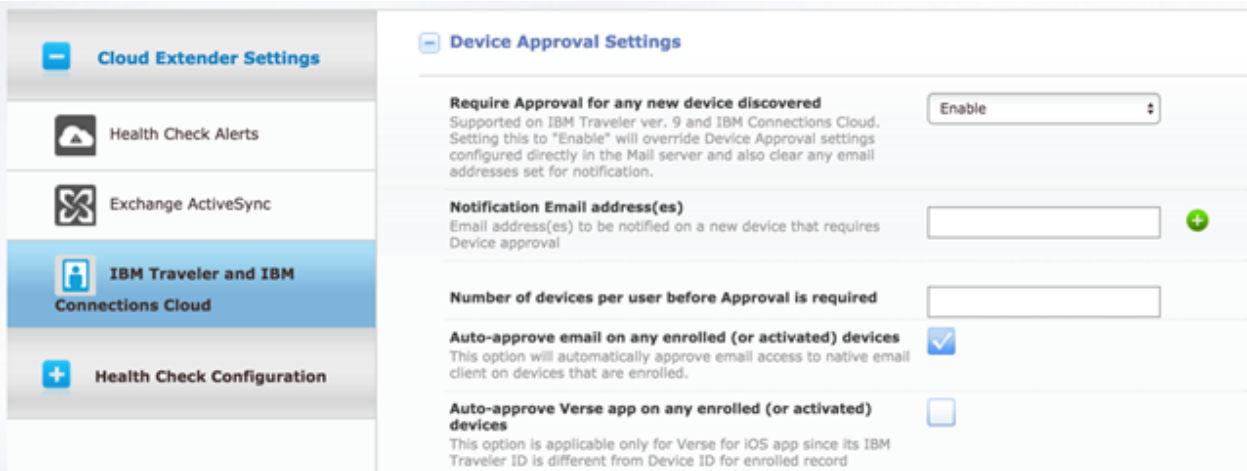
The Auto-Quarantine (AQ) feature for IBM Traveler or IBM SmartCloud provides the following benefits:

1. Prevents new devices from connecting to your email server with ActiveSync
2. Automatically approves devices that are enrolled in MaaS360® Automatically approves devices that receive email settings only from MaaS360
3. Automatically approves Secure Mail records
4. Automatically approves IBM Verse™ client connections

The Auto-Quarantine (AQ) feature is only supported for IBM Traveler 9.0+ and IBM SmartCloud. You can enable this feature directly on IBM Traveler. Existing ActiveSync devices are not affected when you enable Auto-Quarantine (AQ).

10.4.2 Procedure

1. Log in to the MaaS360 Portal with Administrator credentials
2. Select **Setup** > **Cloud Extender Settings**, and then click **Edit**
3. Configure policies in the IBM Traveler and Connections Cloud section



Option	Description
Require approval for any new device discovered	Use the default setting, where the Cloud Extender uses the Auto-Quarantine (AQ) setting that is configured on the IBM Traveler server or enable or disable Auto-Quarantine (AQ). Supports only IBM Traveler 9/0+ and IBM SmartCloud.
Notification email address(es)	A comma-separated list of email addresses that are notified when a new device is quarantined.
Number of devices per user before approval is required	The Auto-Quarantine feature starts working when the user connects a device. If you set the value to two, every user receives email on two devices without being quarantined. The third device that syncs with IBM Traveler is quarantined.
Auto-approve enrolled devices	Automatically approves email connections from devices that are enrolled in MaaS360. The device is briefly quarantined before enrollment is confirmed.
Auto-approve based on policies	Automatically approves email connections from enrolled devices when the email configuration is

	pushed from MaaS360. This setting requires that you configure MDM / Persona policies to push email configuration to devices. This setting blocks connections from the device if the user manually configures email on email clients. Only MDM pushed email configuration is approved.
Auto-approve Verse app on any enrolled device	Automatically approves connections from the IBM Verse app that connects to IBM SmartCloud. This option works only with the IBM Verse for iOS app because it uses an IBM Traveler ID that is different from the device ID for an enrolled record. Android devices are automatically approved based on enrollment status.

4. Click **Save & Publish**. The Secure Mail records are automatically approved regardless of whether Auto-Quarantine (AQ) is enabled from the MaaS360 Portal or enabled directly on IBM Traveler or IBM SmartCloud.

Parent topic: [IBM Traveler Integration Module]

10.5 Enabling Health Check Alerts for IBM Traveler Integration

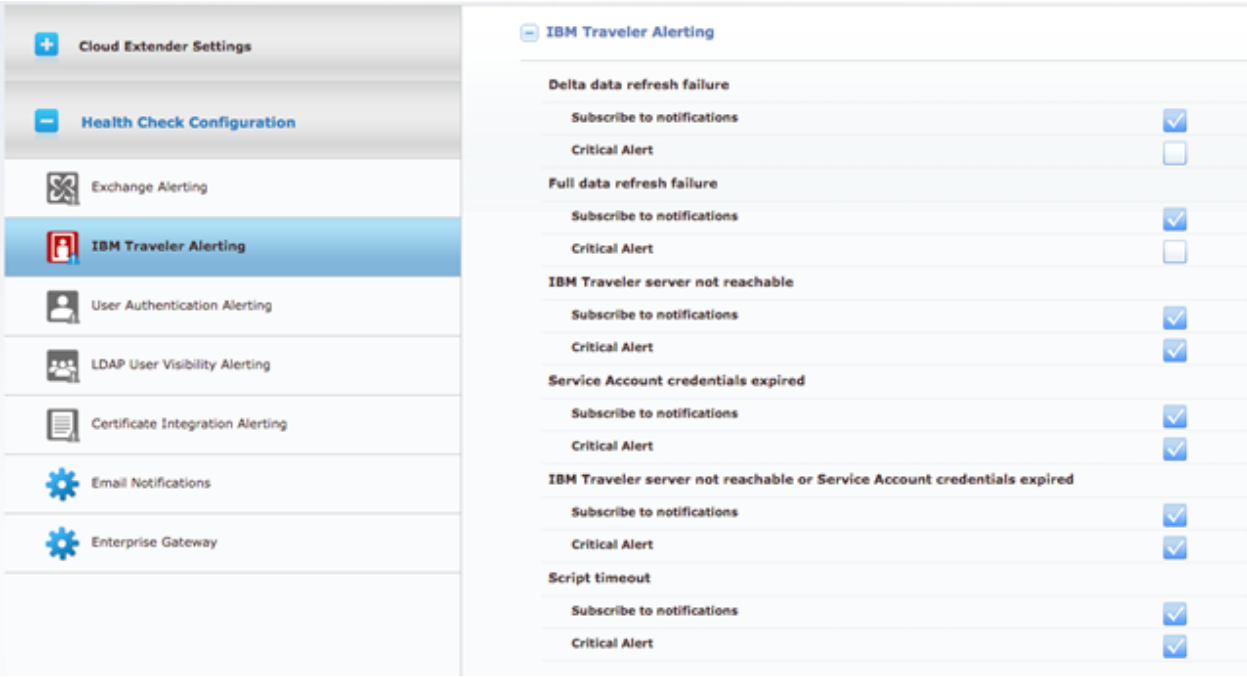
Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™IBM® Traveler Integration module.

10.5.1 Before You Begin

This feature is available only for the Cloud Extender MEG Module 2.86 release.

10.5.2 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**
2. Select **Health Check Configuration** > **IBM Traveler Alerting**. The IBM Traveler
   Alerting list is displayed.



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends

an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
Delta data refresh failure	The Cloud Extender cannot upload new or changed device and policy information from IBM Traveler due to critical errors during the sync.	Verify that the IBM Traveler environment is operational. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to the IBM Traveler or the IBM SmartCloud URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Full data refresh failure	The Cloud Extender cannot upload all the device and policy information from IBM Traveler due to critical errors during the sync.	Verify that the IBM Traveler environment is operational. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to the IBM Traveler or the IBM SmartCloud URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
IBM Traveler server not reachable	The Cloud Extender	Verify that the IBM

	cannot connect to the IBM Traveler server because the server is unreachable or the IBM Traveler Configuration settings in the Cloud Extender are invalid.	Traveler environment is operational. Check for recent firewall or proxy changes that might block access from the Cloud Extender server to the IBM Traveler or the IBM SmartCloud URL. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Service Account credentials expired	The Cloud Extender cannot connect to the IBM Traveler server because the server is unreachable or the service account credentials are invalid.	Verify that the configured IBM Traveler server configuration or URL is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, use the Test Reachability workflow to confirm. Check whether the configured service account is still active and that the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the service account credentials. If this issue continues, collect logs from the

		Cloud Extender, and then contact IBM Support for further assistance.
IBM Traveler server not reachable or service account credentials expired	The Cloud Extender cannot connect to the IBM Traveler server because the server is unreachable or the service account credentials are invalid.	Verify that the configured IBM Traveler server configuration or URL is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, use the Test Reachability workflow to confirm. Check whether the configured service account is still active and that the password is not expired. If required, use the Cloud Extender Configuration Tool in the MaaS360 Portal to update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Script timeout	The device discovery script is taking more time to complete than the configured threshold. The MaaS360 Portal might not contain the	The device discovery script times out due to the following issues: Too many mailboxes and devices in your IBM Traveler

	most recent device information from the IBM Traveler or the IBM SmartCloud® environment.	environment. The Cloud Extender is trying to reach remote mailbox servers that are slowing down the script. Follow these steps to remediate this alert: Use the Cloud Extender Scaling Tool to determine whether you require multiple Cloud Extenders for your environment and whether your current scale meets the criteria. From the MaaS360 Portal Home page, select **Setup** > **Services** > **Enterprise Email Integration** to download the scaling tool. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for guidance on correct scaling or recommendations on how to increase the timeout settings.

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [IBM Traveler Integration Module]

10.6 High Availability (HA) Mode for IBM Traveler Integration

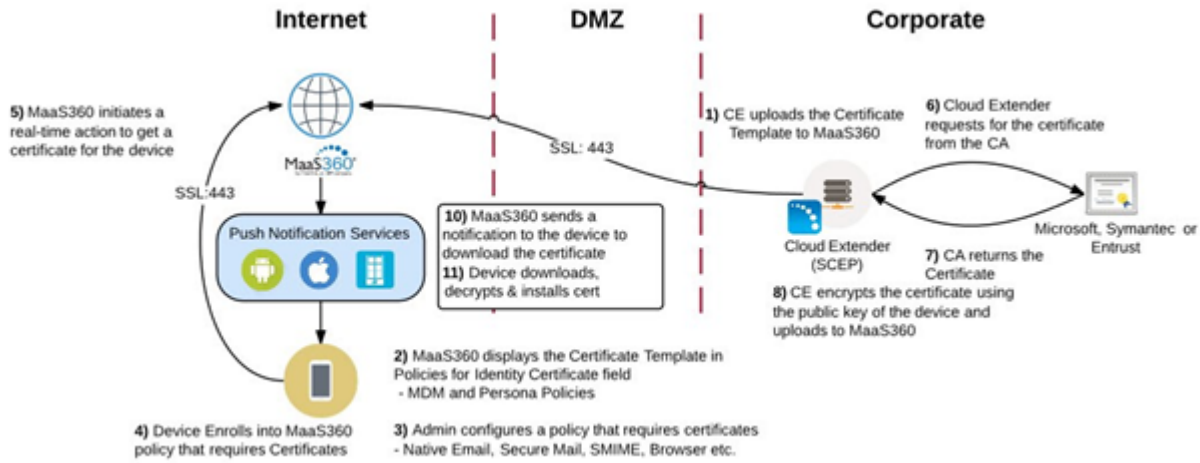
Information about support for High Availability (HA) mode for Cloud Extender™ integration with IBM® Traveler or IBM SmartCloud®.
The Cloud Extender for IBM Traveler Integration does not support High Availability (HA) mode. However, you can set up IBM Traveler or IBM SmartCloud in cluster mode for High Availability (HA).

Parent topic: IBM Traveler Integration Module

11 Certificate Integration Module

The Certificate Integration module allows users to use their existing Certificate Authority (CA) and auto-provision device and user certificates to enrolled devices. Certificates are used for email, Wi-Fi, VPN, or Secure Mail authentication. The Cloud Extender™ interacts with the CA, and then pushes the issued certificates down to enrolled devices by using the following method:

1. Receives certificate requests from the MaaS360® Portal for all enrolled devices that require an identity certificate.
2. Authenticates against the Certificate Authority (CA) or Registration Authority (RA) as a part of the certificate request process.
3. Requests ID certificates by passing the details of the device or user and corresponding attributes as a part of the certificate request.
4. Encrypts the received certificate by using the public key of the requesting device and pushes the encrypted payload to the MaaS360 Portal, which is then delivered to the device.
5. Supports auto-renewals of certificates and makes sure that devices receive the new certificates before the current certificate expires.



Note: For Windows 10 tablets, the Cloud Extender password protects the certificate, encrypts the password by using the public key of the requesting device, and pushes the encrypted payload to the MaaS360 Portal. When the MaaS360 platform receives the password protected certificates (as part of the policy), MaaS360 uses the Windows 10 MDM API to push the encrypted payload to the tablet.

11.1 Supported CA Versions

The Cloud Extender integrates with the following certificate authorities:

1. Microsoft CA installed on 2003, 2008 R2, or 2012 R2
   Requires NDES 2008+
2. Symantec Managed PKI
3. Entrust Identity Guard and Admin Services
4. Verizon MCS PKI

The Cloud Extender must be configured with a certificate template that contains information about the CA server and administrative credentials to authenticate and request device certificates. All types of devices (iOS, Android, Windows Phone, and Mac OS X) that are enrolled in MaaS360 support certificate delivery.

11.2 System Requirements

Before you begin the installation, make sure that your environment meets the following minimum requirements:

1. Microsoft Windows 2008+ for the Cloud Extender installation
2. .NET 3.5 or higher Microsoft: Network Device Enrollment Service (NDES) set up on 2008+ server
3. Symantec: Administrative access to the Symantec PKI hosted solution
4. Entrust: Administrative access to Entrust IdentityGuard Server v10.1 or v10.2, or Entrust Admin Services v8.2 SP1 or v8.3
5. Verizon MCS: Administrative access to the Verizon MCS console
6. High Availability (HA) requirements:
   a. Windows File Share access from the High Availability Cloud Extenders for certificate caching
   b. Required for Microsoft and Symantec PKI only

11.3 Scaling

The Cloud Extender for Certificate Integration can run in Active-Active High Availability (HA) mode. You must import the same certificate template from one Cloud Extender onto all other nodes that are running in HA mode. Set

up additional HA Cloud Extenders for every 10,000 devices that are enrolled in the system.

Example: If 10,000 devices require certificates, install two Cloud Extenders in HA mode. For additional 10,000 devices, install another Cloud Extender for certificates.
If you have 50,000 enrolled devices that require certificates, install six Cloud Extenders for scaling and HA.
The MaaS360 Portal round robins certificate requests between active and connected Cloud Extenders.

Table 1. Scaling requirements for the Certificate Authority Integration module

Item	Requirement
Less than 10,000 devices	CPU: 2 cores Memory: 4 GB
More than 10,000 devices	Scaling: Supports installation on multiple instances of the Cloud Extender with High Availability (HA). Install on a dedicated Cloud Extender or enabled on Cloud Extender with the User Visibility or User Authentication services enabled. For accurate scaling of your environment, see the Cloud Extender scaling document at **Setup** > **Services** > **Enterprise Integration**.

11.4 Device Certificates or User Certificates

From a device perspective, all certificates are treated as user certificates. The Cloud Extender issues device certificates or user certificates to devices based on the certificate template that is defined on the Cloud Extender.
The following table lists the differences between device certificates and user certificates:

Certificate	Description
Device	The Cloud Extender generates a certificate based on requirements and pushes that certificate to the device. The Cloud Extender uses certificate templates to pass user attributes as part of the Subject Name / Alternate Name, which links the certificate to the user and is used as a device certificate. Devices treat all certificates as user certificates. This is the most commonly used certificate template type that supports Microsoft, Symantec, Entrust, and Verizon MCS. Mostly used for authentication.
User	Requires that the certificate is present in Active Directory for the user. Additional requirements to set up key recovery for extracting the private key for the certificate. The Cloud Extender can look up the certificate only if the certificate exists. The Cloud Extender cannot generate missing certificates. Supported only by Microsoft CA. Mostly used for S/MIME certificates to deliver signing and encryption certificates. For user certificates that are used for authentication, choose the device certificate template and provide user attributes to pass to the CA for certificate generation.

Cloud Extender Certificate Integration Configuration

Follow these steps to configure the Cloud Extender Certificate Integration module.

Testing Certificate Integration

Follow these steps to test certificate integration on the Cloud Extender.

Enabling Health Check Alerts for Certificate Integration

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender Certificate Integration module.

High Availability (HA)

The Cloud Extender supports High Availability configuration for the Certificate Integration module. Configure multiple instances of the Cloud Extender with the same certificate template for Active-Active HA configuration.

Troubleshooting Issues with Certificate Integration

Follow these steps to troubleshoot any issues with certificate integration.

Parent topic: Configuring Settings for the Cloud Extender Modules

11.5 Cloud Extender Certificate Integration Configuration

Follow these steps to configure the Cloud Extender™ Certificate Integration module.

11.5.1 Procedure

1. Open the Cloud Extender Configuration Tool and select the **Certificates Integration** tile
    a. Make sure that the Certificate Integration module has been downloaded. (You cannot configure templates until the module has been downloaded and installed)
2. Select the appropriate type of Certificate Authority for your system
3. Choose **Device Identity Certificates** or **User Identity Certificates**
    a. The availability of the two options varies per CA
4. If you already have a template defined that you wish to import, click the **Import Certificate Template** button and browse to your template export file
5. Click the **Next** button

11.5.2 What to Do Next

The next topics provide procedures on how to choose your certificate authority type.

Microsoft CA Integration
MaaS360® allows integration with the Microsoft Active Directory Certificate Services for automatic delivery of device certificates to enrolled devices.

Symantec CA Integration
MaaS360 integrates with the Symantec host PKI certificate authority for automatic delivery of device certificates to enrolled devices.

Entrust CA Integration
MaaS360 integrates with the Entrust certificate authority for automatic delivery of device certificates to enrolled devices.

IDnomic / OpenTrust PKI CA Integration

MaaS360 integrates with the IDnomic/OpenTrust PKI certificate authority (CA) for automatic delivery of user certificates for authentication and S/MIME capabilities (email security) on enrolled devices.

Verizon MCS Integration The Verizon MCS certificate authority uses SCEP (Simple Certificate Enrollment Protocol) to issue certificates.

Parent topic: Certificate Integration Module

11.6 Microsoft CA Integration

MaaS360® allows integration with the Microsoft Active Directory Certificate Services for automatic delivery of device certificates to enrolled devices. You generate signed certificates through the Microsoft Registration Authority (RA) or the Network Device Enrollment Service (NDES) by using the Simple Certificate Enrollment Protocol (SCEP). You must enable NDES on your Windows 2008 server, create certificate templates on the NDES server, create certificate templates in MaaS360, and configure policies in MaaS360 to automatically deliver certificates.

The following prerequisites apply to integration with the Microsoft CA: Microsoft Enterprise CA must be functional on your corporate network. You must have the required administrative rights on the Windows server and the CA.

Installing Microsoft NDES

Follow these steps to install NDES on a Windows server that is available on your network.

Configuring the Certificate Template on the SCEP Server

Follow these steps to configure a certificate template on the SCEP server for use with MaaS360.

Enabling a New Certificate Template on the CA

Follow these steps to enable a new certificate template on the CA.

Setting Up a Default Certificate Template on the NDES Server

Follow these steps to set up a default certificate template on the NDES server.

Increasing the Password Cache Limit on the NDES Server

Follow these steps to increase the password cache limit on the NDES server.

Increasing the Maximum Query String on the NDES Server

Follow these steps to increase the size of the query strings that the Cloud Extender uses to request certificates from NDES for mobile devices.

Restarting IIS on the NDES Server
Follow these steps to restart Internet Information Services (IIS) on the NDES server.

Configuring a Certificate Template on the Cloud Extender
Follow these steps to configure the certificate template on the Cloud Extender.

Configuring MaaS360 Policies to Use the Cloud Extender Certificate Templates
Follow these steps to make sure that the MaaS360 policies are using the Cloud Extender certificate templates.

Parent topic: Cloud Extender Certificate Integration Configuration

11.7 Installing Microsoft NDES

Follow these steps to install NDES on a Windows server that is available on your network.
You can use the same server for certificate integration with Cloud Extender™, but install NDES and the Cloud Extender certificate integration on a different server than your CA.
You must use Windows Server 2008 R2 and Windows Server 2012 R2 to install NDES. The service is installed from the Microsoft Server Manager. If your CA is on Windows Server 2003, you can still install NDES on Windows Server 2008 R2+ and configure NDES to communicate with your CA. The Cloud Extender only needs to communicate with NDES to receive device certificates. If you have not installed NDES on your Windows Server 2008 R2 server, see the Microsoft article here for instructions on how to enable NDES on the Microsoft server.

Note:

1. For Windows Server 2008 and Windows Server 2008 R2, only Enterprise and Datacenter Editions can enable the NDES Service Role. Standard Edition does not support NDES. Choose the right server edition. For Windows Server 2012, the Standard Edition supports NDES.
2. The following permissions are required to set up NDES:

Permission	Description
SCEP Admin	The user who logs into the server and installs NDES. This user must meet the following requirements: • Member of the Local Administrators group • Enroll permissions on the following templates: • Exchange Enrollment Agent (offline request) CEP • Encryption Permissions to add templates to the selected CA Member of the Enterprise Administrator group

SCEP Service Account	The credentials that are used to run the NDES service. This account must have the following credentials: • Member of the local IIS_IUSRS group Request permission on the configured CADomain user account with Read and Enroll permissions on the configured templates (for more information, see the topic Configuring the certificate template on the SCEP server.
Device Administrator	The user who manages the devices and requests a onetime password from the service to enable security enrollment. This user must have Enroll permissions on the certificate template that is used by NDES to request certificates against the CA.

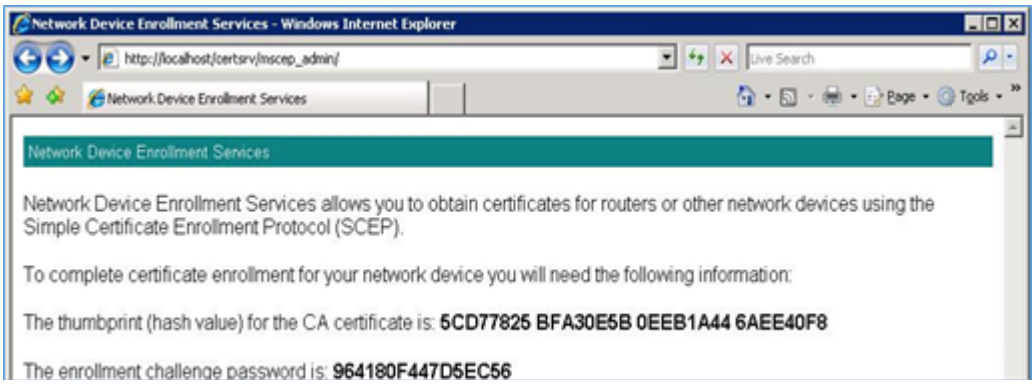
Parent topic: Microsoft CA Integration

11.8 Confirming SCEP is Working on the Cloud Extender Server

Follow these steps to determine whether SCEP is working on the Cloud Extender server.

11.8.1 Procedure

1. From Internet Explorer on the Cloud Extender server, go to the SCEP Admin URL at **Error! Hyperlink reference not valid.**.
2. Provide the credentials for the Device Administrator. As an example, the following type of window might be displayed:



What to Do Next

Configuring the Certificate Template on the SCEP Server

11.9 Configuring the Certificate Template on the SCEP Server

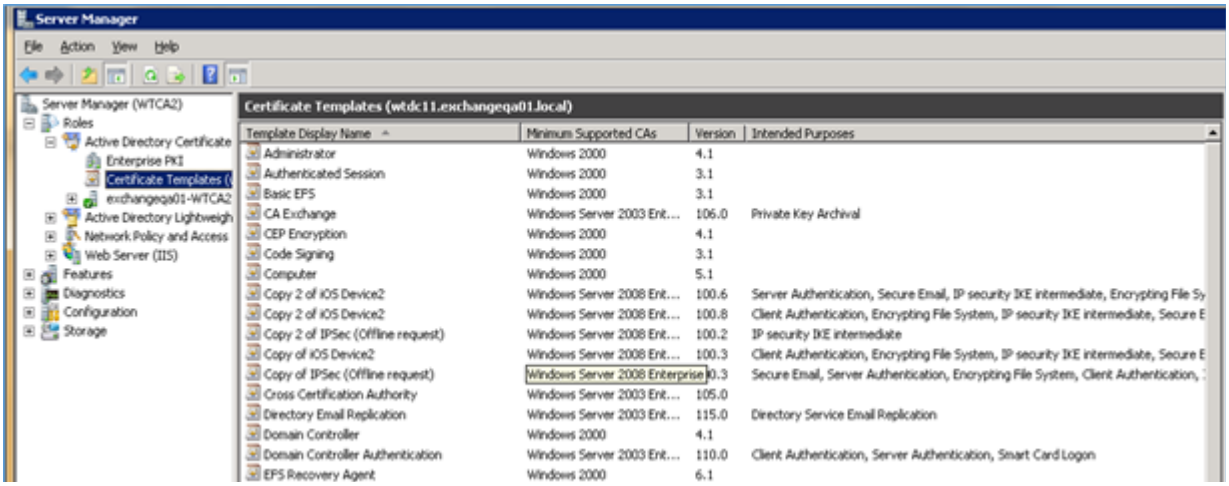
Follow these steps to configure a certificate template on the SCEP server for use with MaaS360®.

11.9.1 Before You Begin

If you already have a working template, use the instructions in this procedure to confirm that your template is configured correctly.

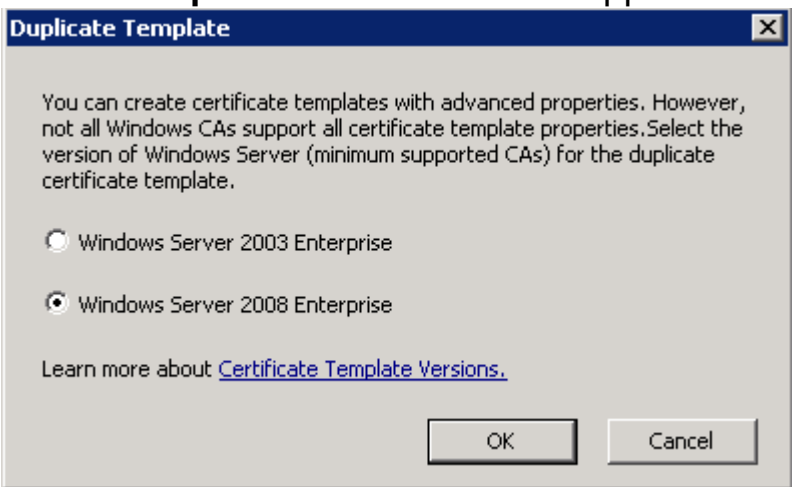
11.9.2 Procedure

1. Log on to the Microsoft SCEP server with the SCEP Admin credentials.
2. Open the Server Manager and select **Roles** > **Active Directory** > **Certificate Services** > **Certificate Templates**.

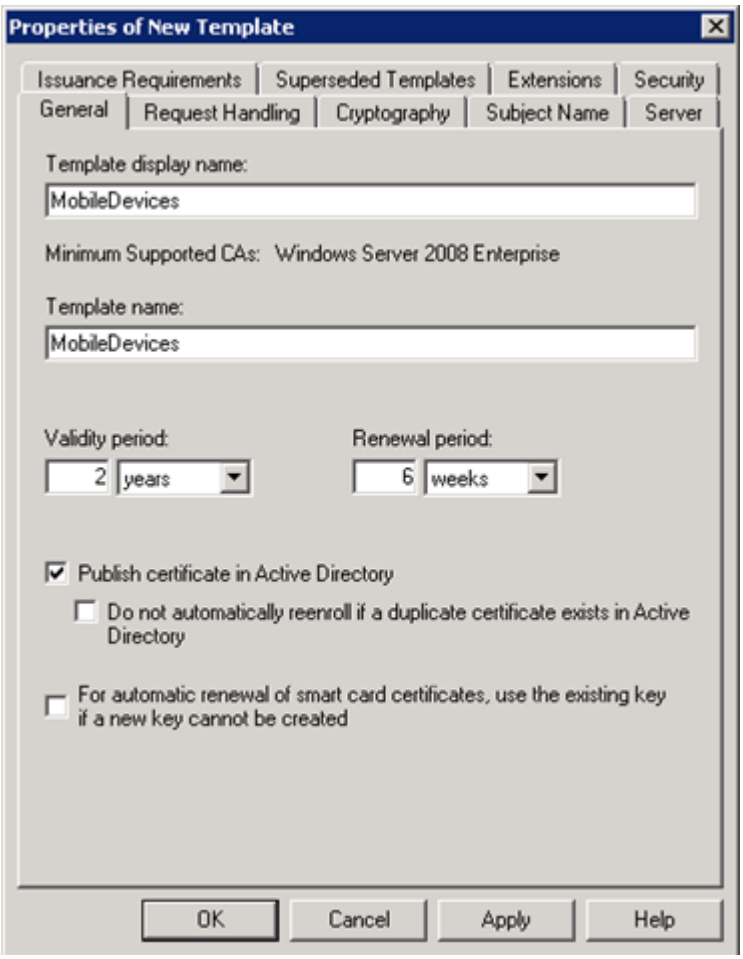


3. Right-click **Computer** > **Duplicate Template**.
   Notes
   a. Do not duplicate a user template. Microsoft SCEP does not work with user templates.
   b. If your template is based on a user template, create a new template based on the computer template.
   c. Devices do not differentiate between a certificate from a user template and a device template. All certificates are treated as user certificates on the iOS device.

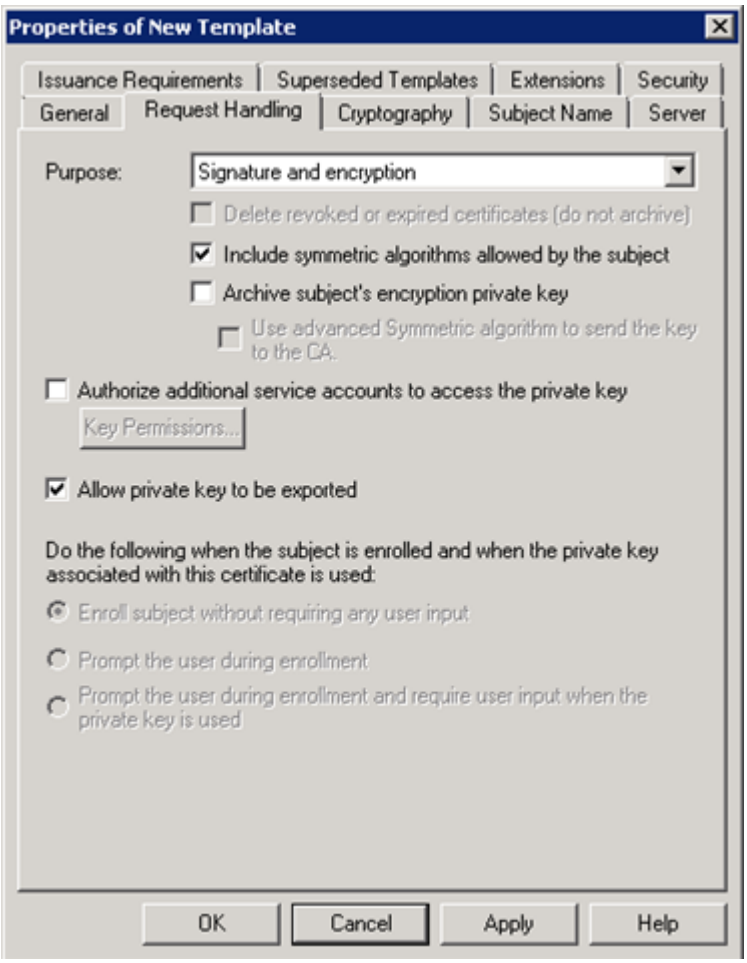
4. To access advanced template properties, select **Windows Server 2008 Enterprise** as the minimum supported CA version.



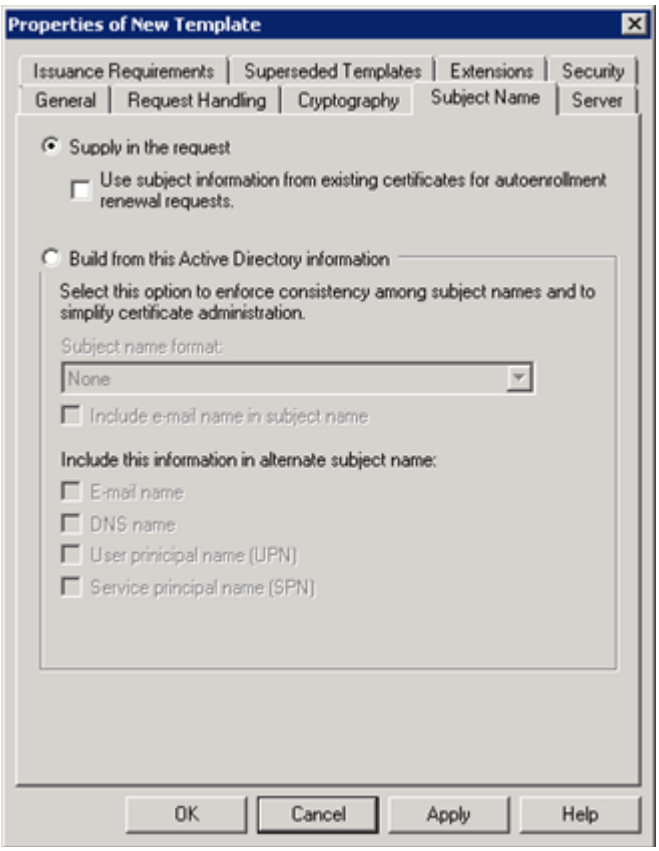
5. From the General tab of the New Template Properties window, complete the following steps:
    a. Provide a template display name
    b. Copy the template name (without spaces) to use later
    c. Optional: Select **Publish certificate in Active Directory**



6. From the Request Handling tab, select the following options:
    a. **Include symmetric algorithms allowed by the subject**
    b. Optional: **Allow private key to be exported**



7. From the Subject Name tab, select **Supply in the request**. The Cloud Extender™ template supplies the subject.



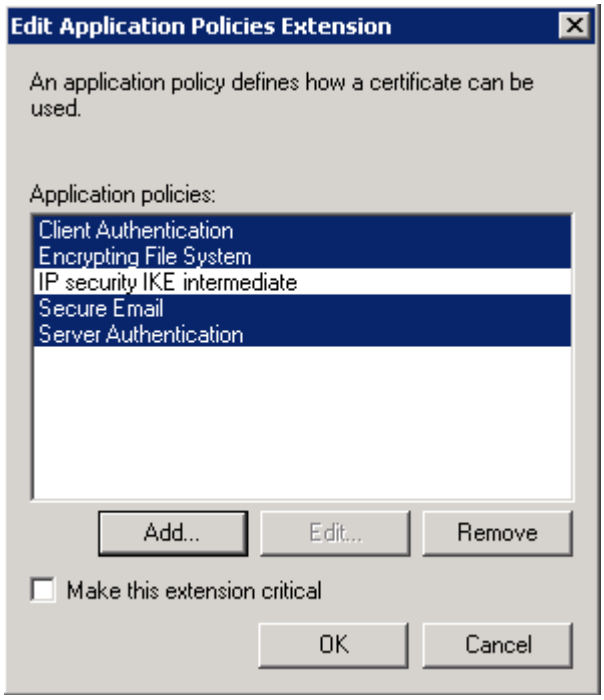
8. From the Security tab, make sure that the following accounts exist and use the correct permissions:

Account	Permission
Authenticate Users	Read
SCEP Service Account (from Installing Microsoft NDES)	Read, Enroll
Domain Administrators	Read, Write, Enroll
Enterprise Administrators	Read, Write, Enroll
Device Administrator (from Installing Microsoft NDES)	Read, Enroll

Note: Add the accounts if necessary.

9. From the Extensions tab, complete the following steps:
    a. Add **Client Authentication** and **Server Authentication**
    b. Optional: Add **Encrypting File System** and **Secure Email**
    c. Confirm **Subject Type = Computer** for **Certificate Template Information**

d. Click **Apply** to close the template



11.9.3 What to Do Next

Enabling a New Certificate Template on the CA

Parent topic: Microsoft CA Integration

11.10 Enabling a New Certificate Template on the CA

Follow these steps to enable a new certificate template on the CA.

11.10.1 Procedure

1. Log on to the CA server with administrative credentials
2. Open the Server Manager and select **Roles** > **Active Directory** > **Certificate Services** > **Certificate Templates**
3. Right-click **Certificate Templates**, and then select **New** > **Certificate Template to Issue**
4. Select the new certificate template and click **OK**

Note: The published certificate template might take some time to become available on all Domain Controllers.

11.10.2 What to Do Next

Setting Up a Default Certificate Template on the NDES Server

Parent topic: Microsoft CA Integration

11.11 Setting Up a Default Certificate Template on the NDES Server

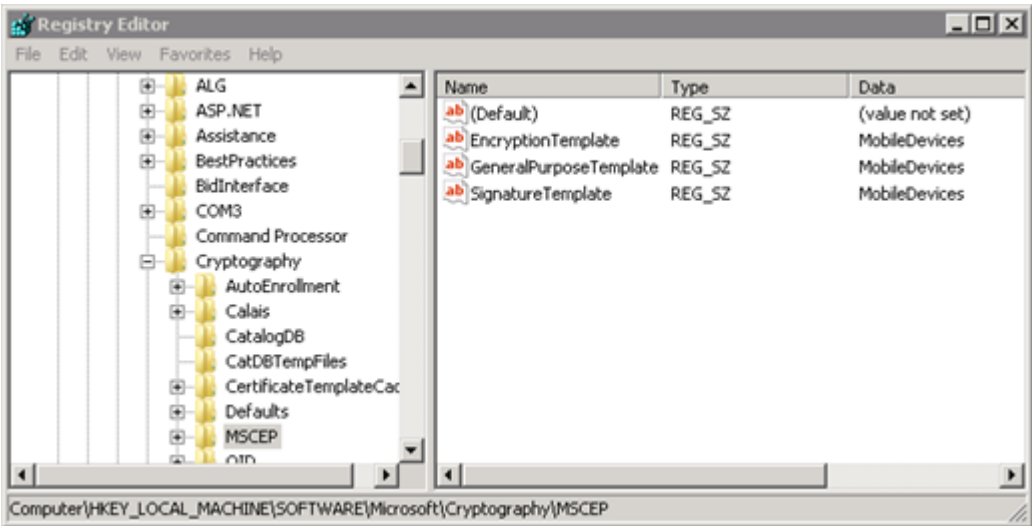
Follow these steps to set up a default certificate template on the NDES server.

11.11.1 About This Task

Use the registry editor on the NDES server to specify a default template that the registration authority (NDES service) uses to request certificates for mobile devices.
Use the certificate template that you created in the topics Configuring the Certificate Template on the SCEP Server and Enabling a New Certificate Template on the CA as the default template on the NDES server.

11.11.2 Procedure

1. Log in to the NDES service with administrative credentials
2. Open the registry editor by using **Start** > **Run** > **Regedit.exe**
3. Go to `HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP`
4. Change the values of the following registry keys to the name of the template:
   a. `EncryptionTemplate`
   b. `GeneralPurposeTemplate`
   c. `SignatureTemplate`
5. You must set these registry keys with the value from the **Template Name** field, not the **Template Display Name** field. The value in the **Template Name** field does not contain spaces.



6. Restart IIS. For more information, see Restarting IIS on the NDES Server.

11.11.3 What to Do Next

Increasing the Password Cache Limit on the NDES Server

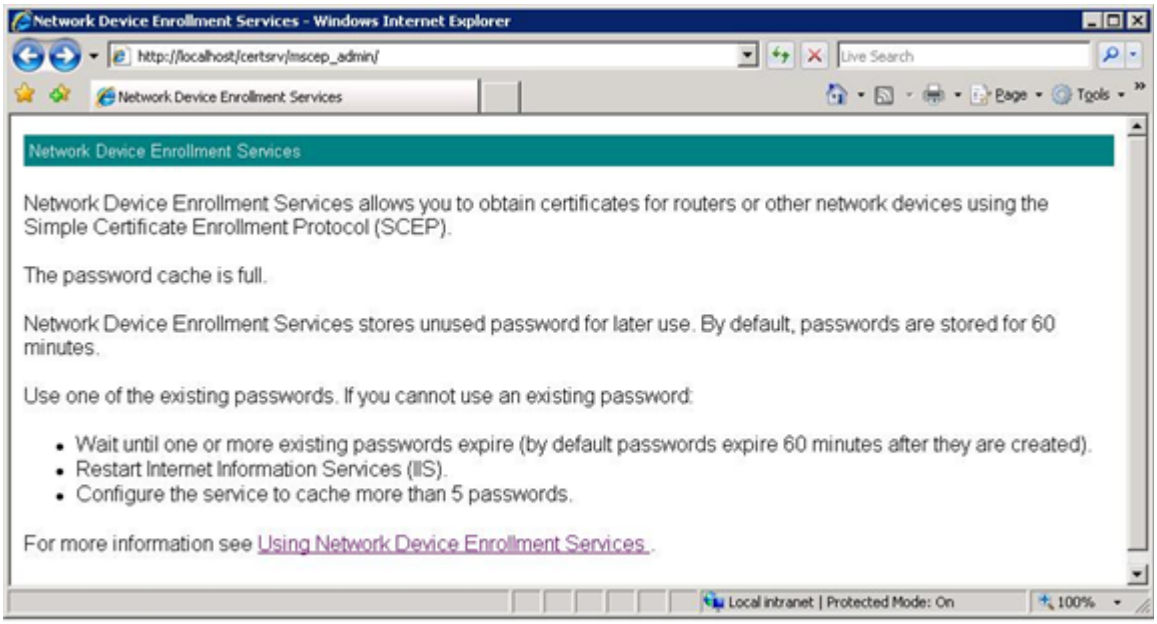
Parent topic: Microsoft CA Integration

11.12 Increasing the Password Cache Limit on the NDES Server

Follow these steps to increase the password cache limit on the NDES server.

11.12.1 About This Task

By default, the NDES server caches challenge passwords when requested by the Device Administrator. The NDES server does not give out new challenge passwords until the existing passwords are used for certificate requests. The default setting on the NDES server is five cached passwords. If you load the SCEP Admin URL five times to test, and then request a challenge password the sixth time, the NDES server displays the following error message:



Use the following procedure to configure NDES to cache more than five passwords.

11.12.2 Procedure

1. Log on to the NDES server with administrative credentials.
2. Open the registry editor by using **Start** > **Run** > **Regedit.exe**.

3. Go to `HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP`.
4. Create a new key named `PasswordMax`.
5. Under the `PasswordMax` key, create a new `DWORD` key named `PasswordMax` and increase the value.
6. Restart IIS. For more information, see Restarting IIS on the NDES Server.

11.12.3 What to Do Next

Increasing the Maximum Query String on the NDES Server

Parent topic: Microsoft CA Integration

11.13 Increasing the Maximum Query String on the NDES Server

Follow these steps to increase the size of the query strings that the Cloud Extender™ uses to request certificates from NDES for mobile devices.

11.13.1 About This Task

By default, IIS is installed with the Request Filtering feature enabled and the default Maximum Query String Size set to 2048 bytes. Any certificate request that requires a longer query string size is filtered out. The Cloud Extender uses query strings during certificate requests that are greater than 2048 bytes. You must increase the size of the query string value to enable Cloud Extender to request certificates against NDES.

11.13.2 Procedure

1. Log on to the NDES server with administrative credentials
2. Select **Start** > **Cmd**, and then right-click **Run As Admin**
3. From the command prompt, copy the following command and press **Enter**:
   ```
   windir%\system32\inetsrv\appcmd set config
   /section:requestFiltering
   /requestLimits.maxQueryString:8192
   ```
   The maximum query limit is set to 8192 bytes.
4. Restart IIS.

11.13.3 What to Do Next

Restarting IIS on the NDES Server

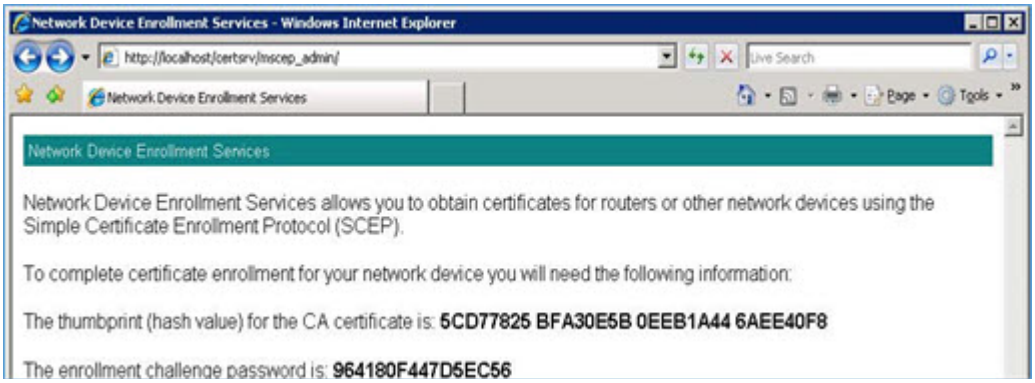
Parent topic: Microsoft CA Integration

11.14 Restarting IIS on the NDES Server

Follow these steps to restart Internet Information Services (IIS) on the NDES server.

11.14.1 Procedure

1. Log on to the NDES server with administrative credentials
2. Select **Start** > **Cmd**, and then right-click **Run As Admin**
3. From the command prompt, type `iisreset`
4. Follow these steps to confirm that the settings are configured correctly:
    a. From Internet Explorer on the Cloud Extender™ server, go to the SCEP Admin URL at **Error! Hyperlink reference not valid.**
    b. Provide your credentials for the Device Administrator
    c. Confirm that the SCEP Admin URL returns a challenge password, like the following example:



11.14.2 What to Do Next

Configuring a Certificate Template on the Cloud Extender

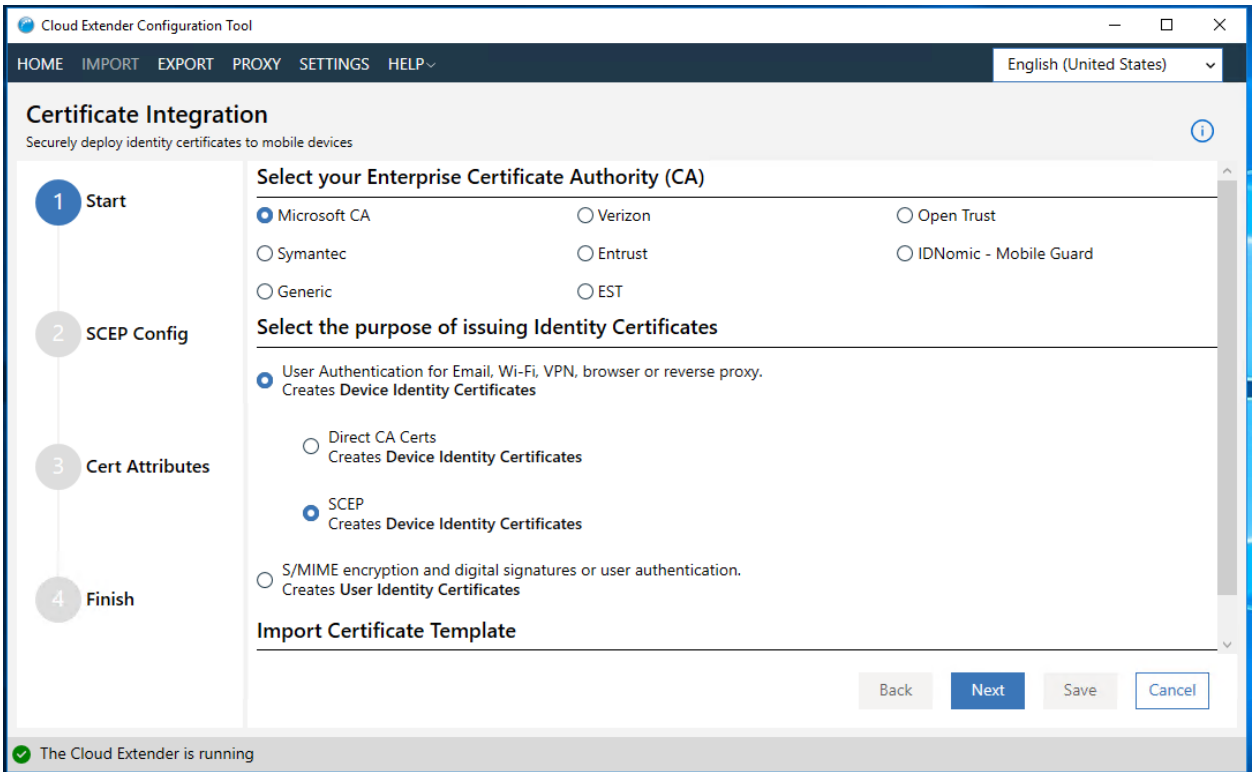
Parent topic: Microsoft CA Integration

11.15 Configuring a Microsoft SCEP Certificate Template on the Cloud Extender

Follow these steps to configure the certificate template on the Cloud Extender™.

11.15.1 Procedure

1. From the Cloud Extender Configuration Tool click the Certificate Integration tile.
2. If you already have one or more templates defined, click the **Add New Template** button, otherwise move to step 3.



3. Select **Microsoft CA**
4. Select **Device Identify Certificates**.
    a. Select SCEP from the options that appear
5. Click the **Next** button
6. Enter the following information

Parameter	Description
Template Name	The name of your template. The template name is displayed in the MaaS360® policies under various configuration sections that use identity certificates
Hostname of SCEP server	The host name of your NDES Server.
SCEP Server challenge type	NDES requires a challenge password to authenticate certificate requests before the service issues an identity certificate. Use a static password each time or a dynamic challenge password that the Cloud Extender parses from the MSCEP Admin page.
Challenge Username	The username of the Device Administrator for SCEP transactions.
Challenge Password	The password of the Device Administrator for SCEP transactions.

7. Click the **Next** button
8. Enter the following information:

Parameter	Description
Subject Name	Use the subject name to configure the certificate template to pass specific attributes of the user or device to the certificate request so that the returned certificate uses these values.The default string for the subject name is `/CN=%uname%/emailAddress=%email%`. The template supports any of the following dynamic parameters: The template also supports the

	following static values: CN (commonName) C (countryName) L (localityName) ST (stateOrProvinceName) O (organizationName) OU (organizationUnitName) G (givenName) S (Surname) I (Initials) UID (uniqueIdentifier) SN (serialNumber) T (title) D (description) The Cloud Extender also supports User Custom Attribute variable names for the subject name of the certificate. If you define the User Custom Attribute and read its value from LDAP or set the value locally on MaaS360, you can pass this value to the certificate request. Use the Advanced mode for detailed configurations of the certificate template.
Subject Alternate Name	Use this field to uniquely identify the user for authentication. This field is one of the most common fields that is used for the subject alternative name. Select from one of the four available options: • None • UPN • Upn and Email • Other
Cache certs on Cloud Extender	Select whether you wish to save enrolled certificates to a file system directory on the Cloud Extender server.
Location of Certificate Cache	If certificate caching is enabled, use this field to specify the directory where certificates should be stored.

9. Click the **Next** button
10. Click the **Advanced** button for access to advanced certificate template settings

Parameter	Description
Key Size	The size of the private key that is used for generated certificates. The key size must match your template on NDES. Default key size: 2048, but also supports 1024 and 4096
Key Usage	The key usage for the generated keys. Default key usage: Digital Signature and Key Encipherment usages
CA Signing Algorithm	The default is SHA-256, but the Cloud Extender also supports other algorithms. The algorithm must match your template on NDES.
CA Encryption Algorithm	The default is 3-DES, but the Cloud Extender also supports DES and Blowfish.
Cert Renewal in Days Before Expiry	The number of days to try to renew the certificate before the certificate expires. The default value is 14 days. For example: If a certificate is valid for one year, 14 days before the end of that year, the Cloud Extender attempts to renew the certificate. The Cloud Extender attempts two renewals per certificate per week.
Retry duration	If a certificate request fails, the Cloud Extender retries the certificate request every 15 minutes. This setting specifies the number of days that the Cloud Extender tries to renew the certificate before it marks the renewal request as a failure. If you have a maintenance window of eight hours for your

	CA environment, the retry automatically issues certificates when the CA is back from maintenance. Set this value to three days at the minimum.
Time in seconds to wait between polling attempts	In certain SCEP environments (such as Verizon MCS), when the Cloud Extender requests a certificate, the server does not always return a certificate. Instead, the server responds with a wait response until it generates the certificate. The Cloud Extender then polls for the certificate every (x) seconds. Use this option to check for certificate availability. The certificate is available within a couple of seconds of the initial certificate request.
Total polling time duration in seconds	Specifies how long the polling lasts for each certificate request. For example, if the polling delay is one second and the polling limit is 10 seconds, the Cloud Extender polls 10 times for the certificate before it marks the polling request as a failure.

11. Click the **Save** button

11.15.2 What to Do Next

Configuring MaaS360 Policies to Use the Cloud Extender Certificate Templates

Parent topic: **Microsoft CA Integration**

11.16 Configuring MaaS360 Policies to Use the Cloud Extender Certificate Templates

Follow these steps to make sure that the MaaS360® policies are using the Cloud Extender™ certificate templates.

11.16.1 Procedure

Verify that the template name appears in the MaaS360 policies under the following sections:

1. **MDM** > **Exchange ActiveSync** > **Identity Certificates**
2. **MDM** > **Wi-Fi** > **Identity Certificates**
3. **MDM** > **VPN** > **Identity Certificates**
4. **Persona** > **Email** > **Authentication Type & Identity Certificates**
5. **Persona** > **Enterprise Gateway** > **Authentication Type & Identity Certificate for gateway authentication**
6. **Persona** > **Enterprise Gateway** > **Identity Certificate for resource authentication**

When these policies are assigned to a device, the platform triggers certificate requests to the Cloud Extender and then pushes the payload to the device when the Cloud Extender receives the certificates.

Parent topic: Microsoft CA Integration

11.17 Symantec CA Integration

MaaS360® integrates with the Symantec host PKI certificate authority for automatic delivery of device certificates to enrolled devices.
The Cloud Extender™ generates signed certificates by using the Symantec API and delivers those signed certificates to devices.
Before you can integrate with the Symantec CA, you must have the following access rights:

1. Administrative access to the Symantec MPKI Portal
2. Administrative access to the Cloud Extender server that implements the certificates

Creating a Certificate Profile on the Symantec PKI Manager
Follow these steps to create a certificate profile in your Symantec Portal if no profile previously exists.

Viewing the Details of a Symantec PKI Certificate Profile
Follow these steps to view the details of a Symantec PKI certificate profile.

Getting an RA Certificate from Symantec
Follow these steps to obtain an RA certificate from Symantec.

Completing the Symantec PKI Certificate Template Configuration
Follow these steps to complete the configuration of the Symantec PKI certificate template.

Parent topic: Cloud Extender Certificate Integration Configuration

11.18 Creating a Certificate Profile on the Symantec PKI Manager

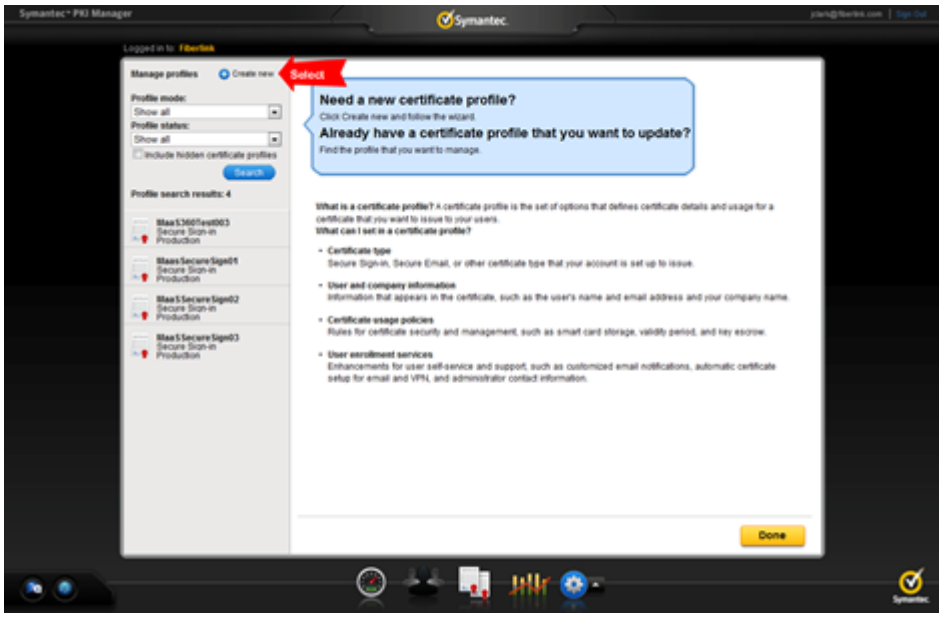
Follow these steps to create a certificate profile in your Symantec Portal if no profile previously exists.

11.18.1 About This Task

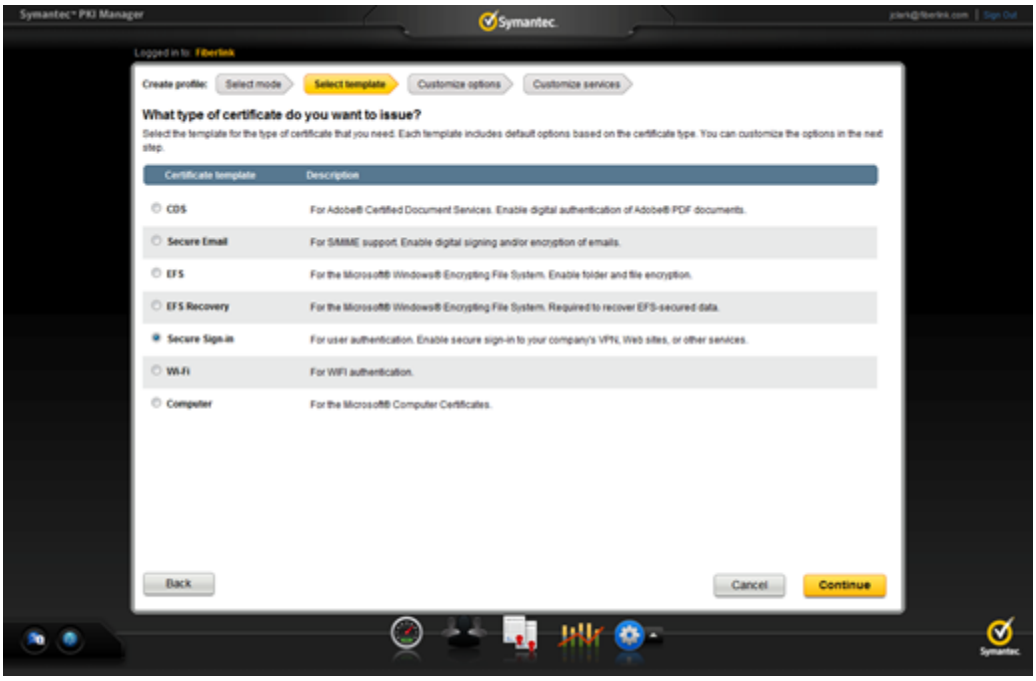
If a certificate profile exists, skip this procedure and go to Viewing the Details of a Symantec PKI Certificate Profile. For more information about creating certificate profiles in the Symantec Portal, see the Symantec documentation.

11.18.2 Procedure

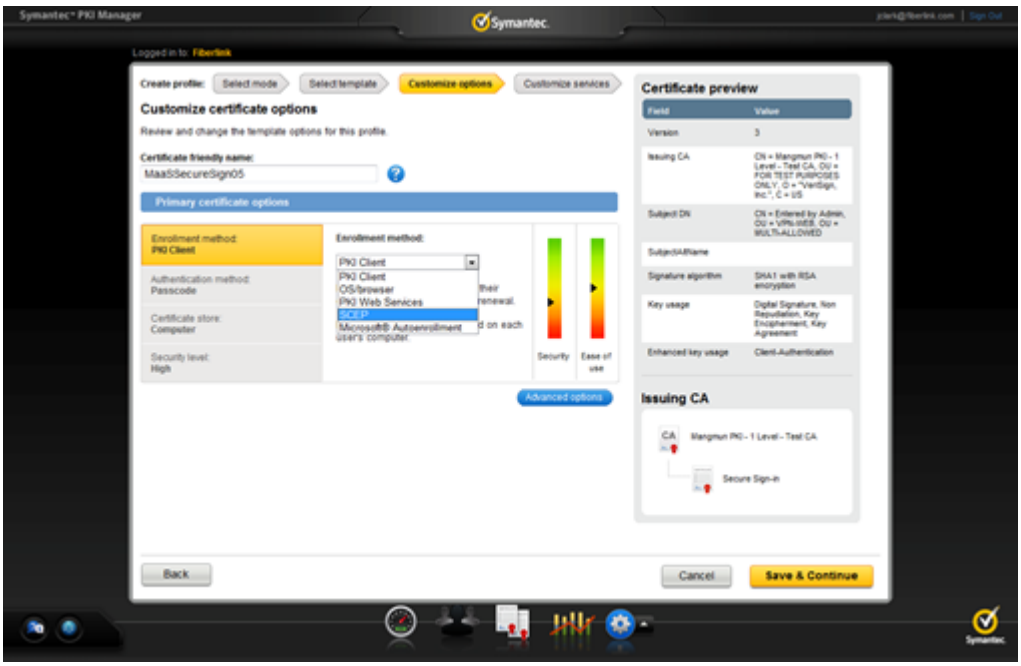
1. Log in to your Symantec PKI Manager account. You can get the URL and the credentials to access your PKI Manager account directly from Symantec.
2. Select **Manage Certificate Profiles** to view the Manage profiles window.
3. Select **Create new** to select the mode to create the profile.



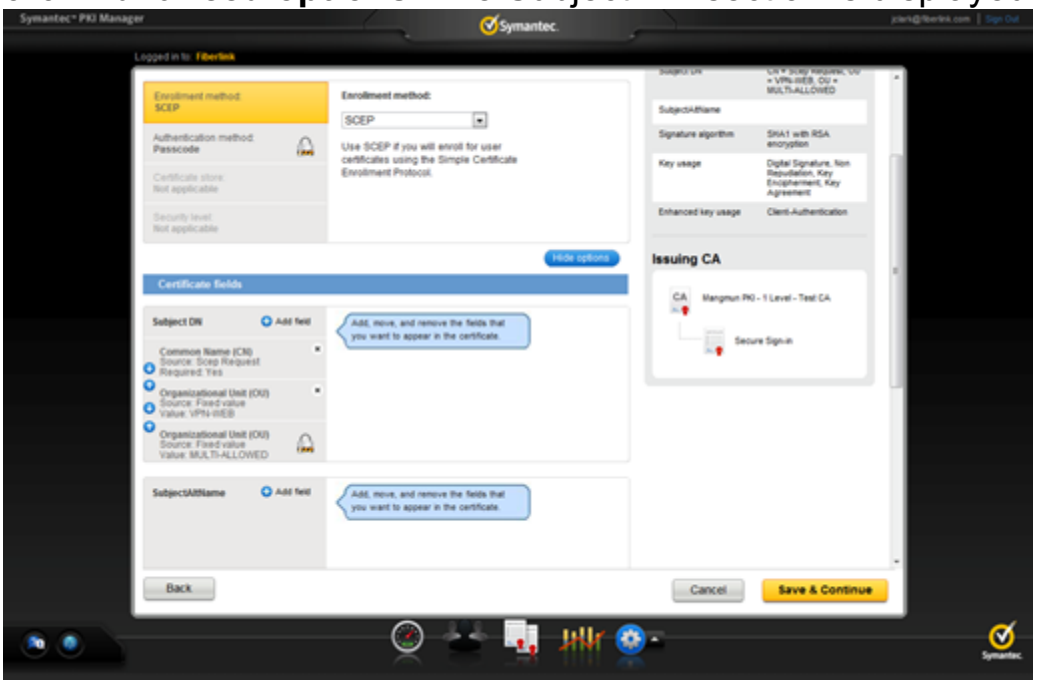
4. Click **Production mode**, and then click **Continue**. The Select template window is displayed.



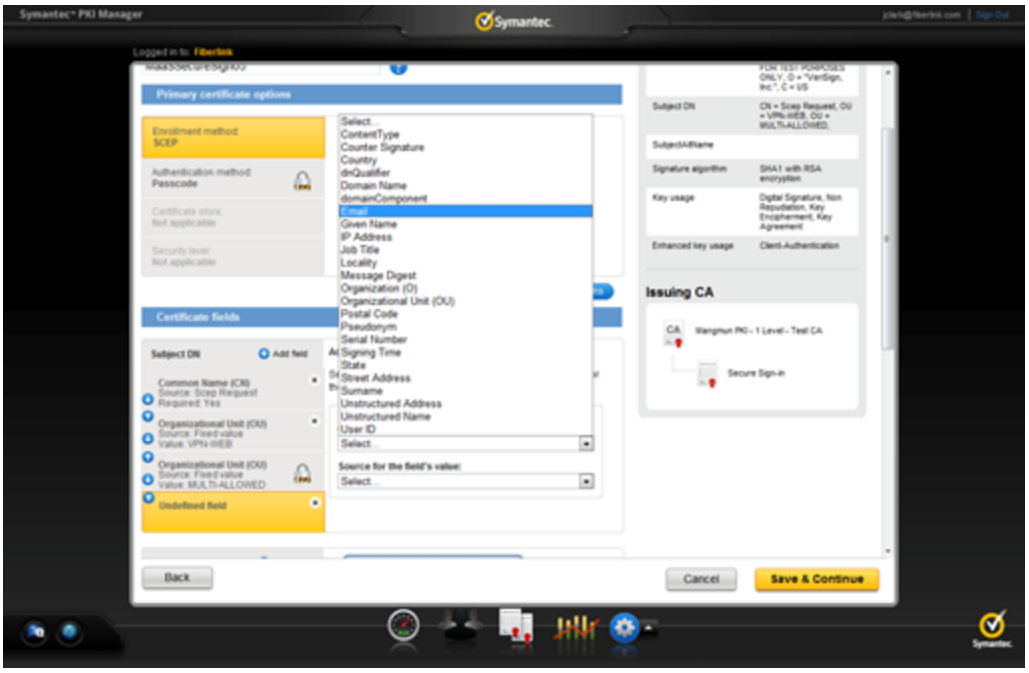
5. Click **Secure Sign-in**, and then click **Continue**. The Customize options window is displayed.



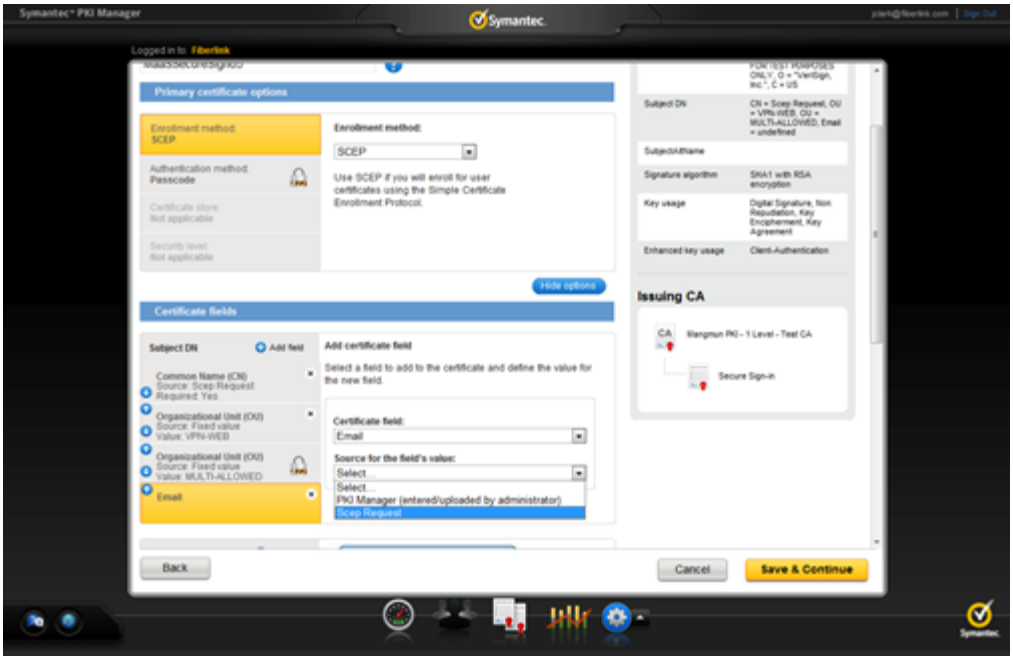
6. From the **Enrollment method** list, select **SCEP**.
7. Type a **Certificate friendly name** for the certificate profile, and then click **Advanced options**. The Subject DN section is displayed.



8. In the Subject DN section, select **Add field** to provide an email address as part of the Subject DN.
9. From the **Certificate field** list, select **Email**.

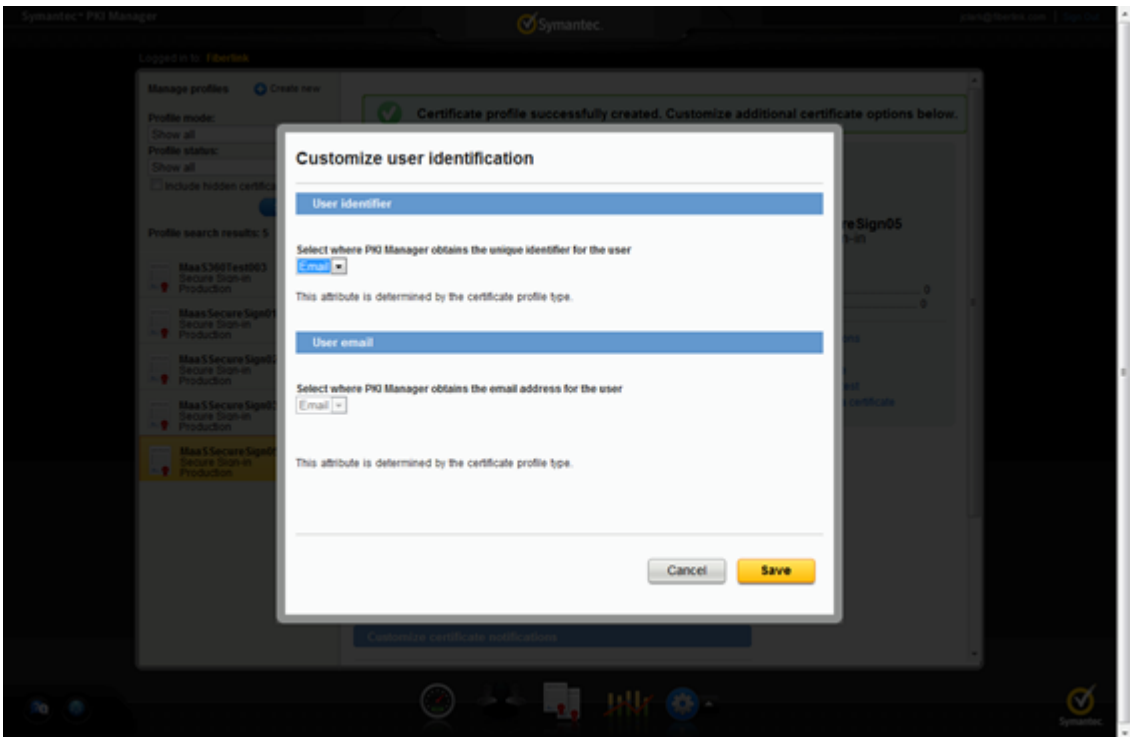


10. From the Source for the field's value list, select Scep Request

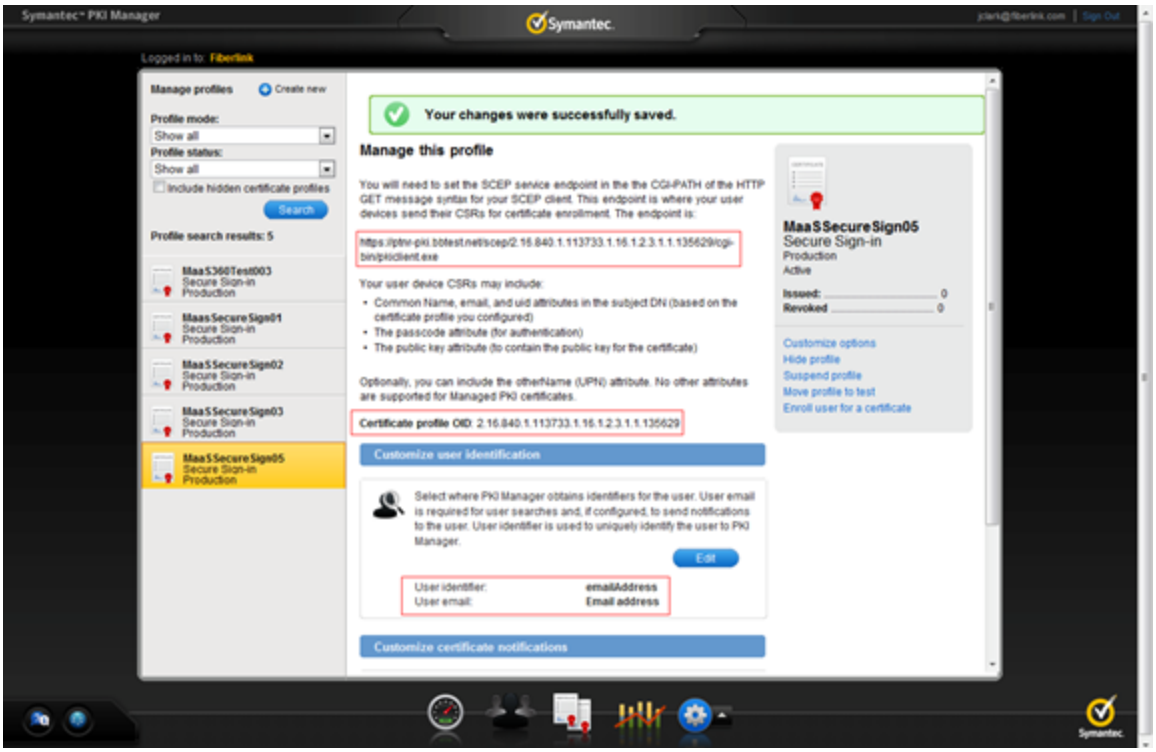


11. Make the **Certificate Field: Email** a required value, and then use the up arrows in the Subject DN section to move the **Email** field to the top of the list.
12. Click the **Common Name (CN)** field, and set the **Required** value to **No**.

13. Click **Save & Continue**.
14. Click **Edit** to display the main profile window for the profile that you created.
15. Make sure that the unique identifier for the user is set to **Email**, and then click **Save**.



A confirmation message displays a successful profile creation that includes the SCEP URL, the certificate profile OID, and the user identification based on the user's email address.



11.18.3 What to Do Next

Getting an RA Certificate from Symantec

Parent topic: Symantec CA Integration

11.19 Viewing the Details of a Symantec PKI Certificate Profile

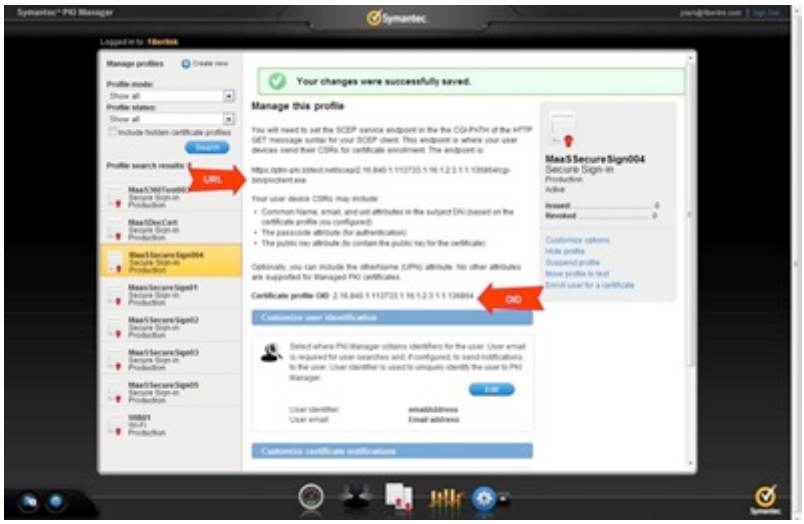
Follow these steps to view the details of a Symantec PKI certificate profile.

11.19.1 Procedure

1. Log in to your Symantec PKI Manager account
2. From your PKI Manager dashboard, select **Manage Certificate Profiles**

The Manage profiles window is displayed.

3. Highlight the certificate profile that you created a template for in the topic Creating a Certificate Profile on the Symantec PKI Manager
4. Copy the URL and Certificate profile OID values from this window for the Cloud Extender™ template configuration



11.19.2 What to Do Next

[Getting an RA Certificate from Symantec]

Parent topic: [Symantec CA Integration]

11.20 Getting an RA Certificate from Symantec

Follow these steps to obtain an RA certificate from Symantec.

11.20.1 Procedure

1. Log in to your Symantec PKI Manager account
2. From the PKI Manager dashboard, select **Get an RA certificate**

3. The **Get an RA** certificate window is displayed
4. Open the Cloud Extender™ Configuration Tool, click **Create New Template**, and then select the **Symantec SCEP** type
5. Provide the profile URL and profile OID from step 2.
6. Click **Don't have a RA Certificate**, and provide a subject name and a password
7. Click **Generate** to generate a CSR (Certificate Signing Request) to obtain your RA certificate from Symantec.
8. Click **Copy To** to copy the CSR to your clipboard.
9. Go back to the Get an RA certificate window in the PKI Manager, and then paste your CSR that you copied to your clipboard.

11.20.2 What to Do Next

[Completing the Symantec Certificate Template Configuration]

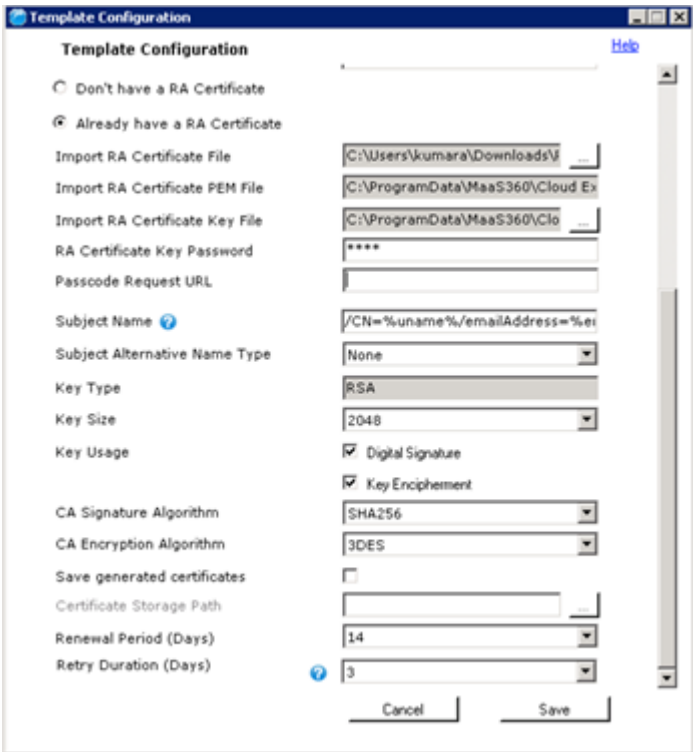
Parent topic: [Symantec CA Integration]

11.21 Completing the Symantec PKI Certificate Template Configuration

Follow these steps to complete the configuration of the Symantec PKI certificate template.

11.21.1 Procedure

1. From the Template Configuration window, click **Already have a RA certificate**.



2. From the **Import RA Certificate File** field, browse for the location of the RA certificate that you downloaded from Symantec. After you select the RA certificate file, the configuration tool populates the values in the following fields:
   a. **Import RA Certificate PEM File**
   b. **Import RA Certificate Key File**
   c. **RA Certificate Key Password**
3. The Template Configuration window also provides the following information:

Option	Description
Type	Use the SCEP type for Symantec CA integration
Subject Name	Use the subject name to configure the certificate template to pass specific attributes of the user or device to the certificate request so that the returned certificate uses these values. The default string for the subject name is `/CN=%uname%/emailAddress=%email%`. The template supports any of the following dynamic parameters: The template also supports the following static values: CN (commonName) C (countryName) L (localityName) ST (stateOrProvinceName) O (organizationName) OU (organizationUnitName) G (givenName) S (Surname) I (Initials) UID (uniqueIdentifier) SN (serialNumber) T (title) D (description) The Cloud Extender™ also supports User Custom Attribute variable names for the subject name of the certificate. If you define the User Custom Attribute and read its value from LDAP or set the value locally on MaaS360, you can pass this value to the certificate request.

Subject Alternative Name Type	Use this field to uniquely identify the user for authentication. This field is one of the most common fields that is used for the subject alternative name. Use one of the following values in this field: **None** **UPN** **UPN and Email** **Other** Open ended configuration that supports all variables as the subject name.
Key Type	The type of key that is used to generate certificates. Default key type: RSA
Key Size	The size of the private key that is used for generated certificates. The key size must match your template on NDES. Default key size: 2048, but also supports 1024 and 4096.
Key Usage	The key usage for the generated keys. Default key usage: Digital Signature and Key Encipherment usages
CA Signature Algorithm	The default is SHA-256, but the Cloud Extender also supports other algorithms. The algorithm must match your template on NDES.
CA Encryption Algorithm	The default is 3-DES, but the Cloud Extender also supports DES and Blowfish.
Save Generated Certificates	If the user reenrolls a device, the Cloud Extender caches certificates locally and repurposes the certificates, instead of contacting the CA for a new certificate. Use

	this option to select a local storage path or a UNC network path that stores certificates.
Certificate Storage Path	The path for the certificate. You can use a local path standalone instance of the Cloud Extender, but you must use a network share for High Availability mode.
Renewal Period (days)	The number of days to try to renew the certificate before the certificate expires. The default value is 14 days. For example, if a certificate is valid for one year, 14 days before the end of that year, the Cloud Extender attempts to renew the certificate. The Cloud Extender attempts two renewals per certificate per week.
Retry Duration (days)	If a certificate request fails, the Cloud Extender retries the certificate request every 15 minutes. This setting specifies the number of days that the Cloud Extender tries to renew the certificate before it marks the renewal request as a failure. If you have a maintenance window of 8 hours for your CA environment, the retry automatically issues certificates when the CA is back from maintenance. Set this value to three days at the minimum.

3. Click **Save**.

Parent topic: [Symantec CA Integration]

11.22 Entrust CA Integration

MaaS360® integrates with the Entrust certificate authority for automatic delivery of device certificates to enrolled devices. The Cloud Extender™ uses the Web Services APIs to communicate with the Entrust CA to obtain identity certificates. The Cloud Extender integrates with version 8.0 of the Web Services API.

The Cloud Extender supports the following variants of Entrust CA:

1. Entrust IdentityGuard Server v10.1 and v10.2
2. Entrust Authority Administration Services v8.2 SP1 and v8.3

Setting Up a Digital ID for Your Entrust CA

Entrust uses Digital IDs to define the format of the certificate that the Entrust CA issues.

Configuring a Certificate Template for Entrust

Follow these steps to complete the configuration of the Entrust certificate template.

Parent topic: Cloud Extender Certificate Integration Configuration

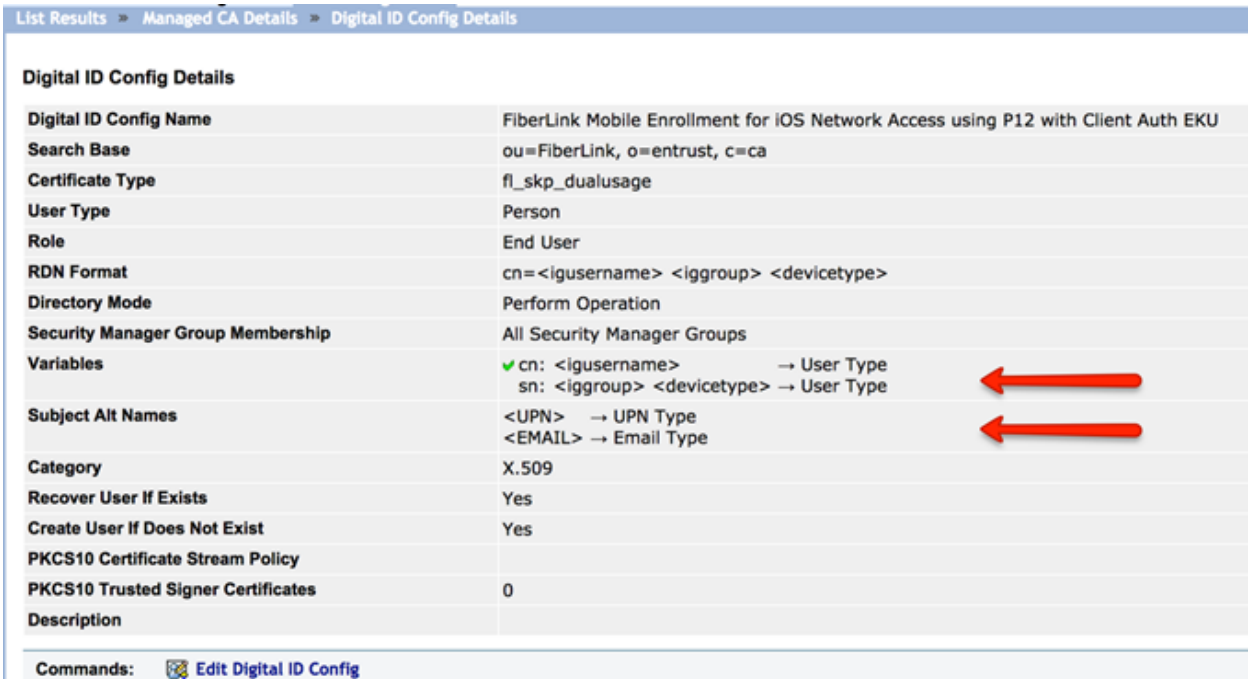
11.23 Setting up a Digital ID for Your Entrust CA

Entrust uses Digital IDs to define the format of the certificate that the Entrust CA issues.
The Cloud Extender™ uses Web Services APIs to receive a certificate from a selected Digital ID. The Cloud Extender provides the values of the Subject Name and the Subject Alternate Name from MaaS360® for the identity certificates. For more information about how to create a Digital ID, contact your Entrust Administrator.

The following sample provides a Digital ID from Entrust IdentityGuard with the following values:

Subject Name displays a username, a group name, and a device type. Entrust uses any supported MaaS360 attribute for these values.

Subject Alternative Name displays UPN type and Email type.



List Results » Managed CA Details » Digital ID Config Details

Digital ID Config Details

Digital ID Config Name	FiberLink Mobile Enrollment for iOS Network Access using P12 with Client Auth EKU
Search Base	ou=FiberLink, o=entrust, c=ca
Certificate Type	fl_skp_dualusage
User Type	Person
Role	End User
RDN Format	cn=<igusername> <iggroup> <devicetype>
Directory Mode	Perform Operation
Security Manager Group Membership	All Security Manager Groups
Variables	✔ cn: <igusername> → User Type sn: <iggroup> <devicetype> → User Type
Subject Alt Names	<UPN> → UPN Type <EMAIL> → Email Type
Category	X.509
Recover User If Exists	Yes
Create User If Does Not Exist	Yes
PKCS10 Certificate Stream Policy	
PKCS10 Trusted Signer Certificates	0
Description	

Commands: Edit Digital ID Config

11.23.1 What to do next

[Configuring a Certificate Template for Entrust]

Parent topic: [Entrust CA Integration]

11.24 Configuring a Certificate Template for Entrust

Follow these steps to complete the configuration of the Entrust certificate template.

11.24.1 Procedure

1. From the Cloud Extender™ Configuration Tool, click the Certificate Integration tile.
2. If you have one or more templates already configured, you will be presented with the template summary page. If so, click the **Add New Template** button.
3. Select **Entrust** from the CA Integration options.
4. Select **User Authentication for Email, Wi-Fi, VPN, browser or reverse proxy. Creates Device Identity Certificates**.
5. Provide the following information for the template:

Parameter	Description
Template Name	The name of your Entrust template. The template name is displayed in the MaaS360® policies under various configuration sections that use identity certificates.
Web Service URL	The web service URL for the Entrust CA.
Administrator Username	Username of the CA administrator.
Password	Password of the CA administrator.
Group Name	The group name that issues all user certificates for Entrust.

6. Click **Continue**. The Cloud Extender makes a web service call to the Entrust CA and receives a list of defined Digital IDs.
7. From the list populated from step 6, choose the appropriate Digital ID.
8. In the RDN Variables field, replace "**%REPLACE%**" strings with supported variables for the Subject Name of the certificate for each of the RDN values. The template supports any of the following dynamic parameters:

Parameter	Description
%udid%	The UDID of the device
%csn%	The MaaS360 device ID
%uname%	The username of the device owner
%domain%	The domain of the user
%email%	The amil address of the user
%imei%	The IMEI number of the device
%model%	The device model
%sim%	The SIM number of the device
%phnumber%	The phone number of the device
%ou% - Note: requires User Visibility Module	Organization Unit
%cn% - Note: requires User Visibility Module	Common Name
%dc% - Note: requires User Visibility Module	Domain Component
%dn% - Note: requires User Visibility Module	Distinguished Name

9. Click the **Next** button
10. Select a name that uniquely identifies the user for authentication from the **Subject Alternative Name Type** list. Choose from the following options:
    a. **None**
    b. **UPN**
    c. **UPN and Email**
    d. **Other**: Open ended configuration that supports all variables as the subject name.
11. Select the number of days in the **Renewal Period (Days)** field to try to renew the certificate before the certificate expires.
    a. The default value is 14 days. For example, if a certificate is valid for one year, 14 days before the end of that year, the Cloud Extender attempts to renew the certificate. The Cloud Extender attempts two renewals per certificate per week.
12. Select the **Search For Entrust User by CN** check box to search for a user by common name instead of searching by user name (which is the default setting).
13. Click the **Save** button

Parent topic: Entrust CA Integration

11.25 IDnomic/OpenTrust PKI CA Integration

MaaS360® integrates with the IDnomic/OpenTrust PKI certificate authority (CA) for automatic delivery of user certificates for authentication and S/MIME capabilities (email security) on enrolled devices.
IDnomic/OpenTrust PKI is a third-party cloud CA that uses the SCEP protocol to deliver a certificate to a device. IDnomic/OpenTrust creates and manages the digital identities of users or devices within a Public Key Infrastructure (PKI).
IDnomic/OpenTrust PKI integrates with Active Directory and supports multiple certificate authorities.

Configuring a Certificate Template for IDnomic/OpenTrust PKI

Follow these steps to complete the configuration of the IDnomic/OpenTrust PKI certificate template.

Parent topic: Cloud Extender Certificate Integration Configuration

11.26 Configuring a Certificate Template for IDnomic/OpenTrust PKI

Follow these steps to complete the configuration of the IDnomic/OpenTrust PKI certificate template.

11.26.1 Procedure

1. From the Cloud Extender™ Configuration Tool, click the Certificates Integration tile.
2. If you have one or more templates already configured, you will be presented with the template summary page. If so, click the **Add New Template** button.
3. Select **IDnomic – Mobile Guard**
4. Select **User Authentication for Email, Wi-Fi, VPN, browser or reverse proxy. Creates Device Identity Certificates**.
5. Click the **Next** button
6. Provide the following information for the template:

Parameter	Description
Template Name	The name of your IDnomic / OpenTrust PKI template. The template name is displayed in the MaaS360® policies under various configuration sections that use identity certificates
Web Service URL	The web service URL for the IDnomic / OpenTrust PKI CA. See the vendor documentation for information on how to obtain this URL.
Authentication Certificate Path	The path for the authentication certificate that is used by the Cloud Extender to authenticate to the PKI server. This certificate is issued by the PKI server on the console. See the vendor documentation for information on how to obtain this certificate.

Certificate Password	The password that is used to encrypt the authentication certificate (p12).

7. Click the **Continue** button
    a. The Cloud Extender makes a web service call to the IDnomic Certificate Authority and receives a list of mandatory fields.
8. Provide the following information for the template:

Parameter	Description
Profile Name	The profile from the MDM service that contains the SCEP parameters (SCEP URL and challenge) that are used to issue the certificate on the device.
Mandatory Fields	Auto-populated when a Profile Name is selected.
Mandatory Fields Replacement	Replace "`%REPLACE%`" with supported variables in MaaS360 to include specific attributes in the certificate request.
Revoke Certificates	Select the conditions which will trigger revocation of a device certificate.

9. Click the **Next** button
10. To modify certificate renewal periods, click the **Advanced** button
    a. On this advanced page you can select your desired renewal period (in days)
    b. On this advanced page you can select the maximum period of time (in days) that the Cloud Extender will retry certificate enrollment attempts if prior attempts have failed
11. Click the **Save** button

Parent topic: [IDnomic / Mobile Guard PKI CA Integration]

11.27 Verizon MCS Integration

The Verizon MCS certificate authority uses SCEP (Simple Certificate Enrollment Protocol) to issue certificates.
Use the Microsoft SCEP Server Type for configuring the Verizon MCS certificate template on the Cloud Extender™. For detailed instructions, see the procedure in the topic Configuring a Certificate Template on the Cloud Extender.

Parent topic: Cloud Extender Certificate Integration Configuration

11.28 Testing Certificate Integration

Follow these steps to test certificate integration on the Cloud Extender™.

11.28.1 Before You Begin

Make sure that you saved the certificate template in the Template Configuration window.

11.28.2 Procedure

1. From the Cloud Extender Configuration Tool, select the Certificate Integration tile.
2. Click the Test icon for the template you wish to test:

3. Enter test values in the data fields required for your test
4. Click the **Test** button
    a. **Note:** The Cloud Extender Configuration Tool substitutes template values that are not collected on the Test Certificate window with `Test` or `Blank`.
    b. The Cloud Extender requests a new test certificate against the configured CA.
    c. Upon completion of a successful test, a link will be displayed which can be clicked to view the location of the test certificate locally on the Cloud Extender.
    d. If the certificate test fails, you can also collect the diagnostic logs for Cloud Extender to troubleshoot the issue.

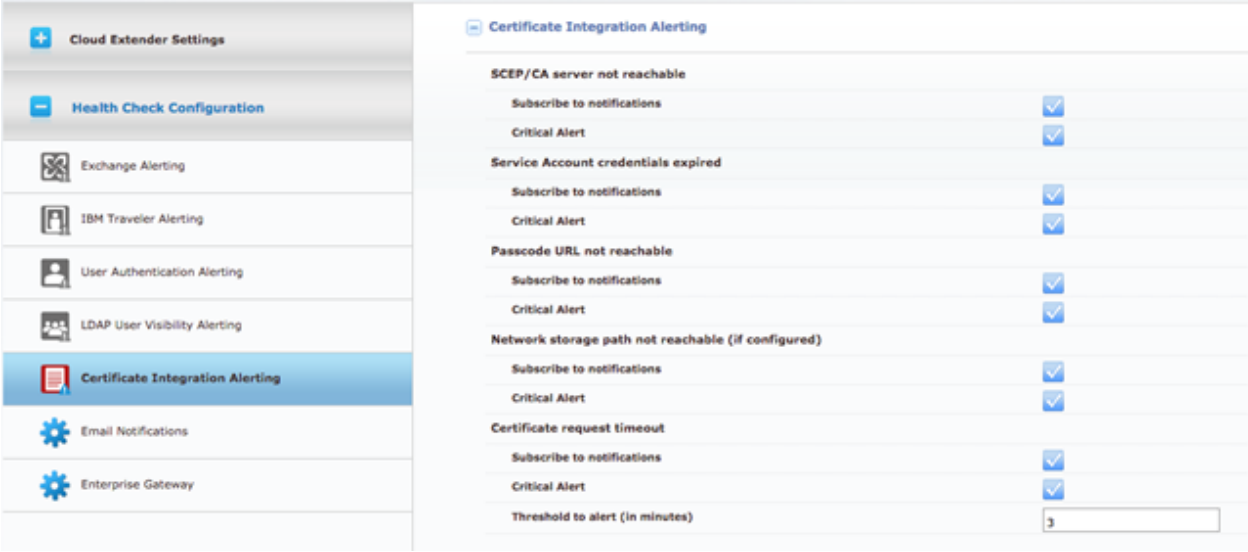
Parent topic: [Certificate Integration Module]

11.29 Enabling Health Check Alerts for Certificate Integration

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ Certificate Integration module.

11.29.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.
2. Select **Health Check Configuration** > **Certificate Integration Alerting**. The Certificate Integration Alerting list is displayed:



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
SCEP/CA Server Not Reachable	The Cloud Extender cannot connect to the configured Certificate Authority (CA) or the	Verify that the Configured Certificate Authority (CA) server is reachable from the

	SCEP URL because the server is unreachable or the specified server URL is invalid.	Cloud Extender server. Verify that the configured SCEP URL is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal use the Certificate Test workflow to confirm certificate generation. If this issue continues, collect logs from the Cloud Extender, and then contact IBM® Support for further assistance.
Service Account Credentials Expired	The Cloud Extender cannot connect to the configured Certificate Authority (CA) server because the server is unreachable or the service account credentials are invalid.	Verify that the Configured Certificate Authority (CA) server is reachable from the Cloud Extender server. From the Cloud Extender Configuration Tool in the MaaS360 Portal, use the Certificate Test workflow to confirm certificate generation. Check whether the service account that is configured in the Certificate Template is still active and the password is not expired. If required, use the Cloud

		Extender Configuration Tool in the MaaS360 Portal to update the service account credentials. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Passcode URL Not Reachable	The Cloud Extender cannot connect to the Challenge Passcode URL to obtain the challenge passcode for certificate requests.	The Cloud Extender connects to the Passcode URL to obtain a one-time challenge passcode that is required for every certificate request. The Cloud Extender cannot reach this passcode URL. Verify that the Passcode URL that is configured on the Certificate Template is valid for that configuration. Verify that the Passcode URL is reachable from the Cloud Extender server. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to run a **Test Certificate** action to confirm certificate generation. If this issue continues, collect logs from the

		Cloud Extender, and then contact IBM Support for further assistance.
Network Storage Path Not Reachable (if configured)	The Cloud Extender cannot connect to the configured certificate storage path for local caching of certificates. This alert refers to multiple Cloud Extenders in High Availability (HA) mode that share a network storage path to cache certificates.	The Cloud Extender uses the certificate storage path to cache identity certificates for future use. This path is either a local path or a network storage path. Verify that the certificate storage location is accessible from the Windows File Manager on the Cloud Extender server. If the location moved to a new path, use the Cloud Extender Configuration Tool to update the location on the Certificate Template. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Certificate Request Timeout	The certificate generation is taking more time to complete than the configured threshold.	By default, the certificate request times out after 3 minutes. Verify that the Certificate Authority (CA) server is reachable from the

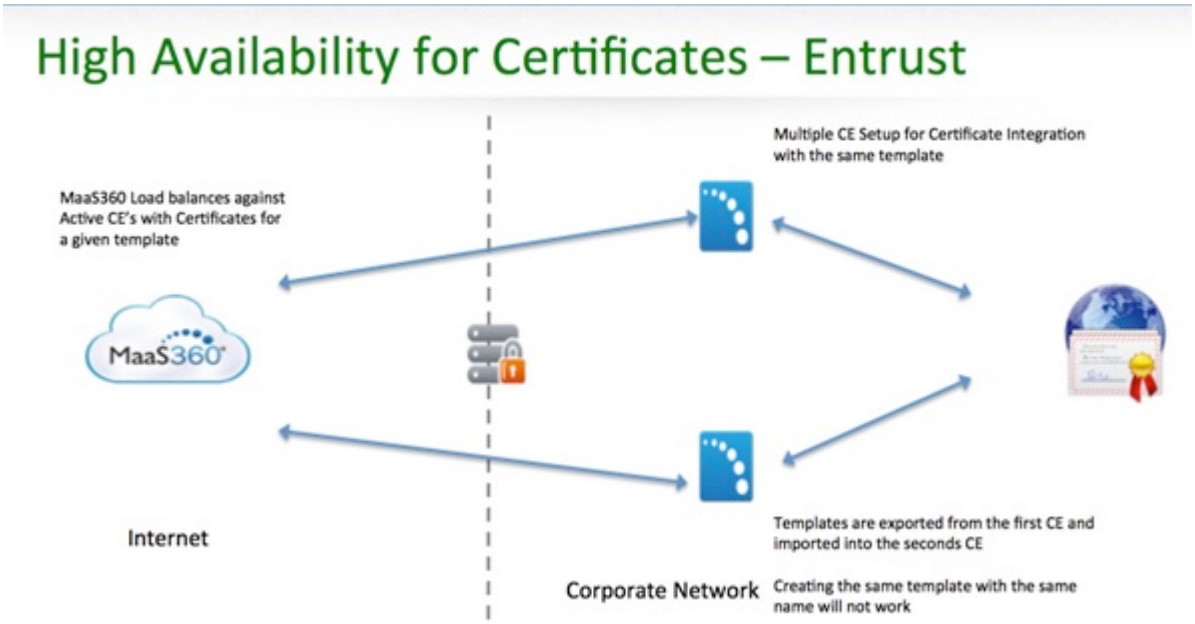
		Cloud Extender server. If you are using an on-premises CA (Microsoft NDES or Entrust), review the event logs or application logs on the CA server for possible issues and resolution steps. If you are using a cloud-based CA (Symantec PKI), contact the vendor for further assistance.

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [Certificate Integration Module]

11.30 High Availability (HA)

The Cloud Extender™ supports High Availability configuration for the Certificate Integration module. Configure multiple instances of the Cloud Extender with the same certificate template for Active-Active HA configuration.
HA configuration for Certificate Integration module involves importing the same certificate on all active Cloud Extenders in the HA cluster.
The MaaS360® Portal balances the load for generating certificates and renewal requests among the active Cloud Extenders by using a round-robin method. The following diagram illustrates HA configuration with two Cloud Extenders:



If you must enable certificate caching for a multiple Cloud Extender setup, the certificate storage path must be a common file share that both Cloud Extenders can write to and share. Even though certificates that are stored on the network share are encrypted with Cloud Extender template level passwords, you can restrict further access to this file share to a specific service account. You can then run the Cloud Extenders for Certificate Integration as that service account by using the Advanced mode from the Cloud Extender Configuration Tool.

Managing Certificates on Multiple Cloud Extenders in an HA Cluster

Follow these steps to export and import certificates to multiple Cloud Extenders in an HA cluster.

Parent topic: Certificate Integration Module

11.31 Managing Certificates on Multiple Cloud Extenders in an HA Cluster

Follow these steps to export and import certificates to multiple Cloud Extenders in an HA cluster.

11.31.1 Procedure

1. Select the Certificates tile from the main window of the Cloud Extender Configuration Tool.
2. Click the Export icon for the template you wish to import:

3. When the certificate template is exported, the Cloud Extender Configuration Tool displays a link to the default exported location of the certificate templates.
4. Copy the exported template(s) onto the remaining Cloud Extenders in the HA cluster.
    a. **Note:** For Symantec, the RA certificate key file and the PEM file must be copied to the remaining Cloud Extenders in the HA cluster and placed in the exact same location as the original Cloud Extender.
5. For the next Cloud Extender in the HA cluster, select the Certificates tile on the main window of the Cloud Extender Configuration Tool.
6. Click the **Import Certificate Template** button.
7. Browse to the exported template files to import the desired template.
8. Click the **Next** button to advance to the final configuration page
9. Click the **Save** button to save the configuration.
10. Run **Test** actions that confirm that test certificates were issued.
11. Repeat steps 4 - 10 on all the Cloud Extenders in the cluster.

Parent topic: [High Availability (HA)]

11.32 Troubleshooting Issues with Certificate Integration

Follow these steps to troubleshoot any issues with certificate integration.

11.32.1 Procedure

1. View the logs at `C:\%ProgramData%\MaaS360\Cloud Extender\logs\EMSAgent_YYYY_MM_DD.log`.
2. Search for `PKIE-CERTACT`.
3. Run the Cloud Extender™ Diagnostic Logs Collection Tool by following these steps:
   a. Log in to the Cloud Extender server.
   b. Go to `C:\Program Files(x86)\MaaS360\Cloud Extender`.
   c. Double-click **DiagnosticCmd.exe**. A compressed file is generated on your desktop.
   d. Contact IBM® Support to troubleshoot the issue.

Parent topic: Certificate Integration Module

12 Exchange Integration for Real-time Mail Notifications Module

MaaS360® uses the Exchange Integration for Real-time Mail Notifications module to support real-time email notifications for iOS and Windows Phone devices. As a part of the IBM® Productivity Suite, Secure Mail provides an office productivity app with email, calendar, and contacts that your employees use to securely collaborate with colleagues while preserving the mobile experience on their corporate or personal devices.
Through authentication and authorization, only approved and valid users can access sensitive email messages and data. Using policies to control the flow of data, you can restrict sharing by users, forwarding of attachments, and copying and pasting.
Devices that are lost, stolen, or compromised can be selectively wiped to remove the secure email container, all attachments, and profiles.
iOS and Windows Phone do not allow an app to continuously run in the background, which creates a challenge for Secure Mail. Because of this design, Secure Mail on iOS or Windows Phone does not notify users about new email messages in their inbox. The Cloud Extender™ fixes this issue by using Exchange Web Services (EWS) to subscribe to email notifications for users and delivers those notifications from the MaaS360 Cloud to enrolled iOS or Windows Phone devices configured with Secure Mail.

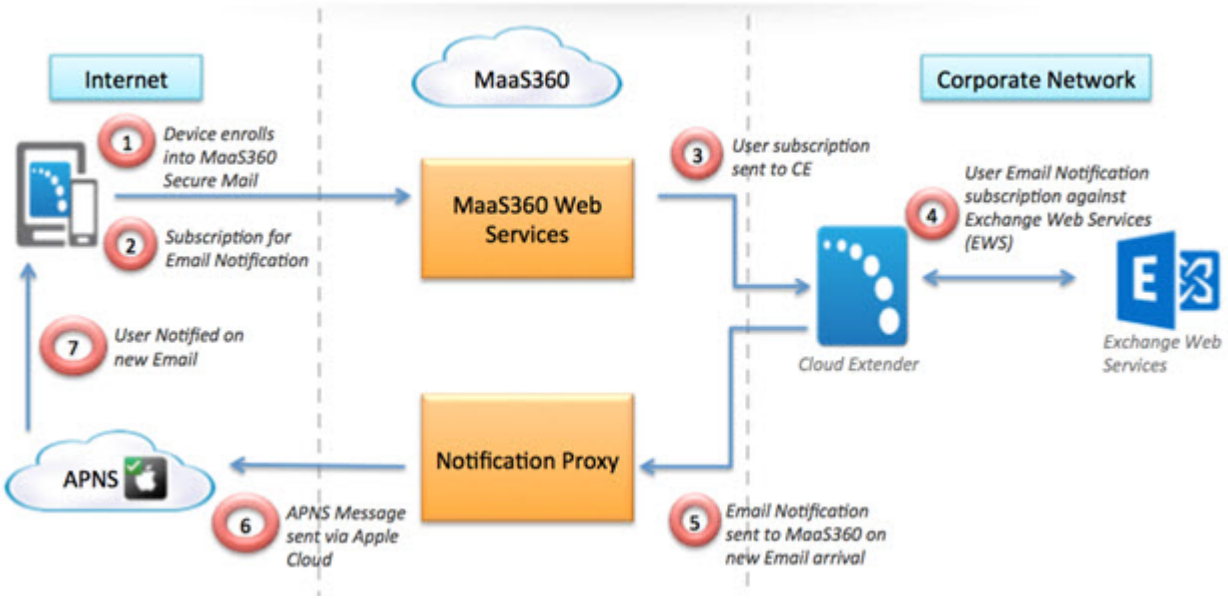
12.1.1 How the Module Works

The Exchange Integration for Real-time Mail Notifications module works in the following way:

1. The user enrolls an iOS or Windows Phone device in MaaS360. Based on the corporate policy, MaaS360 pushes configuration down to set up email in the MaaS360 app and subscriptions for real-time email notifications.
2. When the user completes the email configuration, MaaS360 app calls a Web Service on the MaaS360 Cloud to register this device for notification subscription.
3. MaaS360 then notifies the Cloud Extender to register for notifications.
4. The Cloud Extender uses listener accounts to interact with Exchange Web Services (EWS) and subscribes to email notifications for user mailboxes.

5. When the user receives a new email message in their inbox, EWS notifies the Cloud Extender with basic details of the new email message, such as Subject and Sender.
6. The Cloud Extender notifies the MaaS360 notification proxy to deliver this alert to the user's device.
7. The notification proxy uses Apple Push Notification Service (APNS) or Windows Push Notification Services (WNS) to notify the user about the new email message on the device.

The following diagram illustrates the architecture for the module:



12.1.2 Supported Versions of Exchange

This module supports the following versions of Exchange:

1. Exchange 2007 (must have at least Update Rollup 4 for Service Pack 3 applied)
2. Exchange 2010 (must have at least Update Rollup 4 for Service Pack 2 applied)
3. Exchange 2013 (must have Auto Discovery configured)
4. Office 365 (must have Auto Discovery enabled)

12.1.3 Requirements and Scaling

The MaaS360 Portal provides a Cloud Extender Configuration Tool at **Setup** >
Services > **Enterprise Email Integration** that you can use to set up Cloud Extender for email notifications. The following table provides general guidelines:

Item	Requirement
Less than 15,000 devices	CPU: 2 cores Memory: 4 GB .NET 3.5
More than 15,000 devices	CPU: Use more Cloud Extenders Memory: N/A Scaling: Supports installation on multiple instances of the Cloud Extender, but does not support High Availability (HA). Install on a dedicated Cloud Extender, but cannot enable on Cloud Extender with other services enabled. For accurate scaling of your environment, see the Cloud Extender scaling document at **Setup** > **Services** > **Enterprise Email Integration**.

12.1.4 Network Traffic

The Cloud Extender uses Exchange Web Services (EWS) to subscribe to notifications for user's mailboxes. The Cloud Extender is notified several ways when the user receives an email. The Cloud Extender uses Push Notification and Streaming Notification methods for the integration.

12.1.4.1 Push Notifications

1. The Cloud Extender uses this approach for Exchange 2007 only.

2. A Client Access Server (CAS) sends Push Notifications by using HTTP. The subscriber (Cloud Extender) for push notifications must have a server listener handling HTTP requests.
3. For Exchange 2007 integration, an available inbound port must be configured on the Cloud Extender server to receive these notifications.

12.1.4.2 Streaming Notifications

1. The Cloud Extender uses this approach for Exchange 2010/2013 and Office 365 integration.
2. Streaming Notification is a callback mechanism. The Cloud Extender contacts the Exchange server when something relevant changes on a user's mailbox.
3. All connections from the Cloud Extender are outgoing HTTPS. No inbound ports need to be open.
4. These connections are persistent and remain open for the lifetime of the subscription.

About Listener Accounts

Listener accounts are accounts that subscribe to notifications for users against Exchange Web Services (EWS) to detect new mail and calendar invites.

Enabling Health Check Alerts for Email Notifications

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender Exchange Integration for Real-time Mail Notifications module.

Troubleshooting Issues with Exchange Integration

Troubleshooting issues with integrating Exchange for the Real-time Mail Notifications module.

Parent topic: Configuring Settings for the Cloud Extender Modules

12.2 About Listener Accounts

Listener accounts are accounts that subscribe to notifications for users against Exchange Web Services (EWS) to detect new mail and calendar invites. Listener accounts must use specific impersonation rights for real-time mail notification integration. Each listener account must use the following permissions:

1. Member of Domain Users
2. Local Admin access on the Cloud Extender™ server
3. Impersonation permissions on your Client Access Server (CAS)

Each listener account monitors up to 1,250 mailboxes. You can configure a maximum of 12 listener accounts for each Cloud Extender, which equals a maximum number of 15,000 mailboxes monitored by each Cloud Extender.

Setting Up a Listener Account
Follow these steps to set up a listener account on different versions of Exchange.

Adjusting Throttling Policies
Follow these steps to associate a new throttling policy that does not enforce restrictions for listener accounts.

Configuring Exchange Email Notifications
Follow these steps to configure settings for the Exchange Integration for Real-time Mail Notifications module.

Testing Exchange Email Notifications
Follow these steps to test the email notification integration for Exchange.

Configuring Workplace Persona Policies for Secure Mail Notifications
Follow these steps to configure the WorkPlace Persona policy for Secure Mail notification.

Parent topic: Exchange Integration for Real-Time Mail Notifications Module

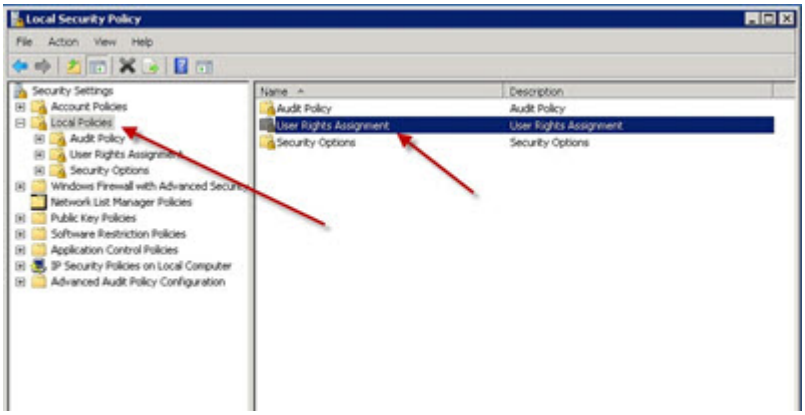
12.3 Setting Up a Listener Account

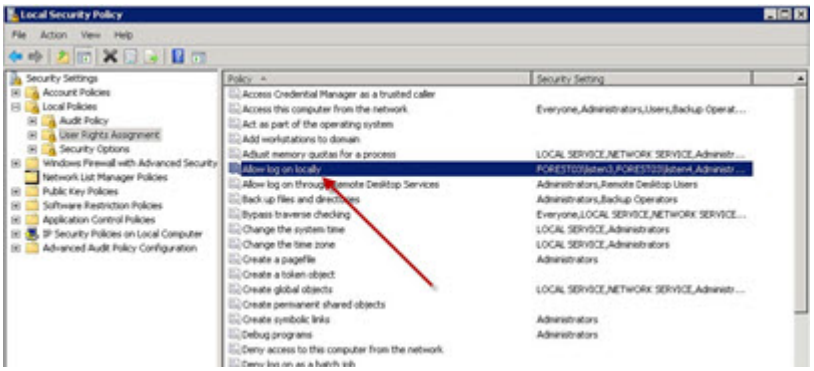
Follow these steps to set up a listener account on different versions of Exchange.

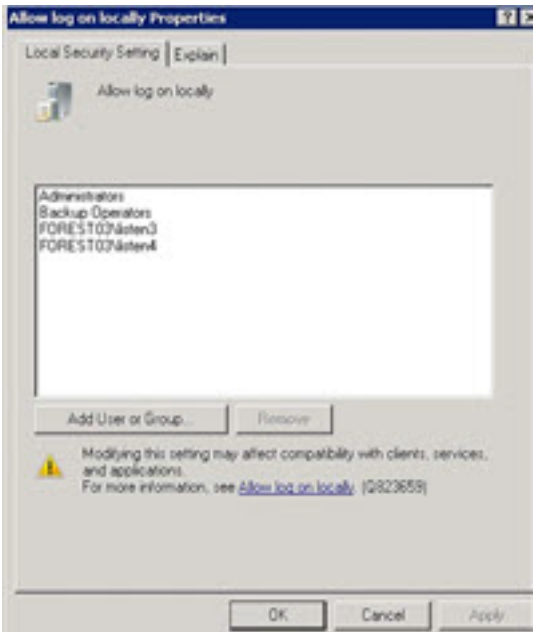
12.3.1 Procedure

For Exchange 2007, follow these steps:

1. Create a Domain User account on your Active Directory.
2. Log in to your CAS server as the administrator account.
3. Provision the **Allow Log on Locally** user right from the Local Security Policy (mmc) for the listener account.







4. For Exchange 2010 and 2013, open Exchange Management Shell and use the following PowerShell command to enable impersonation rights for your listener account:

```
New-ManagementRoleAssignment
&ndash;Role:ApplicationImpersonation &ndash;User:<userid>
```

   For more information about impersonation rights, see the Microsoft documentation at http://msdn.microsoft.com/en-us/library/bb204095.aspx.

5. For Office 365, you must assign application impersonation rights to the listener accounts on Office 365. To set up a group with these permissions, follow these steps:
   a. From the Office 365 Exchange admin center, click **Start**.
   b. On the left navigation menu, click **ADMIN** > **Exchange**.
   c. Click **Permissions** > **admin roles**.
   d. If the role group is available, select **Discovery Management**.
   e. From the Roles section, edit the group, and then click the plus sign (+) and choose **Application Impersonation**.
   f. Add every listener account that is used by the Cloud Extender™ under this role group.

12.3.2 What to Do Next

Adjusting Throttling Policies

Auto Discovery in Exchange 2013 and Office 365
Exchange 2013 and Office 365 both use the Microsoft Autodiscover service to determine the Client Access Server (CAS) URL associated with a specific email address.

Parent topic: About Listener Accounts

12.4 Auto Discovery in Exchange 2013 and Office 365

Exchange 2013 and Office 365 both use the Microsoft Autodiscover service to determine the Client Access Server (CAS) URL associated with a specific email address.
The CAS URL must be determined for each mailbox to subscribe to notifications, which is the default mode of operation for notifications in both Exchange 2013 and Office 365. The Exchange Integration for Real-time Mail Notifications module runs auto discovery (the Microsoft Autodiscover service) during the subscription process for an email address. After the subscription process, the URL is cached for the user and mailbox, and then another auto discovery occurs only if the subscription fails. Caching the URL speeds up the subscription process.

If auto discovery is configured correctly in your environment, the process takes only a few seconds to resolve the CAS URL for a specific email address.
For more information about the Autodiscover service, see the following Microsoft documentation here.

Parent topic: Setting Up a Listener Account

12.5 Adjusting Throttling Policies

Follow these steps to associate a new throttling policy that does not enforce restrictions for listener accounts.

12.5.1 About This Task

If you set up throttling policies in your environment, the listener accounts might be affected by these policies and email notifications might not work well. To avoid issues with throttling policies, create a new throttling policy that does not enforce limits on listener accounts.
Note: For all listener accounts, you must associate a new throttling policy that does not enforce restrictions.

12.5.2 Procedure

For Exchange 2010, follow these steps:

1. Log on to the Exchange Server as the administrator, and then open the Exchange Management Shell.
2. At a command prompt, type the following command to create and set a new throttling policy:

```
New-ThrottlingPolicy MaaS360ThrottlingPolicy
-EWSMaxConcurrency $null
-EWSPercentTimeInAD $null
-EWSPercentTimeInCAS $null
—EWSPercentTimeInMailboxRPC $null
-EWSMaxSubscriptions $null
-EWSFastSearchTimeoutInSeconds $null
-EWSFindCountLimit $null
```

3. Type the following command to disable policy enforcement:

```
Set-Mailbox "<userid>"
-ThrottlingPolicy  MaaS360ThrottlingPolicy
```

For Exchange 2013, follow these steps:

1. Log on to the Exchange Server as the administrator, and open the Exchange Management Shell.
2. At a command prompt, type the following command to create a new throttling policy:

```
New-ThrottlingPolicy MaaS360ThrottlingPolicy
```

3. Type the following command to set the throttling policy:

```
Set-ThrottlingPolicy MaaS360ThrottlingPolicy
-RCAMaxConcurrency Unlimited
-EWSMaxConcurrency Unlimited
-EWSMaxSubscriptions Unlimited
—CPAMaxConcurrency Unlimited
-EwsCutoffBalance Unlimited
- EwsMaxBurst Unlimited
—EwsRechargeRate Unlimited
```

4. Type the following command to disable policy enforcement: `Set-Mailbox "<userid>" -ThrottlingPolicy MaaS360ThrottlingPolicy`

For Office 365, the administrator does not have control over throttling policies for Office 365. The EWS uses the standard throttling limits set on the Office 365 tenant and the MaaS360® listener accounts work accordingly.

12.5.3 What to Do Next

Configuring Exchange Email Notifications

Parent topic: About Listener Accounts

12.6 Configuring Exchange Email Notifications

Follow these steps to configure settings for the Exchange Integration for Real-time Mail Notifications module.

12.6.1 Before You Begin

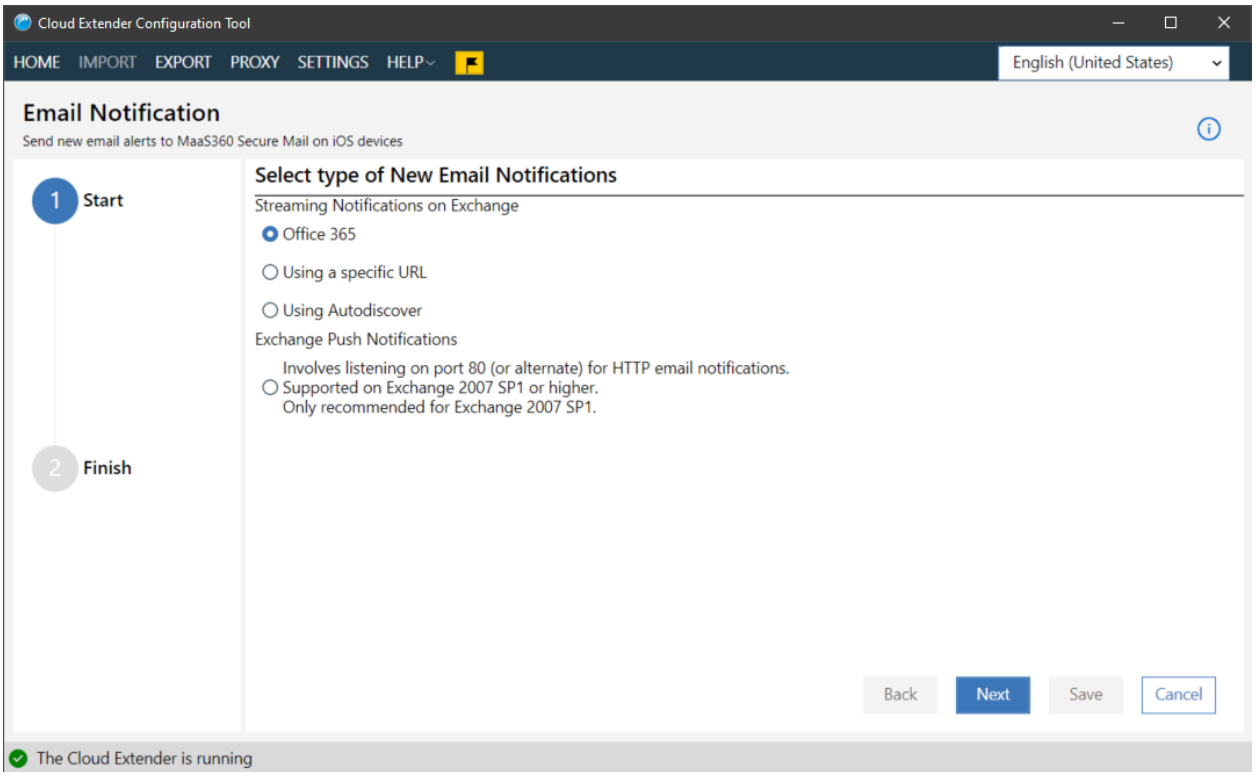
The Secure Mail feature must be enabled for your account. If Secure Mail is not enabled, contact IBM® Support.

12.6.2 Procedure

1. From **Setup** > **Services**, expand and then select the message icon next to the Secure Mail section to enable email notifications for iOS devices in the MaaS360® Portal.

2. Open the Cloud Extender™ Configuration Tool and select the **Email Notification** tile.

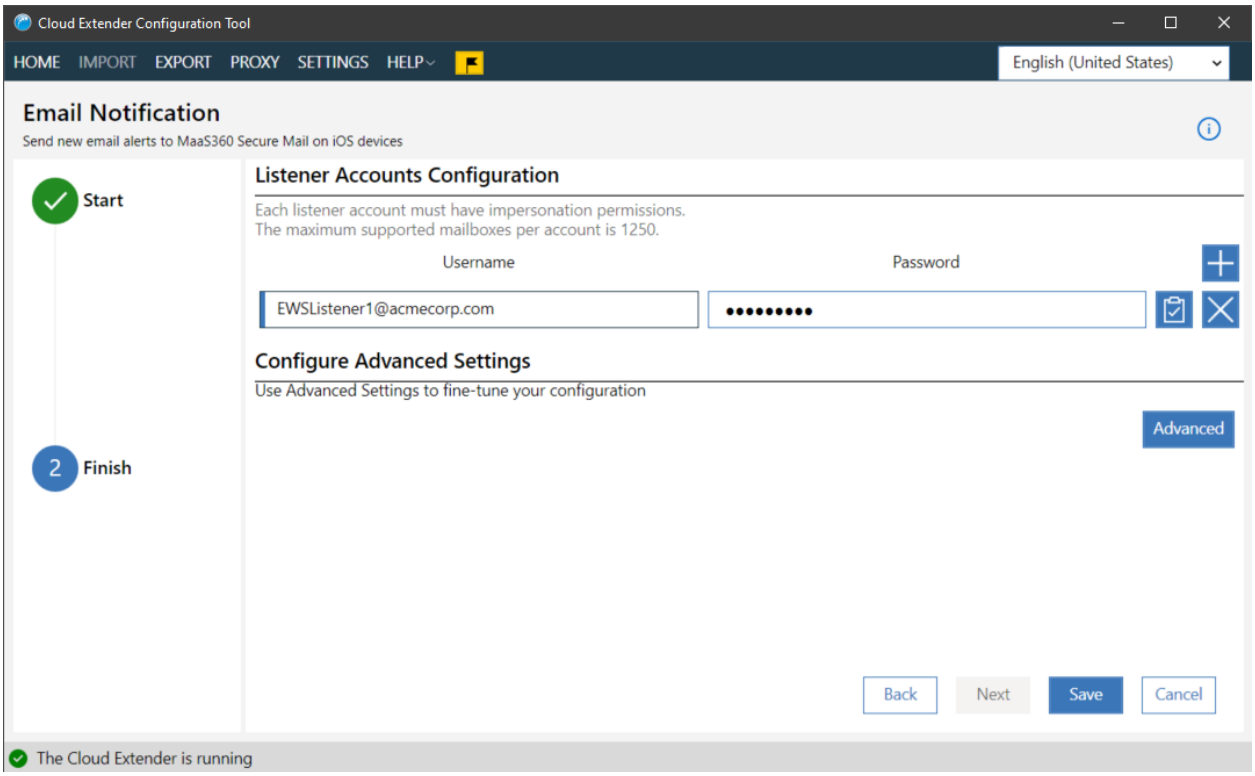
3. Choose the appropriate configuration for your exchange environment:



4. Click the **Next** button
5. Configure settings for any of the following versions of Exchange or Office 365. The technology chosen to use Notifications is not dependent upon the version of Exchange being used, however the underlying technology must be working correctly:

12.6.3 Office 365

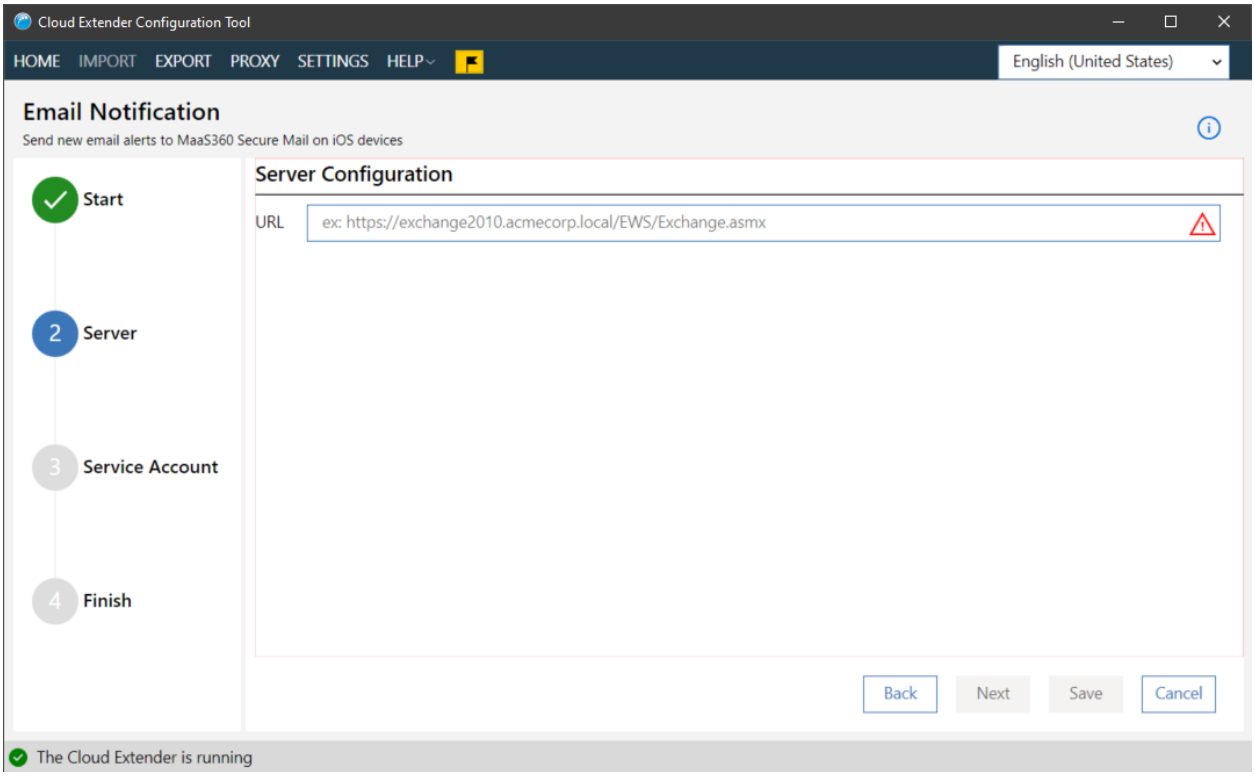
1. Configure listener accounts



Note: Each listener account can subscribe to a maximum of 1,250 mailboxes. One Cloud Extender accepts up to 12 listener accounts.

12.6.4 Using a Specific URL

1. Supply the URL in Config Tool as shown in the following screenshot:

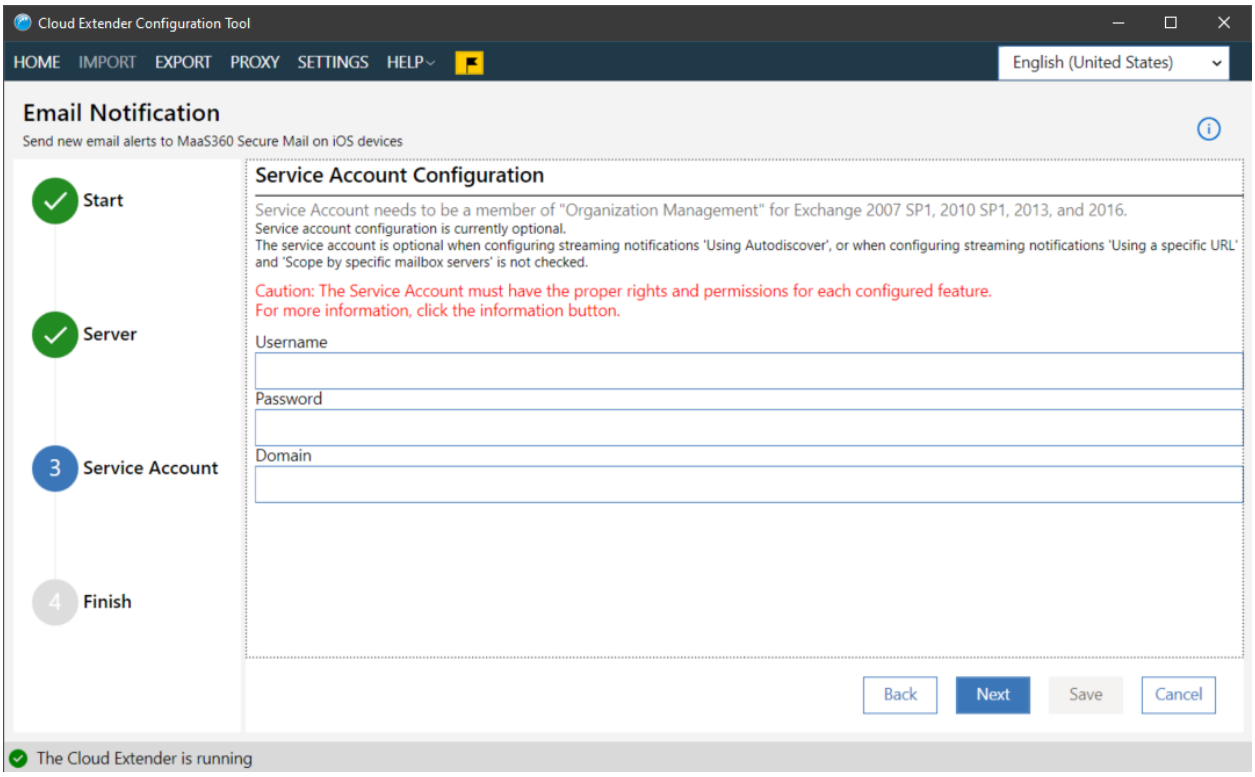


2. Use the following command from the Exchange Management Shell to determine the Web Service URL:

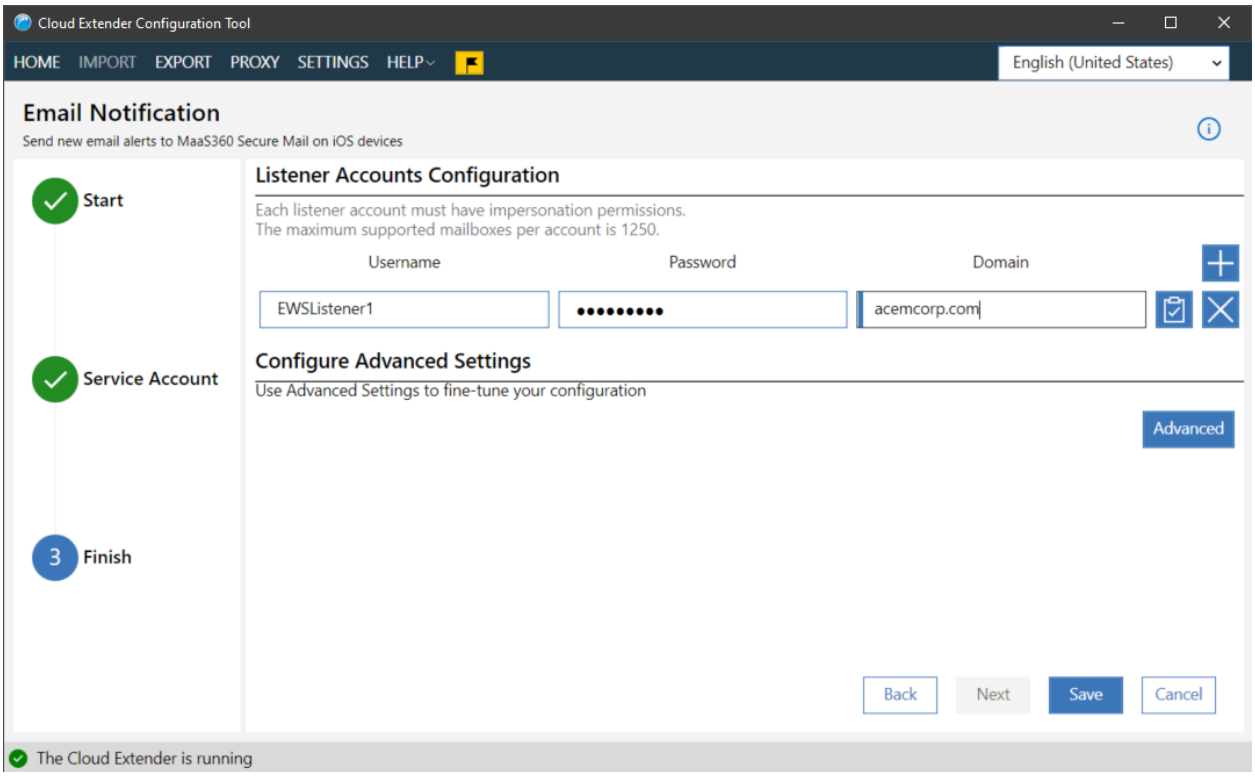
```
Get-WebServicesVirtualDirectory | Select name,*url* |fl
```

Note: An internal URL is typically used for this URL.

3. Click the **Next** button
4. If necessary, add the Service Account details:



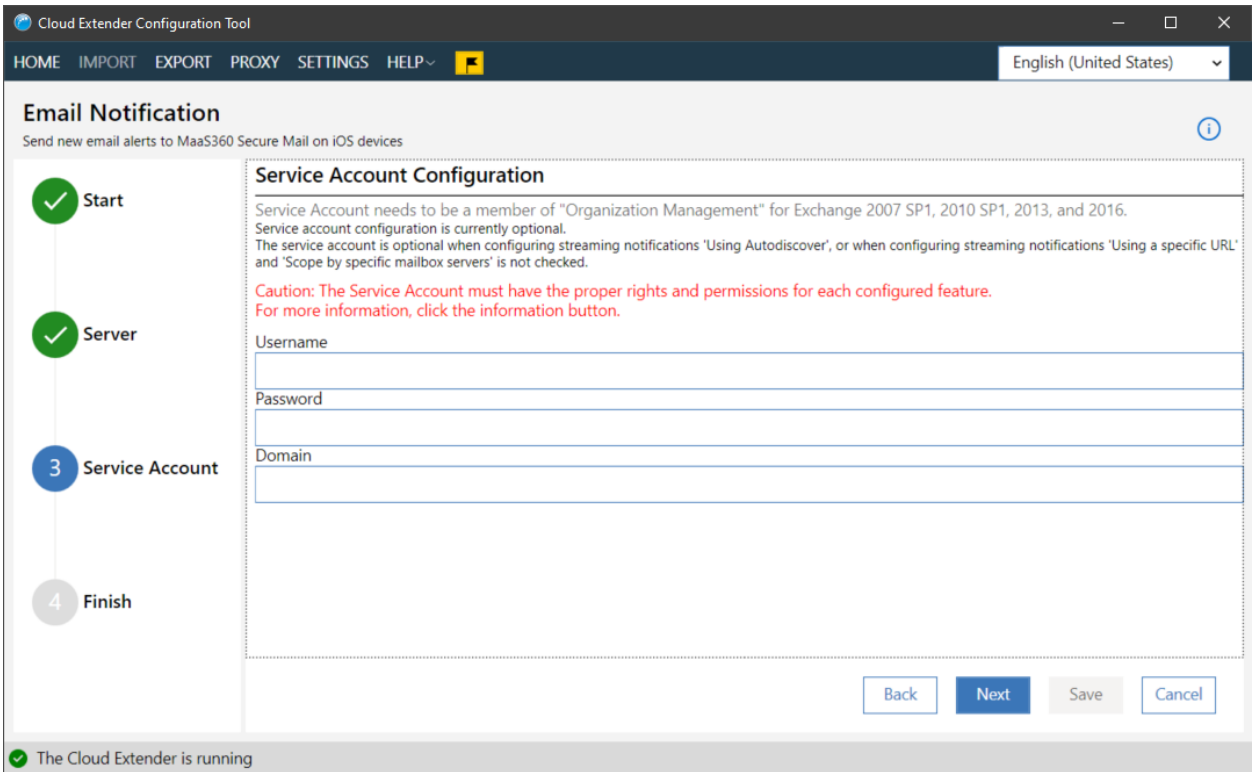
5. Click the **Next** button
6. Add listener account details.



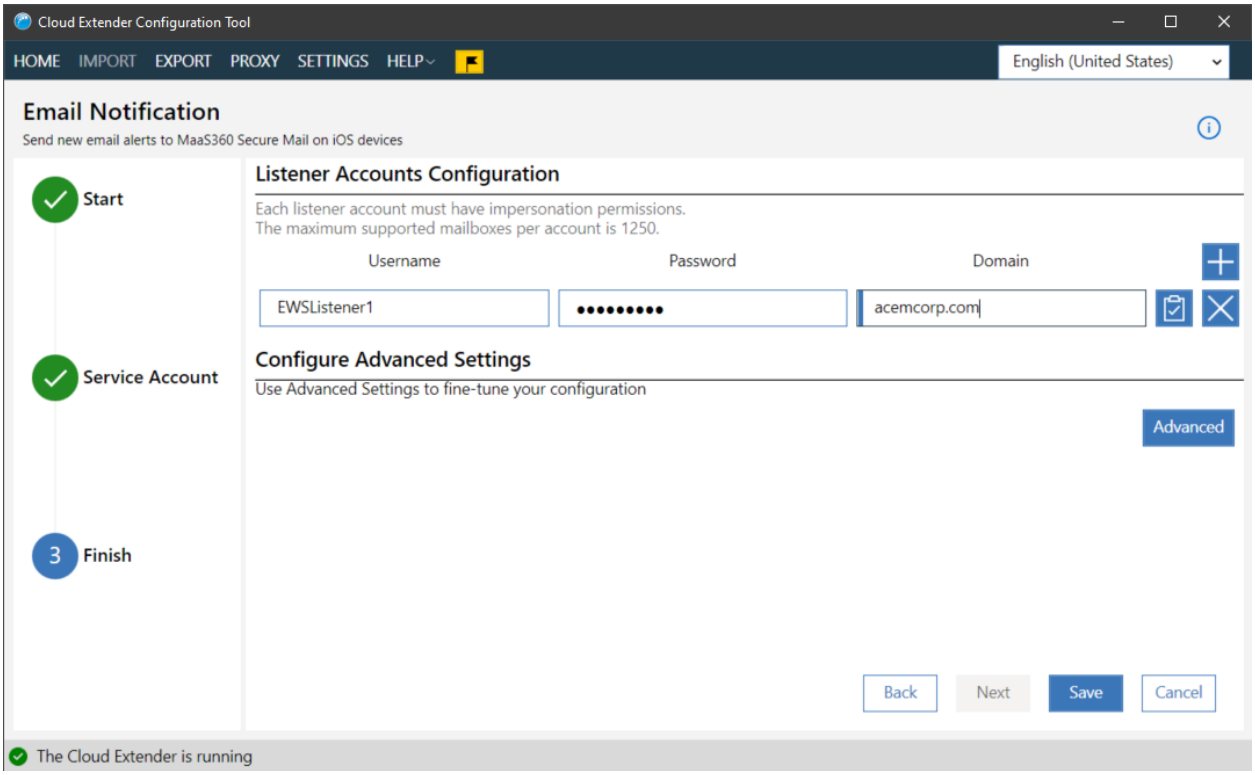
NOTE: Each listener account can subscribe to a maximum of 1,250 mailboxes. One Cloud Extender accepts up to 12 listener accounts.

12.6.5 Autodiscover

1. If necessary, configure the service account



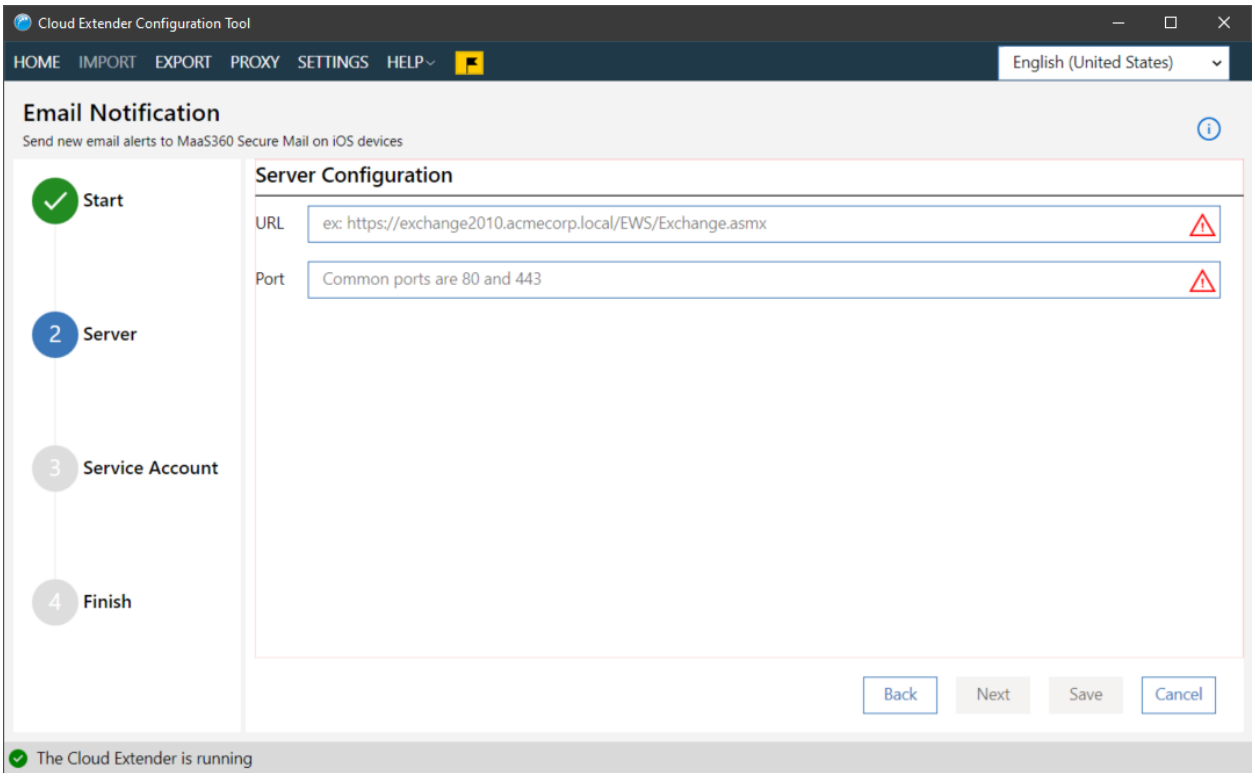
2. Click the **Next** button
3. Add listener account details.



NOTE: Each listener account can subscribe to a maximum of 1,250 mailboxes. One Cloud Extender accepts up to 12 listener accounts.
No URL is necessary, Notifications will use the Autodiscover service to find mailbox details for Grouping and Exchange URL.

12.6.6 Push Notifications

1. Choose the URL that the Cloud Extender will use to connect to Exchange and the port on which Exchange will return notifications. **Note** that this port will need to be opened to incoming connections on the machine the Cloud Extender is installed on.

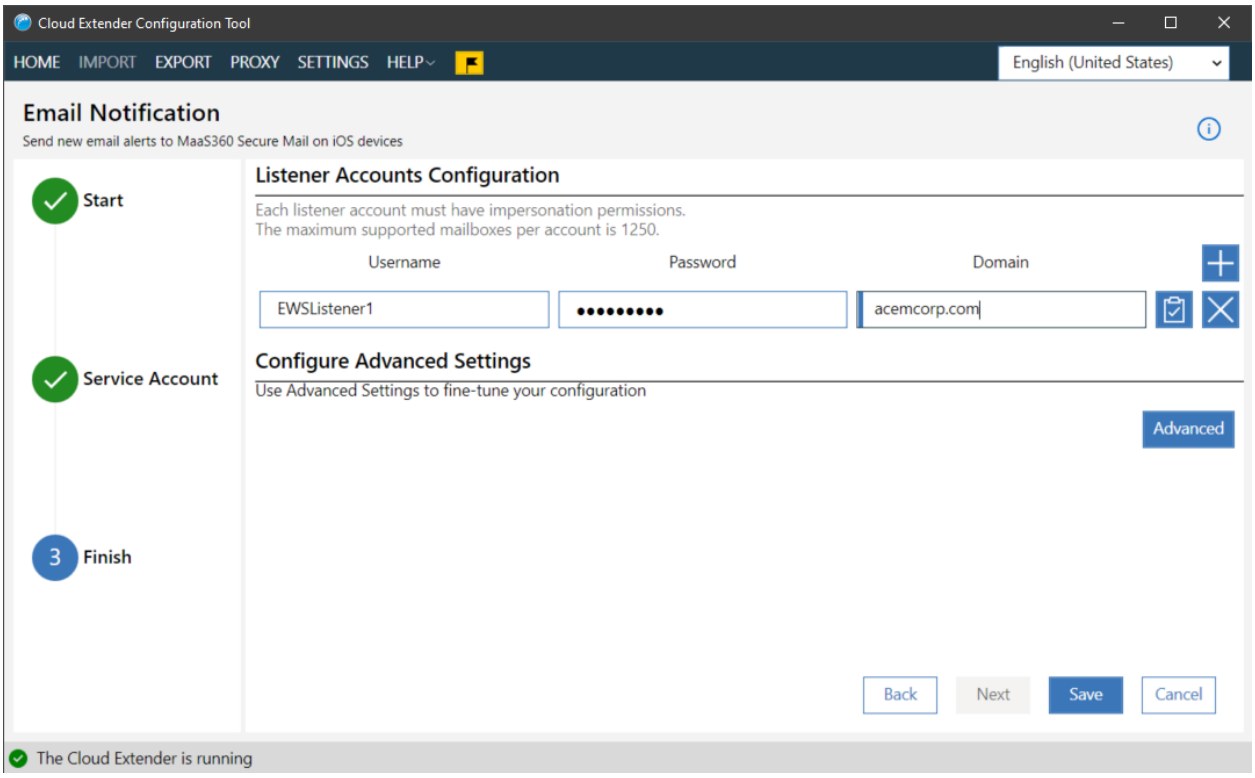


2. Click the **Next** button
3. For determining the URL for the EWS service, use the following command from the Exchange Management Shell:

```
Get-WebServicesVirtualDirectory | Select name,*url* | fl
```

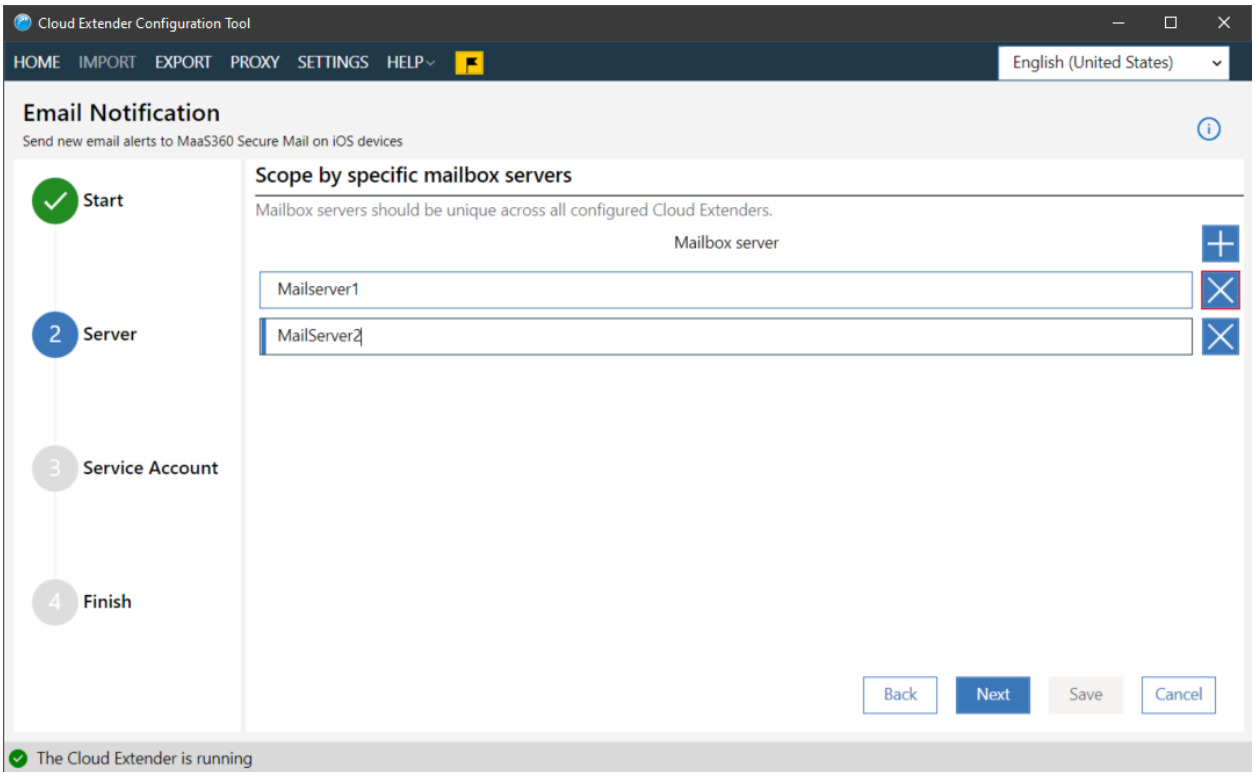
Note: An internal URL is typically used for this URL. If a new email message is available, the Exchange Web Services uses Push Notifications to notify a listener service. You must open an inbound port on the Cloud Extender server. Specify the port number for this field.

4. Add listener account details.



Note: Each listener account can subscribe to a maximum of 1,250 mailboxes. One Cloud Extender accepts up to 12 listener accounts.

5. Click the Next button
6. Specify mailbox servers
   Note: For all on premises exchange servers, notifications can be limited to only connect to specified mailbox servers.



7. Click the **Next** button
8. When configuration is complete, click the **Save** button

Parent topic: [About Listener Accounts]

12.7 Testing Exchange Email Notifications

Follow these steps to test the email notification integration for Exchange.

12.7.1 Procedure

1. After you configure settings for the Exchange Integration for Real-time Mail Notifications module, click **Test**. The Test Integration window is displayed.
2. In the **Test mailbox email address** field, provide the email account that you want to listen to.
3. From your corporate email client, send an email message with `Test` as the **Test Email Subject** to test the email address that you entered in the **Test mailbox email address** field. An integration message is displayed when the email integration is successful.

12.7.2 What to Do Next

Configuring Workplace Persona Policies for Secure Mail Notification

Parent topic: About Listener Accounts

12.8 Configuring WorkPlace Persona Policies for Secure Mail Notification

Follow these steps to configure the WorkPlace Persona policy for Secure Mail notification.

12.8.1 About This Task

After you set up Exchange Integration for Real-time Mail Notifications module and test the integration on your Cloud Extender™, you must turn on your WorkPlace Persona policy so that iOS users can subscribe to notifications for Secure Mail.

12.8.2 Procedure

1. Log in to the MaaS360® Portal.
2. From **Security** > **Policies**, click **Edit** on your WorkPlace Persona policy.
3. Under **Email** > **Configuration**, select **Allow Real-time Notifications**.

4. Select the users who receive new email messages in the **New Mail Notifications** field.
5. Click **Save**, and then publish the policy.
6. Assign the policy to users or devices. When a user receives the policy and configures Secure Mail, the MaaS360 app initiates email notification subscription for the user. The MaaS360 Portal broadcasts the subscription request to all the Cloud Extenders that are running the Exchange Integration for Real-time Mail Notifications module and completes a successful subscription.

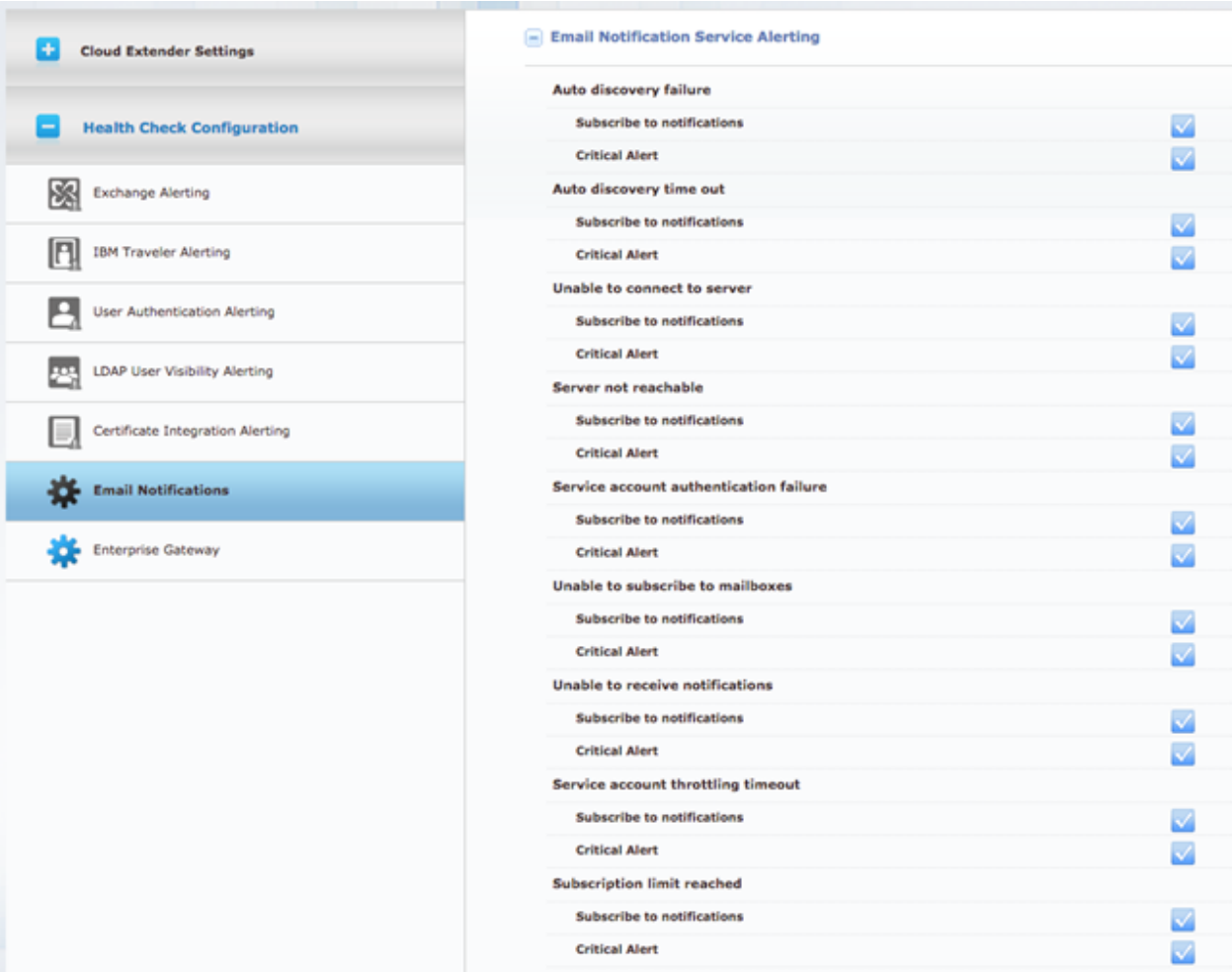
Parent topic: [About Listener Accounts]

12.9 Enabling Health Check Alerts for Email Notifications

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ Exchange Integration for Real-time Mail Notifications module.

12.9.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.
2. Select **Health Check Configuration** > **Email Notifications**. The Email Notification Service Alerting list is displayed:



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
Auto Discovery Failure	The auto discovery process failed for a specific mailbox. The Cloud Extender uses the auto discovery process to evaluate the subscription URL for a specific mailbox.	The Cloud Extender re-subscribes users for email notifications once each day. This alert indicates that the resubscription process failed for the user `%email%`. Check whether the EWS URL that is configured for the Cloud Extender is still valid and reachable from a browser on the Cloud Extender server. Check whether the user's mailbox is still active on your Exchange server. Check whether the user's mailbox is on a mailbox server that is configured in the Email Notification settings. **Note:** If mailbox filtering is not set up on the Cloud Extender, you cannot use this option. Use the Cloud

		Extender Configuration Tool in the MaaS360 Portal to run a **Test** action on the Email Notification configuration for the affected mailbox. If this issue continues, collect logs from the Cloud Extender, and then contact IBM® Support for further assistance.
Auto Discovery Timeout	The auto discovery process is taking more than 3 minutes to complete on a specific mailbox.	The Cloud Extender re-subscribes users for email notifications once each day. This alert indicates that the resubscription process did not complete within the expected timeframe. Check whether the EWS URL that is configured for the Cloud Extender is still valid and reachable from a browser on the Cloud Extender server. Verify that the EWS URL resolves to a regional server to minimize latency. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

Unable to Connect to Server	The Cloud Extender cannot connect to the EWS URL because of an SSL/TLS handshake error.	Verify that your EWS URL uses the correct SSL certificate. Install the EWS server certificate on the certificate store (machine store) for your Cloud Extender server. Access your EWS URL from a browser on the Cloud Extender server to verify that you do not receive a server certificate validation error. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Server Not Reachable	The Cloud Extender cannot connect to the EWS URL because the EWS URL is unavailable or issues with network connectivity.	Check whether the EWS URL that is configured for the Cloud Extender is still valid and reachable from a browser on the Cloud Extender server. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to run a **Test** action on the Email Notification configuration for the affected mailbox. If this issue continues, collect logs from the

		Cloud Extender, and then contact IBM Support for further assistance.
Service Account Authentication Failure	The Cloud Extender cannot connect to the EWS URL because of an authentication failure with a connection to the configured service account.	Check whether all listener accounts that are configured on the Cloud Extender are enabled or use valid passwords. Reset passwords for one or more affected service accounts and reconfigure your Cloud Extender with the updated credentials. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to run a **Test** action on the Email Notification configuration. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Unable to Subscribe to Mailboxes	The email notification subscription failed for a specific user.	The user cannot receive email notifications for iOS Secure Email. Check whether the user's mailbox is still active on your Exchange server. Check whether the user's mailbox is on a

		mailbox server that is configured in the Email Notification settings. **Note:** If mailbox filtering is not set up on the Cloud Extender, you cannot use this option. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to run a **Test** action on the Email Notification configuration for the affected mailbox. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Unable to Receive Notifications	The Cloud Extender is experiencing mailbox subscription failure (more than 50% of the retry queue is full).	The Cloud Extender is experiencing failures with email notification subscriptions for multiple mailboxes. Verify that your Exchange environment is not undergoing maintenance. Check whether the EWS URL that is configured for the Cloud Extender is still valid and reachable from a browser on the

		Cloud Extender server. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.
Service Account Throttling Timeout	The service account is experiencing throttling, which is causing requests to take more than 20 minutes to complete.	The Exchange server is repeatedly rejecting requests from a service account. One or more service accounts might be throttled. Check whether your Exchange server is overloaded and unable to process notification requests. Check the throttling policies on your Exchange and evaluate whether to adjust limitations to accommodate Cloud Extender email notification requests. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to add service accounts to distribute the load among all service accounts. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

Subscription Limit Reached	The Cloud Extender cannot add more mailboxes for subscription. The Cloud Extender reached the limit for email notification subscriptions.	The Cloud Extender is subscribed to the maximum number of mailboxes for the configured service accounts. New users who enroll Secure Mail cannot subscribe to email notifications. Use the Cloud Extender Configuration Tool in the MaaS360 Portal to add service accounts to continue with subscriptions. If you reach the maximum number of configurable service accounts on one Cloud Extender, install a new Cloud Extender (requires Advanced configuration with mailbox server filtering) to continue with new subscriptions. **Note:** Use this option with the on-premises version of Exchange only. If this issue continues, collect logs from the Cloud Extender, and then contact IBM Support for further assistance.

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [Exchange Integration for Real-Time Mail Notifications Module]

12.10 Troubleshooting Issues with Exchange Integration

Troubleshooting issues with integrating Exchange for the Real-time Mail Notifications module.

12.10.1 Why aren't devices receiving email notifications?

The most common issue that you might experience is that email notifications are not being sent to the device. Follow these steps to troubleshoot this issue:

1. Make sure that your EWS URL is using a valid certificate (if you are using SSL) and the certificate is installed on the Cloud Extender™ server.
2. Make sure that your EWS URL is reachable from the Cloud Extender server (use a web browser to confirm that the URL is reachable).
3. Make sure that the listener accounts are not locked out or that passwords are not expired.
4. Run the Test Action on the Cloud Extender for the affected mailbox to check whether the integration is working as expected.
5. Watch the logs from `C:\%ProgramData%\MaaS360\Cloud Extender\logs\EWSNotifications_YYYY_MM_DD.log`.
6. Run the Cloud Extender Diagnostic Logs Collection Tool:
    a. Log in to the Cloud Extender server.
    b. Browse to `C:\Program Files(x86)\MaaS360\Cloud Extender`.
    c. Double-click **DiagnosticCmd.exe** to generate a compressed file on your desktop.
    d. Contact IBM® Support to diagnose the issue.

12.10.2 Why doesn't the Email Notifications test for the Cloud Extender Configuration Tool work?

If the Cloud Extender Configuration Tool test returns an immediate failure, check the `EWSNotificationsConfig` log files for the following message: `"[ListenerThreadManager::AssignSubscriptionsToConnections] ERROR!`

`Got exception trying to assign subscriptions to connect`
If you receive this error message, you do not have the required version of .NET installed. You must install NET version 3.5. You can install this version over other versions that might be installed. Download .NET from Microsoft at https://www.microsoft.com/en-us/download/details.aspx?id=21.

Parent topic: Exchange Integration for Rea-Time Mail Notifications Module

13 Mobile Enterprise Gateway (MEG) Module

IBM® MaaS360® Mobile Enterprise Gateway (MEG) provides simple, seamless, and secure access to behind-the-firewall information resources for mobile users beyond implementing a new VPN-like technology.
The Mobile Enterprise Gateway (MEG) module provides the following benefits:

1. Seamless logon
2. Credential caching
3. One-time logon across multiple MaaS360 applications
4. Single sign-on to protect intranet resources with strong authentication schemes like NTLM, Kerberos, SPNEGO, and identity certificates

The Mobile Enterprise Gateway (MEG) module provides maximum security by authenticating users and devices based on corporate directory credentials and MaaS360 Enrollment Identity Certificates, which satisfies two-factor authentication requirements for intranet resources. All communication between mobile devices and Mobile Enterprise Gateway (MEG) is fully encrypted and secured end-to-end, which prevents man-in-the-middle attacks.
All data on a mobile device is stored in the MaaS360 container solution fully encrypted and protected from data leakage. The containers are fully controlled by MaaS360 container security policies based on your security requirements. The following extra security benefits apply to Mobile Enterprise Gateway (MEG) implementations:

1. Seamless background reauthentication of users and devices without prompting users for credentials Authentication token requirements for every intranet resource
2. Proxy access list validation on the gateway

The Mobile Enterprise Gateway (MEG) is tightly integrated with the MaaS360 Portal, where you define lockout policies and control access to the gateway based on automated compliance rules. The Mobile Enterprise Gateway (MEG) helps your organization mobilize corporate resources to your ever-growing mobile population while still maintaining control over the data flow and associated data security. The Mobile Enterprise Gateway (MEG) includes the following key features:

1. Seamless integration with MaaS360, including easy and simple configuration
2. Strong gateway authentication schemes
3. Cross Forest / Cross Domain authentication
4. Support for SSO for Gateway across multiple apps on a device
5. Support for Kerberos, SPNEGO, and NTLM v2 authentication against sites
6. Internal proxy support for sites
7. Granular proxy access list
8. Seamless High Availability (HA) configuration
9. High-scaling up to 100,000 devices
10. Regional gateway cluster support and automatic local gateway routing
11. Streaming scenarios for large files and videos
12. Web Distributed Authoring and Versioning (WebDAV) support for Windows file shares
13. Relay DR support

13.1 About Gateway Modes

The Mobile Enterprise Gateway (MEG) operates in one of the following modes:

Mode	Description
Relay Access Mode	The gateway establishes outbound access to the MaaS360 relay server. The devices talk only to the relay server and not directly to the gateway.
Direct Mode	The devices talk directly to the Mobile Enterprise Gateway (MEG) for direct resource access and bypass the MaaS360 hosted relay servers. You can also install the gateway as a standalone gateway for smaller deployments or as a clustered gateway for High Availability (HA).

13.2 Requirements and Scaling

Table 1. Requirements for the Mobile Enterprise Gateway (MEG)

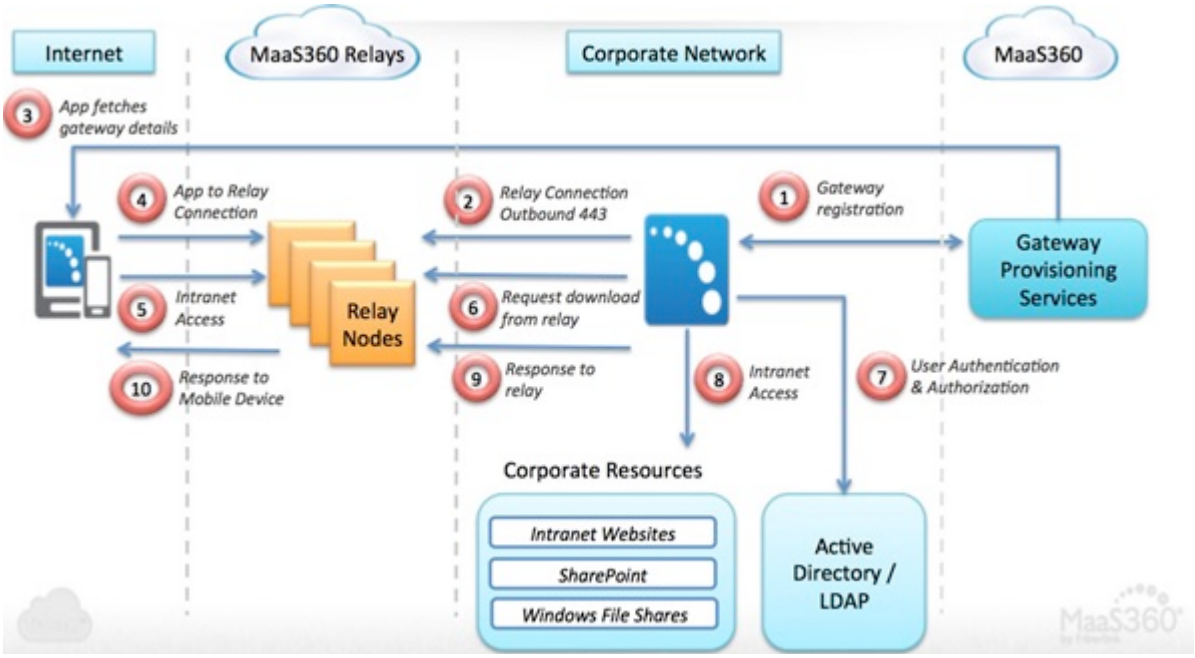
Item	Minimum Requirement
Hardware Component	Physical or virtual machine with Windows Server 2012 RC2, 2012
Mobile Device Clients	iOS 6.0 and later, Android 4.2 or later (carrier versions)
Permissions	A service account that the Mobile Enterprise Gateway (MEG) runs as a member of the Domain User group on your Active Directory and as a member of the Local Administrator group on the server.
Network	Access to the following URLs from the machine that is running the Mobile Enterprise Gateway (MEG): Port 443: The gateway uses this outbound port to communicate with the MaaS360 Backend and Web Services (see networking requirements). If you are using Relay Access Mode, the gateway uses Port 443 to communicate with relay services. No inbound port is used for relay.**Note:** If you are an on-premises customer, the Cloud Extender™ must communicate outbound to your MaaS360 instance within your environment. For Relay Access Mode, use the following relays: For the MaaS360 backend services, use the following

	instances: Direct Mode: An inbound connection is required from the internet to the gateway. Configure this port during the Mobile Enterprise Gateway (MEG) installation and configuration process.
Scaling	Less than 10,000 devices: CPU: 2 core (2.8 GHz) Memory: 4 GB Storage: 2 GB More than 10,000 devices: Use more Gateways in HA mode
Scaling for High Availability	Non-HA Gateway less than 10,000 devices: One gateway is sufficient, no HA possible HA Gateway for more than 10,000 devices: Two Gateways running in clustered mode Note: Even if one gateway can handle the load, you should use another Gateway instance from a High Availability perspective.

13.3 Mobile Enterprise Gateway (MEG) Architecture (Relay Access Mode)

The following diagram illustrates the architecture for the Mobile Enterprise Gateway

(MEG) in Relay Access Mode:



For the client:

1. The MaaS360 app for iOS and Android, the MaaS360 Secure Mobile Browser, and any enterprise app wrapped within MaaS360 or integrated with the MaaS360 SDK communicates with the Mobile Enterprise Gateway (MEG).
2. MaaS360 apps are available from iTunes or Google Play or pushed to devices through the App Catalog.
3. The apps connect to the relay services by using HTTPS, post requests, and pick up responses.
4. In addition to SSL connections to the relays, the payloads are encrypted with AES-256 bit encryption end-to-end between the app and the gateway.

5. Corporate data is secured in the MaaS360 app container and with policy enforcement.
6. To preserve network security and isolation, a mobile device is never on the organization's network and MaaS360 apps do not have direct access to the network.

For the gateway:

1. Windows based server software that runs on a physical host machine or virtual machine (VM) on your organization's internal network or DMZ.
2. Packaged along with the Cloud Extender as a module.
3. The gateway establishes outbound connections to the MaaS360 relay services in the cloud over port 443.
4. Downloads intranet access requests from the relays, fetches the resource, and posts the resulting payloads to the relay services. These payloads are encrypted end-to-end with AES-256 bit encryption. The key is shared only with the device.
5. Gateway authenticates users against Active Directory or LDAP servers.
6. Supports Single Sign-On (SSO) for upstream sites that challenge for NTLM, Kerberos, SPNEGO, and Identity Certificate-based authentication.

For gateway provision services:

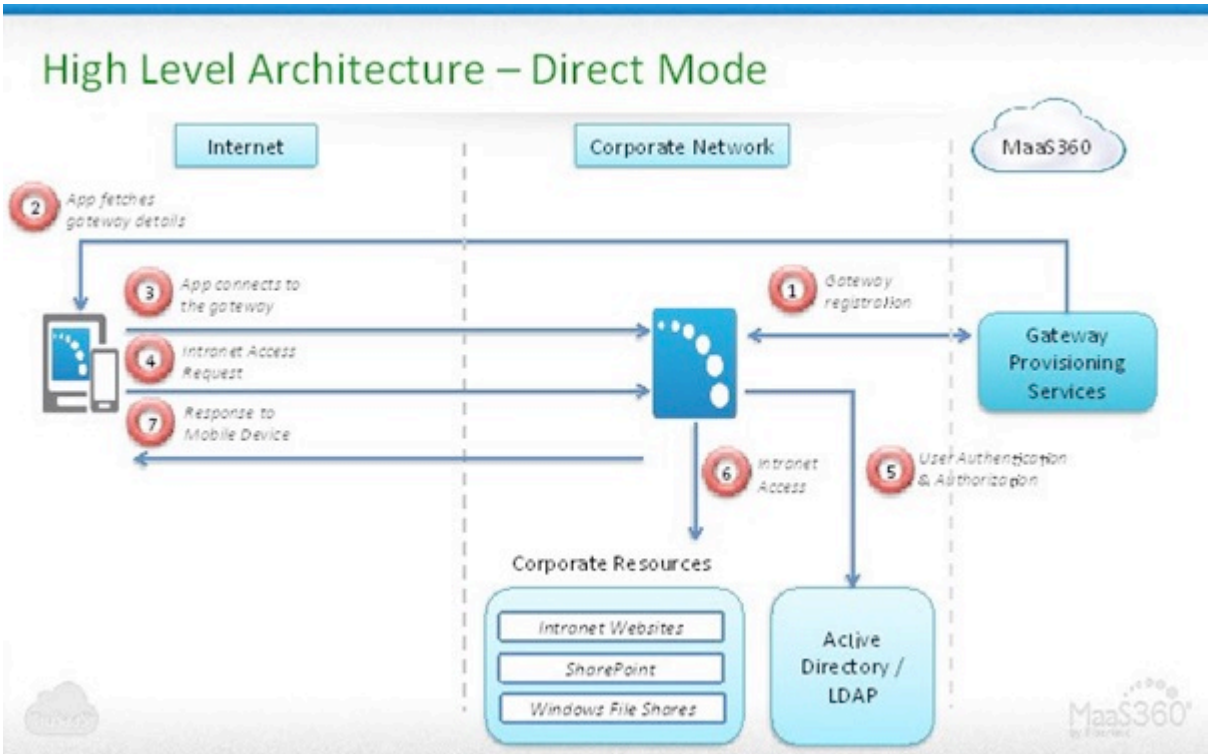
1. Gateway activation happens against this service.
2. MaaS360 issues an identity certificate to the gateway to uniquely identify and authenticate gateways.
3. The devices or apps contact the provisioning server to receive the address of the relay server to use for the respective gateway.

For the relay server:

1. Web services in the cloud that facilitate communications between the clients and your gateway.
2. The Link service cannot read the encrypted communication between the clients and the gateway.

13.4 Mobile Enterprise Gateway (MEG) Architecture (Direct Mode)

The following diagram illustrates the architecture for the Mobile Enterprise Gateway (MEG) in Direct Mode:



For the client:

1. The MaaS360 app for iOS and Android, MaaS360 Secure Mobile Browser, and any enterprise app wrapped within MaaS360 or integrated with the MaaS360 SDK can communicate with the Mobile Enterprise Gateway (MEG).
2. MaaS360 apps are available from iTunes or Google Play or pushed to devices through the App Catalog.
3. The apps connect directly to the gateway for intranet resource access.
4. Access with HTTPS if an SSL certificate is used.
5. In addition to SSL connections to the gateway, the payloads are encrypted with AES-256 bit encryption end-to-end between the app and the gateway.

6. Corporate data is secured in the MaaS360 app container and with policy enforcement.

For the gateway:

1. Windows based server software that runs on a physical host machine or virtual machine (VM) on your organization's internal network or DMZ.
2. Packaged along with the Cloud Extender as a module.
3. Your network must allow inbound traffic to the gateway server with a configurable port.
4. Receives intranet access requests from mobile devices, fetches resources, and posts the resulting payloads back to the mobile devices.
5. These payloads are encrypted end-to-end with AES-256 bit encryption. The key is shared only with the device.
6. Gateway authenticates users against Active Directory / LDAP servers.
7. Supports Single Sign-On (SSO) for upstream sites that challenge for NTLM, Kerberos, SPNEGO, and Identity Certificate based authentication.

Installing the Mobile Enterprise Gateway (MEG)

Follow these steps to install the Mobile Enterprise Gateway (MEG).

Configuring Mobile Enterprise Gateway (MEG) in Standalone Mode

Follow these steps to configure your gateway in Standalone mode.

Mobile Enterprise Gateway (MEG) in High Availability (HA) Mode

The Mobile Enterprise Gateway (MEG) runs in Active-Active mode in a clustered High Availability (HA) configuration, where all gateways are active and handling requests.

Configuring Gateway Settings for the Cloud Extender

Follow these steps to configure gateway authentication, WebDAV, and intranet proxy settings for the Cloud Extender.

Configuring Access to the Secure Browser

Follow these steps to configure access in the MaaS360 Portal to the MaaS360 Secure Browser, where your users access intranet sites through the Mobile Enterprise Gateway (MEG).

Configuring Access to Secure Document for SharePoint and CMIS

Follow these steps to configure access in the MaaS360 Portal to MaaS360 Secure Document for SharePoint and CMIS.

Configuring Access to Secure Document for Windows File Share

Follow these steps to configure access in the MaaS360 Portal to MaaS360 Secure Document for Windows File Share.

Viewing Gateway Settings in the MaaS360 Portal

The Cloud Extender view in the MaaS360 Portal displays your gateway settings, including the online status of the gateway.

Enabling Health Check Alerts for Mobile Enterprise Gateway (MEG)

Follow these steps to enable health check alerts from the MaaS360 Portal for the Cloud Extender Mobile Enterprise Gateway (MEG) module.

Viewing All Gateways and Gateway Clusters in the MaaS360 Portal

The Mobile Enterprise Gateway (MEG) view in the MaaS360 Portal displays a consolidated view of your gateways and clusters, including configuration mode and node counts for each cluster.

Working With Active Gateway Sessions

Information about viewing or terminating active gateway sessions from the gateway monitoring console.

Configuring Mobile Apps Through the Enterprise Gateway

Follow these steps to configure your iOS or Android device through the enterprise gateway.

Using Cross-Forest and Cross-Domain Authentication for Mobile Enterprise Gateway (MEG)

Before users can access intranet resources, Mobile Enterprise Gateway (MEG) requires users to authenticate against corporate directory services. Mobile Enterprise Gateway (MEG) integrates with both Active Directory and LDAP servers for this type of user authentication.

Parent topic: Configuring Settings for the Cloud Extender Modules

13.5 Installing the Mobile Enterprise Gateway (MEG)

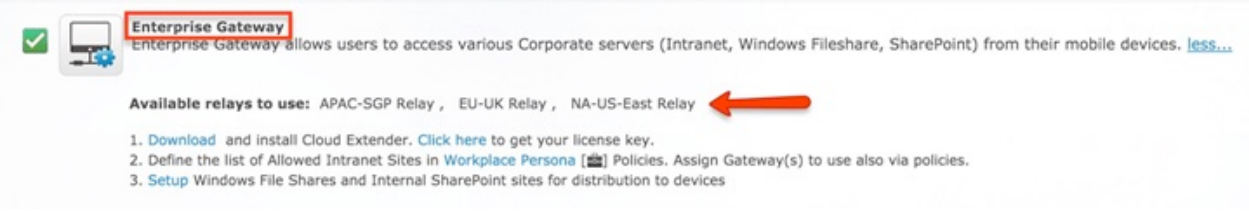
Follow these steps to install the Mobile Enterprise Gateway (MEG).

13.5.1 Before You Begin

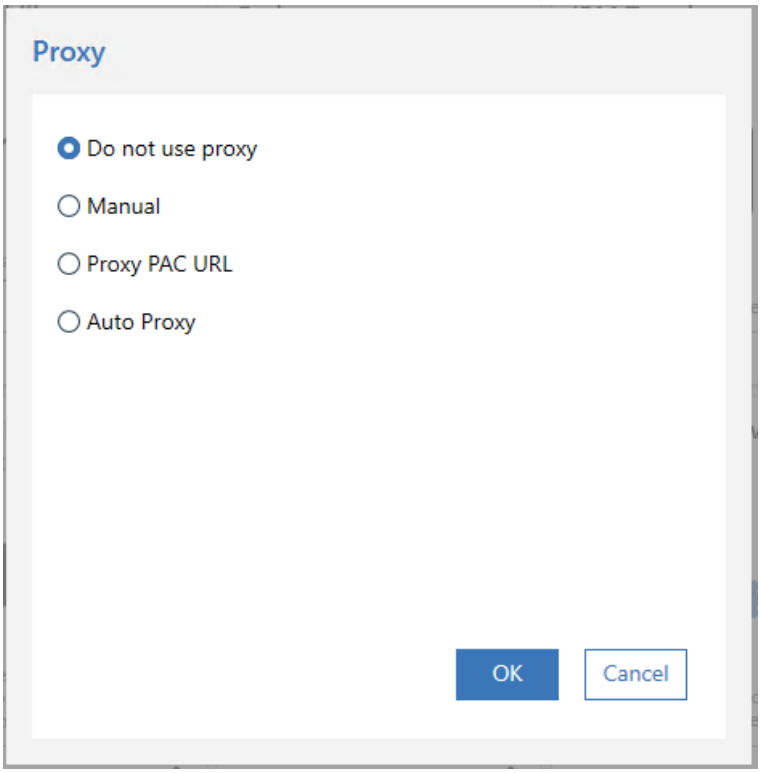
You must purchase the Enterprise Gateway feature separately from the Cloud Extender™ software. To purchase this feature, contact IBM® Support.

13.5.2 Procedure

1. Log in to the MaaS360® Portal and select **Setup** > **Services**. If the Enterprise Gateway feature is enabled, the Enterprise Gateway window displays a list of available relay servers (only for relay access mode). The servers on this list might be different depending on your account settings.
   Note: Contact IBM Support if the Enterprise Gateway feature is not enabled.



2. Download the Cloud Extender and obtain the license key.
3. Follow the steps in the installation wizard to install the Cloud Extender. When the installation is complete, the Cloud Extender Configuration Tool is displayed.
4. (Optional) If you use a proxy server for outbound access, configure proxy settings for the Cloud Extender. The Cloud Extender uses these settings to communicate with relay services and the MaaS360 backend services for overall configuration and management. From the Cloud Extender Configuration Tool, choose one of the following options:



Option	Description
Do not use proxy	If the Cloud Extender is not installed in a proxy environment, select this option to establish a direct connection between the Cloud Extender and the MaaS360 Cloud.
Manual	The static proxy address and the proxy port for your proxy server
Proxy PAC URL	The URL of the proxy PAC file that is hosted in your environment
Auto Proxy	Automatically searches for the Proxy PAC file from your DNS or DHCP server

5. From the Cloud Extender Configuration Tool, select the **Enterprise Gateway** file from the main screen.
   Note: After you install the Cloud Extender, the Mobile Enterprise Gateway (MEG) module might take a few minutes to download. If the

Enterprise Gateway option is not displayed in the Cloud Extender Configuration Tool window, close the Cloud Extender Configuration Tool, wait a few minutes, and then start the Cloud Extender Configuration Tool again.

13.5.3 What to Do Next

Configuring Mobile Enterprise Gateway (MEG) in Standalone Mode

Parent topic: Mobile Enterprise Gateway (MEG) Module

13.6 Configuring Mobile Enterprise Gateway (MEG) in Standalone Mode

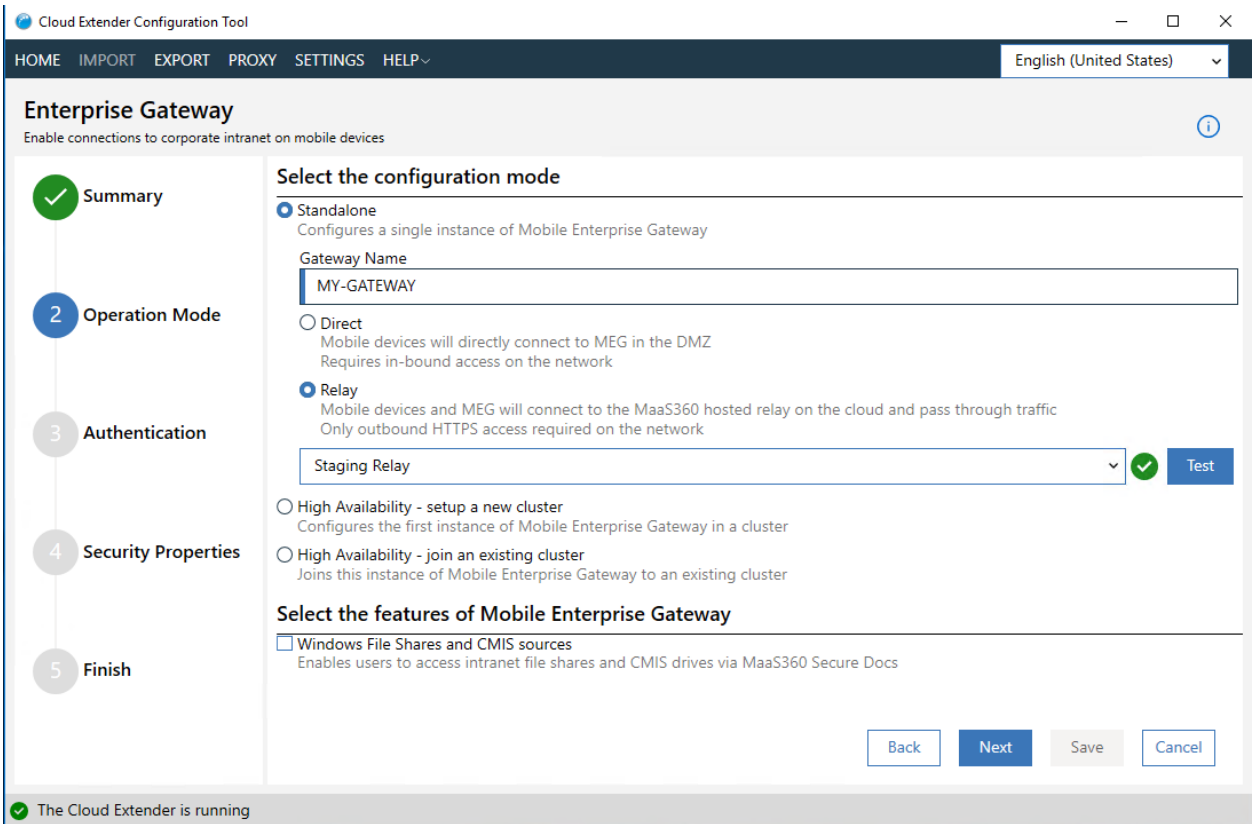
Follow these steps to configure your gateway in Standalone mode.

13.6.1 About This Task

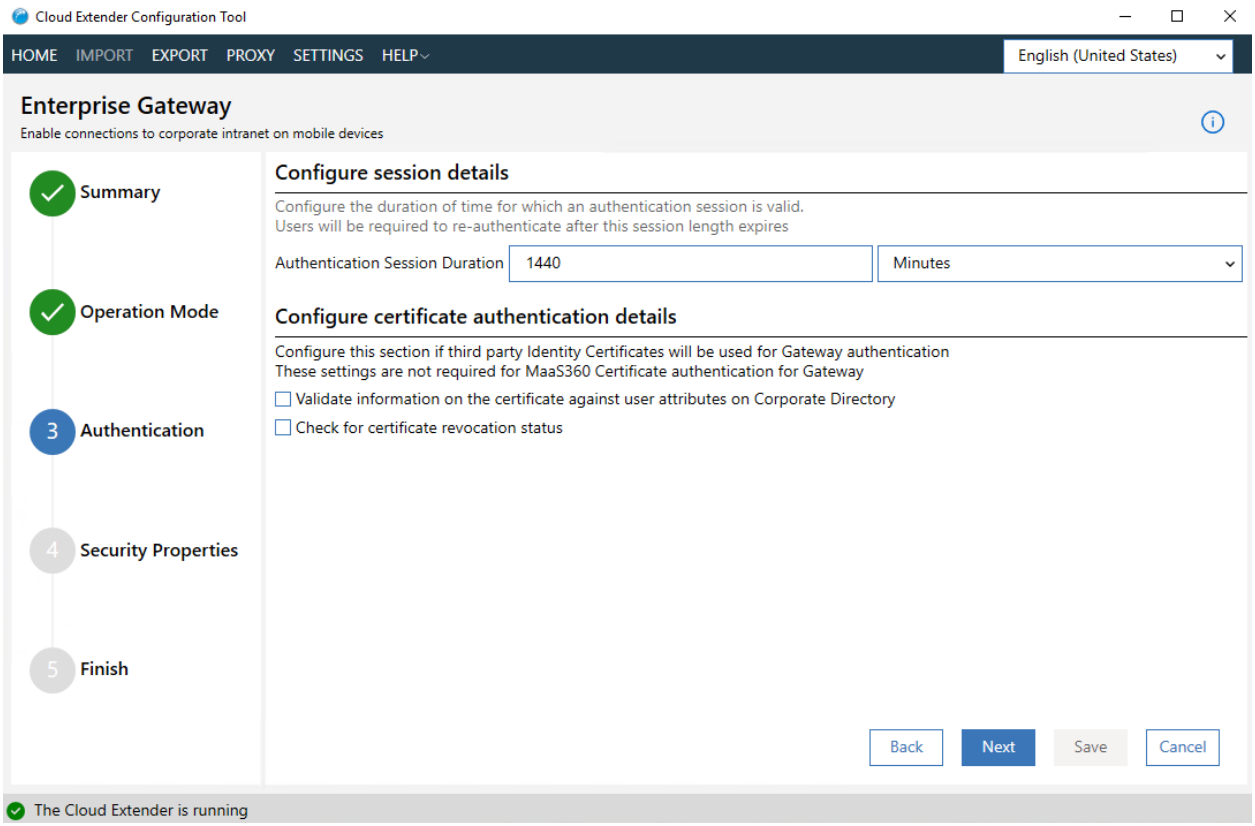
To set up your gateways in a High Availability (HA) cluster, go to Mobile Enterprise Gateway (MEG) in High Availability (HA) Mode. You cannot switch the gateway mode from Standalone to High Availability (HA) mode for a gateway that is already configured.

13.6.2 Procedure

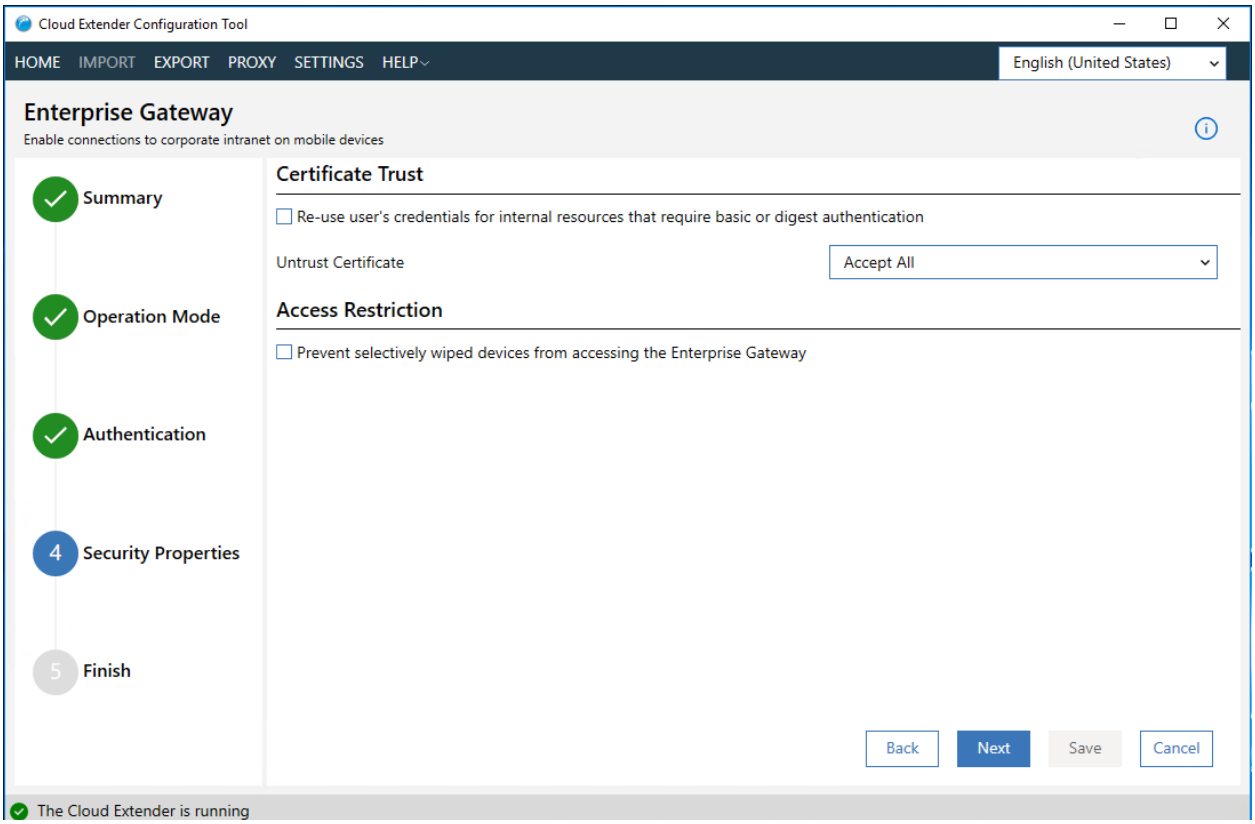
1. Click on the **Enterprise Gateway** tile of the Configuration Tool
2. Select the Standalone option
3. Enter a name for your gateway. This name is displayed in all MaaS360 Portal workflows.
4. Select the Relay option
5. Select the desired relay from the available options in the relay list
6. If this gateway will be part of a High Availability cluster, select whether this configuration will create the cluster or whether the cluster already exists and this gateway will join the cluster.
7. If you wish to enable file sharing in Enterprise Gateway, check the file sharing checkbox



8. Click the **Next** button
9. On the next screen, configure the settings according to your desired authentication policy (typically left as default values)



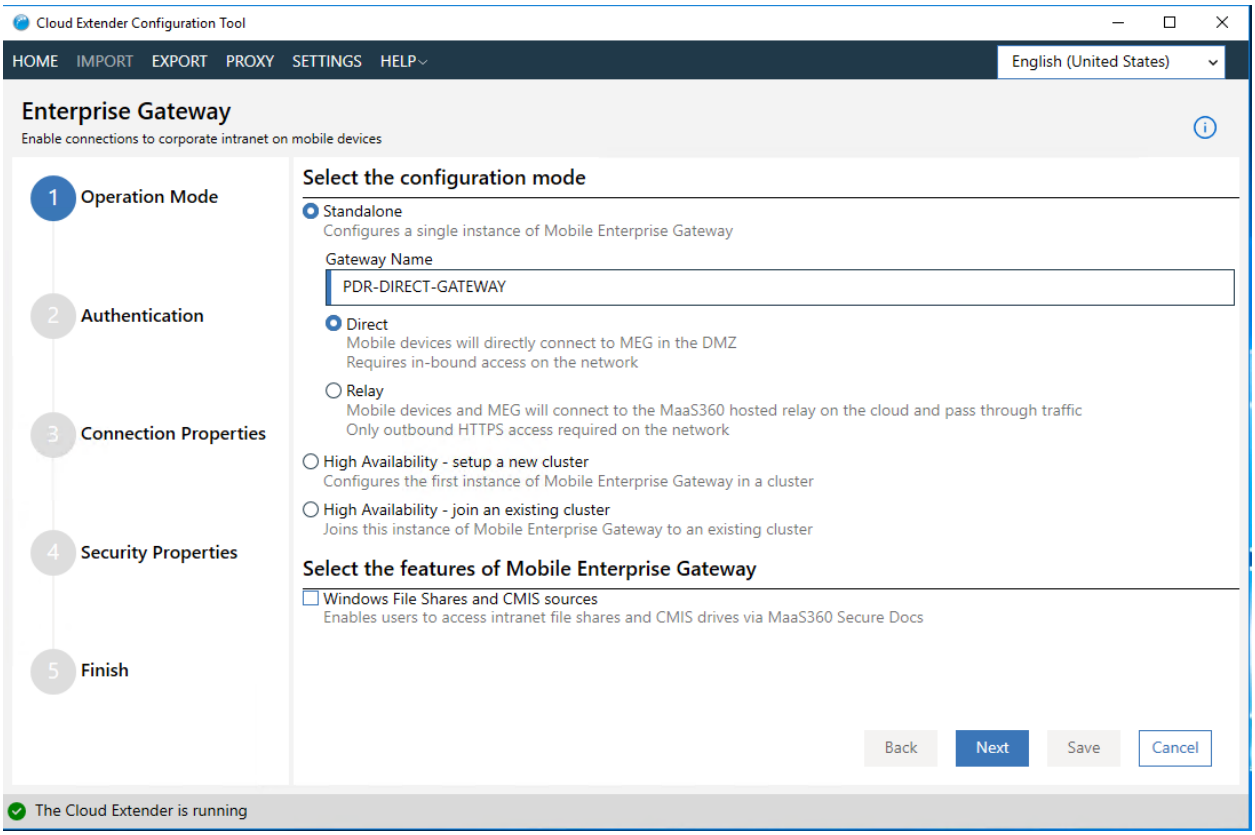
10. Click the **Next** button
11. On the next screen, configure Certificate Trust and Access policies according to your desired policy. If your intranet site uses a self-signed certificate, you will need to set the **Untrust Certificate** option to **Accept All**. When you enable this option, the untrusted certificate exception is ignored, and the request is served by the gateway. For security reasons, disable this option and install the site SSL certificates to the certificate store of the gateway server instead.



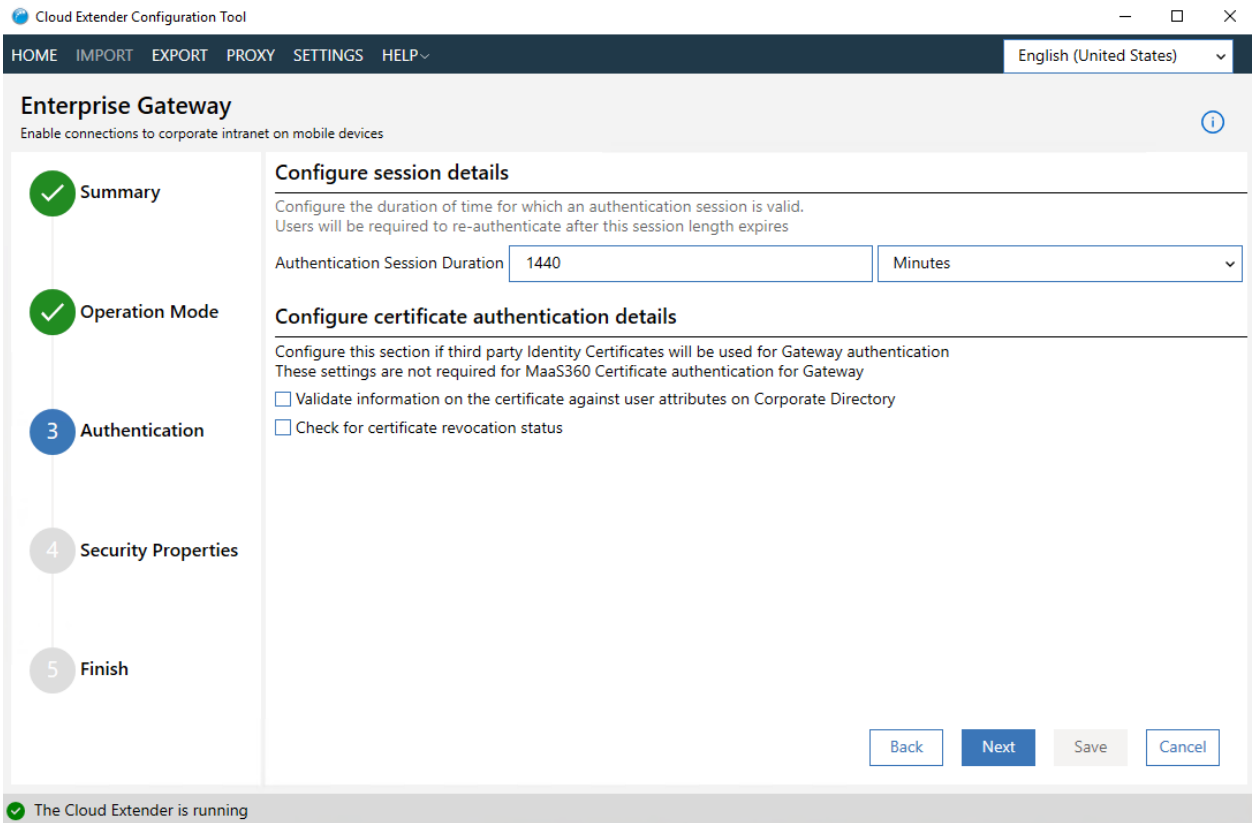
1. Click the **Next** button
2. Click the **Save Gateway Certificate** button to save the cluster certificate. Select an appropriate directory for saving the file as it will be needed for any future gateways that wish to join this cluster.
3. Click the **Save** button

To run Enterprise Gateway in Direct mode, configure these settings:

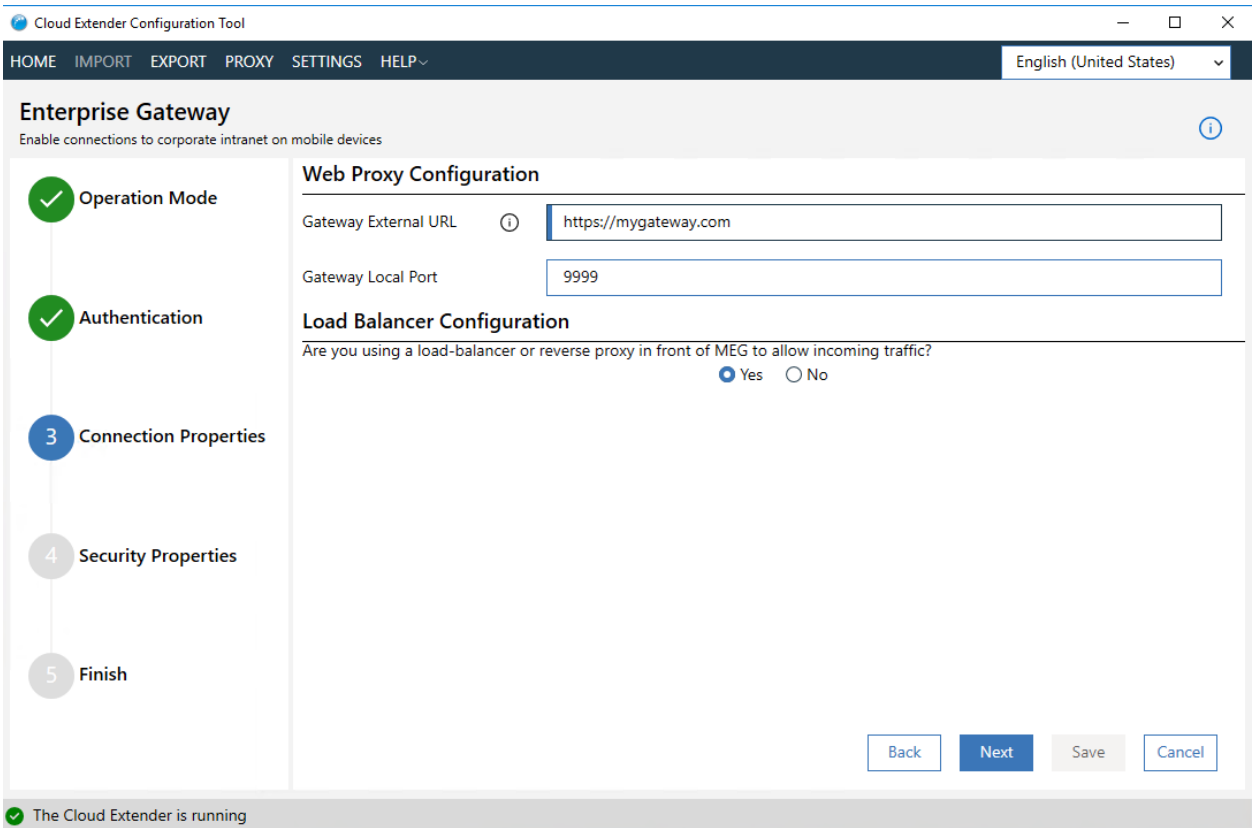
1. Click the **Enterprise Gateway** tile on the Configuration Tool
2. Select the **Standalone** option
3. Select the **Direct** option
4. Enter a name for your gateway. This name is displayed in all MaaS360 Portal workflows.



5. Click the **Next** button
6. On the next screen, configure the settings according to your desired authentication policy (typically left as default values)



7. In the **Gateway External URL** field, provide the gateway URL (or the external URL or host name of your load balancer) if you use a load balancer in front of the gateway. If you do not use a load balancer in front of the gateway, the gateway URL is the host name of this gateway server. This external URL includes the port, if this port is different from the standard ports for HTTP or HTTPS.
8. In the **Gateway Local Port** field, provide the port that runs the gateway server and listens for requests. If you use a load balancer, make sure that the load balancer redirects traffic to this gateway port. If you do not use a load balancer, the gateway port is any open port on this gateway server.
9. Specify whether you are using a load balancer in front of the Enterprise Gateway



10. Click the **Next** Button
11.
12. Select Yes or No for securing incoming traffic with SSL. This enables AES-256 end-to-end encryption to secure communication further between a mobile device and the gateway.
    Note: Using SSL encryption is optional. If you choose not to use SSL, the security of the Mobile Enterprise Gateway (MEG) is not compromised.

If you do not use a load balancer, a mobile device uses the SSL certificate that you enter in the **SSL Certificate** field to initiate an SSL session to the gateway.
If you use a load balancer, the load balancer uses the SSL certificate that you enter in the **SSL Certificate** field to initiate an SSL session to the gateway. The load balancer SSL certificate secures the traffic between a mobile device and your load balancer. For more information, see your load balancer documentation.

13. In the **SSL Certificate** field, provide the path to the SSL certificate (`PEM`) file. If you do not use a load balancer, SSL terminates on your gateway. In this case, you cannot use self-signed certificates. You must receive an SSL certificate from a public certificate authority (CA).
14. In the **SSL Certificate Private Key** field, provide the private key for the SSL certificate (`.key`) file.
15. If your intranet site uses a self-signed certificate, you will need to set the **Untrust Certificate** option to **Accept All**. When you enable this option, the untrusted certificate exception is ignored and the request is served by the gateway. For security reasons, disable this option and install the site SSL certificates to the certificate store of the gateway server instead.
16. Click the **Next** button
17. Click the **Save Gateway Certificate** button to save the cluster certificate. Select an appropriate directory for saving the file as it will be needed for any future gateways that wish to join this cluster.
18. Click the **Save** button

For procedures on how to set up a high availability database, see Setting Up a Shared Database for High Availability (HA).

13.6.3 What to Do Next

Configuring Gateway Settings for the Cloud Extender

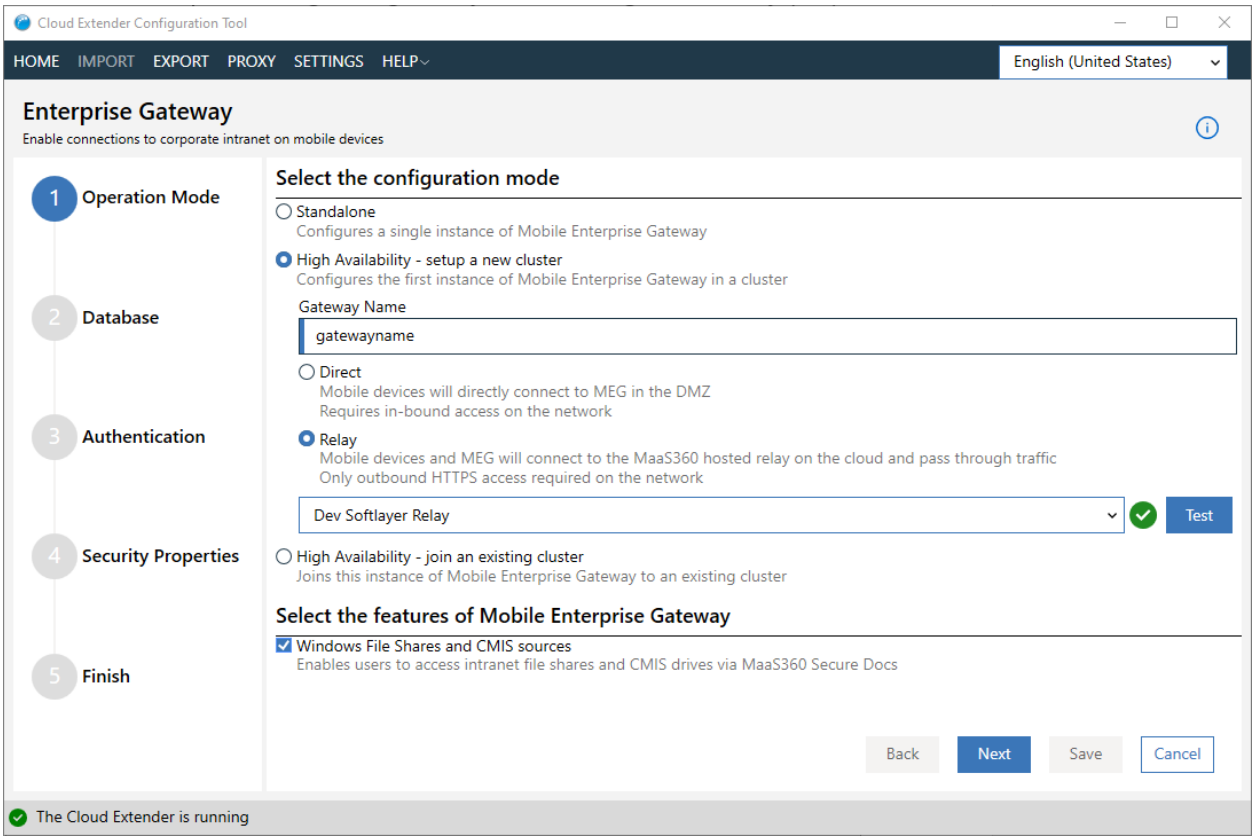
Parent topic: Mobile Enterprise Gateway (MEG) Module

13.7 Configuring Mobile Enterprise Gateway (MEG) in High Availability (HA) Mode

Follow these steps to configure a gateway cluster in High Availability (HA) mode.

13.7.1 **Procedure**

1. Run the Cloud Extender Configuration Tool and click the Enterprise Gateway tile
2. Select the configuration mode

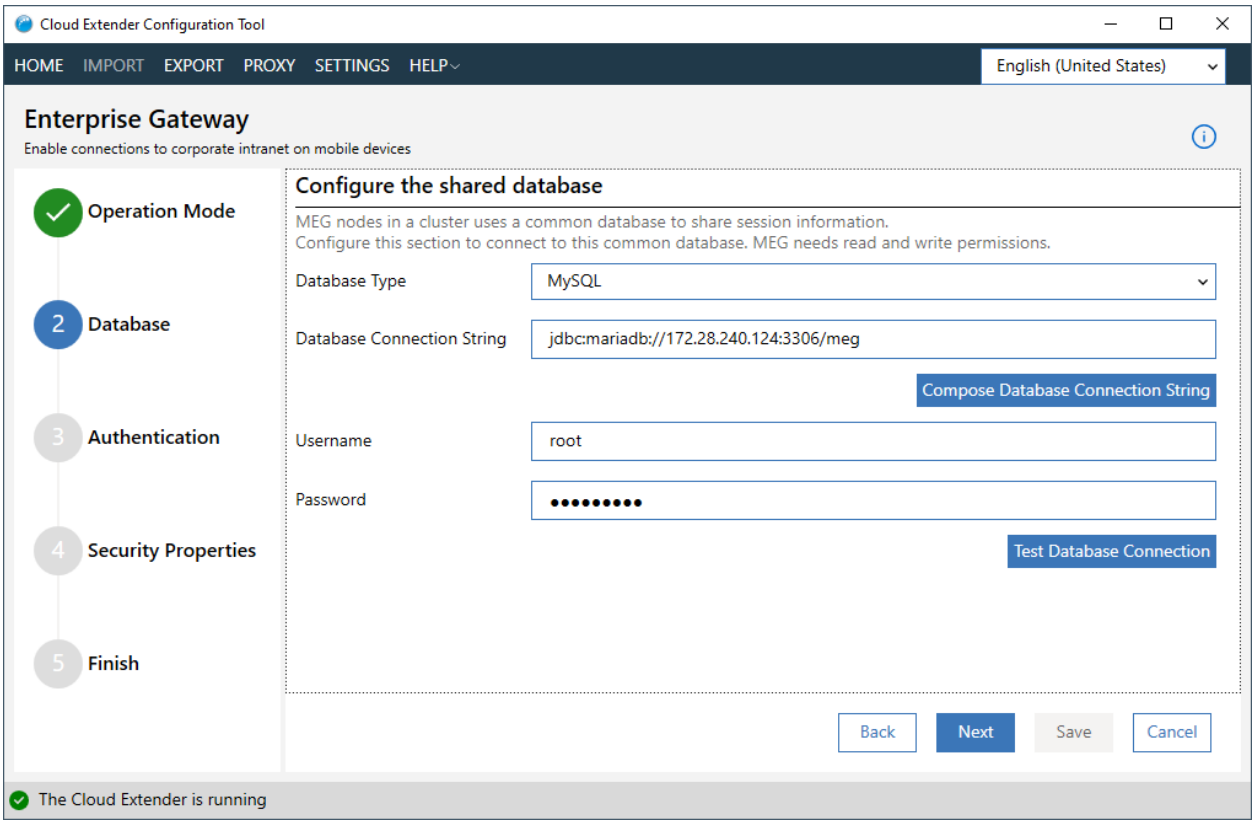


   a. Choose the **High Availability – setup a new cluster**
   b. Check the **Windows File Share and CMIS sources** if you want to use WebDAV
   c. Click the **Next** button

3. Configure the High Availability shared database

Option	Description
MySQL	`jdbca:mariadb://`*{HOST}:{PORT}/{DB_NAME}*
Microsoft SQL Server	For Active Directory: `jdbc:sqlserver://`*{IP_ADDR}:{PORT};databaseName={DB_NAME}* For LDAP:
DB2	`jdbc:db2://`*{HOST}:{PORT}/{DB_NAME}*

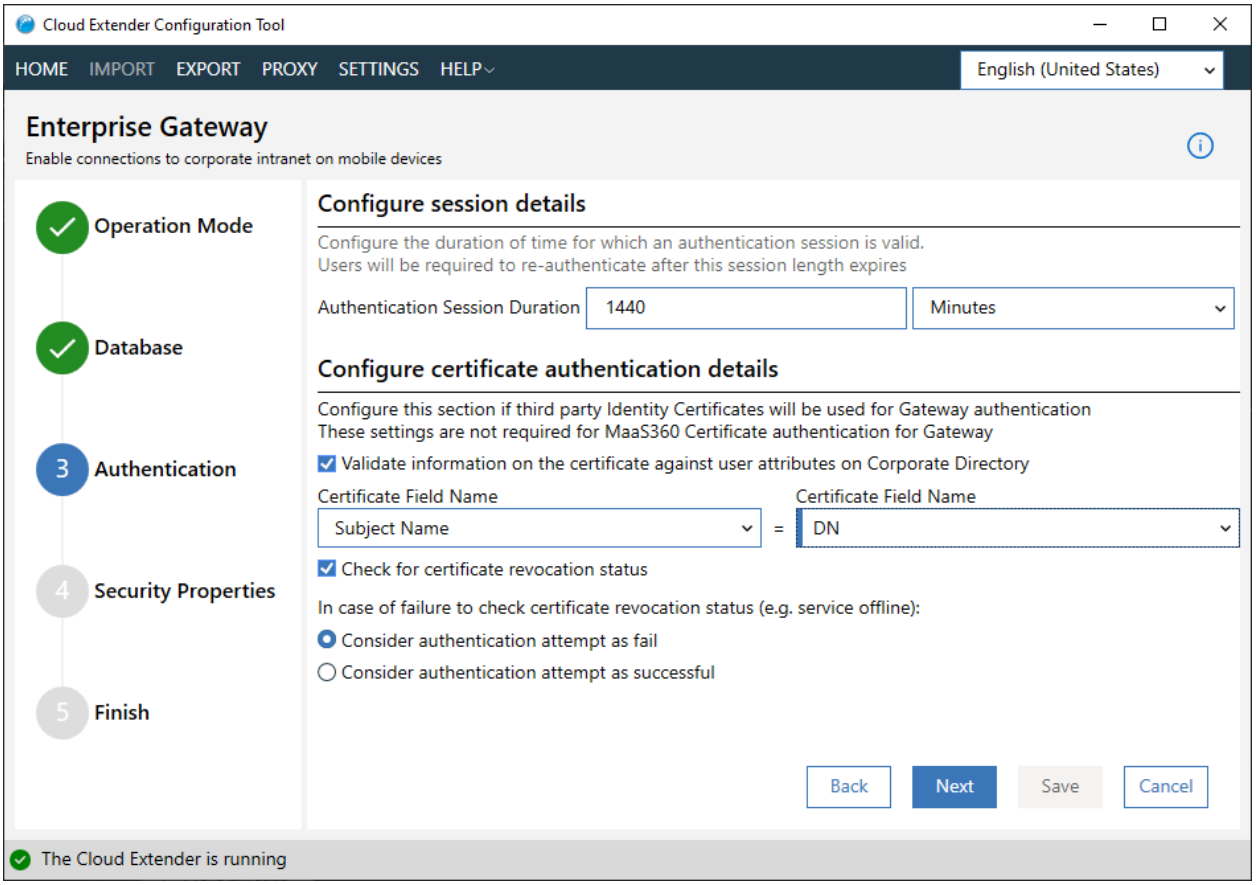
Note: Replace the *{HOST}*, *{IP_ADDR}*, *{PORT}*, and *{DB_NAME}* with actual values from your database requirements



a. Select database type from the **Database Type** field MySQL/MSSQL/DB2
b. Enter the connection string in **Database Connection String** field
   NOTE: For simple connection string, you can use the **Compose Database Connection String** button to help you.

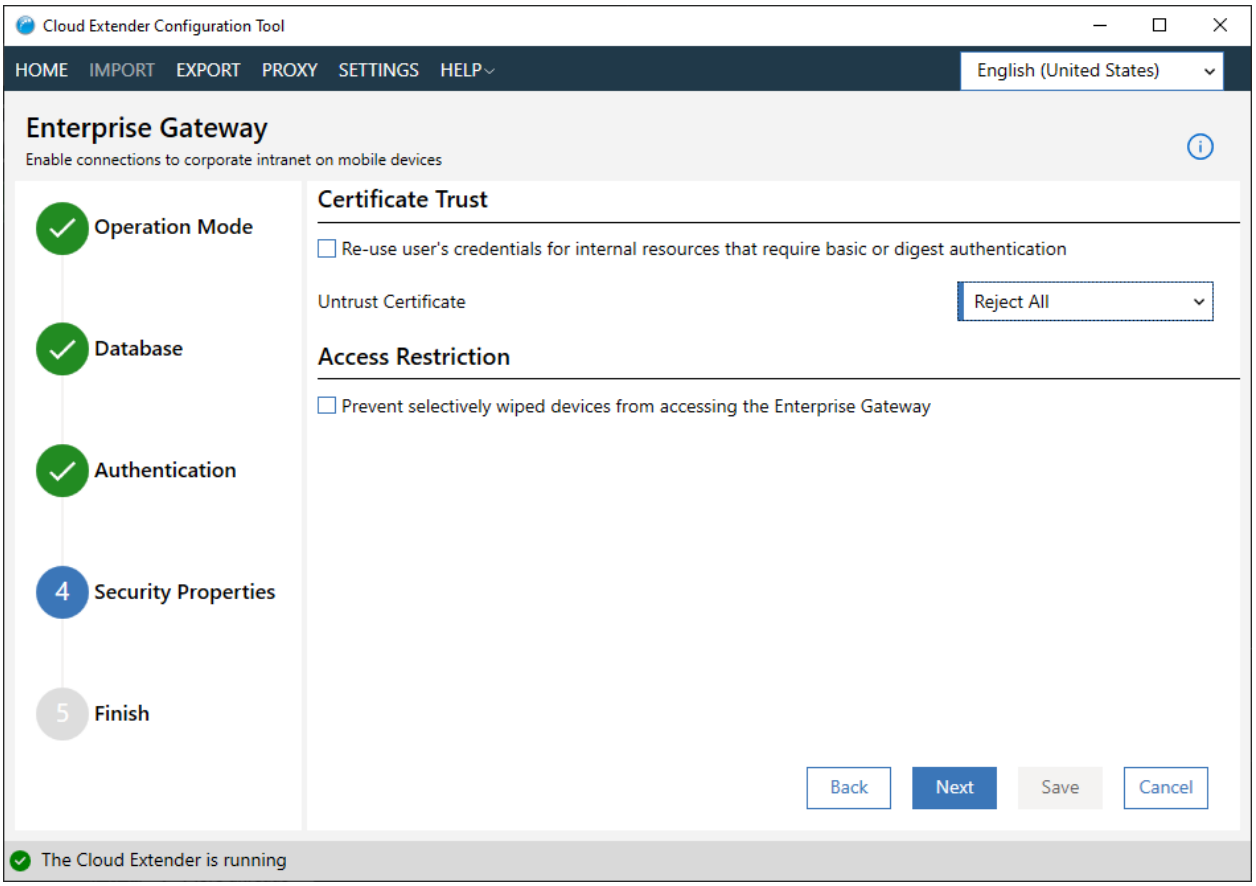
c. Type in database username and password
d. For Microsoft SQL Server in Active Directory authentication mode only (not available in LDAP): Select the **Use Service Account** checkbox so that gateway will use Service Account to access Database
e. Click **Test Database Connection** to verify.
f. Click the **Next** button

4. Configure session details



a. Enter the authentication session duration and duration units
b. If you are not using certificate authentication, you don't need to check "**Validate information on the certificate against user attributes on Corporate Directory**" and "**Check for certificate revocation status**"
c. Click the **Next** button

5. Configure Certificate Trust settings



a. **Re-use user's credentials for intranet resources that require Basic or Digest authentication**: Enable this option under the following circumstances:
   i. If an internal site challenges for Basic or Digest access authentication, the gateway provides the user credentials that it received during gateway authentication and passes it back to the site, seamlessly signing the user on to the site. If authentication fails, the challenge for credentials is sent back to the user on the MaaS360 app. When the user provides credentials, a new authentication is attempted. However, a failed authentication attempt occurs for the user before the user can authenticate. If you disable this option, all Basic or Digest access authentication challenges are propagated back to the user to enter manually.

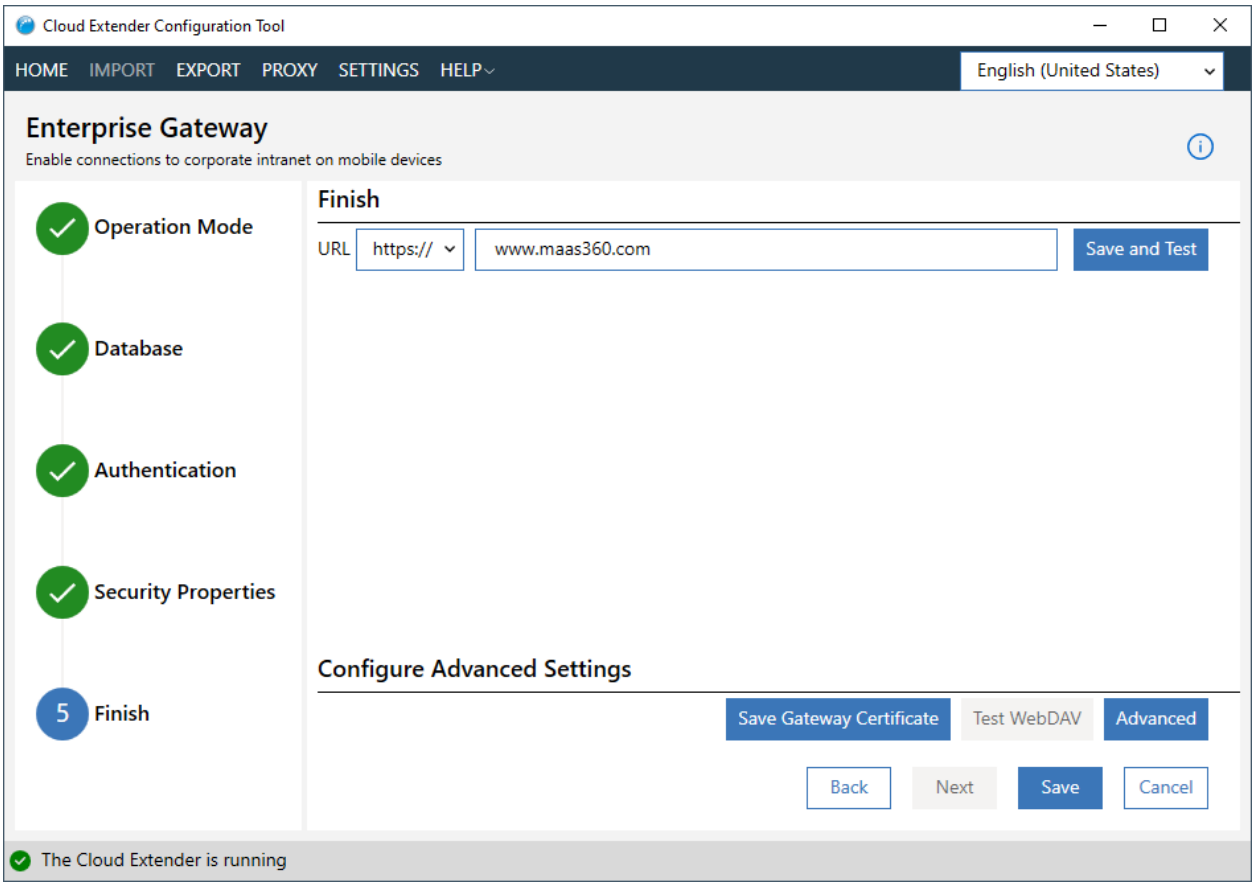
b. Select how to handle **Untrusted Certificates**
   For example, if your intranet site uses a self-signed certificate,

then access to this site produces a certificate exception. When you enable this option, the exception is ignored, and the request is served by the gateway. For security reasons, disable this option and install the site SSL certificates to the certificate store of the gateway server instead.

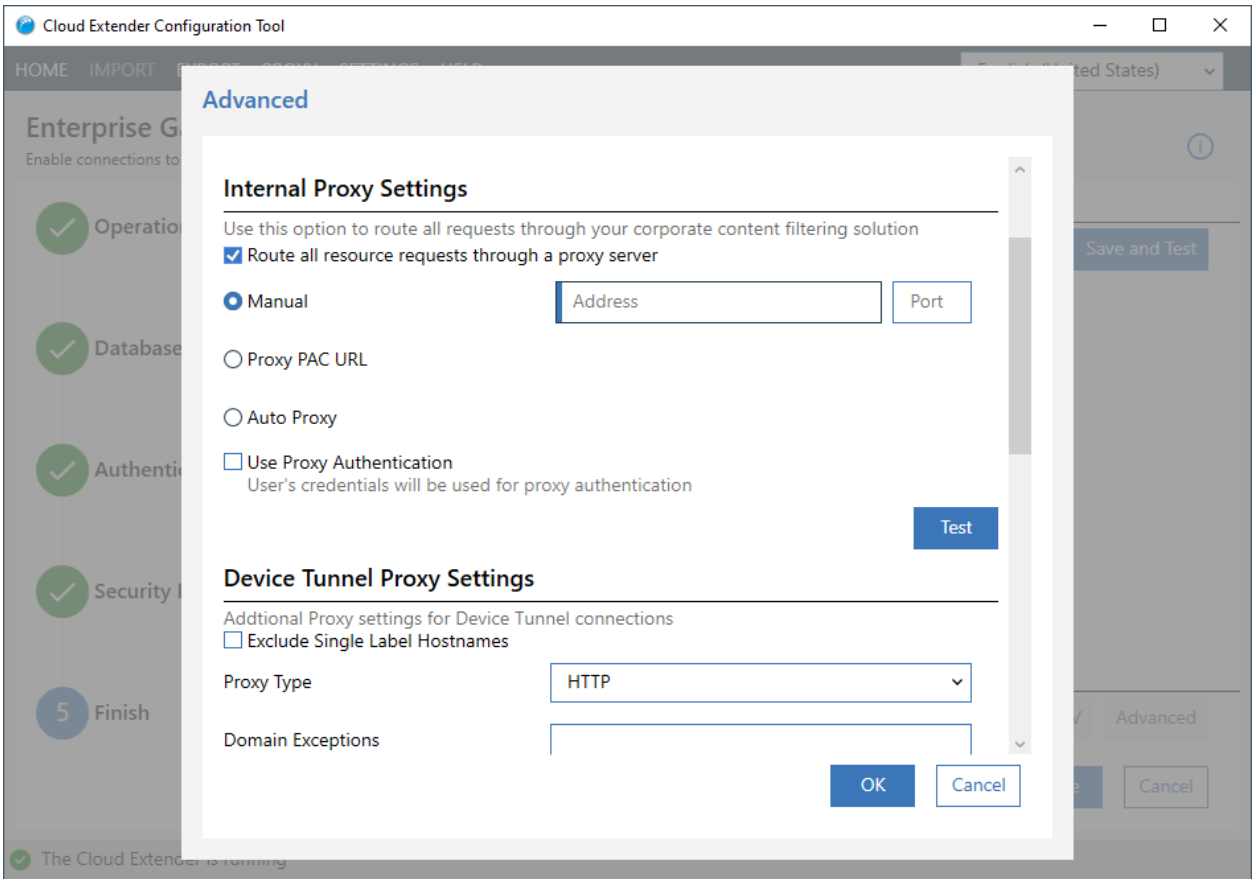
i. **Reject All**: Configures the gateway to reject all untrusted certificates. The user cannot access a website with an untrusted certificate.
ii. **Accept All**: Configures the gateway to accept all untrusted certificates. The user cannot prevent access to a website with an untrusted certificate.
iii. **Prompt**: The user decides whether to access a website with an untrusted certificate. If you select the **Prompt** option and the user accesses a website from the MaaS360 Secure Mobile Browser through Mobile Enterprise Gateway (MEG) that uses an invalid SSL certificate, the user receives a prompt on how the browser handles the exception. The user can either accept the exception and continue to the website or the user can reject the exception and cancel navigation to the website.

c. Click the **Next** button

6. Test and Save Configuration



a. If you don't have an internal proxy, click **Save** to save the configuration.
b. It would ask you to save the gateway certificate, which can be used on another Cloud Extender™ to join HA cluster.
c. The gateway should be up and running in a few minutes.



a. Click **Advanced** button on Finish step
b. Enter internal proxy settings. You can choose **Manual**, **Proxy Pac**, or **Auto Proxy**

   Manual: Enter the hostname (IP) and port of the proxy server.
   Proxy Pac: The URL to the PAC file that is hosted in your environment.
   Auto Proxy: The PAC file is typically hosted in your DHCP or DNS server as a Web Proxy Auto-Discovery Protocol (WPAD) file.

   Proxy authentication uses the user's AD/LDAP authentication.
c. **Device Tunneling** and **DNS** settings are for new Gateway. It won't show up if you are not in beta.

13.7.2 Results

The gateway cluster is now set up. The gateway generates an encrypted identity certificate for the cluster configuration and prompts you to save the certificate.

13.7.3 What to Do Next

Joining a Gateway to an Existing High Availability (HA) Cluster

Parent topic: Mobile Enterprise Gateway (MEG) in High Availability (HA) Mode

13.8 Joining a Gateway to an Existing High Availability (HA) Cluster

Follow these steps to add a gateway to an existing High Availability (HA) cluster.

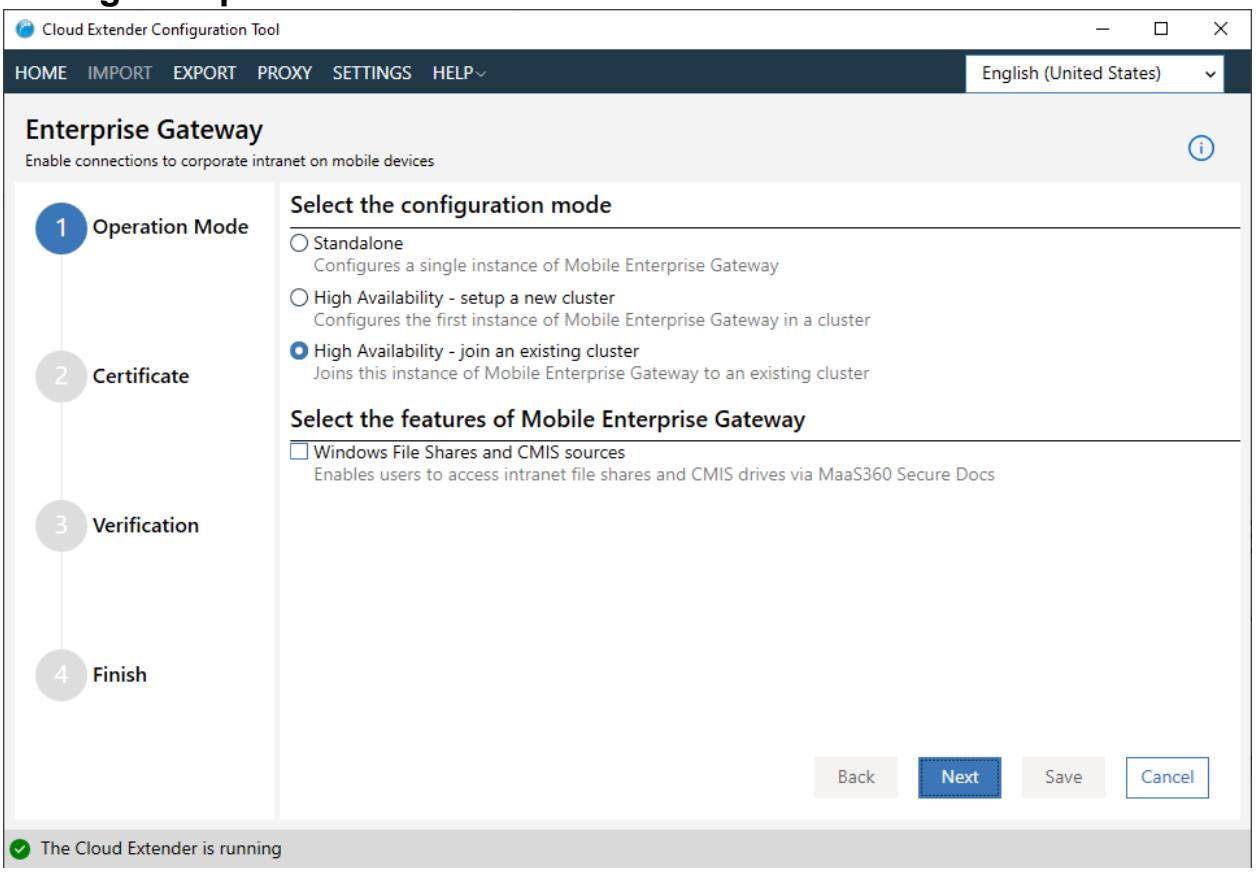
13.8.1 Before You Begin

You must use the encrypted identity certificate that was generated by the gateway for cluster configuration before you can join new gateways to a High Availability (HA) cluster. If you cannot locate this certificate, follow these steps to download the certificate again from your first gateway:

1. Open Cloud Extender™ Configuration Tool, Navigate to **Finish** step click **Save Gateway Certificate**.
2. In the **Configuration Mode** section, select **High Availability - Join an existing Gateway cluster**.
3. Browse to the location of the gateway certificate. All settings are automatically downloaded to the new gateway node.

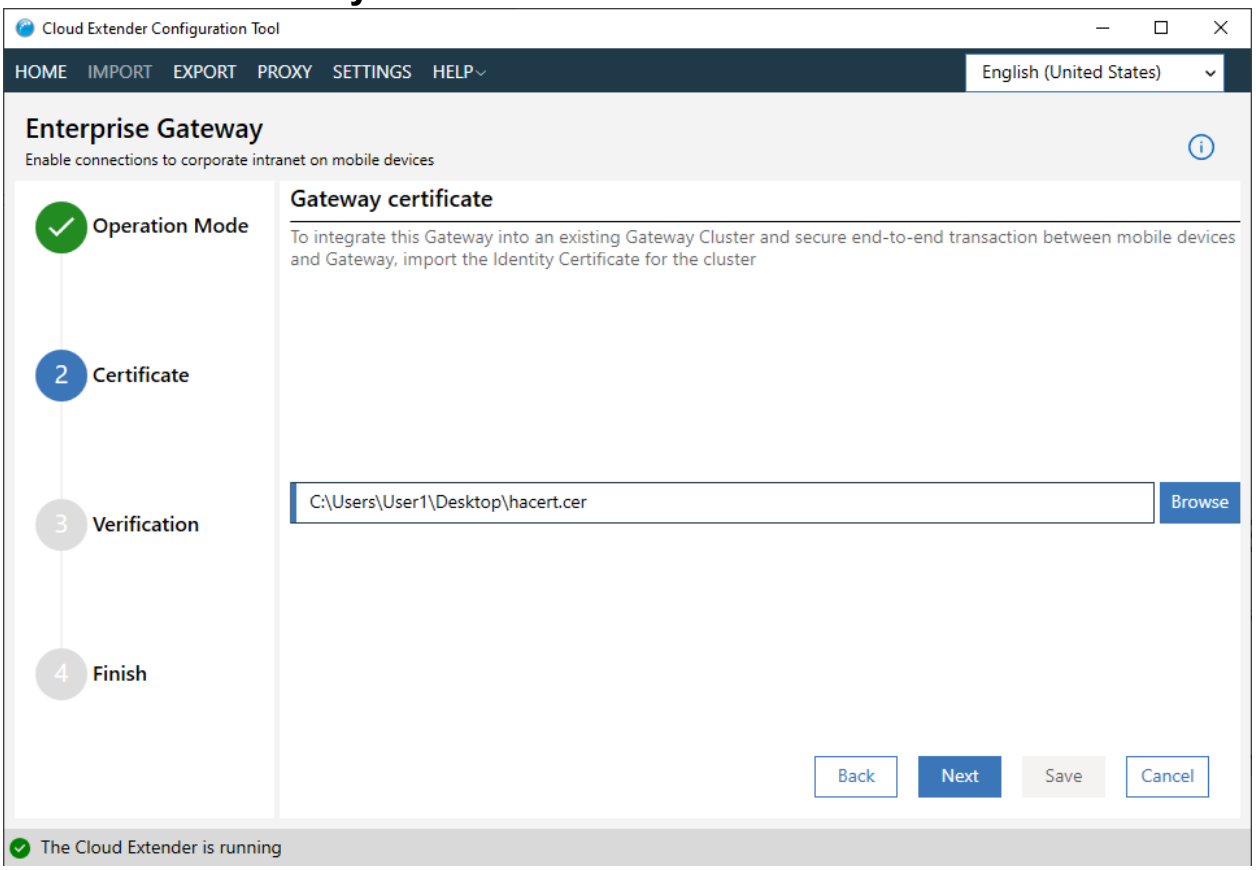
13.8.2 Procedure

1. **Configure Operation Mode**



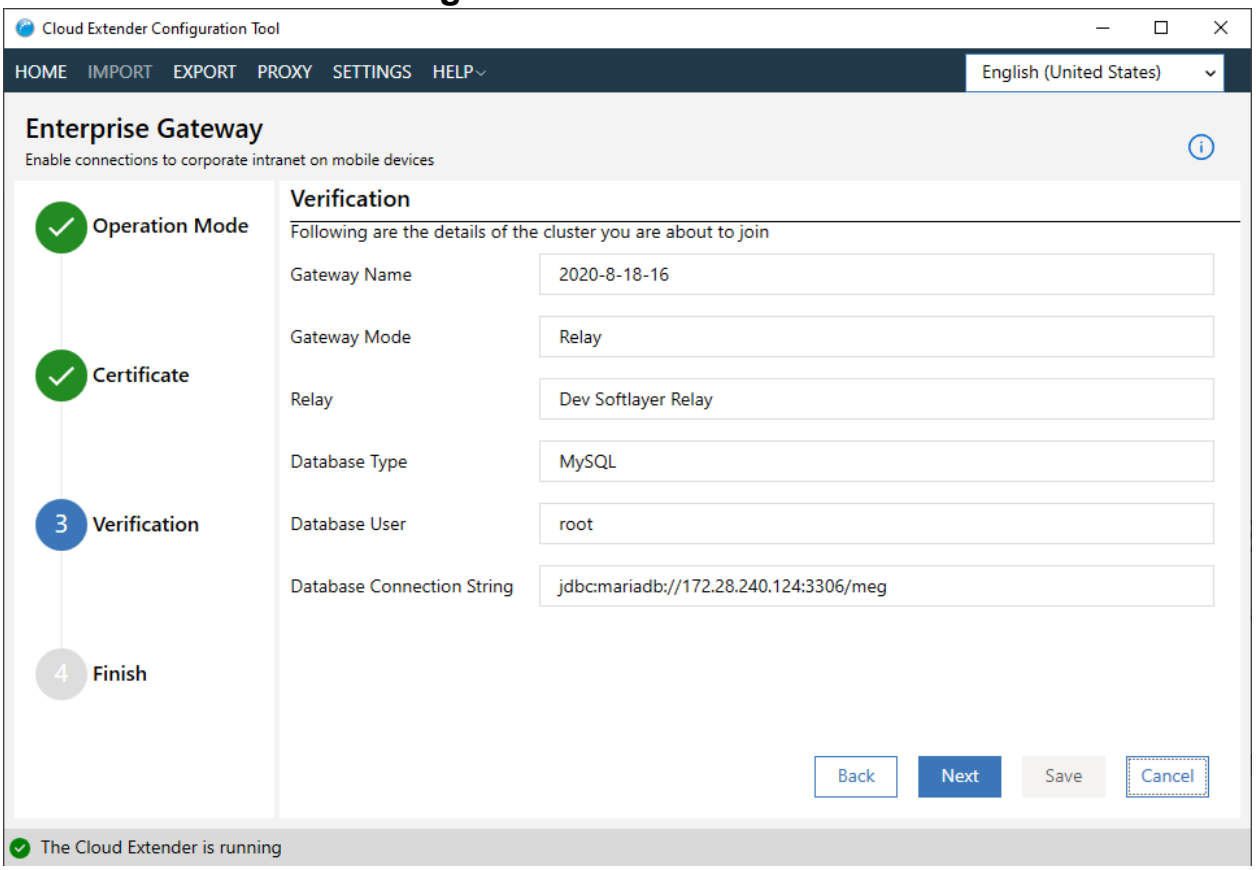
   a. Select High Availability – join an existing cluster
   b. Click the **Next** button

2. Provide the Gateway Certificate



a. Click the **Browse** button to select the gateway certificate that is saved from HA master node
b. Click the **Next** button

3. **Review Certificate Settings**



   a. Check if all settings are correct
   b. If you are using direct mode with the SSL, it would ask for SSL cert and private key.
   c. If you are using Service Account for MSSQL database, it would ask for Service Account credentials.
   d. Click the **Next** button

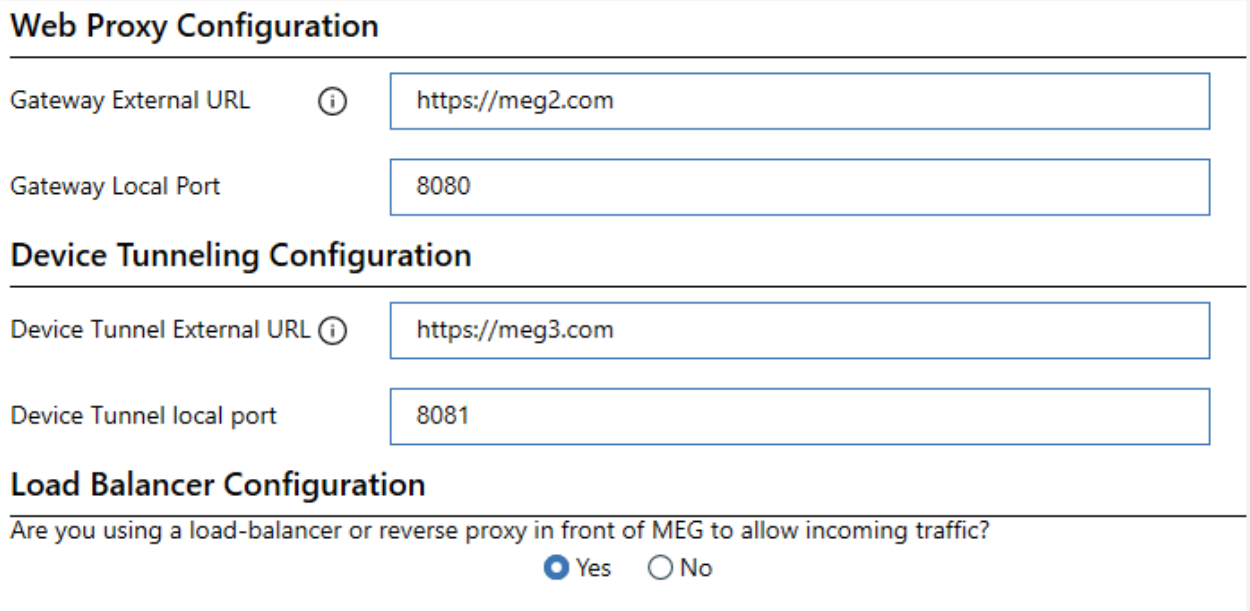
4. **Finish**
   Same as Setting up new High Availability Mode.
   Click the **Save** button to finish joining

Parent topic: [Mobile Enterprise Gateway (MEG) in High Availability (HA) Mode]

13.9 Configuring Mobile Enterprise Gateway (MEG) in Direct Mode

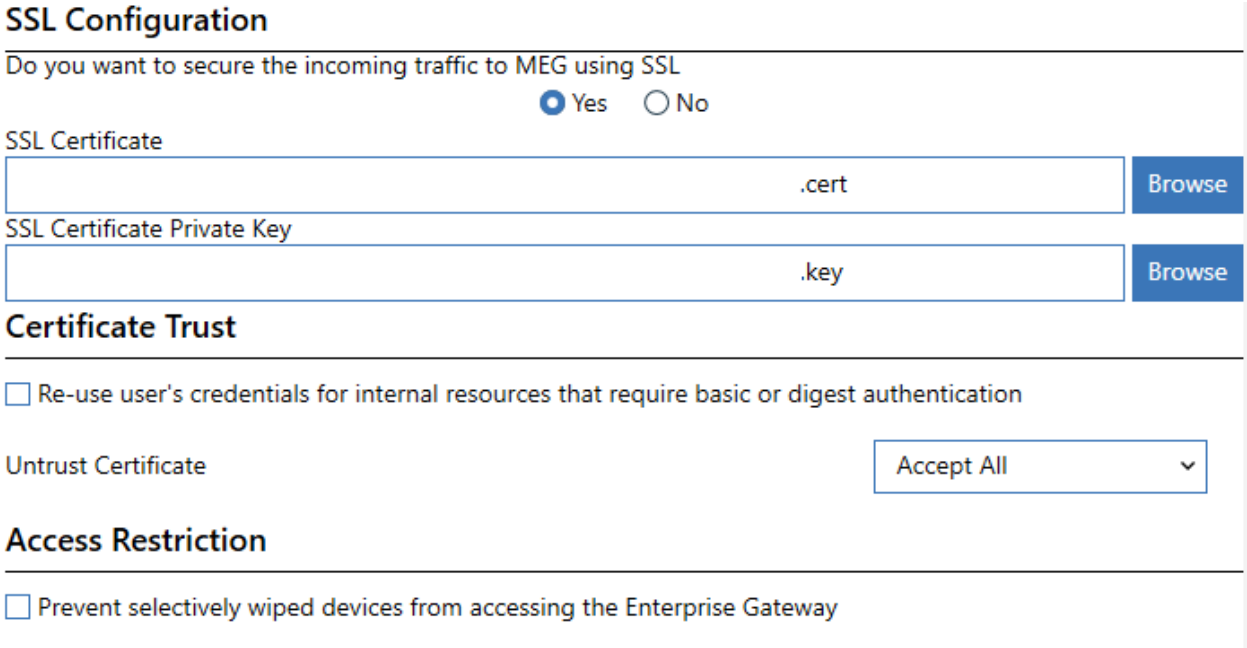
When you select Direct Mode in Standalone or High Availability, Cloud Extender™ Configuration Tool requires you to provide networking information.

1. In **Connection Properties** step



   a. Web Proxy Configuration is for MEG 2.0, which operates on HTTP layer
   b. Device Tunneling Configuration is for MEG 3.0, which operates on TCP layer, this configuration is invisible if MEG 3.0 is not enabled
   c. Enter URL and port.
   d. If you have a load balancer in front of the MEG, select **Yes.**
   e. Click **Next**

2. **Security Properties**
   You can encrypt your direct traffic by enabling SSL encryption. But if you have a load-balancer with SSL in front of MEG, this is not recommended since it would slow down the performance.



   a. Select **Yes**
   b. Provide cert and key. This cert must be trusted on the device.
   c. Click **Next**

13.10 Configuring Access to the Secure Browser

Follow these steps to configure access in the MaaS360® Portal to the MaaS360 Secure Browser, where your users access intranet sites through the Mobile Enterprise Gateway (MEG).

13.10.1 About This Task

Configure WorkPlace Persona policies in the MaaS360 Portal to set up Secure Browser access to intranet sites.

13.10.2 Procedure

1. From the MaaS360 Portal, open the WorkPlace Persona policy.
2. Select **MaaS360 Gateway Settings**, and configure the following policy settings:

Option	Description
Allowing Caching of Corporate Credentials in the App	Enable this setting to save user credentials in the encrypted database for the Secure Browser app and protected overall by container security. The browser reauthenticates against the gateway with these credentials, but does not prompt the user to reenter credentials each time. Users are prompted for credentials only when their passwords change and the

	browser fails to authenticate against the gateway.
Identity Certificate	Select the **Identity Certificate Template** (from your Cloud Extender™ Certificate Integration setup). This identity certificate is used by the gateway to authenticate against upstream intranet sites that challenge for identity certificate credentials for authentication.
Enable Corporate Network Detection to skip use of Enterprise Gateway	Enable this setting to allow browser traffic for intranet sites to skip the gateway route when the specified corporate network server is resolved by the browser.
Configure Corporate Network Detection	Enable this setting to require sites that use identity certificate-based authentication stop working. Site authentication does not work because the gateway presents the identity certificate to intranet sites that challenge for the same, but for the corporate network, the gateway route is bypassed.

3. Select **Browser**, and then select **MaaS360 Enterprise Gateway** to configure the following settings:

Option	Description
Default Enterprise Gateway	Select one of the gateways or gateway clusters that you set up. The name of the gateway displays automatically in the list. If you do not configure regional gateways, all devices that are associated with this policy communicate with the default gateway.
Configure Regional Gateways	Enable this setting to route devices to regional gateways or gateway clusters based on the location of the device. Specifies the country and the regional gateway that the devices in that country communicate with. The location (country) of the device is determined by the time zone setting on the device and the GPS location of the device. Use this setting to manage one Persona policy for all devices, but still maintain awareness of the location of all devices around the globe.
Access List for Intranet Resources	Specifies the domains or IP addresses for intranet sites that are allowed by devices that connect to the gateway. This setting allows wildcards for domains such as `*.companydomain.com` (regular expressions). Restrict this access list to only intranet sites and domains, not proxy traffic to public sites.
Exceptions	Use an exception list, if you set your access list to `*.companydomain.com`, but you do not want to proxy traffic such as email messages or OWA from the

	gateway. Add the domain name of the mail server (`email.companydomain.com`) to the exception so traffic connects directly to your server on the internet and does not use the gateway.

Parent topic: [Mobile Enterprise Gateway (MEG) Module]

13.11 Configuring Access to Secure Document for SharePoint and CMIS

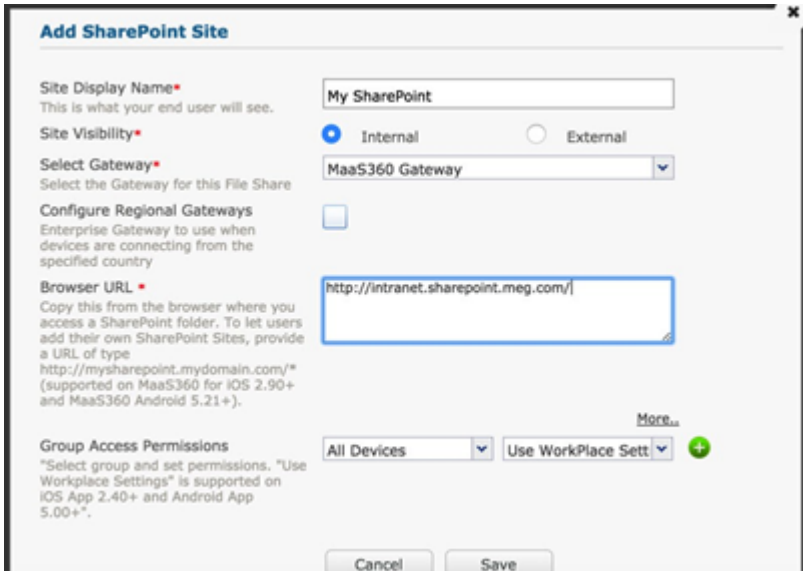
Follow these steps to configure access in the MaaS360® Portal to MaaS360 Secure Document for SharePoint and CMIS.

13.11.1 About This Task

Secure Document for SharePoint and CMIS provides your users with access to SharePoint and CMIS repositories and the capability to view all files in Document view from their mobile devices.

13.11.2 Procedure

1. From the MaaS360 Portal Home page, select **Docs** > **Content Sources**.
2. Click **Add New Source** > **SharePoint Site**. The Add SharePoint Site window is displayed:



3. Provide the following settings:

Option	Description

Site Display Name	Specifies the name of the SharePoint site display to users on their mobile devices.
Site Visibility	Specifies whether to route traffic through the Gateway (internal) or whether Gateway access is not required because the SharePoint site is publicly hosted (external).
Select Gateway	Specifies the gateway or gateway cluster that connects to the SharePoint site and whether you want the site accessible from your corporate intranet. **Note:** This gateway is either your corporate gateway or the MaaS360 Mobile Enterprise Gateway (MEG).
Configure Regional Gateway	Routes devices to regional gateways or gateway clusters based on the location of the device. Specifies the country and the regional gateway that the devices in that country communicate with. The location (country) of the device is determined by the time zone setting on the device and the GPS location of the device. Use this setting to manage one distribution for all devices, but still maintain awareness of the location of all devices around the globe.
Browser URL	Specifies the URL that displays the SharePoint site name.
Group Access Permissions	Distributes the SharePoint site to target devices along with access permissions associated with the distribution.

Parent topic: [Mobile Enterprise Gateway (MEG) Module]

13.12 Configuring Access to Secure Document for Windows File Share

Follow these steps to configure access in the MaaS360® Portal to MaaS360 Secure Document for Windows File Share.

13.12.1 About This Task

Secure Document for Windows File Share provides your users with access to Windows File Shares and the capability to view all files in Document view from their mobile devices.

13.12.2 Procedure

1. From the MaaS360 Portal Home page, select **Docs** > **Content Sources**.
2. Click **Add New Source** > **Windows File Share**. The Add Windows File Share window is displayed.
3. Provide the following settings:

Option	Description
Display Name	Specifies the name of the Windows File Share that is display to user on their mobile devices.
Gateway Type	Specifies the type of gateway that connects to the Windows File Share: **Legacy**: Use your existing gateway **MaaS360 Enterprise Gateway**: Use the MaaS360 Mobile Enterprise Gateway (MEG)
Select Gateway	Specifies the gateway or gateway cluster that connects to the network file share and whether you want the share accessible from your corporate intranet.

	Note: This gateway is either your corporate gateway or the MaaS360 Mobile Enterprise Gateway (MEG).
Configure Regional Gateways	Routes devices to regional gateways or gateway clusters based on the location of the device. Specifies the country and the regional gateway that the devices in that country communicate with. The location (country) of the device is determined by the time zone setting on the device and the GPS location of the device. Use this setting to manage one distribution for all devices, but still maintain awareness of the location of all devices around the globe.
Folder Path	Specifies the UNC path to folder that is shared: `\\server\share\file_path` You must enable WebDAV on your gateways. If the folder names are the same as MaaS360 user names, use the *%username%* variable to distribute user-specific file shares.
Group Access Permissions	Distributes file shares to target devices along with access permissions associated with the distribution.

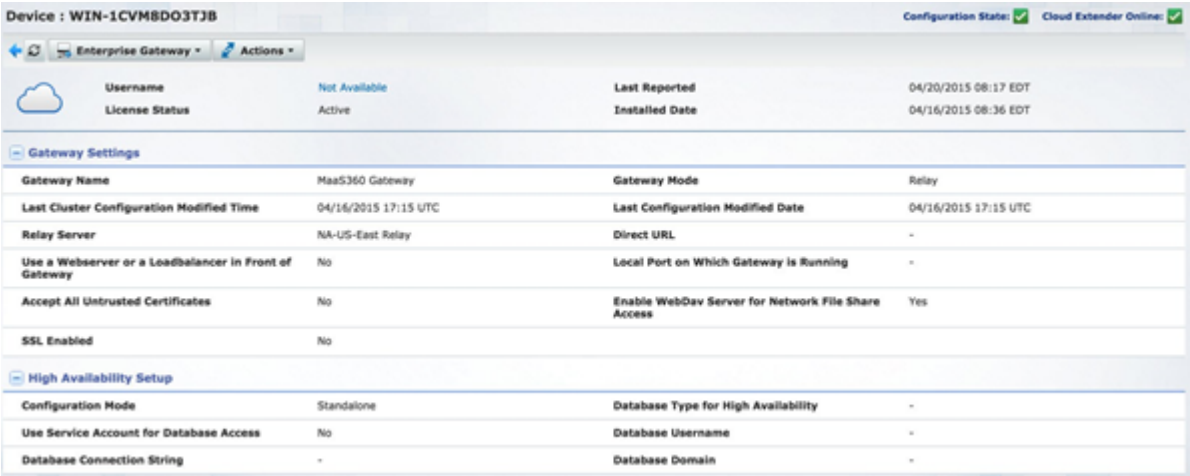
Parent topic: **Mobile Enterprise Gateway (MEG) Module**

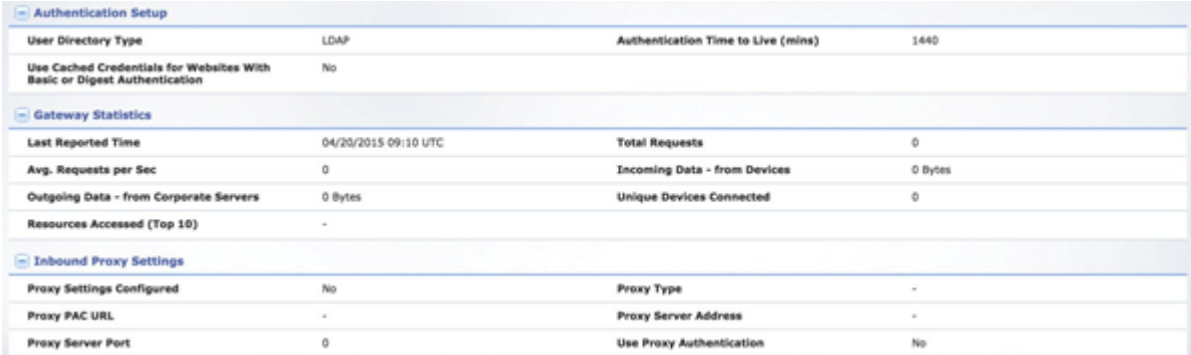
13.13 Viewing Gateway Settings in the MaaS360 Portal

The Cloud Extender™ view in the MaaS360® Portal displays your gateway settings, including the online status of the gateway.

13.13.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender**.
2. Choose your gateway server and select **Summary** > **Enterprise Gateway**. The Cloud Extender Summary page is displayed. This page displays the following settings:
    a. Gateway settings that include name, mode, relay server details, WebDAV server details, and related settings.
    b. High Availability details that include mode, database type, and service accounts.
    c. Authentication mode that includes Active Directory or LDAP and associated authentication settings.
    d. Gateway statistics
    e. Internal Proxy details (if configured)





Authentication Setup			
User Directory Type	LDAP	Authentication Time to Live (mins)	1440
Use Cached Credentials for Websites With Basic or Digest Authentication	No		
Gateway Statistics			
Last Reported Time	04/20/2015 09:10 UTC	Total Requests	0
Avg. Requests per Sec	0	Incoming Data - from Devices	0 Bytes
Outgoing Data - from Corporate Servers	0 Bytes	Unique Devices Connected	0
Resources Accessed (Top 10)	-		
Inbound Proxy Settings			
Proxy Settings Configured	No	Proxy Type	-
Proxy PAC URL	-	Proxy Server Address	-
Proxy Server Port	0	Use Proxy Authentication	No

3. Click **Actions** > **Test Reachability (Enterprise Gateway)** to test reachability to intranet sites. The Test Reachability window is displayed:

4. Enter the host name and the intranet site to confirm reachability to the intranet

Note: The MaaS360 Portal sends the test to the gateway but does not traverse through the relays. You cannot use this test to test accessibility through the relay.

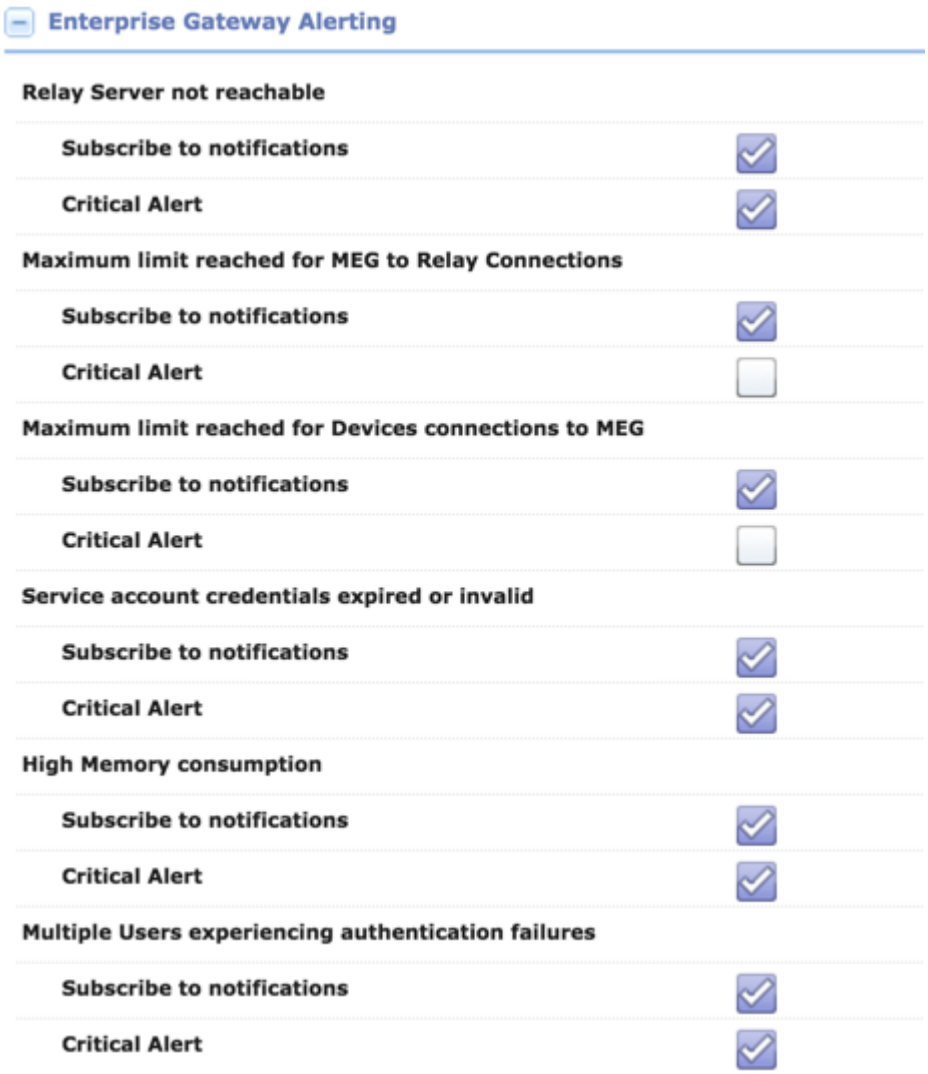
Parent topic: [Mobile Enterprise Gateway (MEG) Module]

13.14 Enabling Health Check Alerts for Mobile Enterprise Gateway (MEG)

Follow these steps to enable health check alerts from the MaaS360® Portal for the Cloud Extender™ Mobile Enterprise Gateway (MEG) module.

13.14.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**
2. Select **Health Check Configuration** > **Enterprise Gateway**. The Enterprise Gateway Alerting list is displayed:



3. From the list, enable the alerts that apply to your environment. If you set an alert subscription to **Critical Only**, the Cloud Extender sends an email message or a text message to the administrator for all alerts that are marked as **Critical**. The following table provides a description of each alert and the steps you take to remediate the alert:

Alert Name	Alert Description	Remediation Steps
Relay Server Not Reachable	The Cloud Extender triggers an alert when the MaaS360 relay server is not reachable by Mobile Enterprise Gateway (MEG). This alert might be triggered due to the following issues: Recent changes to firewall rules that block outbound communication from the Mobile Enterprise Gateway (MEG) to the relay server. The proxy between the Mobile Enterprise Gateway (MEG) to the relay server is down. A failure in the handshake between the Mobile Enterprise Gateway (MEG) and the relay server.	This alert is remediated when the Mobile Enterprise Gateway (MEG) reestablishes a connection with the assigned relay server.
Maximum Limit Reached for MEG to Relay Connections	The Cloud Extender triggers an alert when the number of relay connections that are in use from the Mobile Enterprise Gateway	This alert is remediated when the number of relay connections falls below the lower bound threshold, which is set

	(MEG) exceeds 90% of the predefined maximum threshold. Configure the upper bound and lower bound in the Mobile Enterprise Gateway (MEG) properties: The default minimum number of connections from the Mobile Enterprise Gateway (MEG) to the relay is 18. The default maximum number of connections from the Mobile Enterprise Gateway (MEG) to the relay is dynamically calculated by the Mobile Enterprise Gateway (MEG), or approximately 5% of the total device connections. For example, if 1,000 devices connect to the Mobile Enterprise Gateway (MEG), the Mobile Enterprise Gateway (MEG) determines that the maximum number of connections, or the maximum threshold, is around 50. If the Mobile Enterprise Gateway (MEG) uses 45 out of the 50	to 80% of the predefined maximum threshold. From the example, if the Mobile Enterprise Gateway (MEG) uses less than 40 out of the 50 connections, it is using less than 80% of the predefined maximum threshold, which remediates the alert.

	connections, the Mobile Enterprise Gateway (MEG) must reach the 90% mark to trigger an alert.	
Maximum Limit Reached for Device Connections to MEG	The Cloud Extender triggers an alert when the number of device connections to the gateway exceeds 90% of the predefined threshold. The predefined threshold is set to 10,000 connections. Configure this setting in the Mobile Enterprise Gateway (MEG) properties to trigger an alert. This setting applies to the Direct Mode of operation for the Mobile Enterprise Gateway (MEG). This alert indicates that the Mobile Enterprise Gateway (MEG) might need to be scaled up to meet volume requests from devices.	This alert is remediated when the number of connected devices falls below the 80% mark of the predefined threshold.
Service Account Credentials Expired or Invalid	The Cloud Extender triggers an alert when the service account is invalid during a Mobile Enterprise Gateway (MEG) authentication request (the LDAP	This alert is remediated when the service account becomes valid during the next Mobile Enterprise Gateway (MEG) authentication.

	binding account is expired, disabled, or invalid).	
High Memory Consumption	The Cloud Extender triggers an alert when the Mobile Enterprise Gateway (MEG) application memory heap usage exceeds 95% of the predefined threshold of the available memory. The default maximum heap size is 2 GB, but you can increase this size in the Mobile Enterprise Gateway (MEG) properties. Increasing the heap size to greater than 95% of 2 GB triggers an alert.	The alert is remediated when the memory heap usage falls below 90% of the predefined threshold (2 GB).
Multiple Users Experiencing Authentication Failures	The Cloud Extender triggers an alert when 10 unique users failed to authenticate with the Mobile Enterprise Gateway (MEG). For example, if a user tries to authenticate 10 times and fails to authenticate, but other users successfully authenticate, the Cloud Extender does not trigger an alert because the issue is not system wide.	This alert is remediated when a user logs in successfully. The authentication failure counter is then set back to 0.

	This authentication failure might be caused by user error or a locked user account. If 10 authentication requests fail in succession from distinct users, the Cloud Extender triggers an alert to indicate a potential problem with the Mobile Enterprise Gateway (MEG) authentication.	

4. Publish the Cloud Extender settings to activate the alerts.

Parent topic: [Mobile Enterprise Gateway (MEG) Module]

13.15 Viewing All Gateways and Gateway Clusters in the MaaS360 Portal

The Mobile Enterprise Gateway (MEG) view in the MaaS360® Portal displays a consolidated view of your gateways and clusters, including configuration mode and node counts for each cluster.

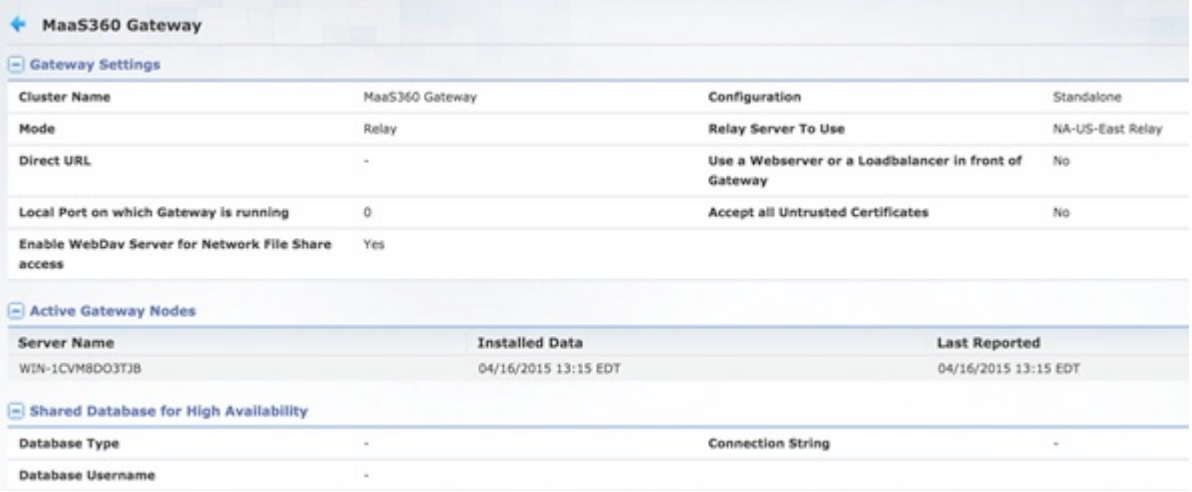
13.15.1 Procedure

1. From the MaaS360 Portal Home page, select **Setup** > **Mobile Enterprise Gateway**
2. A summary of all settings from a cluster point of view and details of all the active nodes is displayed:

Mobile Enterprise Gateway

Cluster Name	Mode	Configuration	Node Count	Installation Date	Last Modified D...
MaaS360 Gateway View	RELAY	Standalone	1	04/16/2015 13:15 EDT	04/16/2015 13:15 EDT

Consolidated view:



MaaS360 Gateway

Gateway Settings

Cluster Name	MaaS360 Gateway	Configuration	Standalone
Mode	Relay	Relay Server To Use	NA-US-East Relay
Direct URL	-	Use a Webserver or a Loadbalancer in front of Gateway	No
Local Port on which Gateway is running	0	Accept all Untrusted Certificates	No
Enable WebDav Server for Network File Share access	Yes		

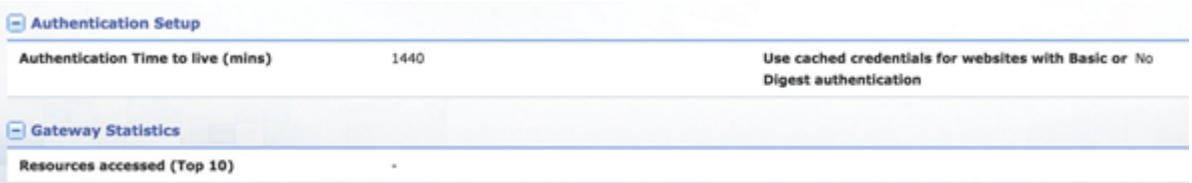
Active Gateway Nodes

Server Name	Installed Data	Last Reported
WIN-1CVM8DO3TJB	04/16/2015 13:15 EDT	04/16/2015 13:15 EDT

Shared Database for High Availability

Database Type	-	Connection String	-
Database Username	-		

Detailed view:



Authentication Setup

Authentication Time to live (mins)	1440	Use cached credentials for websites with Basic or Digest authentication	No

Gateway Statistics

Resources accessed (Top 10)	-

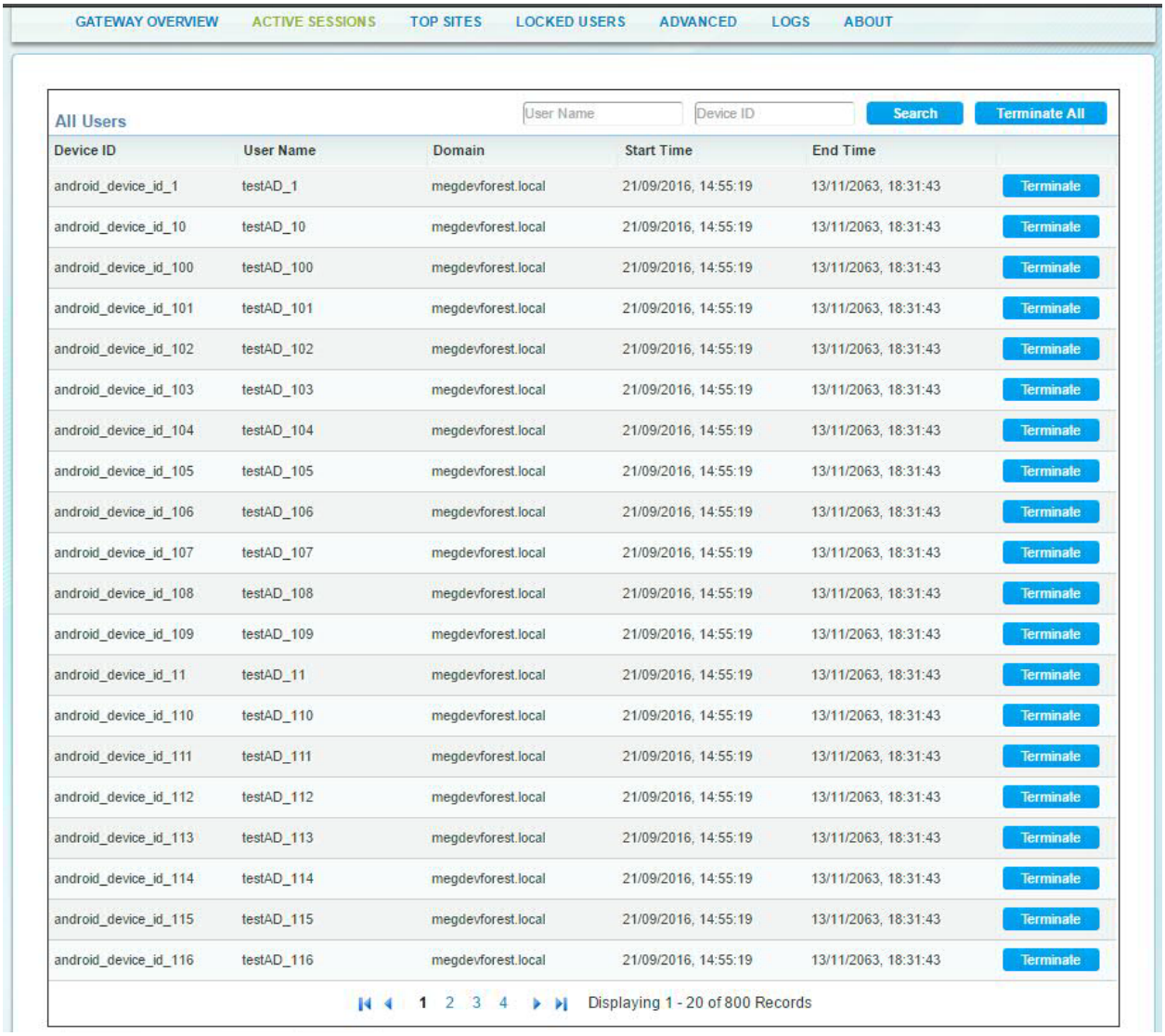
Parent topic: Mobile Enterprise Gateway (MEG) Module

13.16 Working with Active Gateway Sessions

Information about viewing or terminating active gateway sessions from the gateway monitoring console.

13.16.1 Viewing Active Gateway Sessions in the Gateway Monitoring Console

In the 2.89 release, the administrator can now view all active sessions in the gateway monitoring console (**Cloud Extender™ Configuration Tool** > **Monitor**). The number of sessions that is displayed per page in the gateway monitoring console increased from 10 sessions to 20 sessions:

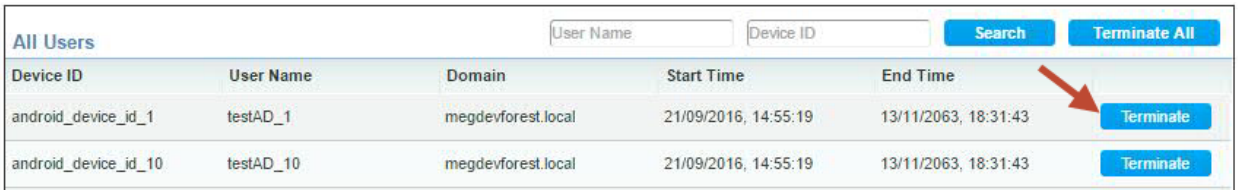


13.16.2 Terminating Active Gateway Sessions in the Gateway Monitoring Console

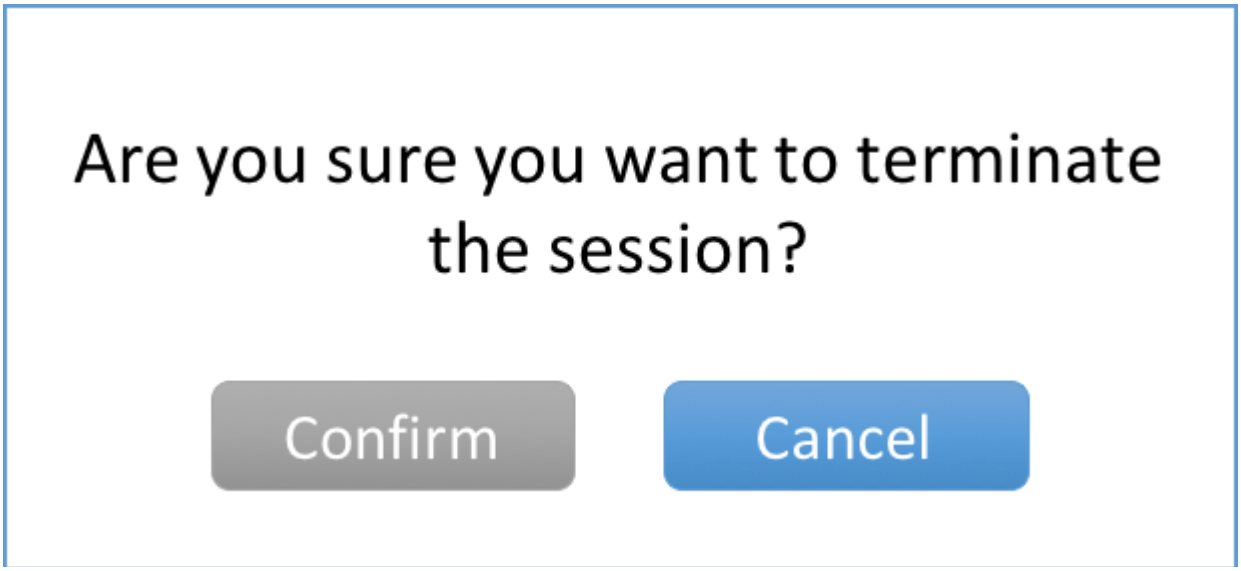
In the 2.89 release, the Mobile Enterprise Gateway (MEG) module provides administrators an action in the gateway monitoring console to terminate any active session.

To terminate one active session, follow these steps:

1. Click **Terminate** next to the active session that you want to stop.

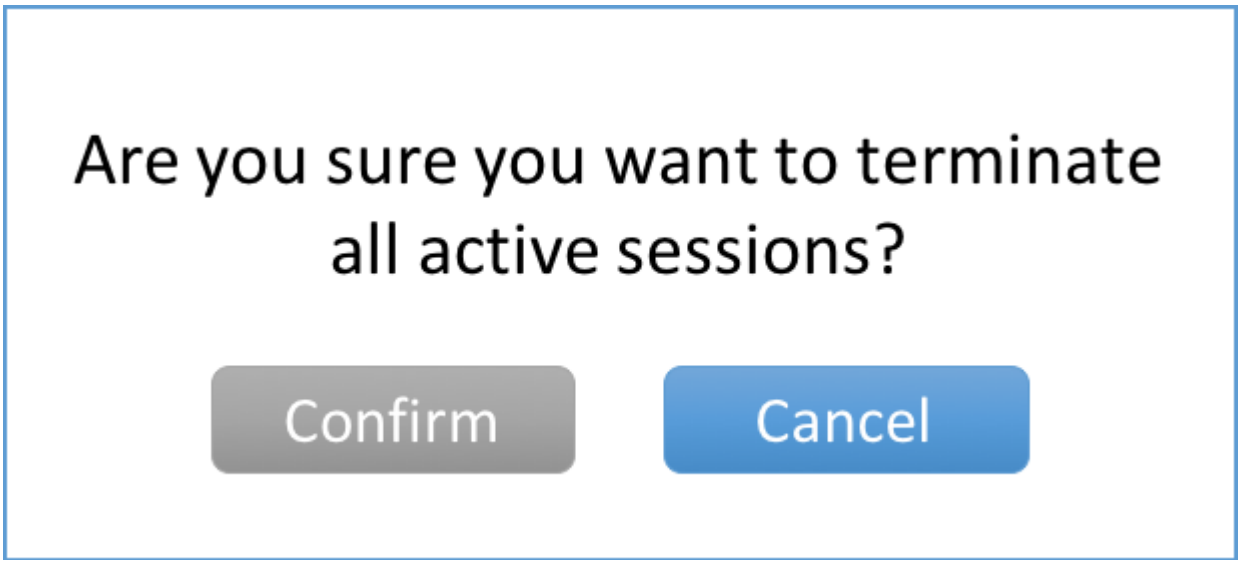


   a. The Terminate session confirmation message is displayed.



2. Click **Confirm** to terminate the active session.
3. To terminate all active sessions, follow these steps:
   a. Click **Terminate All** to stop and remove all active sessions from the gateway monitoring console.

b. The Terminate all active sessions confirmation message is displayed.



4. Click **Confirm** to terminate all active sessions.

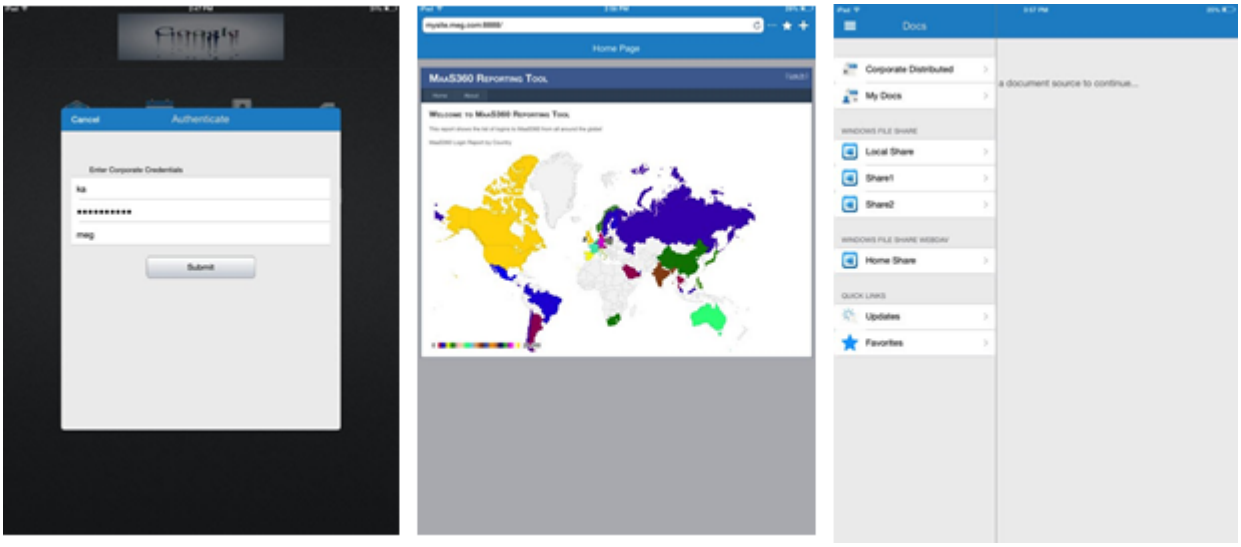
Parent topic: [Mobile Enterprise Gateway (MEG) Module]

13.17 Configuring Mobile Apps Through the Enterprise Gateway

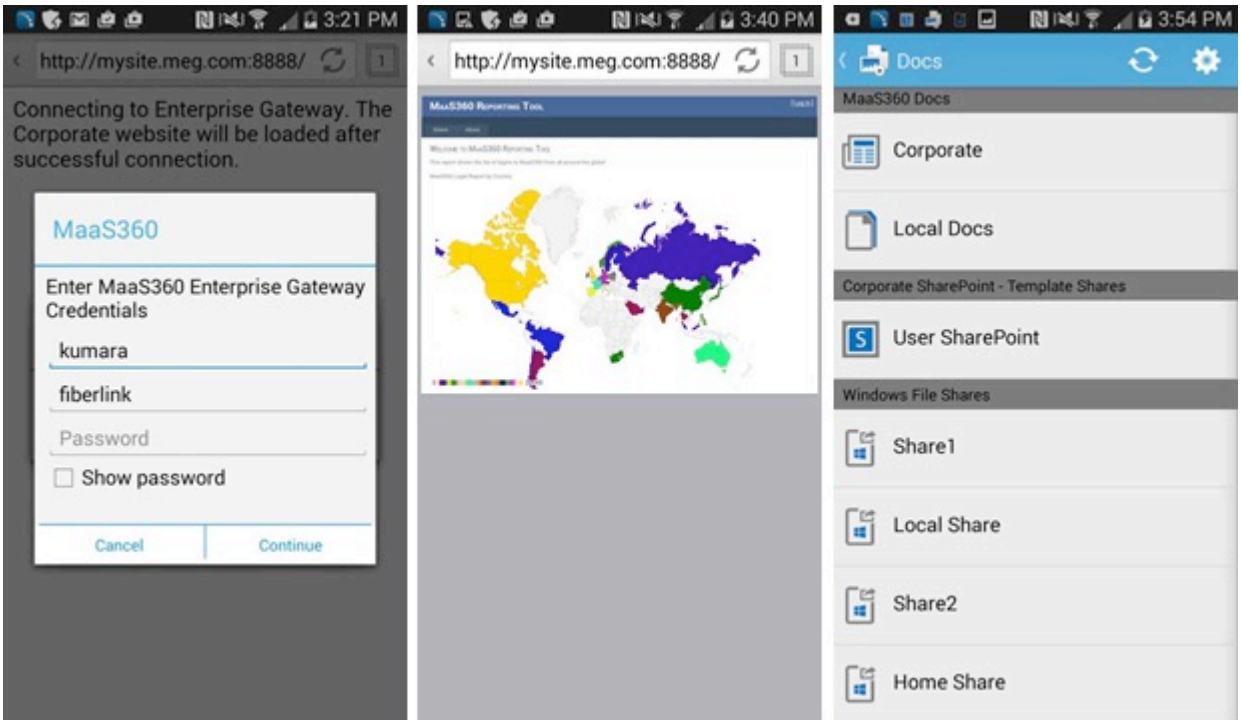
Follow these steps to configure your iOS or Android device through the enterprise gateway.

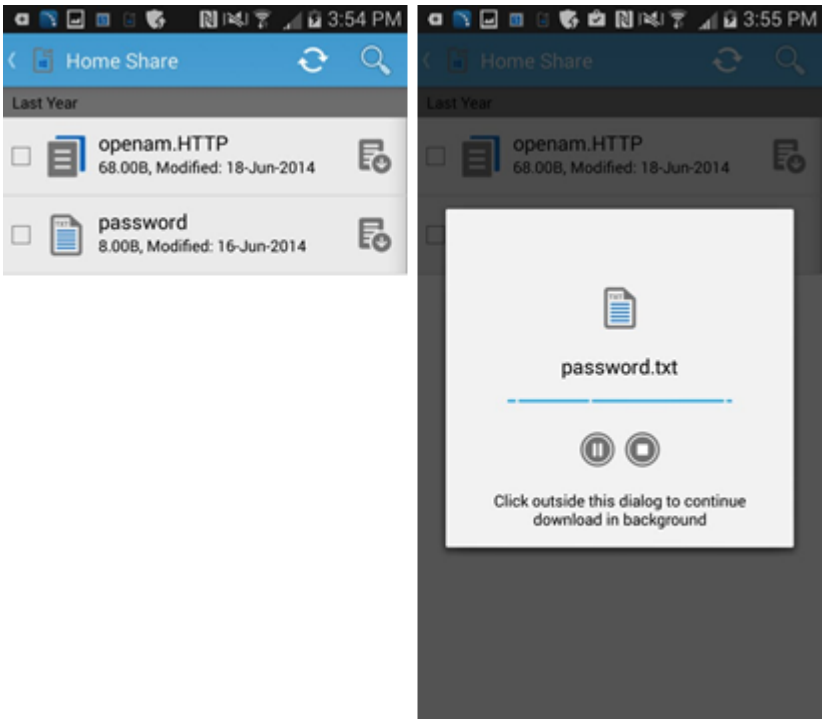
13.17.1 Procedure

1. From the MaaS360® Portal Home page, enroll your iOS or Android device.
2. Assign the Persona policy with the Secure Browser feature enabled.
3. Open a browser, and then provide your credentials to access intranet sites.
    a. For iOS, use the settings on the following image as an example for enrolling your iOS device:



b. For Android, use the settings on the following images as an example for enrolling your Android device:





Troubleshooting Issues with Configuring Mobile Apps

Troubleshooting issues with configuring your mobile device and the Secure Browser feature.

Parent topic: Mobile Enterprise Gateway (MEG) Module

13.18 Troubleshooting Issues with Configuring Mobile Apps

Troubleshooting issues with configuring your mobile device and the Secure Browser feature.

13.18.1 My users cannot access an intranet site through the Secure Browser. How do I fix this?

1. Make sure that the intranet site is included in the proxy access list for the Persona policies.
2. Log on to the server where you installed the gateway, open a browser and then try to access the intranet site.
3. Try to connect to the device on the corporate network from the VPN or by using Wi-Fi to determine whether the site is accessible.
4. If steps 1 - 2 do not fix the issue, the intranet site might be offline.
5. Open the browser on the gateway, use developer tools and capture logs as you load the intranet site.
6. Collect gateway logs and send the logs to IBM® Support for analysis.

13.18.2 My users cannot access any of the intranet sites through the Secure Browser. How do I fix this?

1. Log on to the server where you installed the gateway, open the Services console and make sure that the Cloud Extender™ service is running. If the Cloud Extender service is not running, start the service.
2. With a test device, start the Secure Browser app, authenticate (if required) and make sure that you are able to access the intranet sites.
3. If you cannot access intranet sites, open the browser on the gateway server and try to access intranet sites that are published. Check whether there are recent firewall or proxy changes to your internal network that might be blocking access.
4. Collect gateway logs and send the logs to IBM Support for analysis.

13.18.3 How do I collect gateway logs?

1. Replicate the issue that you are experiencing and write down the time stamp.
2. Log on to the server where you installed the gateway
3. Browse to the `C:\Program Files(x86)\MaaS360\Cloud Extender` folder.
4. Double-click `DiagnosticCmd.exe`. The tools runs and collects all relevant logs for the gateway and generates a compressed file on your desktop.
5. Send the file to IBM Support along with a detailed description of the issue you are experiencing, the time stamp of the issue, and your account number.

13.18.4 How do I collect Secure Browser logs?

1. Replicate the issue that you are experiencing with Secure Browser and write down the time stamp.
2. For iOS, open the browser, and select **Settings** > **Email Logs** to start your email client with a new email and logs as attachments.
3. For Android, follow these steps:
    a. Open the MaaS360® app and select **Settings** > **Email Logs**.
    b. From the **Secure Browser Settings** menu, enable **Verbose Logging**.

13.18.5 Where do I find the log files on the Mobile Enterprise Gateway (MEG)?

1. Go to `C:\%ProgramData%\MaaS360\Cloud Extender\logs`. The following logs are available in this folder:

    `MobileGateway.log` contains all gateway activities.

    `MobileGatewayAuth.log` contains all authentication attempts.

`MobileGatewayAccess.log` provides details of all the intranet resources that users accessed.
`MobileGatewayWebResAuth.log` contains all authentication attempts against intranet resources.

13.18.6 How do I check the version of the Secure Browser that is installed on my device?

1. For iOS, go to **Settings** > **Browser**. The **Version** field displays the version of the browser.
2. For Android, go to **Settings** > **Application Manager** > **Browser** to access the version.

13.18.7 How do I restore debug-level logging to the `mobilegateway-log4j.xml` file after I update Mobile Enterprise Gateway (MEG)?

When you update the Mobile Enterprise Gateway (MEG), the `C:\ProgramData\MaaS360\Cloud Extender\logs\mobilegatewaylog4j.xml` file is replaced with a new copy. If you have manually modified the `mobilegateway-log4j.xml` file to change logging levels, those changes are lost during the update. Follow these steps to preserve your manual changes to the file before you update the Mobile Enterprise Gateway (MEG):

1. Back up a copy of the `mobilegateway-log4j.xml` file before you start the Mobile Enterprise Gateway (MEG) update.
2. After the Mobile Enterprise Gateway (MEG) update, manually restore your modifications to the `mobilegateway-log4j.xml` file line by line.
3. Do not overwrite the contents of the new `mobilegateway-log4j.xml` file with the backup copy of the file because new logging configurations might be added during the Mobile Enterprise Gateway (MEG) update.

Parent topic: [Configuring Mobile Apps Through the Enterprise Gateway]

13.19 Using Cross-Forest and Cross-Domain Authentication for Mobile Enterprise Gateway (MEG)

Before users can access intranet resources, Mobile Enterprise Gateway (MEG) requires users to authenticate against corporate directory services. Mobile Enterprise Gateway (MEG) integrates with both Active Directory and LDAP servers for this type of user authentication.

13.19.1 About This Task

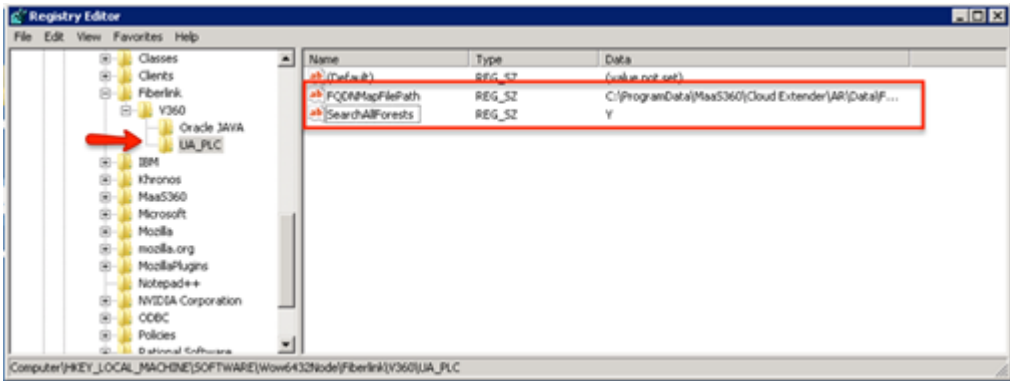
For integration with Active Directory for user authentication, you must configure the gateway as a service account that is a domain user for a particular domain. By default, the gateway authenticates only users that belong to a particular domain within the forest. If you want to run multiple Active Directory environments that use multiple domains in a forest or multiple forests, use the Mobile Enterprise Gateway (MEG) implementation for Active Directory for user authentication to enable trust for multi-forest/multi-domain environments.

For example, your Active Directory environment contains 2 forest and 3 domains that trust each other. When you enable user authentication for Active Directory, the default implementation only authenticates users within the context of the service account domain.
To extend the authentication scope to all forests and domains, you must manually modify a registry key to support multi-forest/multi-domain authentication for the gateway.

13.19.2 Procedure

1. Open the Registry Editor (`regedit.exe`) on the Cloud Extender™ server.
2. From `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360`, create a value in the V360 key:
   `"ADD_REG_POLICY_GROUP"="UA_PLC”`.
   Note: If the `ADD_REG_POLICY_GROUP` value exists, you must append `UA_PLC` to the list separated by a semicolon (;).

3. Create a key under the V360 key named `UA_PLC`.
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\UA_PLC`
4. Create two new string values under `UA_PLC`:
   `“FQDNMapFilePath”=”C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data\FQDNMap.txt”“SearchAllForests”=”Y”`



5. Create a mapping of all your trusted domains in new text file called `FQDNMap.txt` by using any plain text editor. This mapping file is a text file that contains one entry per line of text for each domain in the environment. Each line entry in the file looks like the following example, with the short domain to the left of the `=` (equals) sign and the `FQDN` to the right of the `=` (equals) sign:

   `shortDomainName=FQDN` and `FQDN=FQDN`
   (make sure to map both combinations).
   For example:
   ```
   domainA =
   domainA.rootDomain1.mycorp.com
   domainB = domainB.rootDomain1.mycorp.com
   domainC = domainC.rootDomain2.mycorp.com
   domainA.rootDomain1.mycorp.com = domainA.rootDomain1.mycorp.com
   domainB.rootDomain1.mycorp.com = domainB.rootDomain1.mycorp.com
   domainC.rootDomain2.mycorp.com = domainC.rootDomain2.mycorp.com
   ```
   Each line in the file must end with either a `<CRLF>` (DOS line ending convention) or a `<LF>` (UNIX line ending convention.)

6. Save the file as `FQDNMap.txt`.
7. Copy the FQDN Map File `FQDNMap.txt` to the folder `C:\ProgramData\MaaS360\Cloud Extender\AR\Data\`.
7. Restart the Cloud Extender service.

Note: If you are running a gateway cluster in High Availability (HA) mode, follow these steps on all gateways that implement the User Authentication service.

Parent topic: **Mobile Enterprise Gateway (MEG) Module**

14 MaaS360 VPN Module

The MaaS360® VPN module is a VPN solution that allows users to access their corporate network from an iOS or an Android device.

14.1 How the Module Works

You install the MaaS360 VPN server on a Windows Server that is located on your corporate network. Users install the MaaS360 VPN app on their iOS or Android device and use the app on their device to connect to the corporate network. The MaaS360 VPN module supports the following devices:
iOS 9.0 and higher
Android L and higher

14.2 MaaS360 VPN components

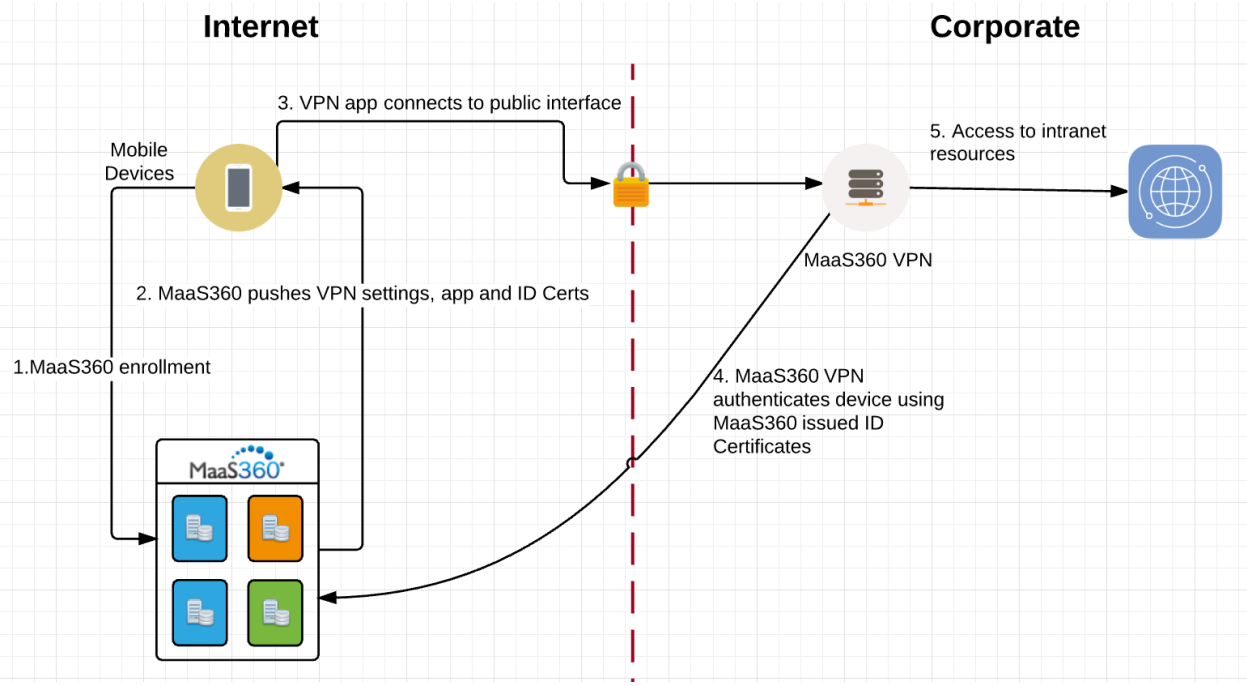
The MaaS360 VPN module requires the following components:

1. IBM® MaaS360 Cloud Extender™ - Cloud Extender is the delivery and maintenance mechanism for the MaaS360 VPN server. The MaaS360 VPN server is designed as a Cloud Extender module that you deploy and then configure from the Cloud Extender Configuration Tool.
2. MaaS360 VPN server - You install the MaaS360 VPN server on your corporate network and assign a public IP address or DNS name to the server so that clients can connect to the server from the Internet. You can install the VPN server as a standalone server or as a member of a cluster in High Availability (HA) mode. To support a large number of devices, you can install the MaaS360 VPN module on more than one server and use a DNS load balanced URL.
3. MaaS360 VPN apps - MaaS360 VPN apps are available for iOS and Android. You configure the iOS or the Android MDM policy to use the VPN apps. The VPN apps use client identity certificates that are issued by the MaaS360 Portal to authenticate with the server. You do not need to enter a user password to connect to the VPN. You configure the MaaS360 VPN for all apps to connect to the VPN.
4. MaaS360 platform - The MaaS360 platform enables the MaaS360 VPN solution. The MaaS360 platform functions as follows:

a. Enables the MaaS360 VPN service and pushes the MaaS360 VPN module to the Cloud Extender.
b. Stores VPN configuration for usage and policies on the MaaS360 platform.
c. Generates and distributes client identity certificates for MaaS360 VPN authentication.
d. Publishes data for compliance checks for MaaS360 VPN access.
e. Reports on MaaS360 VPN servers installed in the corporate network.

14.3 MaaS360 VPN Architecture

The following diagram illustrates the MaaS360 VPN architecture:



MaaS360 VPN Deployment Scenarios
Information about deploying MaaS360 VPN in your environment.

Configuring Windows Routing and Remote Access for MaaS360 VPN
MaaS360 VPN can route all traffic through the VPN or route specific subnets through the VPN (split tunneling).

Setting Up a Cluster for MaaS360 VPN

Follow these steps to set up a VPN cluster when the number of inbound VPN connections exceeds the number of connections that a single instance of the MaaS360 VPN server can handle.

Configuring the MaaS360 VPN Policy in the MaaS360 Portal

Information about creating and defining the MaaS360 VPN policy for devices in the MaaS360 Portal.

Installing the MaaS360 VPN App

The MaaS360 VPN app allows users to connect to and access the MaaS360 VPN server that is installed on the corporate network.

Troubleshooting Issues with MaaS360 VPN

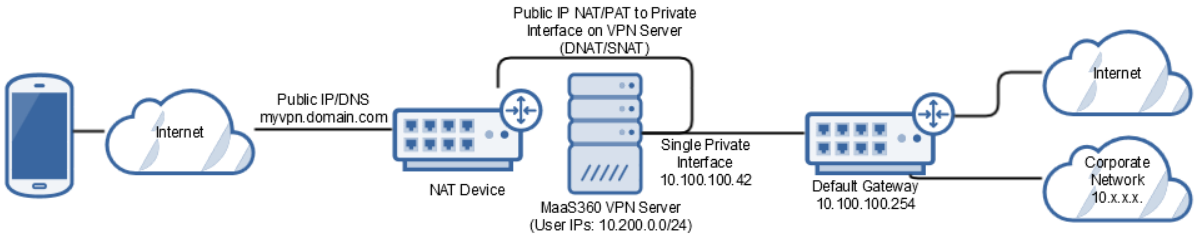
Troubleshooting issues with configuring MaaS360 VPN.

Parent topic: Configuring Settings for the Cloud Extender Modules

14.4 MaaS360 VPN Deployment Scenarios

Information about deploying MaaS360® VPN in your environment.

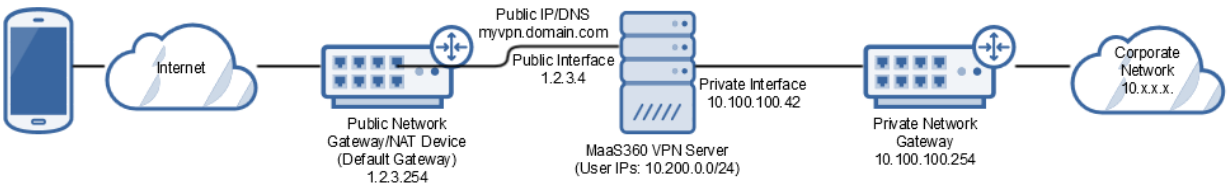
14.4.1 MaaS360 VPN Deployment Example: Single Interface Server with NAT Mode or IP Forward Mode (One-Arm Mode)



In this example, the MaaS360 VPN server uses a single physical interface to connect to the internal network. A Network Address Translation (NAT) device (for example, firewall or load balancer) maps the public address of the MaaS360 VPN to the internal address and port of the MaaS360 VPN server.

Depending on your network setup, the NAT device and default gateway router might be the same device. If you are not using the same device for the NAT device and the default gateway, the Source NAT (SNAT) is applied to the public IP and to the private interface NAT; otherwise return traffic from the VPN server to the endpoint might be sent to the default gateway instead of the NAT device, resulting in routing failures.

14.4.2 MaaS360 VPN Deployment Example: Multiple Interface VPN Server with NAT Mode or IP Forward Mode (Multi-Arm Mode)



In this example, the MaaS360 VPN server uses two interfaces: one interface for incoming connections to the VPN server and one interface to access the corporate network resources. The public IP is assigned directly to the incoming interface on the VPN server, however this setup can also use a separate private IP address, assuming that the public IP is translated to this private IP by using Network Address Translation (NAT) or Private Address Translation (PAT) (see the single interface server deployment example).

Since Windows does not support multiple default gateways, the default gateway is set on the public side interface to facilitate the return traffic to the endpoints during the creation of the VPN tunnel. If the default gateway is assigned to the private interface on the VPN server, the VPN connection process fails since inbound requests arrive on a different interface than the reply request. If you applied a source NAT on the incoming traffic to the VPN server, you can define a persistent static route on the public interface of the VPN for the Source NAT IPs to make sure that the return traffic uses the same interface that is used for new tunnel connections. Set the default gateway to the private interface on the VPN server.

Parent topic: [MaaS360 VPN Module]

14.5 Configuring Windows Routing and Remote Access for MaaS360 VPN

MaaS360® VPN can route all traffic through the VPN or route specific subnets through the VPN (split tunneling).
By default, MaaS360 VPN uses Network Address Translation (NAT) to route traffic from the MaaS360 VPN server to your corporate network.
Before the MaaS360 VPN module can function on your network, you must complete the following steps:

Install Windows Routing and Remote Access Roles on Windows Server 2012 R2

Install MaaS360 VPN and Configure the MaaS360 VPN Tap Adapter on Windows Server 2012 R2

14.5.1 Requirements

The following table lists the installation and setup requirements that apply to the MaaS360 VPN installation:

Item	Requirement
Server	Microsoft Windows Server 2012 R2 (physical or virtual) **Note:** MaaS360 VPN might function on Windows Server 2008 R2, but this setup is not currently supported by IBM®. At least one interface with access or routes to the resources that are accessed by the MaaS360 VPN. Supports one-arm mode which uses the same interface for incoming VPN connections and outgoing traffic to the network or multi-arm mode which uses different interfaces for incoming VPN connections and outgoing traffic to the network.

MaaS360 VPN	The external DNS name or the IP address, and the port that is used to configure external user connections. External DNS name or IP address: The DNS name or the IP address that end user agents use to connect to the MaaS360 VPN. The public IP address is assigned directly to an interface on the Windows Server or translated to the private address of the Windows Server by using a router, firewall, load balancer, or reverse proxy (highly recommended). Port: The default port is 1194. You can change this port. MaaS360 VPN currently uses the UDP protocol, which you cannot change. The administrator must make sure that the port that is entered in the Cloud Extender™ Configuration Tool is open to the server that is provisioning MaaS360 VPN. You should block other ports for security reasons.
MaaS360 VPN Software	The internal IP address and the port that the MaaS360 VPN software uses. Internal IP address: You must use a valid IP address of a physical adapter on the Windows Server. Port: The default port is 1194. You can change this port. **Note:** The internal port does not need to match the VPN external port if there is a load balancer, firewall, router, or reverse proxy in front of the VPN server handling the translation.
MaaS360 VPN Tunnel	One or more valid subnets (IP address and netmask) that are used to assign IP addresses to inbound user connections for the VPN tunnel (Virtual IP and Virtual Subnet Mask). Use subnets in a private range that include enough IP addresses to handle all users

	that connect to each MaaS360 VPN server. One subnet is needed for each MaaS360 VPN server. The subnet must include enough IP addresses to handle the maximum number of users that can connect to the server at single instance. Since NAT is used on outgoing traffic from the server, you can use the same subnet for each MaaS360 VPN server. However, this setup might impede troubleshooting efforts. Use unique subnets in the network that do not create overlap or confusion with the network routing.
DNS Server	One or more DNS servers that are used by end user agents. The DNS server must be accessible from the network interface on which the MaaS360 VPN is installed. The DNS server must resolve public and private addresses, even if split tunneling is used (or, add a second public DNS to the list).
Subnets	A list of subnets (IP address and netmask) that are used to route through the MaaS360 VPN (if you are using split tunneling). **Note:** If you are not using split tunneling, all traffic (private and public) is routed through the tunnel and might increase the load on the server with non-corporate traffic.

14.5.2 Next Steps

Installing the Routing and Remote Access Role on Windows Server 2012 R2

Follow these steps to install the routing and remote access role on Windows Server 2012 R2.

Installing MaaS360 VPN and Configuring the MaaS360 TAP Adapter on Windows Server 2012 R2

Follow these steps to install MaaS360 VPN, including the MaaS360 VPN TAP Adapter, on Windows Server 2012 R2.

Parent topic: MaaS360 VPN Module

14.6 Setting Up a Cluster for MaaS360 VPN

Follow these steps to set up a VPN cluster when the number of inbound VPN connections exceeds the number of connections that a single instance of the MaaS360® VPN server can handle.

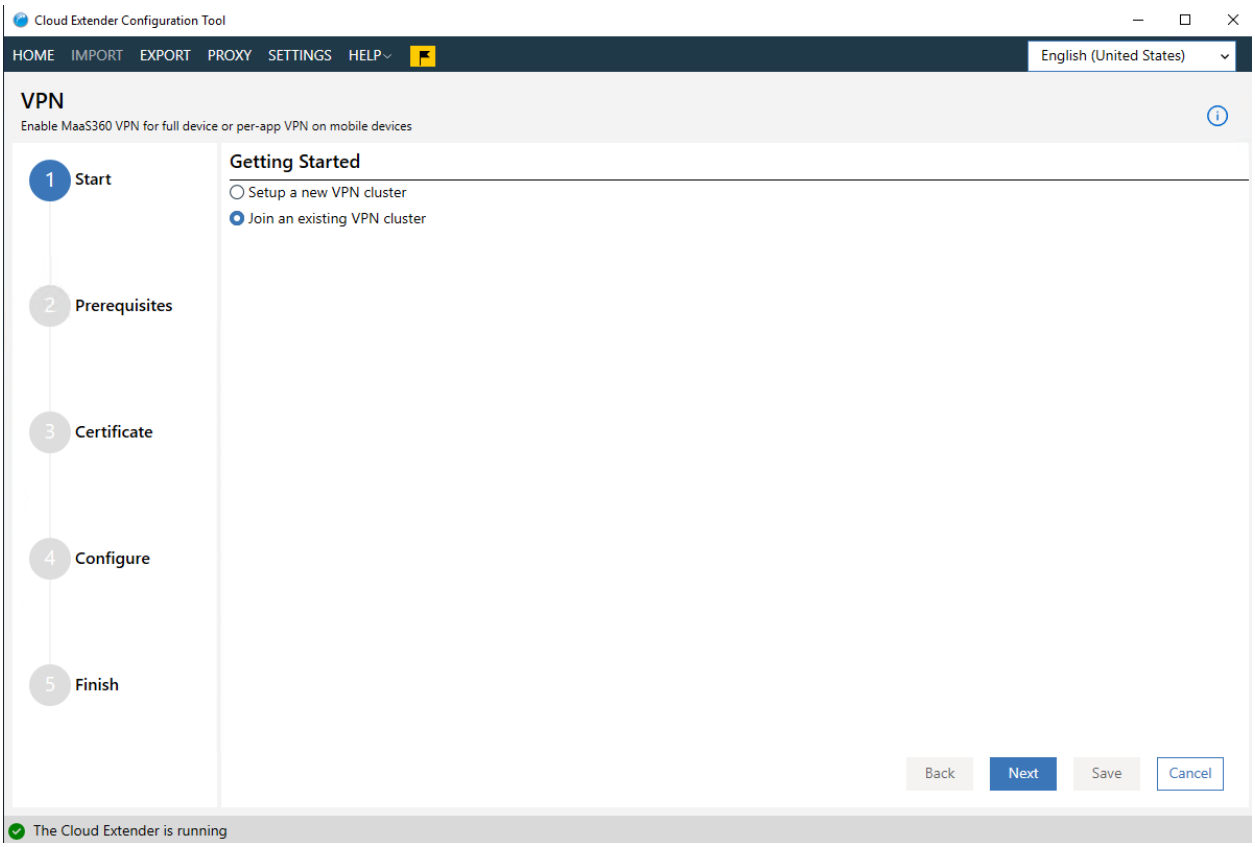
14.6.1 About This Task

The MaaS360 VPN does not load balance traffic between nodes in a cluster. Use a front-end load balancer to balance traffic between multiple members of the cluster. Use one of the following options to load balance traffic between multiple members in a cluster by balancing the external URL assigned for the VPN between round robin DNS and a load balancer:

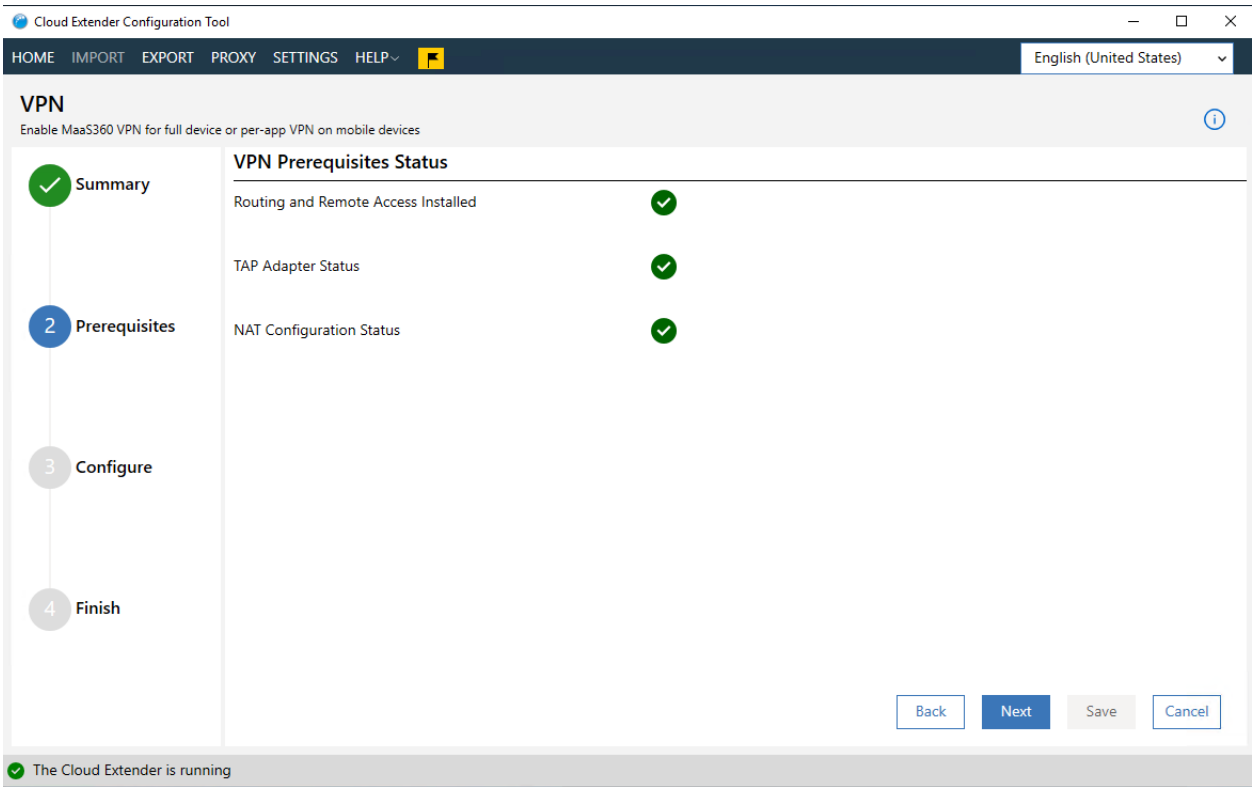
1. Use round robin DNS to alternate traffic between various endpoints. **Note:** Round robin DNS cannot compensate for a node that is offline or unavailable.
2. Use a load balancer to handle traffic that is distributed between endpoints. **Note:** Use a persistence profile that locks traffic between each device endpoint to a single server during a session. Consult with your network administrator for the best method to use with this option.

14.6.2 Procedure

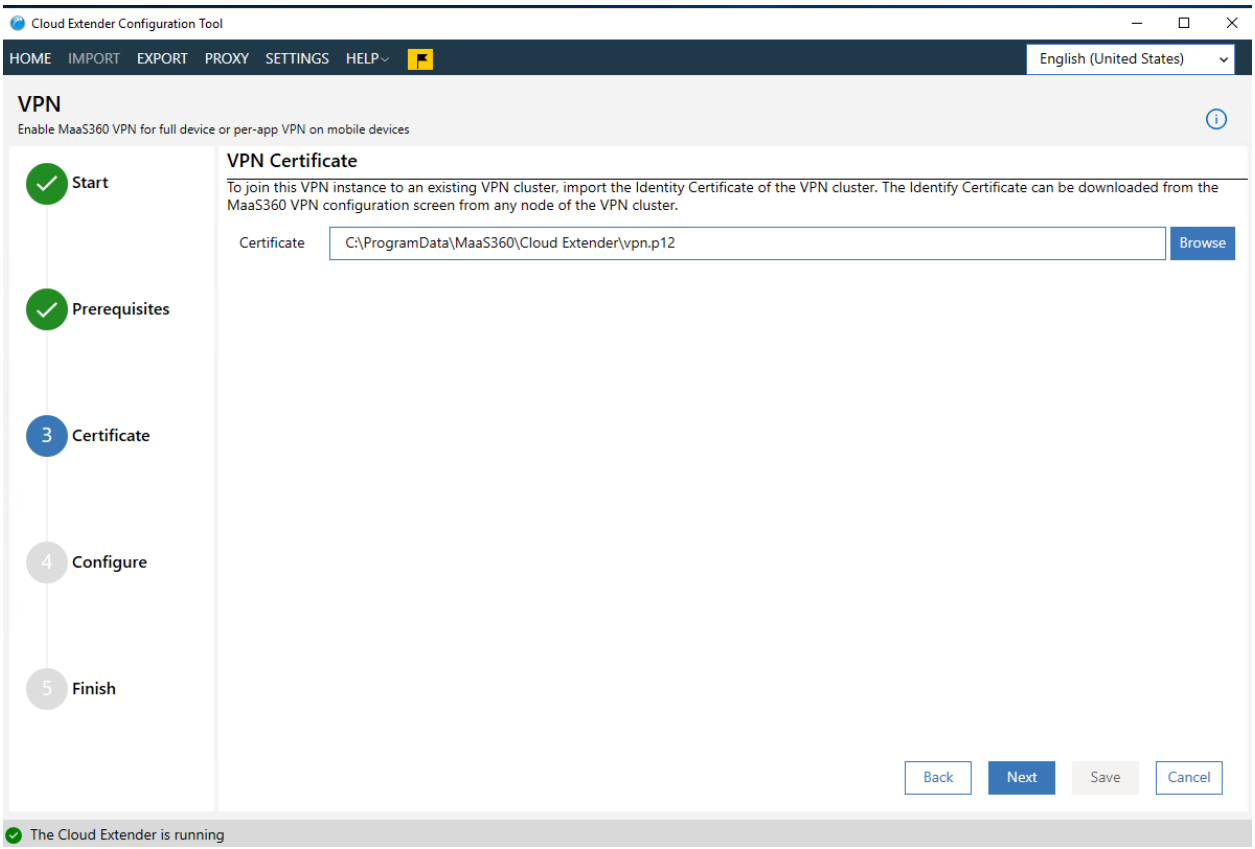
1. Follow the steps in Installing MaaS360 VPN and Configuring the MaaS360 VPN TAP Adapter on Windows Server 2012 R2 to configure the first node of the cluster.
2. Download the cluster certificate (`p12` format) and save the certificate to use on the other servers. **Important:** Do not lose this certificate.
3. Install the MaaS360 VPNC loud Extender™ software on additional servers in the cluster. Follow the steps in Installing MaaS360 VPN and Configuring the MaaS360 VPN TAP Adapter on Windows Server 2012 R2 to install the MaaS360 VPN TAP Adapter.
4. Launch the Config Tool and select the VPN tile on the main window.
5. Select **Join an existing VPN cluster**.



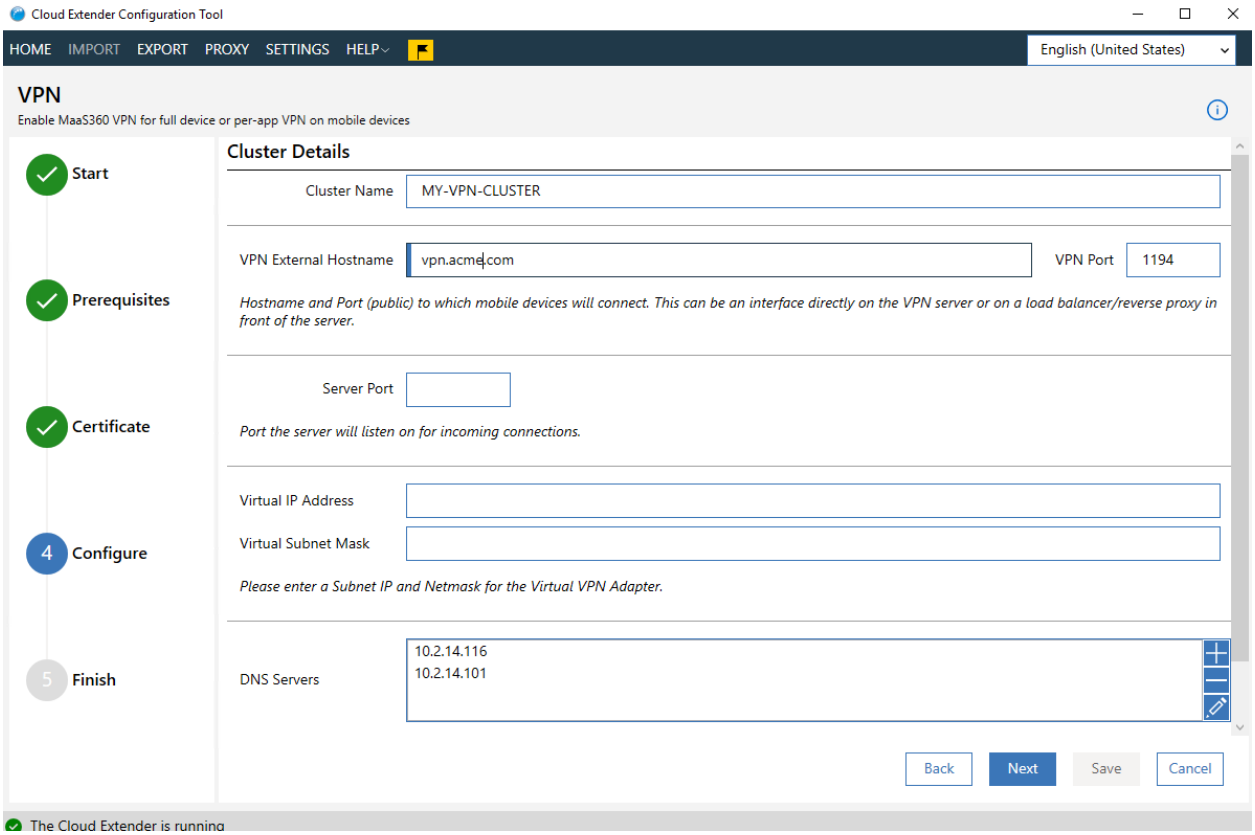
6. Click the **Next** button
7. Verify that all VPN prerequisites have been satisfied
    a. Routing and Remote Access installed and enabled
    b. TAP Adapter installed
    c. NAT configured



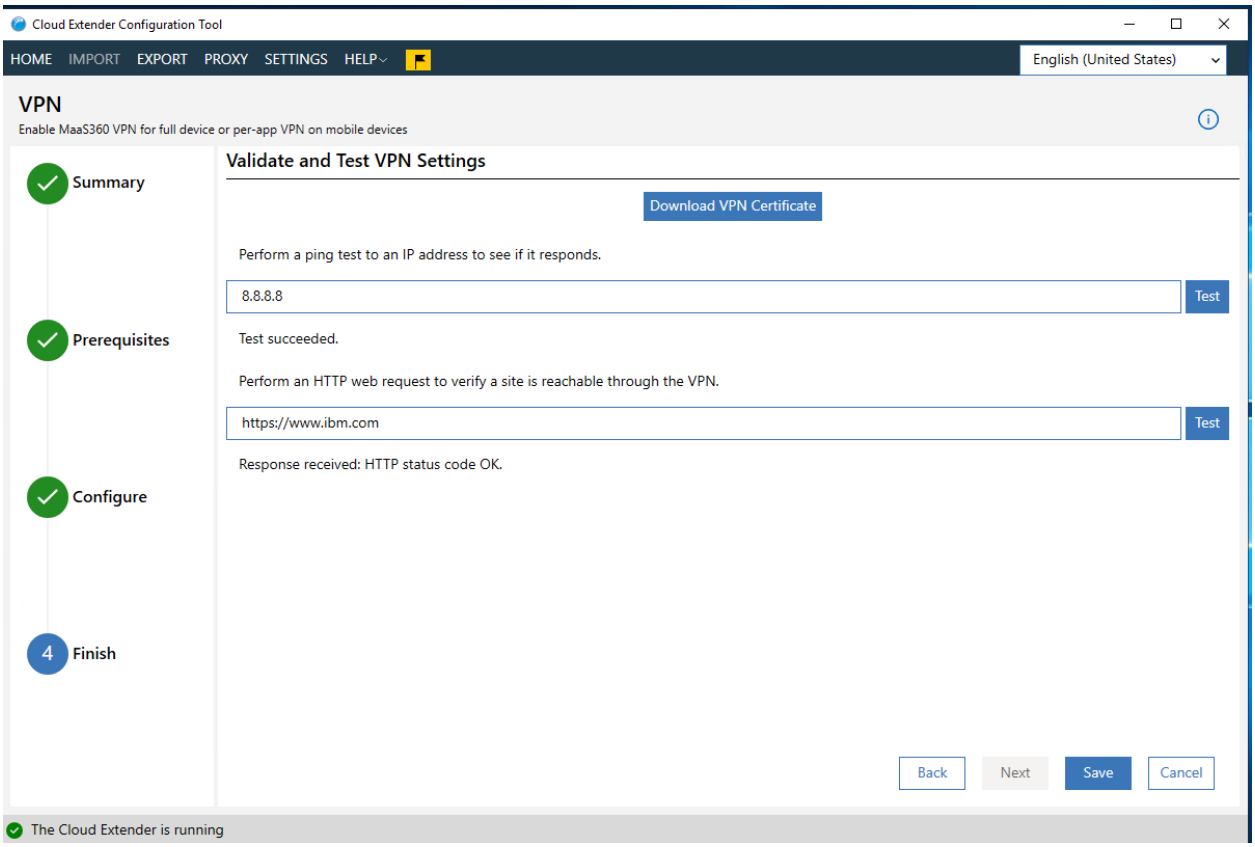
8. Click the **Next** button
9. Click the **Browse** button to find the VPN cluster certificate for the cluster you wish to join



10. Click the **Next** button
11. The Config Tool will retrieve the cluster settings from MaaS360 portal and populate the fields in the next window
12. Enter proper values for the fields that are unique to each node in the cluster
    a. Server Port
    b. Virtual IP Address
    c. Virtual Subnet Mask



13. Click the **Next** button
14. On the final configuration screen you can run test to determine if your VPN is properly configured



15. Click the **Save** button
16. Repeat this procedure for all other nodes/servers in the cluster. You do not need to change user policies in the MaaS360 Portal to support clusters. All members of a cluster use the same name. The distribution of traffic between those members is handled by a front-end load balancer, not by MaaS360.

Parent topic: [MaaS360 VPN Module]

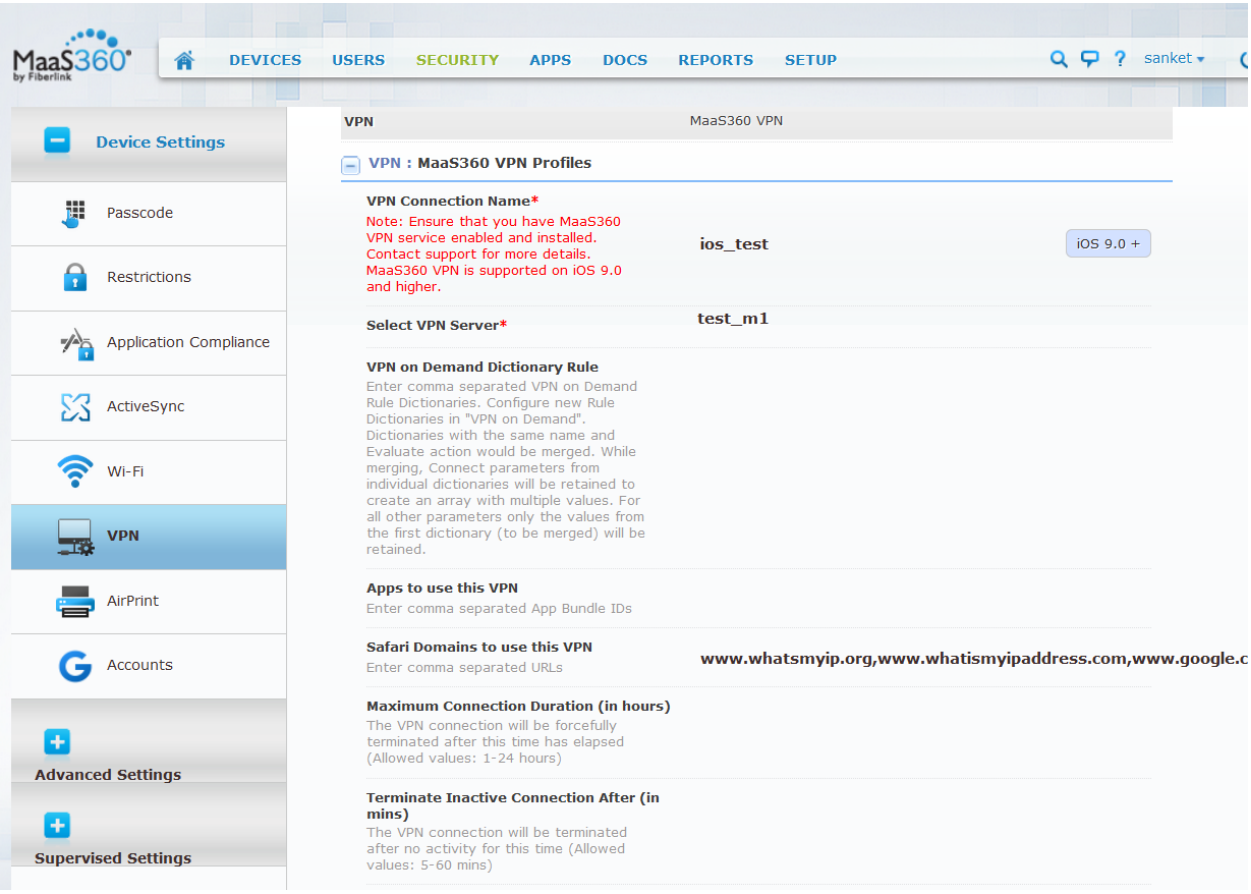
14.7 Configuring the MaaS360 VPN Policy in the MaaS360 Portal

Information about creating and defining the MaaS360® VPN policy for devices in the MaaS360 Portal.

14.7.1 iOS Policy Settings for MaaS360 VPN

The VPN setting in the default iOS MDM policy provides theMaaS360 VPN policy profile settings that you apply to your iOS devices. Follow these steps to create a MaaS360 VPN policy for iOS devices:

1. From theMaaS360 Portal Home page, select **Security** > **Policies**. The Policies window is displayed.
2. Click **Add Policy**. The Add Policy window is displayed.
3. Enter a policy name, select **iOS MDM** as the policy type, and then click **Continue**.
4. From the Device Settings list, select **VPN**. The MaaS360 VPN Profile window is displayed. If the MaaS360 VPN profile settings are not displayed, contact IBM® Support to enable theMaaS360 VPN service.
5. Provide the following settings:



Setting	Description
VPN Connection Name	The name of the VPN profile
Select VPN Server	The VPN server that you defined in the Cloud Extender Configuration Tool
VPN on Demand Dictionary Rule (Optional)	The on-demand rules that determine how the VPN connection is used by iOS
Apps to Use This VPN	The comma-separated list of apps that you use to configure the VPN in iOS
Safari Domains to Use This VPN	The list of Safari domains that can use the VPN
Maximum Connection Duration (in hours)	The maximum session time for the VPN connection before it terminates a connection. Allowed values: 1 – 24 hours

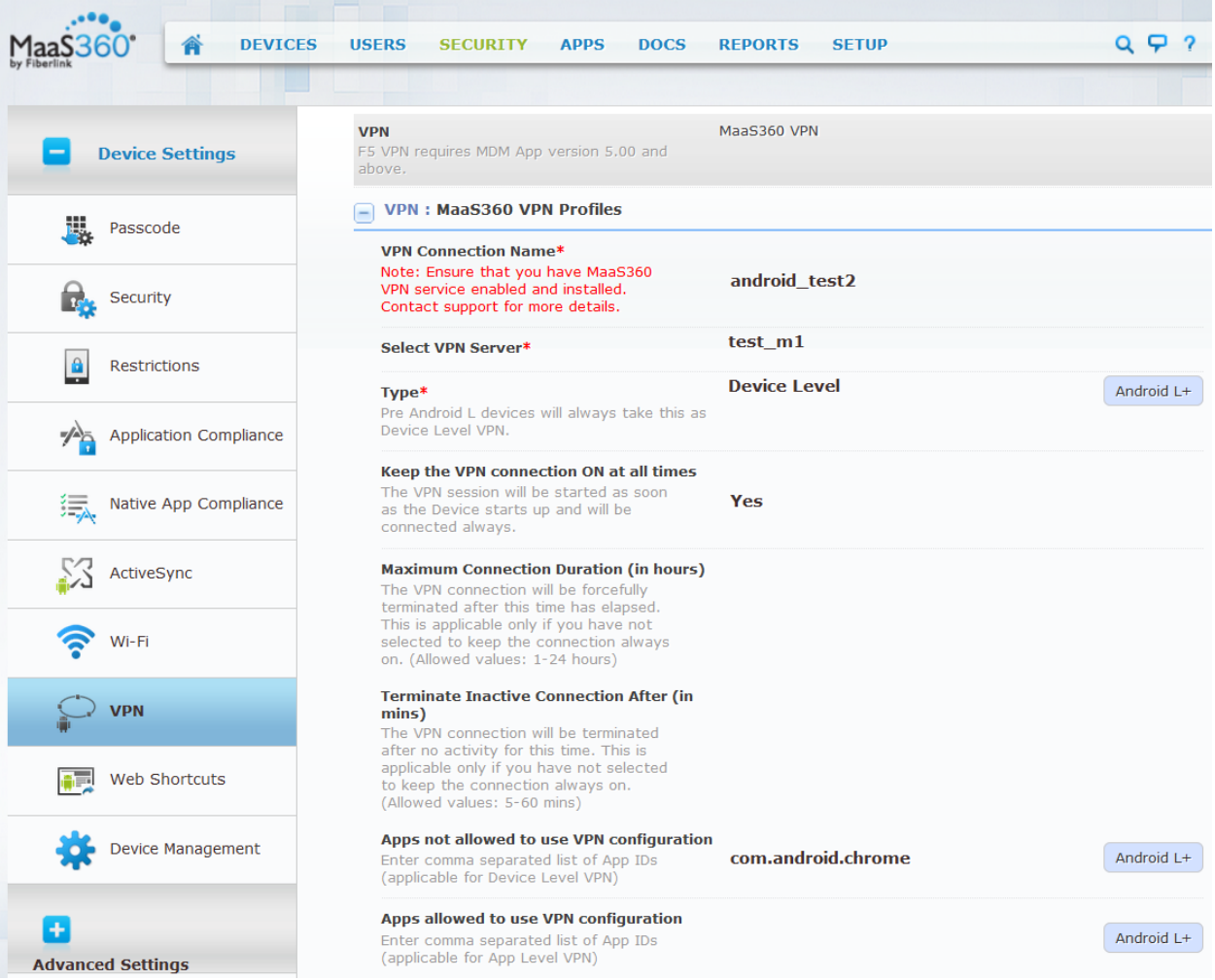
Terminate Inactive Connection After (in mins)	The amount of time the VPN connection waits before it terminates a connection on a device with no activity. Allowed values: 5 – 50 minutes

6. Click **Save & Publish**.

14.8 Android Policy Settings for MaaS360 VPN

The VPN setting in the default Android MDM policy provides the MaaS360 VPN policy profile settings that you apply to your Android devices. The following settings are available for the MaaS360 VPN policy for Android devices:

1. From the MaaS360 Portal Home page, select **Security** > **Policies**. The Policies window is displayed.
2. Click **Add Policy**. The Add Policy window is displayed.
3. Enter a policy name, select **Android MDM** as the policy type, and then click **Continue**.
4. From the Device Settings list, select **VPN**. The MaaS360 VPN Profile window is displayed. If the MaaS360 VPN profile settings are not displayed, contact IBM Support to enable the MaaS360 VPN service.
5. Provide the following settings:



Setting	Description
VPN Connection Name	The name of the VPN profile
Select VPN Server	The VPN server that you defined in the Cloud Extender Configuration Tool
Type	The VPN is configured at the device level or app level
Keep the VPN Connection ON at all times	The VPN is always connected. Allowed values: **Yes** or **No**
Maximum Connection Duration (in hours)	The maximum session time for the VPN connection before it terminates a connection. Allowed values: 1 – 24 hours
Terminate Inactive Connection After (in mins)	The amount of time the VPN connection waits before it terminates a connection on the device. This option only applies if you disabled **Always On**, where the VPN is always connected. Allowed values: 5 – 60 minutes
Apps not allowed to use VPN configuration	If the VPN **Type** is set to **Device Level**, the comma-separated list of apps that cannot use the VPN connection
Apps allowed to use VPN configuration	If the VPN **Type** is set to **App Level**, the comma-separated list of apps that can use the VPN connection

6. Click **Save & Publish**.

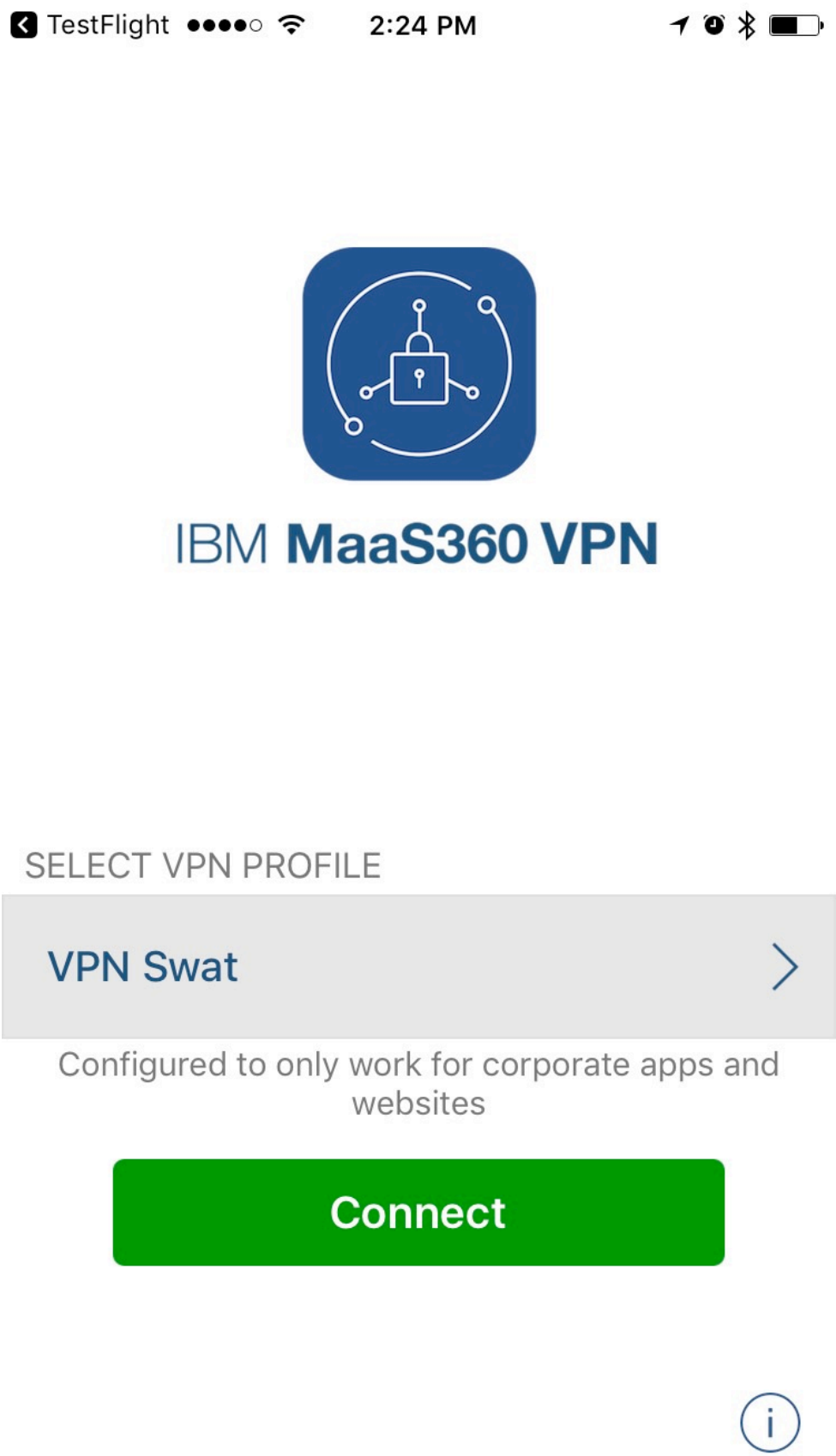
Parent topic: [MaaS360 VPN Module]

14.9 Installing the MaaS360 VPN App

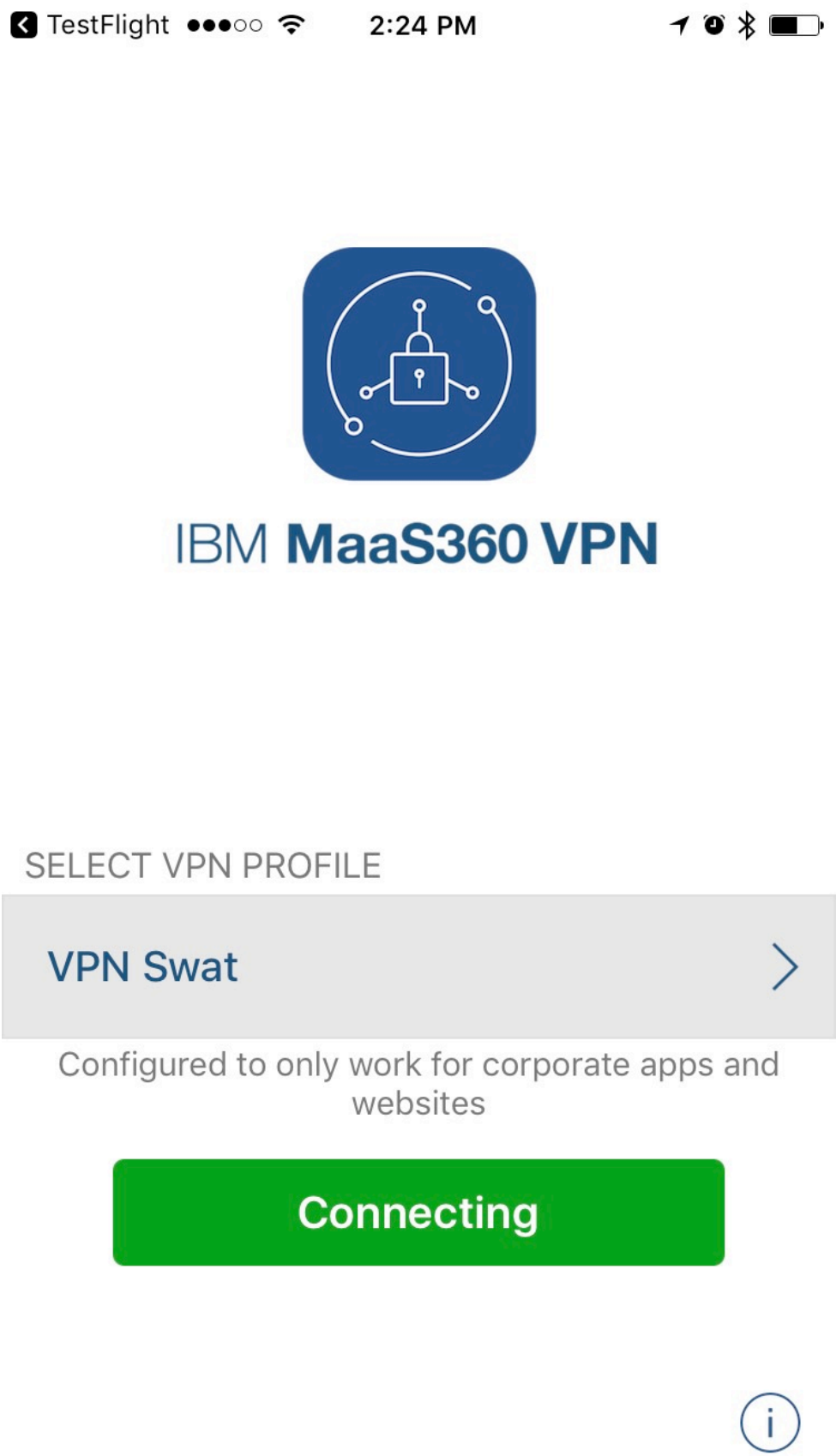
The MaaS360® VPN app allows users to connect to and access the MaaS360 VPN server that is installed on the corporate network.

14.10 MaaS360 VPN App for iOS

1. From iTunes, download the IBM® MaaS360 VPN app and tap **Install**. The Home screen for the app is displayed.

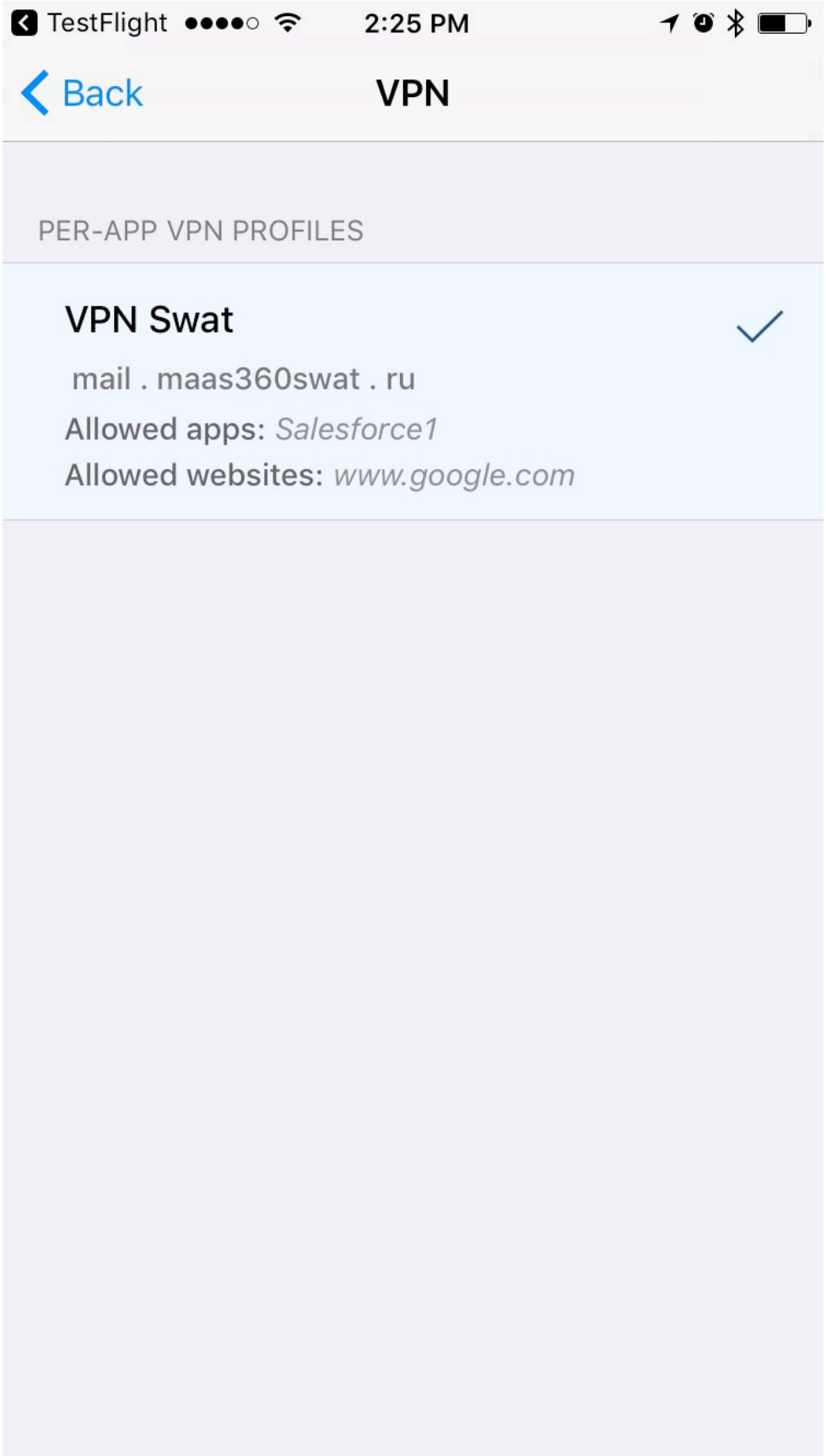

TestFlight
2:24 PM
IBM MaaS360 VPN
SELECT VPN PROFILE
VPN Swat
Configured to only work for corporate apps and websites
Connect

2. Tap **Connect**
3. Select a VPN profile

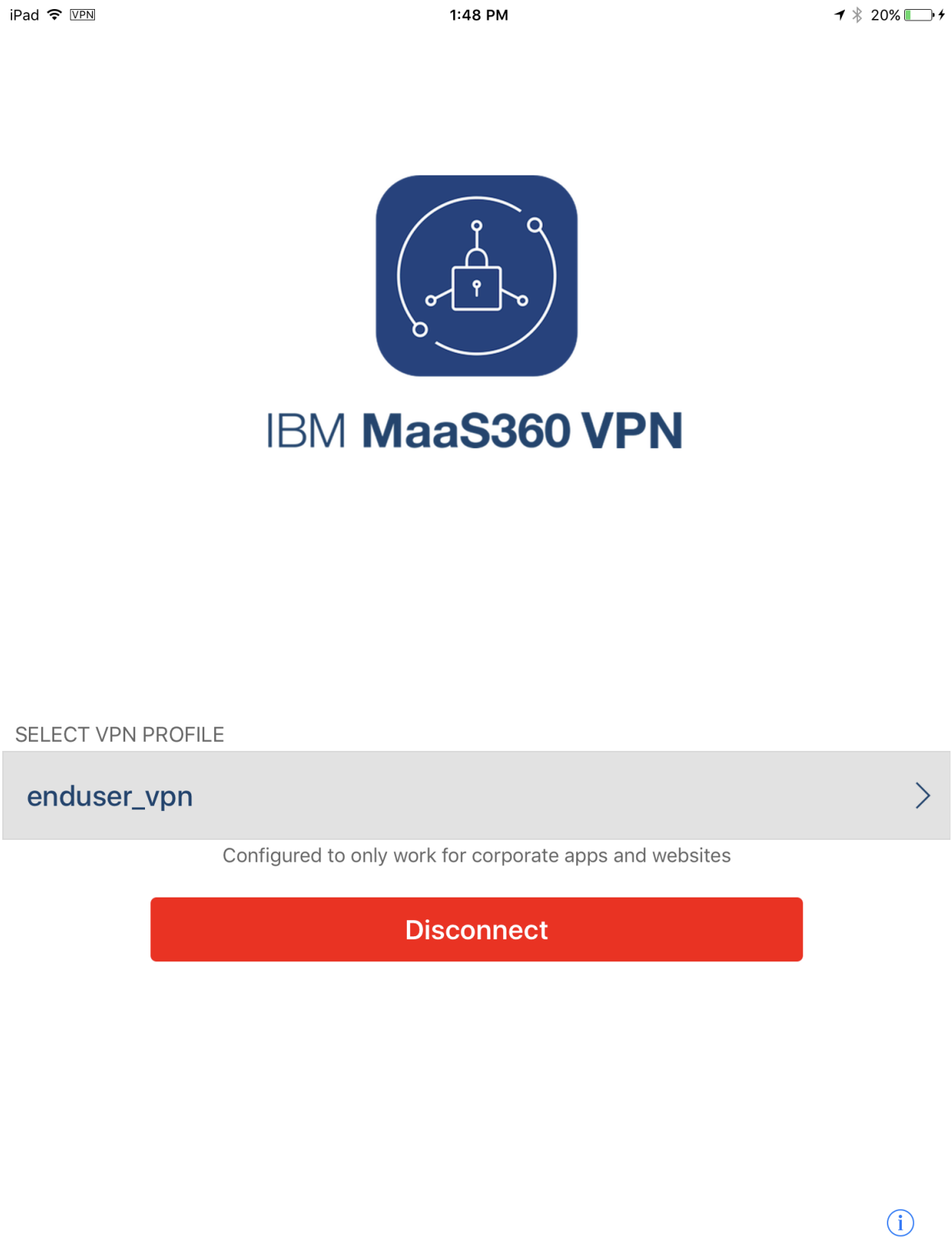

TestFlight
2:24 PM
IBM MaaS360 VPN
SELECT VPN PROFILE
VPN Swat
Configured to only work for corporate apps and websites
Connecting

The profile displays the following configuration settings:

1. The name of the MaaS360 VPN configuration
2. The address of the MaaS360 VPN server
3. The apps and the websites that are allowed to use the MaaS360 VPN Connection.

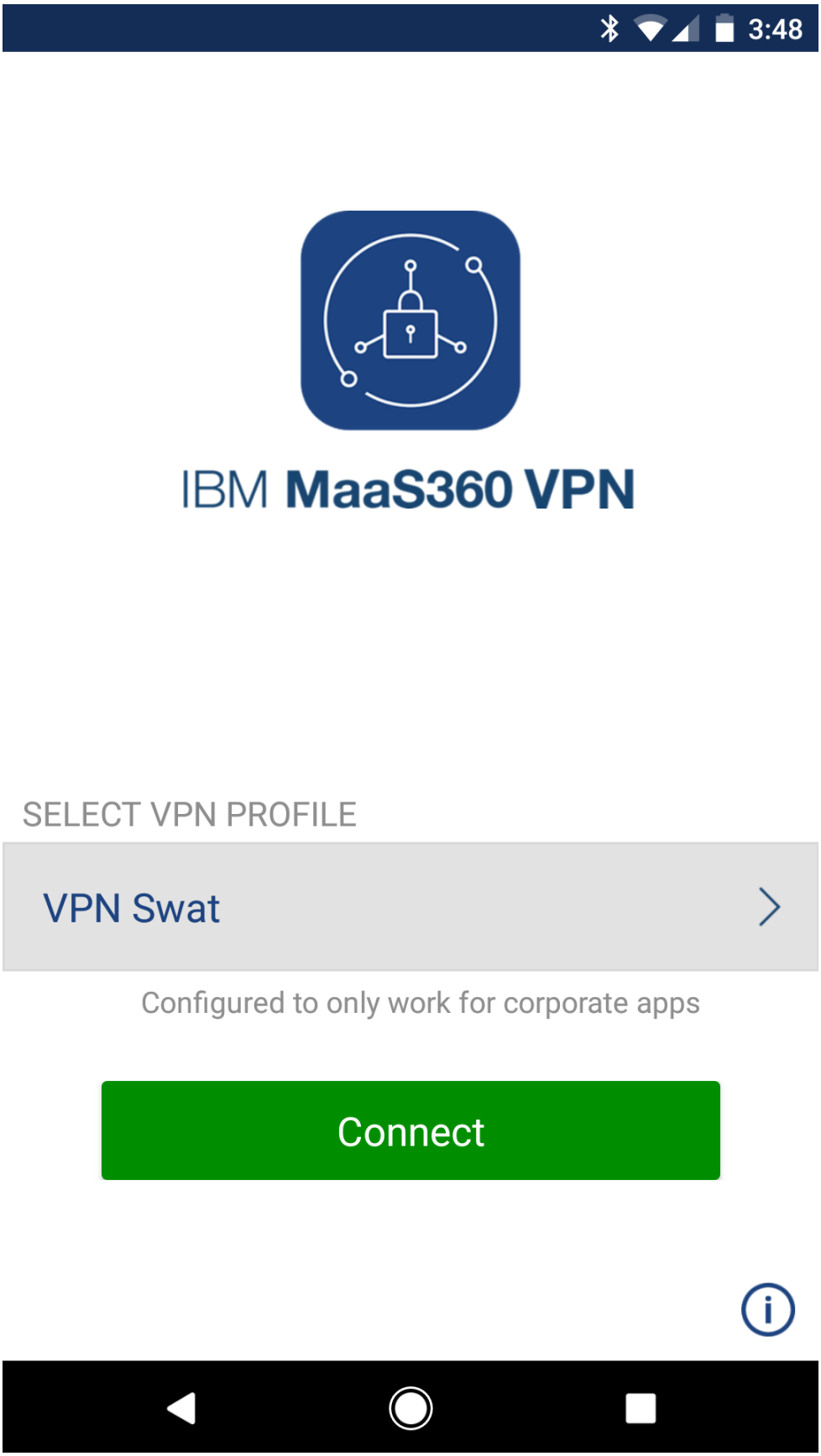

TestFlight
2:25 PM
Back
VPN
PER-APP VPN PROFILES
VPN Swat
mail . maas360swat . ru
Allowed apps: Salesforce1
Allowed websites: www.google.com

When the app is connected to theMaaS360 VPN, you can tap **Disconnect** to disconnect from the MaaS360 VPN service.

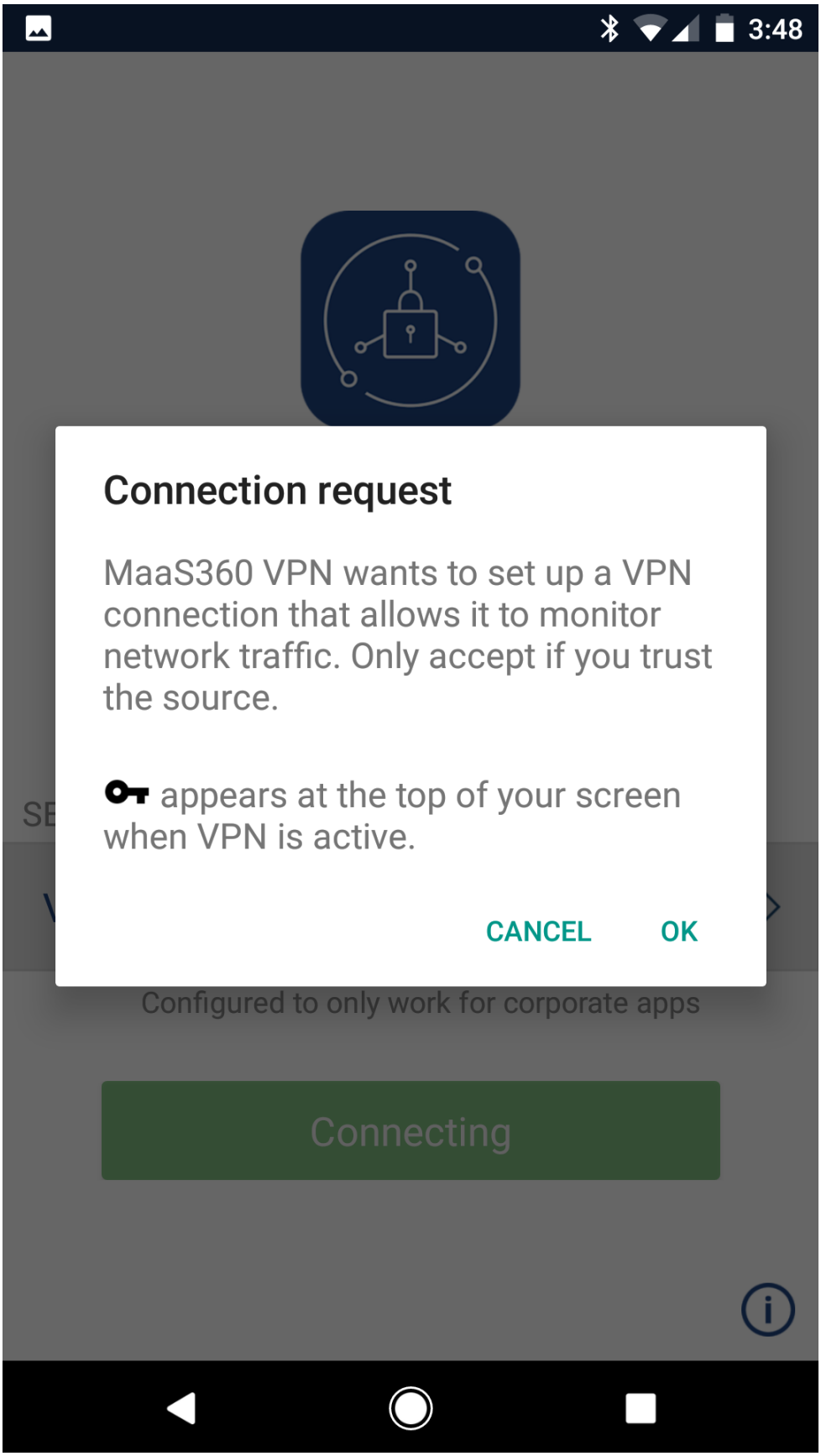

iPad
VPN
1:48 PM
20%
IBM MaaS360 VPN
SELECT VPN PROFILE
enduser_vpn
Configured to only work for corporate apps and websites
Disconnect

MaaS360 VPN App for Android

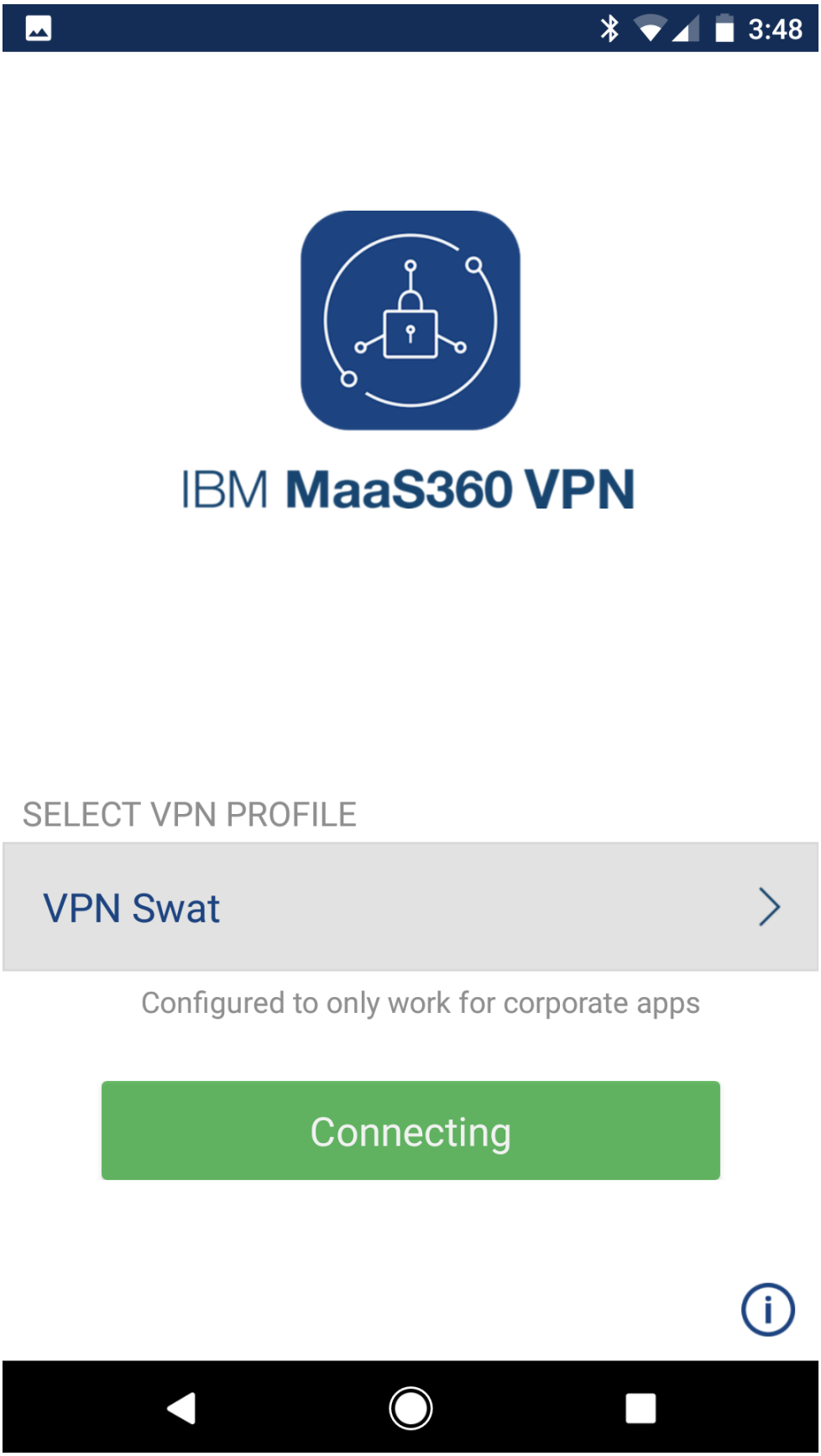
1. From the Google Play store, download the IBM MaaS360 VPN app and tap **Install**. **Note:** If a profile is in **Always On** mode, you cannot connect to or disconnect from another profile. The Home screen for the app is displayed.


3:48
IBM MaaS360 VPN
SELECT VPN PROFILE
VPN Swat
Configured to only work for corporate apps
Connect

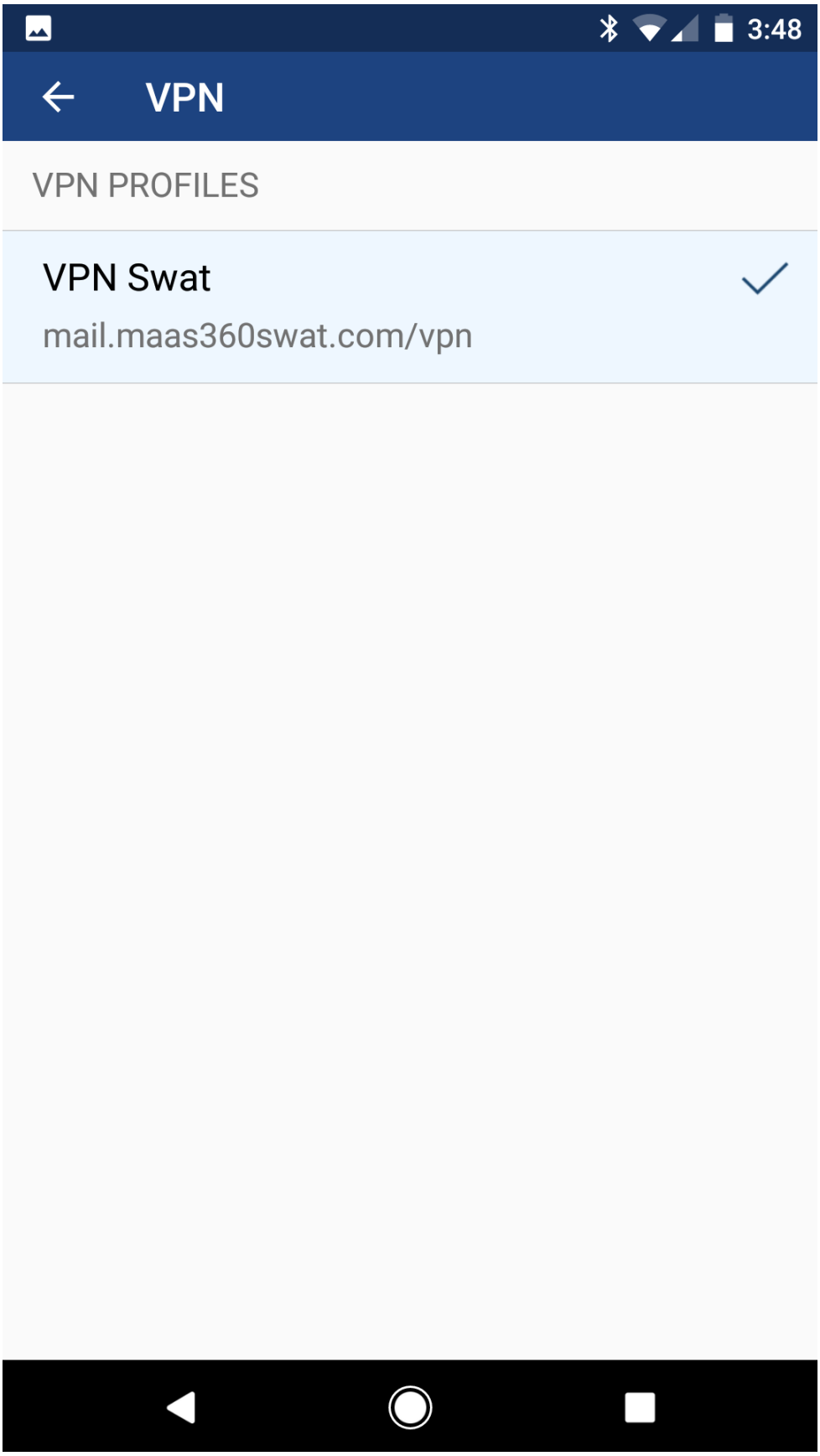
2. Tap **Connect**. A connection request message is displayed.


3:48
Connection request
MaaS360 VPN wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.
appears at the top of your screen when VPN is active.
CANCEL
OK
Configured to only work for corporate apps
Connecting

3. Click **OK** to start the connection.


3:48
IBM MaaS360 VPN
SELECT VPN PROFILE
VPN Swat
Configured to only work for corporate apps
Connecting

4. Select a VPN profile.


3:48
VPN
VPN PROFILES
VPN Swat
mail.maas360swat.com/vpn

When the app is connected to the MaaS360 VPN, you can tap **Disconnect** to disconnect from the MaaS360 VPN service.

Parent topic: MaaS360 VPN Module

14.11 Troubleshooting Issues with MaaS360 VPN

Troubleshooting issues with configuring MaaS360® VPN.

14.11.1 After configuring MaaS360 VPN, why am I unable to connect to the MaaS360 VPN server?

1. Open the Cloud Extender™ Configuration Tool and check the prerequisites screen to determine if there are any issues being reported
2. Open the Routing and Remote Access Service management console and select **Disable Routing and Remote Access**.
3. Reinstall the **TAP Adapter**:
    a. From a command line, enter:
        i. C:\Program Files (x86)\MaaS360\Cloud Extender\tapinstall.exe remove tapmaasvpn01
    b. Close and restart the Cloud Extender Configuration Tool
    c. Select VPN configuration and advanced to the prerequisites screen
    d. Click the **Install TAP Adapter** button
4. Repeat the steps for enabling Network Address Translation (NAT) on the outgoing interface for the MaaS360 VPN. See the procedure for enabling NAT in Installing MaaS360 VPN and Configuring the MaaS360 VPN TAP Adapter on Windows Server 2012 R2.

14.11.2 How do I uninstall the MaaS360 VPN?

1. To uninstall the MaaS360 VPN, follow these steps:
   Remove the MaaS360 VPN TAP Adapter first. From the command line, enter:
    a. `C:\Program Files (x86)\MaaS360\Cloud Extender\tapinstall.exe remove tapmaasvpn01.`
2. Uninstall the Cloud Extender software

Parent topic: MaaS360 VPN Module