



Cloud Extender Installation Guide

Contents

Chapter 1. Cloud Extender Overview . . . 1

Cloud Extender Use Cases	1
Cloud Extender Architecture	1
Basic Requirements for Cloud Extender	4

Chapter 2. Cloud Extender Installation Overview 7

Download the License Key and software	7
Install the Cloud Extender	8
Start Cloud Extender Configuration	9

Chapter 3. User Authentications Module Configuration 15

Start Authentication Module Configuration	16
Configure LDAP Integration for User Authentication	17
Configure Active Directory for User Authentication	20
Configure Cross-Forest Authentication	21
Troubleshooting Authentication Problems	22

Chapter 4. User Visibility Module Configuration 25

Start User Visibility Module Configuration	26
Configure LDAP Integration for User Visibility	27
Configure Active Directory for User Visibility	29
Restrict Active Directory Integration to the Current Domain	30
Troubleshooting User Visibility	31

Chapter 5. Exchange (2007, 2010, 2013, Office365) Integration Module Configuration 33

About Exchange Administrator Roles	36
Configure Exchange Integration	36
About Auto-Discovery Configuration	38
Enable Auto-Removal with Exchange	39
Enable Auto-Quarantine for Exchange	41
Best Practices for Exchange Auto-Quarantine	41
Exchange Integration for Real-Time Mail Notifications	43
About Throttling Policies	46
Configure Exchange Notifications	47
Configure Exchange Policies	51
Troubleshooting Exchange Integration	51

Chapter 6. Lotus Traveler Integration Module Configuration 53

Configure Lotus Traveler Integration	54
Lotus Traveler Configuration Options	56
Best Practices for Lotus Traveler Auto-Quarantine	58

Chapter 7. Certificate Authority Integration (SCEP) Overview 61

Configure for SCEP Integration	62
Use a Microsoft CA	63
Use a Symantec CA	66
Use an Entrust CA	71
About Microsoft NDES for Certificate Integration	74
Microsoft NDES Installation	75
Enable the New Certificate Template on the Certificate Authority	81
Set up the Default Certificate Template on NDES	82
Increase the Password Cache Limit on NDES	83
Increase the Maximum Query String Size on NDES	84
Restart IIS on NDES	84
Assign Policies to Devices for Certificate Delivery	85
Update a Certificate on iOS	86

Chapter 8. High Availability (HA). 87

Configure for High Availability (HA).	87
Troubleshooting High Availability	88

Chapter 9. Mobile Enterprise Gateway Module. 91

About Gateway Modes	92
Requirements and Scaling for Mobile Enterprise Gateway	92
Mobile Enterprise Gateway Architecture	94
Install the Mobile Enterprise Gateway	96
Configure Mobile Enterprise Gateway in Standalone Mode	97
Configure SSL for Direct Mode	99
About Gateway in High Availability Mode	100
Configure Gateway As HA in Relay Mode	103
Configure Gateway As HA in Direct Mode	104
Database Setup for High Availability	106
Join the Gateway to an Existing HA Cluster	109
Configure Gateway Authentication Details and WebDAV	110
Configure Intranet Proxy Settings for the Cloud Extender	112
Configure Secure Browser and Docs Access	113
Configure Secure Browser Settings	114
Configure Secure Document for SharePoint / CMIS Access	116
Configure Secure Document for Windows File Share Access	117
Portal Management Workflows	119
About Mobile App Configuration	121
Troubleshooting Mobile App Configuration	124

Chapter 1. Cloud Extender Overview

This document is intended to provide a high-level technology and architecture summary to help you understand the overall approach and to help plan and implement the MaaS360 Cloud Extender solution.

The MaaS360 Platform is a multi-tenant, cloud-based platform for managing and securing notebooks, smartphones, and tablets, and the data that resides on them. Customers using MaaS360 reap the benefits of cloud technology that offers ease of deployment and low cost. To provide integration with important systems within the customer environment, IBM offers the IBM MobileFirst Protect (MaaS360) Cloud Extender.

The patented MaaS360 Cloud Extender technology uses a lightweight agent. It can run with minimal resources; easily traverse customer proxy environments; and provide secure messaging and data transfer between the MaaS360 Platform and customer systems such as corporate email, corporate directories, and application and content servers.

The MaaS360 Cloud Extender can be downloaded from the **Setup > Services** section in the MaaS360 portal. The Cloud Extender is an application, and once installed automatically launches the MaaS360 Cloud Extender Configuration Tool. This tool can also be executed manually by an administrator after installation by opening the start menu and navigating to Cloud Extender Configuration Tool.

Cloud Extender Use Cases

The Cloud Extender is used for many scenarios in a customer's mobile program. These following use cases are most common:

- Enrollment with Corporate Active Directory credentials (User Authentication)
- Limiting enrollments to certain user groups (User Authentication)
- Creating policies for a specific ActiveDirectory/LDAP groups (User Visibility)
- Maintaining an up to date list of active devices in ActiveSync (Exchange/ActiveSync)
- Block new ActiveSync mailboxes that are configured outside of MaaS360 (Exchange/ActiveSync)
- Create Device Certificates automatically within an Internal CA for authentication to WiFi, VPN, ActiveSync/Traveler, F5/Load Balancer pass-through, SMIME, etc...
- Allowing access to internal corporate resources, such as Sharepoint, File Shares or Intranet sites (Mobile Access Gateway)

There are countless combinations of use cases for the Cloud Extender, depending on the size of the environment.

Cloud Extender Architecture

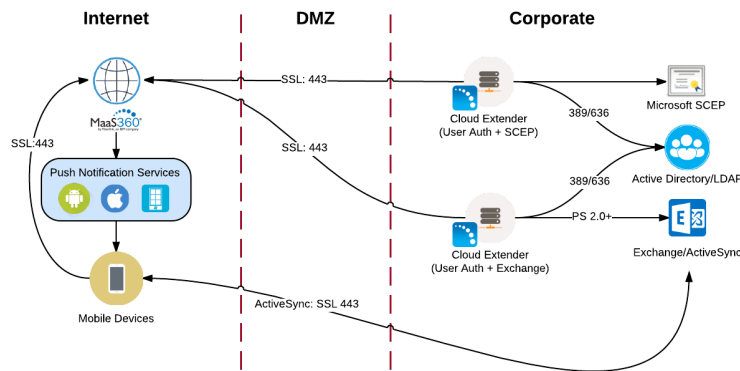
Overview

The Cloud Extender is a small Windows application (approx. 12MB) that is typically installed behind the customer firewall with network access to the appropriate internal systems. The Cloud Extender makes an *outbound connection* to the IBM MobileFirst Protect (MaaS360) Cloud or IBM MobileFirst Protect (MaaS360) On-Premise instance over port 443 (SSL AES256 encryption) and uses XMPP protocol to maintain the connection with the MaaS360 Cloud.

The Cloud Extender is proxy-aware and can automatically configure proxy settings. Once the connection is made, it is used to facilitate two-way communication between the MaaS360 Cloud and the Cloud Extender customer instance required for the integration functions. The Cloud Extender is modular, which means the Cloud Extender can use multiple services at once (ie. ActiveSync, User Visibility and User Authentication).

If a new feature is enabled, the related module and the associated configuration elements are automatically provisioned in the customer’s Cloud Extender instance. All updates are automatic unless otherwise configured. The Cloud Extender’s modular architecture provides mechanisms for module versioning and the limited release of modules to support pre-production testing.

For MaaS360 Cloud SaaS – the following diagram represents a typical small/medium sized business infrastructure incorporating SCEP, Exchange, and LDAP Authentication in High Availability.



Data Collection and Upload

The Cloud Extender periodically queries for device and corporate directory information from customer systems, and uploads it to the MaaS360 Cloud for reporting and management functions.

Resilience and Scalability

In most cases, multiple Cloud Extenders can be installed in the customer environment to provide scale and resilience, with the exception of the User Visibility. The MaaS360 Cloud is aware of all the Cloud Extender instances for a specific customer and uses them 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.

MaaS360 Real-Time Notification Services

Leveraging 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. No inbound connection is required to the Cloud Extender and therefore the Cloud Extender may be placed on the internal network.

For example, when the administrator issues a Block command for a specific device from the MaaS360 Portal (or an automated rule needs to block a device), this command is sent to the appropriate customer Cloud Extender instance. This instance executes the command using APIs available on the email server. The result of the command is sent back to the MaaS360 Cloud to close the loop.

Modules

The Cloud Extender enables “Modules” which essentially tell the cloud extender to turn on or off certain services within the portal. These modules can be enabled in conjunction with each other but be mindful of your system specifications, and ensure you have properly followed the scaling guide in the next sections.

The Cloud Extender has the following modules available:

ActiveSync Auto-Discovery, Quarantine and Blocking for MS Exchange 2007/2010/2013/Office365/BPOS-D—The Cloud Extender facilitates interaction with the Exchange Server. This allows MaaS360 to acquire information on ActiveSync-connected devices, upload device information to the MaaS360 Cloud, carry out actions (such as Approve and Block) sent from MaaS360 and apply ActiveSync device policies.

Exchange Integration for New Email Notifications (Workplace)— This is for use with a workplace persona policy that has Email Notifications enabled and applied to iOS devices using the MaaS360 container. Email notifications are not supported by third-party iOS applications in that the application is notified of changes while the app is not active. Therefore, users are not notified of new email. This integration piece allows the Cloud Extender to gain visibility into Exchange to provide devices with notifications provided by APNS to notify the user of new email.

ActiveSync Auto-discovery for Lotus Traveler and IBM Connect Cloud—The Cloud Extender facilitates interaction with information acquired from Lotus Traveler and IBM Connect Cloud about ActiveSync-connected devices, uploads device information to the MaaS360 Cloud and facilitates carrying out actions sent from MaaS360.

Corporate Directory Authentication—The Cloud Extender facilitates interaction with Active Directory and leading LDAP solutions to provide user validation as part of the self-service device enrollment and when authentication is required by policy for portal logins to the administrative portal and end user portal.

Supported LDAP Architectures:

- LDAP for Active Directory
- OpenLDAP
- Novell eDirectory
- Oracle Directory Server

- IBM Domino LDAP

User Visibility for Corporate Directory User and Group Assignments—The Cloud Extender leverages the corporate directory groups to allow for the assignment and distribution of policies, apps and docs. These groups are imported by the MaaS360 Administrator and can also be used to control administrator access. LDAP filters can be used to limit the groups and organization imported.

Certificate Authority (CA)—The Cloud Extender facilitates the automatic provisioning and distribution of digital certificates for wireless, VPN and email profiles (both Native and Secure Mail) to managed mobile devices using your existing Microsoft CA, Symantec CA, or Entrust Admin Services & Identity Guard.

BlackBerry Enterprise Server (BES)—The Cloud Extender uses the BES 5.0 Administrator APIs to provide complete visibility and control of BlackBerry devices.

Mobile Enterprise Gateway—The Cloud Extender provides gateway and relay functionality, giving secure mobile application access to behind-the-firewall information and resources such as SharePoint, Windows File Share, Connections etc. This provides a more efficient and targeted approach than traditional VPNs.

Basic Requirements for Cloud Extender

The Cloud Extender is a very scalable piece of software that can increase the depth of view and allows high availability at the click of a mouse.

Software

The Cloud Extender can be installed on a Physical or Virtual Machine with Windows Server 2012 RC2, 2012, 2008 RC2, 2008, or 2003.

Note: The Cloud Extender can be installed directly on the Exchange Server or Active Directory Server, but this is not recommended.

Before beginning the installation, make sure the following requirements are met:

Item	Meets Requirement
Physical or Virtual Machine with Windows Server 2012 RC2, 2012, 2008 RC2, 2008, or 2003.	
.NET Framework 3.5 must be installed	

Refer to the individual module sections for recommended resource sizing.

Networking

Networking with the Cloud Extender is fairly simple. The Cloud Extender makes an *outbound connection* to the MaaS360 cloud or MaaS360 On-Premises installation. The table below outlines the outbound connection requirements for each instance of MaaS360 SaaS and On-Premises. If you are on the SaaS, you can find the instance where your portal lives in two places:

1. By looking at the first digit of your Billing ID (located at the bottom of your portal after you have logged in)

2. By looking at the login URL which corresponds with the URLs in the table below.

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
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)

On-Premises
Services VM URL Port 443
Enroll VM URL Port 443
upload.fiberlink.com:80 72.21.0.0/16

Cloud Extender updates require firewall access to the MaaS360 Content Delivery service provided by dl.maas360.com which does not have a specific IP range.

In addition to the networking requirements above, **Cloud Extenders need outbound connections open to their respective module.** Eg. if you enable User Authentication for LDAP, the respective LDAP ports need to be open.

If support is needed, it is wise to open outbound connections to upload.fiberlink.com so that Customer Support remotely collect device logs from the your Cloud Extenders. This saves time and emails, and allows IBM to begin supporting you almost immediately, but is not required.

Chapter 2. Cloud Extender Installation Overview

Procedure

1. "Download the License Key and software."
2. "Install the Cloud Extender" on page 8.
3. Configure the necessary modules.
 - Chapter 3, "User Authentications Module Configuration," on page 15
 - Chapter 4, "User Visibility Module Configuration," on page 25
 - "Configure Exchange Integration" on page 36
 - "Configure Lotus Traveler Integration" on page 54

Download the License Key and software

Before you begin

Before installing the Cloud Extender, you must first acquire the application and license key. If you have not installed the Cloud Extender before, you can acquire this key via email from the MaaS360 Portal.

About this task

You need the License Key for installation.

Procedure

1. Log in to the portal with your administrator credentials.
2. Go to **Setup > Services** and for each service you want to integrate, enable the services that requires a Cloud Extender to operate.
 - Enterprise Email Integration
 - Mobile Enterprise Gateway
3. If you have never installed a Cloud Extender, do the following.
 - a. Go to **Setup > Cloud Extenders**.
 - b. Click **Download** to obtain the application for the Cloud Extender.
 - c. Click the **Send License Key** link to send the license key to your administrator email address.
4. If you have previously installed a Cloud Extender, do the following.
 - a. Go to **Setup > Services**.
 - b. Find the **Enterprise Email Integration** or **Mobile Enterprise Gateway** service and click **More...**
 - c. Click **Download** to obtain the application for the Cloud Extender.
 - d. Next, select **Click Here** to get your license key sent to your administrator email address.

If you downloaded the CE installer to a machine upon which you do not want to install the CE, copy the CE installer to correct machine to proceed

5. Launch the MaaS360 Cloud Extender installation package.

Install the Cloud Extender

About this task

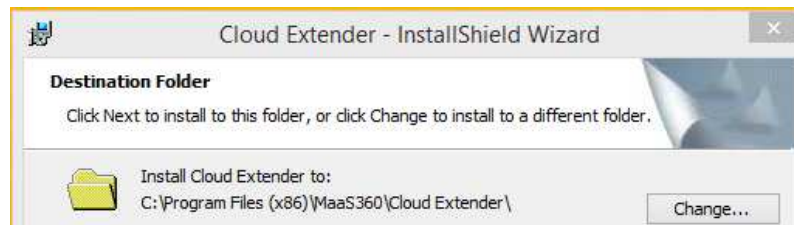
The installation of the Cloud Extender installs the base Visibility Module. This connects your Cloud Extender to your portal to download a list of available modules for configuration. In some cases, some modules are not available by default and must be enabled via the Portal through **Setup > Services**.

Procedure

1. Double Click the MaaS360 Cloud Extender installer.



2. Click **Next** to advance to the Install Location screen.
3. Choose your destination folder and click **Next**.

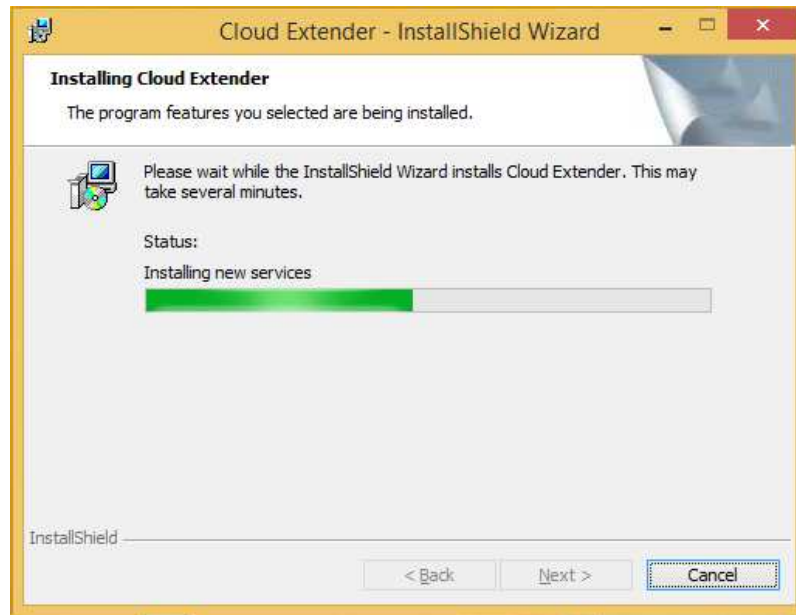


4. Enter the License Key provided to you in the Welcome Email.

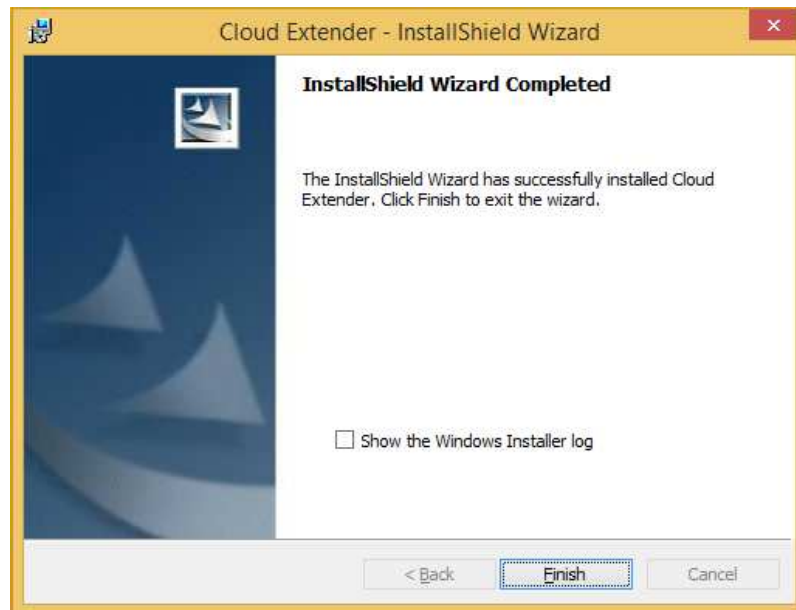


- Note:** You may have to copy and paste each section of the key at a time
5. Click **Next** to advance.

6. Click **Install** then click **Next** to continue the installation.



7. When prompted, click **Finish**.



The Cloud Extender Configuration Tool launches.

Note: After installation, the CE should launch automatically but if not, it can be launched from either the Start Menu or directly via: %Program Files (x86)%\MaaS360\Cloud Extender\ASConfig.exe

Start Cloud Extender Configuration

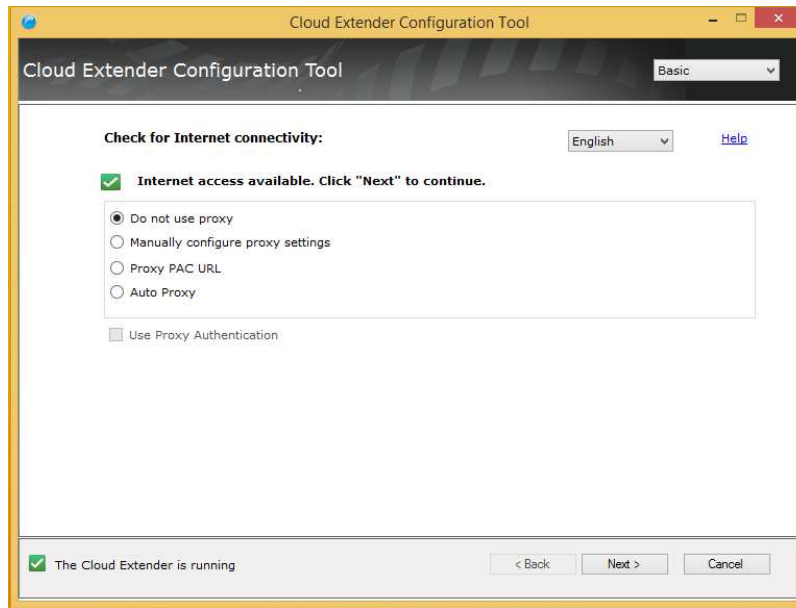
About this task

Once the Configuration Tool launches, you are guided through a set of configuration options.

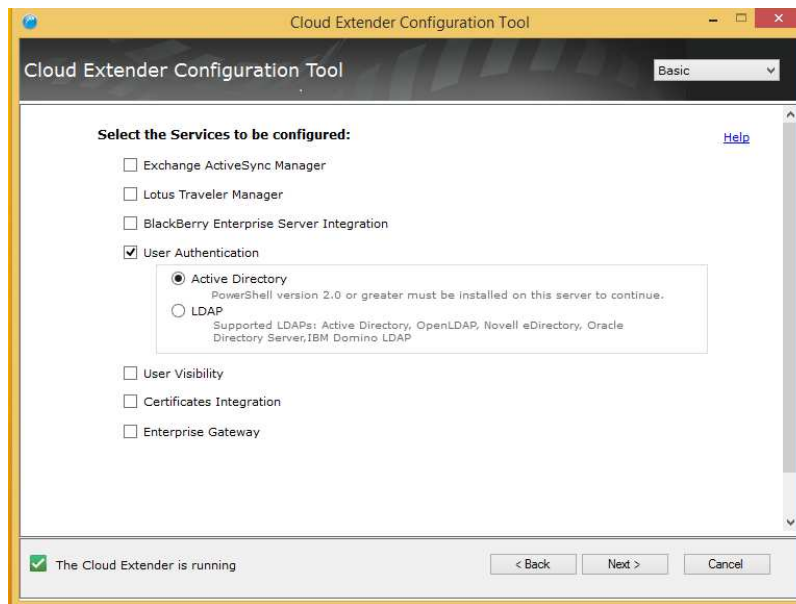
Procedure

1. Select the mode of Internet Access.
 - For manual proxy configuration, the Cloud Extender supports Direct, PAC or Auto Proxy. In addition, you have the ability to set credentials for proxy authentication.
 - If no proxy is required to reach the Internet, use the **Do not use any proxy** option

When Internet access is configured successfully a green check mark appears on the **Check for Internet connectivity** screen as seen below.



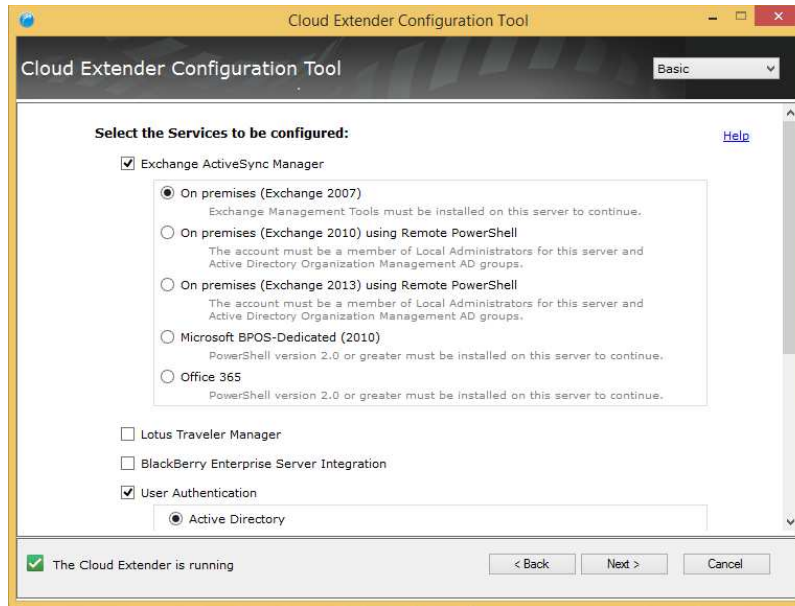
2. Click **Next** to continue to select your services.



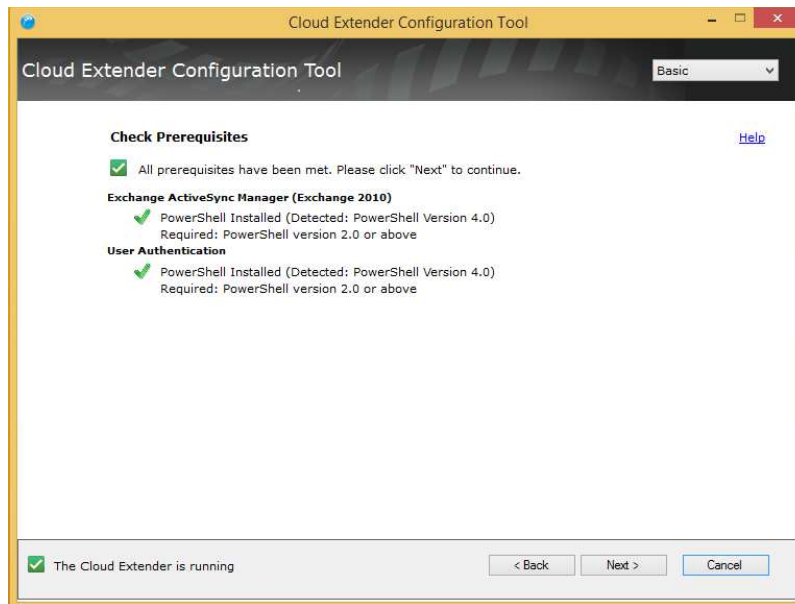
3. Note the service modules that are at your disposal and refer to the respective module's section of this document to guide you through configuration.

Important: If you are missing a module that you believe should be present, please contact your assigned IBM resource or send an email to ops@fiberlink.com with your question.

4. Once a module is selected, you see additional options displayed.

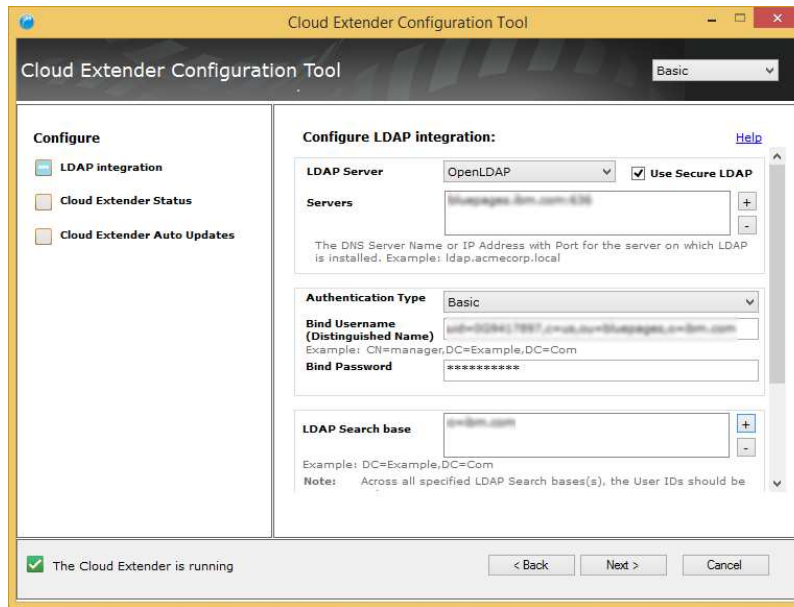


5. Select the module and options you want to configure and click **Next**.
6. Click **Next** to verify the prerequisites were met.

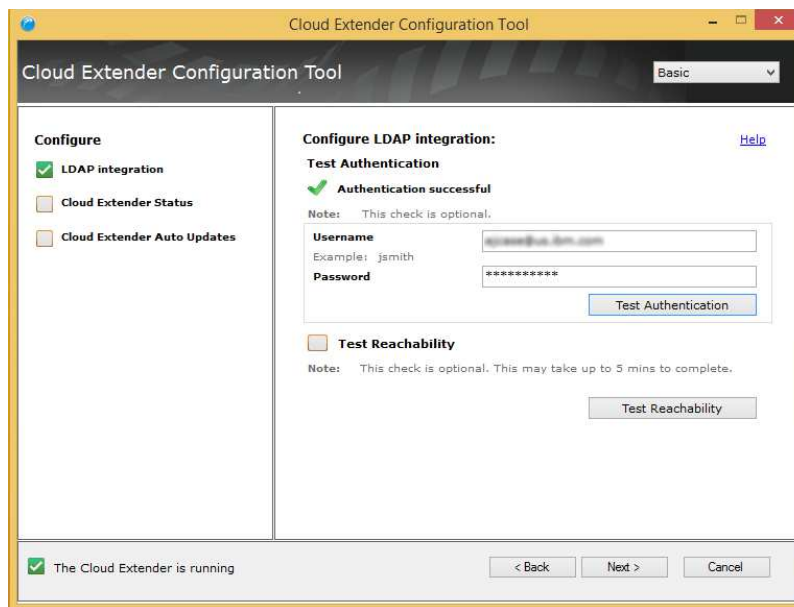


This screen could vary based on your selections.

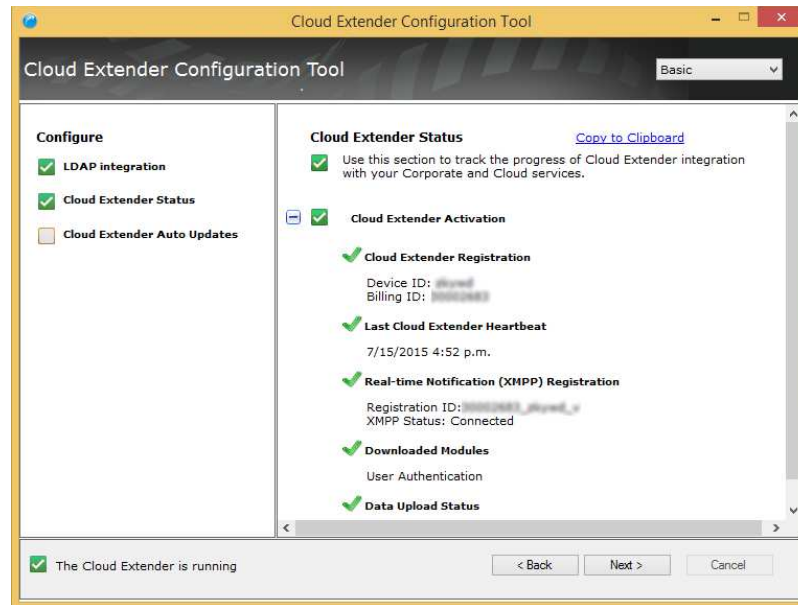
7. Click **Next** to configure the settings on each module you selected.



- Once you have configured the services and ran module test actions, click **Next** to continue.



The Cloud Extender Status screen appears with each item receiving a green check when successfully downloaded and configured with MaaS360



9. Click **Next** to proceed and enable or disable Automatic Updates to finish the configuration.

Note: Automatic Update should remain enabled so the latest modules are downloaded for the installation. After you have all the proper modules, Automatic Updates can be disabled. If the Automatic Updates check box is greyed out, that means the modules are still being downloaded.

10. Click **Finish** to close out the Cloud Extender. After a few minutes data are collected and uploaded to MaaS360. You can check this process by logging into MaaS360 via your portal URL and go to the **Setup > Manage Cloud Extenders** workflow. By this point, the Cloud Extender in the portal should show that is connected and the configured services. However, depending on the speed of your installation and the number and size of modules you enabled, you may see a slight delay.

Chapter 3. User Authentications Module Configuration

Once the Base Cloud Extender piece has been installed and the configuration tool has been launched, you need to configure your Cloud Extender for the services you want for it to perform. Find the module in the following sections that correspond with your deployment needs.

Overview

The Cloud Extender facilitates AD/LDAP authentication for the following scenarios:

- For self-service enrollment
- For use of the End User Portal to manage their device if corporate credentials were used to enroll
- When authentication is required before accessing secured applications and documents
- When a Workplace PIN is reset by the user
- When a user authenticates to the Mobile Enterprise Gateway

The Cloud Extender receives the credentials from the MaaS360 Cloud (client originated) and validates them against the customer Directory server. The credential information is passed from the client through MaaS360 to the customer Cloud Extender, and is not persistently stored in any way.

When the Cloud Extender is configured for corporate directory authentication, it performs the following activities:

1. When an authentication is required by policy, the user is prompted to enter their Directory credentials as part of the validation process. These credentials are passed to the MaaS360 Portal.
2. The credentials are then passed to the appropriate customer Cloud Extender instance.
3. The Cloud Extender binds to the Directory server using the credentials provided. If the credentials are valid, the bind is successful. The Cloud Extender sends a message back to the MaaS360 Platform indicating that the credentials are good and the validation return a success.
4. The User Authentication module can be configured with two different connection methods, Active Directory using Powershell and LDAP protocol. The requirements for both differ in many ways, therefore ensure you are using the correct requirements for your chosen implementation. It is recommended to use LDAP for most implementations for more detailed configuration steps.

Requirements and Scaling

The User Authentication module for LDAP or Active Directory is not known to have scaling limits. However the specifications recommended below are the minimum any server should have to perform this operation. You most certainly can increase these limits for better server functionality and usability.

In large environments, deploy separate Cloud Extenders instances to service Corporate Directory Integration to provide predicable performance of all functions.

Any number of Cloud extender instances can be deployed. In any situation however, it is recommended to enable two User Authentication modules on two cloud extenders for redundancy.

Scaling (for both Active Directory and LDAP implementations)

CPU	Memory	Storage	Limits
2 Cores	2-8GB	50GB	None known

Network traffic

Authentication request/response = 1 KB per request

Active Directory Requirements

Item	Meets Requirement
Hardware Specs meet minimum requirements stated above	
PowerShell 3.0+ is installed	
Windows Operating System is joined to the domain	
Service Account <ul style="list-style-type: none"> • Domain User • Password does not expire (Recommended) • Local Administrator on Cloud Extender server 	

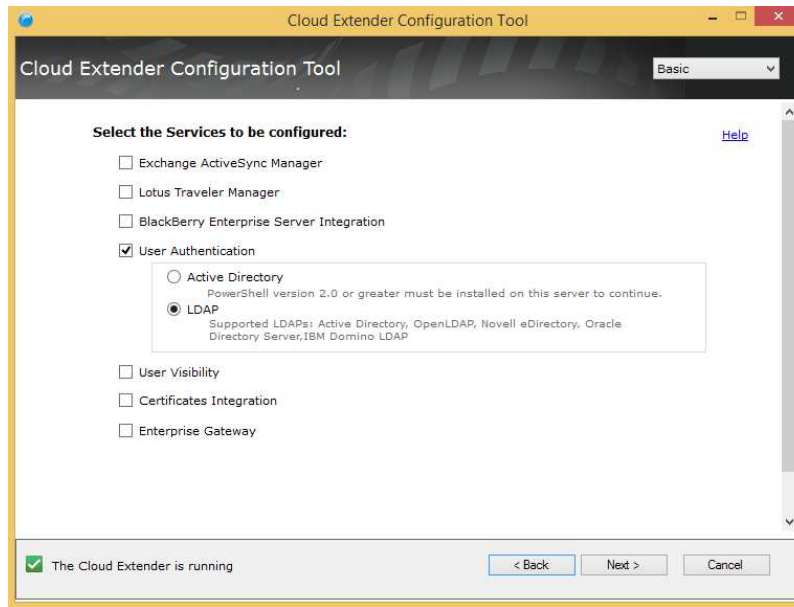
LDAP Requirements

Item	Meets Requirement
Hardware Specs meet minimum requirements stated above	
Service Account <ul style="list-style-type: none"> • User name and Password to bind to LDAP server • Password does not expire (Recommended) 	

Start Authentication Module Configuration

Procedure

1. Open the Cloud Extender Configuration Tool and enable the **User Authentication module**.
2. Choose which method of authentication you would like to configure and click **Next**.
 - “Configure LDAP Integration for User Authentication” on page 17
 - “Configure Active Directory for User Authentication” on page 20
 - “Configure Cross-Forest Authentication” on page 21



Configure LDAP Integration for User Authentication

Before you begin

Ensure connectivity to your LDAP server through telnet or any other mechanism before setting up the Cloud Extender.

About this task

Currently the Cloud Extenders supports a wide variety of LDAP Protocols:

- LDAP for Active Directory
- OpenLDAP
- Novell eDirectory
- Oracle Directory Server
- IBM Domino LDAP

Procedure

1. Choose your LDAP server protocol from the pop-up menu.
2. Check the box to the right if Secure LDAP is to be used.

Configure LDAP integration:

[Help](#)

LDAP Server **Use Secure LDAP**

OpenLDAP +

Servers

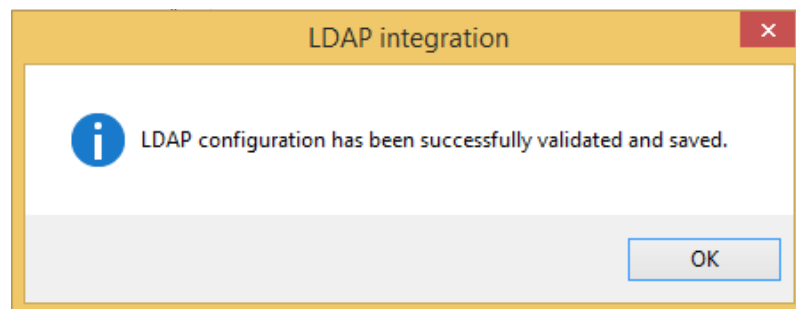
The DNS Server Name or IP Address with Port for the server on which LDAP is installed. Example: ldap.acmecorp.local

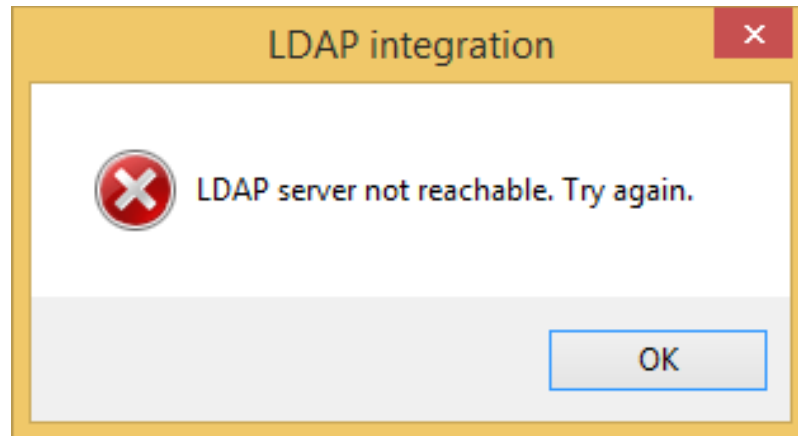
3. Click the Plus (+) sign on the right to add a new LDAP server to the list. Cloud Extender supports multiple LDAP servers if they are mirroring LDAP servers
4. Choose your Authentication type (Basic or Digest).

5. Enter the user name and password of the user you want to bind. Keep in mind this may not be your typical user name you would use to authenticate normally such as user@company.com. Most LDAP protocols use the Distinguished Name of the user to bind such as uid=username,c=us,ou=subdomain,o=company.com
6. Click the plus (+) button to add a new LDAP Search Base in Distinguished Name format.
7. Enter your user search attribute to be used for the user name upon authentication.

This varies between the LDAP types and only one attribute can be used.
Common user search attributes:

- Active Directory
 - email (user@company.com)
 - userPrincipalName (user@domain.company.com)
 - samAccountName (DOMAIN\username)
 - OpenLDAP
 - mail (user@company.com)
 - uid (user)
 - Novell eDirectory
 - mail (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)
8. Optionally, add a group to filter authentication.
Test Authentication does not inherit this filter section but restricts enrollments to this group
This option is discouraged; use the Deployment Settings workflow in the portal to define enrollment group limitations
 9. Click **Next** to validate the credentials.





If you see a failure message, verify LDAP connectivity as well as syntax of the server URL, port, user name/password, etc

10. Test the Authentication using a normal user name and password.

Configure LDAP integration: [Help](#)

Test Authentication

✓ **Authentication successful**

Note: This check is optional.

Username Example: jsmith	<input type="text" value="jsmith@us.ibm.com"/>
Password	<input type="password" value="*****"/>

11. Test Reachability so you can see how deep into the directory your service account can view.

✓ **Test Reachability**

Note: This check is optional. This may take up to 5 mins to complete.

Reachable LDAP Search Bases:	1
Number of OUs:	1
Number of Users:	1

12. Click **Next** to complete the configuration and view the connection summary.
13. Click **Next** to make adjustments to Automatic Updates if necessary.
14. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

Configure Active Directory for User Authentication

Procedure

1. Verify that your computer meets the Active Directory prerequisites.

Check Prerequisites

All prerequisites have been met. Please click "Next" to continue.

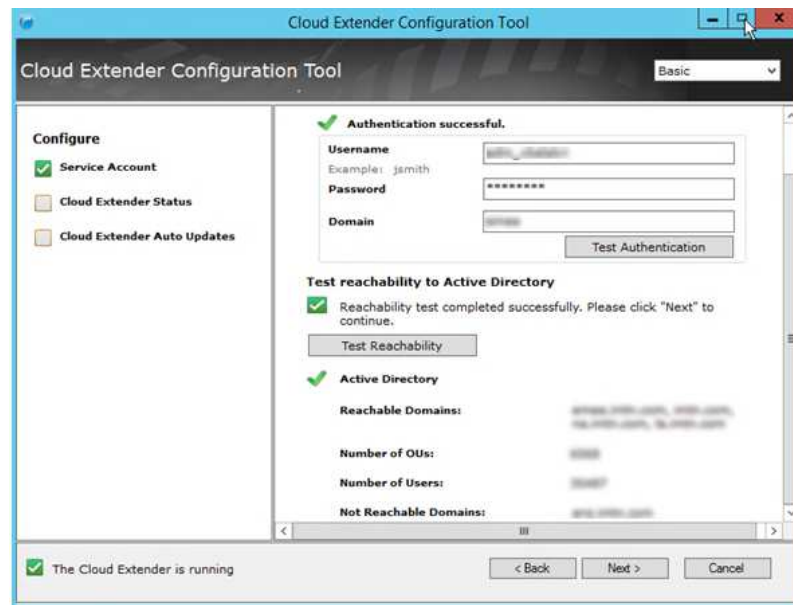
User Authentication

PowerShell Installed (Detected: PowerShell Version 4.0)
Required: PowerShell version 2.0 or above

2. Enter your user name, password and domain of the Service Account that was created for this purpose.

Note: Remember to add this user as a local administrator on server before continuing

3. Once the credentials have been validated, test the authentication with a normal user name and password.
4. Test Reachability so you can see how deep into the directory your service account can view.



5. Click **Next** to complete the configuration and view the connection summary.
6. Click **Next** to make adjustments to Automatic Updates if necessary.
7. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

Configure Cross-Forest Authentication

About this task

In some situations, a standard configuration of the Cloud Extender using the traditional workflow is not sufficient. In medium to larger enterprises where Active Directory and multi-forests and multi-domains exist, you need a special configuration.

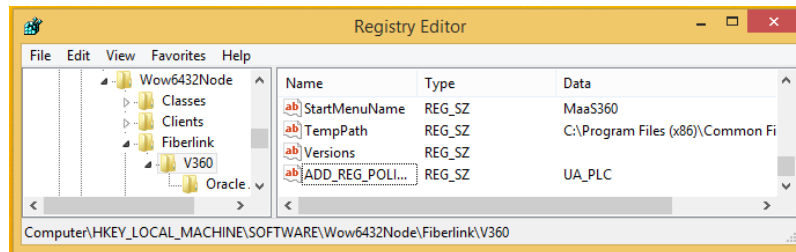
The Cloud Extender can typically only authenticate users belonging to one particular domain or domain controller. Domain Forests without trusts between them are currently not supported. However, there is a way to accomplish multi-forest/multi-domain authentication through advanced configuration of the Cloud Extender.

Registry key additions and/or modifications are needed in order for the Cloud Extender to support multi-domain/forest authentication. This must be done manually because the keys may already exist.

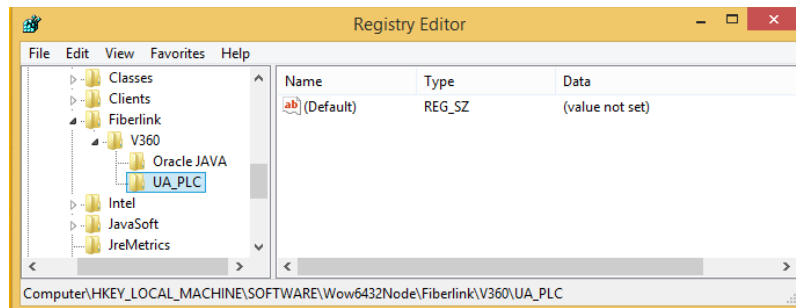
Procedure

1. Open the Registry Editor (regedit.exe) on the Cloud Extender server.
2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360.
3. Create a new String Value in the V360 Key. "ADD_REG_POLICY_GROUP"="UA_PLC"

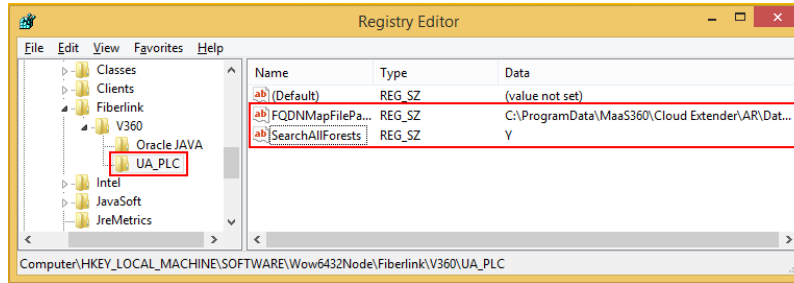
Note: This may already exist; you need to append UA_PLC to the list separated by a semicolon (;)



4. Create a new key under the V360 key named UA_PLC. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\UA_PLC



5. Create two new string values under UA_PLC. "FQDNMapFilePath"="C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data\FQDNMap.txt"
"SearchAllForests"="Y"



6. Create a new text file called *FQDNMap.txt* 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

As per the above example, the file contents should look like the following, with the short domain on the left side of the "=" sign and the FQDN on the right. It is very important to map both combinations. shortDomainName = FQDN
FQDN = FQDN

Example

```
palm = palm.f01.example.local
maple = maple.f01.example.local
oak = oak.example.local
palm.f01.example.local = palm.f01.example.local
maple.f01.example.local = maple.f01.example.local
oak.example.local = oak.example.local
```

Each line in the file must be terminated with either a <CRLF> (DOS line ending convention) or a <LF> (UNIX line ending convention.)

Tip: Create this file in notepad so there is not any doubt about the line termination

7. Save the file as *FQDNMap.txt*.
8. Copy the FQDN Map File "*FQDNMap.txt*" to the folder *C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data*.
9. Restart the Cloud Extender Service.
10. Test authentication again on all domains to verify the configuration is complete.

What to do next

If multiple Cloud Extenders are implemented in an HA fashion, implement the same steps on all Cloud Extenders that have the User Authentication module enabled (including any new Cloud Extenders added in the future).

If Implementing the Mobile Enterprise Gateway, these advanced authentication settings are need as well.

Troubleshooting Authentication Problems

Authentication and Reachability Errors during Setup

When setting up the Cloud Extender for User Authentication, you can debug the errors by accessing the log: *C:\%ProgramData%\MaaS360\Cloud Extender\AR\Data.*

Review the *LDAPAuthTest_Debug.log* and *LDAPReachability_Debug.log* to review the error messages.

Users Cannot Authenticate when Enrolling 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 gzip format. The newest EMSAgent log says 0kb in size, but open the file to display the data.

To find the Authentication success or failure, you can search for `LDAP-AUTH`, `AuthStatus: Success`, or `AuthStatus: Failure`.

High Availability – Find which Cloud Extender was used for authentication

When multiple Cloud Extenders are used for User Authentication High Availability, MaaS360 uses a round-robin style authentication to equally balance requests to all Cloud Extenders. However, knowing which Cloud Extender was used for authentication is not always straight forward.

To find the Cloud Extender that was 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 are looking for, you can search for the record by using the workflow underneath the Action History headline.



Once you have found the record, you can see on the first and third columns which Cloud Extender was used. The first column gives the Computer Name and the third column gives you the device ID. Debug the issue now by logging into the Cloud Extender server and obtain the EMS agent logs looking for failures using the LDAP-AUTH search string.

The image shows a table of Action History records. The table has columns: Device Name, Platform, Device ID, Action Date, Action, and Action By. The first row of data shows: Device Name: W098-8206, Platform: (Cloud Extender), Device ID: 810001, Action Date: 07/16/2015 23:18 EDT, Action: User Authentication, Action By: josh@msa.com.

Device Name	Platform	Device ID	Action Date	Action	Action By
W098-8206	(Cloud Extender)	810001	07/16/2015 23:18 EDT	User Authentication	josh@msa.com

Chapter 4. User Visibility Module Configuration

Overview

The MaaS360 Cloud Extender collects Organization Units (OU), containers and user information from the corporate directory and sends the information to populate user information in the MaaS360 Cloud. This user and group information facilitates grouping for the assignment and distribution of policies, apps and docs as well as administrative role-based access.

When the Cloud Extender is configured for the corporate directory for user visibility, it performs the following actions:

1. Initially, the MaaS360 Cloud Extender connects to the corporate directory and retrieves user and OU information for the configured domains, which is stored in local temporary files
2. The information in the temporary file is parsed into structured messages
3. The messages are uploaded to the MaaS360 Cloud
4. The process is repeated periodically, and changes are processed and uploaded in delta messages
5. OUs without users in them are not be imported to the MaaS360 portal.

Scaling for Active Directory

Customers with a single domain or a forest with multiple cross-forest trusted domains.

	< 10000 users	10000-20000 users	20000-40000 users	> 40000 users
CPU	2 Cores	2 Cores	2 Cores	Use LDAP Configuration for AD
Memory	2 GB	2 GB	4 GB	

Scaling for LDAP

Supports AD, Oracle, Lotus, Novell, and Open LDAP **users 10000 - 100000 users**

	< 100000 users	> 100000 users
CPU	2 Cores	2 Cores
Memory	2 GB	4 GB

Network Traffic

Traffic exchange between MaaS360 Cloud Extender and LDAP/AD

- First time upload data usage: 0.5 MB
- Steady state data usage per month: 90 MB

Traffic between MaaS360 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 lined for 1000 users
- Data upload frequency
 - Incremental Data upload frequency = 4 hours
 - Full Data upload frequency = 1 week
- Environment change
 - On every incremental query, 1% of users have attribute changes
- Average data packet size per user = 0.5 KB
- Average ratio of encryption & compression of data uploaded to MaaS360 = 70%

LDAP Requirements

Item	Meets Requirement
Hardware Specs meet minimum requirements stated above	
Service Account <ul style="list-style-type: none"> • User name and Password to bind to LDAP server • Password does not expire (Recommended) 	

Active Directory Requirements

Item	Meets Requirement
Hardware Specs meet minimum requirements stated above	
PowerShell 3.0+ is installed	
Windows Operating System is joined to the domain	
Service Account <ul style="list-style-type: none"> • Domain User • Password does not expire (Recommended) • Local Administrator on Cloud Extender server 	

Start User Visibility Module Configuration

Procedure

1. Open the Cloud Extender Configuration Tool and enable the User Authentication module.
2. Choose which method of authentication you would like to configure and click **Next**.

Configure LDAP Integration for User Visibility

Before you begin

Ensure connectivity to your LDAP server through telnet or any other mechanism before setting up the Cloud Extender.

About this task

Currently the Cloud Extenders supports a wide variety of LDAP Protocols:

- LDAP for Active Directory
- OpenLDAP
- Novell eDirectory
- Oracle Directory Server
- IBM Domino LDAP

Procedure

1. Choose your LDAP server protocol from the pop-up menu.
2. Check the box to the right if Secure LDAP is to be used.

Configure LDAP integration:

[Help](#)

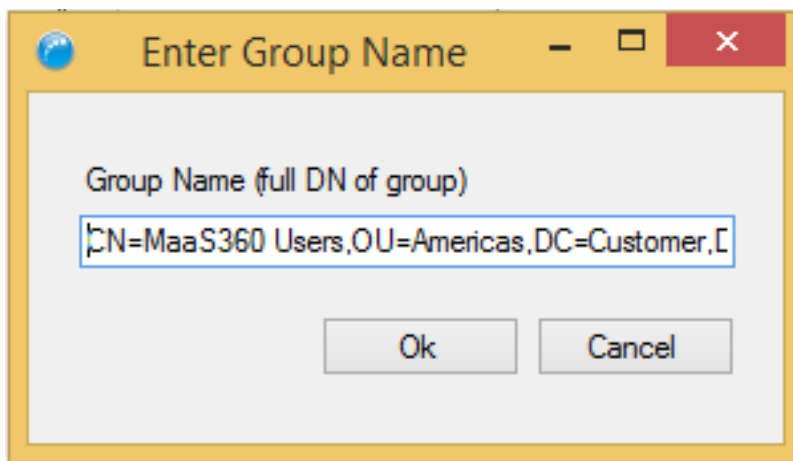
The screenshot shows a configuration window for LDAP integration. At the top, there is a label "Configure LDAP integration:" and a "Help" link. Below this, there is a form with the following elements: a "LDAP Server" dropdown menu currently showing "OpenLDAP", a checked checkbox labeled "Use Secure LDAP", and a "Servers" list box. To the right of the "Servers" list box is a plus sign (+) button. Below the list box is a text input field with a plus sign (+) button to its right. Below the input field is a note: "The DNS Server Name or IP Address with Port for the server on which LDAP is installed. Example: ldap.acmecorp.local".

3. Click the Plus (+) sign on the right to add a new LDAP server to the list. Cloud Extender supports multiple LDAP servers if they are mirroring LDAP servers
4. Choose your Authentication type (Basic or Digest).
5. Enter the user name and password of the user you want to bind. Keep in mind this may not be your typical user name you would use to authenticate normally such as user@company.com. Most LDAP protocols use the Distinguished Name of the user to bind such as uid=username,c=us,ou=subdomain,o=company.com
6. Click the plus (+) button to add a new LDAP Search Base in Distinguished Name format.
7. Enter your user search attribute to be used for the user name upon authentication.

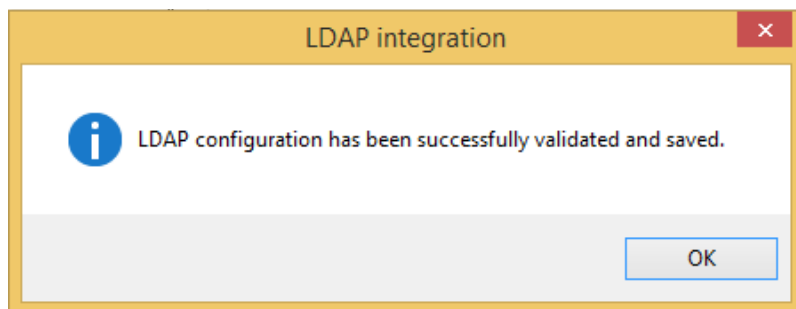
This varies between the LDAP types and only one attribute can be used. Common user search attributes:

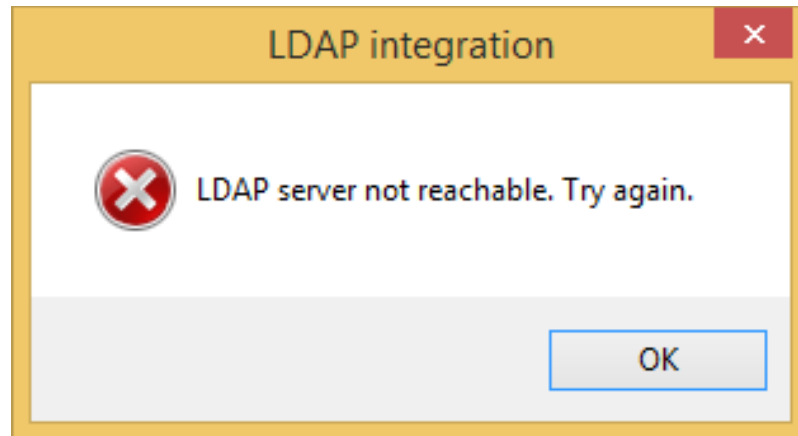
- Active Directory
 - email (user@company.com)
 - userPrincipalName (user@domain.company.com)
 - samAccountName (DOMAIN\username)
- OpenLDAP
 - mail (user@company.com)
 - uid (user)
- Novell eDirectory

- mail (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)
8. Filter on groups to limit the number of users/groups uploaded to MaaS360. Multiple groups can be added here. This filter is meant to stop MaaS360 from uploading every user in the LDAP environment. Start very granular and open it up as you get comfortable.



9. Optionally, add a group to filter authentication. Test Authentication does not inherit this filter section but restricts enrollments to this group. This option is discouraged; use the Deployment Settings workflow in the portal to define enrollment group limitations.
10. Click **Next** to validate the credentials.





If you see a failure message, verify LDAP connectivity as well as syntax of the server URL, port, user name/password, etc

11. Test Reachability so you can see how deep into the directory your service account can view.

Test Reachability

Note: This check is optional. This may take up to 5 mins to complete.

Test Reachability

Reachable LDAP Search Bases: "dc=example,dc=com"
Number of OUs: 4
Number of Users: 1


12. Click **Next** to complete the configuration and view the connection summary.
13. Click **Next** to make adjustments to Automatic Updates if necessary.
14. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

Configure Active Directory for User Visibility


Procedure

1. Verify that your computer meets the Active Directory prerequisites.

Check Prerequisites

 All prerequisites have been met. Please click "Next" to continue.


User Authentication

 PowerShell Installed (Detected: PowerShell Version 4.0)
Required: PowerShell version 2.0 or above

2. Enter your user name, password and domain of the Service Account that was created for this purpose.

Note: Remember to add this user as a local administrator on server before continuing

3. Once the credentials have been validated, test the authentication with a normal user name and password.
4. Test Reachability so you can see how deep into the directory your service account can view.

 **Test Reachability**

Note: This check is optional. This may take up to 5 mins to complete.

Test Reachability

Reachable LDAP Search Bases: 1
Number of OUs: 4
Number of Users: 1

5. Click **Next** to complete the configuration and view the connection summary.
6. Click **Next** to make adjustments to Automatic Updates if necessary.
7. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

Restrict Active Directory Integration to the Current Domain

Get data from current Active Directory domain only.

About this task

The User Visibility Module usually gets data from the whole AD, but it provides flexibility to get data only from the current domain based on a policy value (or) using a registry key setting.

Procedure

Create the following registry keys on the Cloud Extender Server. **X86 (32-bit Windows)**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Fiberlink\V360]
"ADD_REG_POLICY_GROUP"="AD_UV_PLC"
[HKEY_LOCAL_MACHINE\SOFTWARE\Fiberlink\V360\AD_UV_PLC]
"CurrentDomainUsersOnly"="Yes"
```

X64 (64-bit Windows)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360]
"ADD_REG_POLICY_GROUP"="AD_UV_PLC"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\AD_UV_PLC]
"CurrentDomainUsersOnly"="Yes"
```

Troubleshooting User Visibility

No user or group information in MaaS360

Verify reachability to the LDAP/AD server using the Cloud Extender Configuration Tool

Verify OUs that have been targeted have at least 1 within that OU and not two levels deep

Why OUs under system containers are not shown in MaaS?

Module does not get any data from System Containers. They are AD built-in objects and not usually users are created under it, they are being excluded during data collection.

User Visibility Module queries too often and is affecting LDAP/AD resources

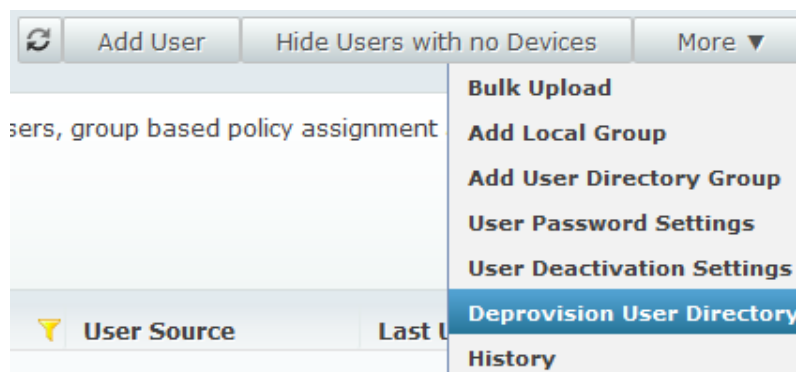
If a customer has tens, or hundreds, of thousands of users, groups, and OUs then pulling this information every 4 hours may burden servers.

In the portal, go to **Setup > Manage Cloud Extender Settings** and change the policy to run the scripts once every 24 hours.

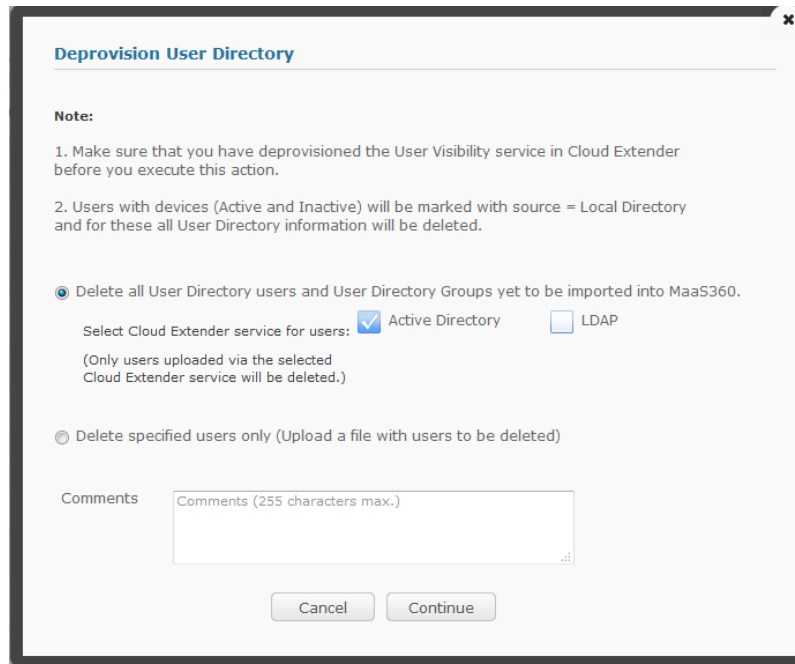
Help! I turned on User Visibility and every user in the Corporate Directory was imported!

Many times, customers setup the Cloud Extender to point to AD during configuration for User Visibility which results in all users being imported to MaaS360. Naturally, this was not the intention, and a purge of old user records. Customers can now accomplish this in the MaaS360 workflow. Users can be purged in two different ways, all users or via an uploaded CSV file. A sample file is available in the MaaS360 Workflow.

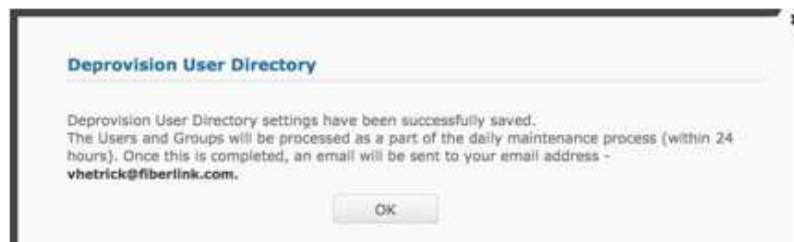
1. Go to **Users > Directory**
2. Click the **More** pop-up to the far right and choose **Deprovision User Directory**.



1. Follow the prompts on the screen to either remove all users from the AD or LDAP or to upload a file to remove users.



2. Click **Continue**, a confirmation message appears after entering your password.
 - a. If you use the file upload, the number of users to be removed are also displayed.
 - b. The admin receives an email when the job is finished.



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

Chapter 5. Exchange (2007, 2010, 2013, Office365) Integration Module Configuration

Overview

The Cloud Extender provides visibility into all existing devices connected to the mail system and enables auto-quarantine functionality to prevent new devices from connecting without authorization. The Cloud Extender performs a number of functions on behalf of the MaaS360 Cloud to provide visibility and management of ActiveSync-connected devices. The Cloud Extender performs the following activities when integrated with Exchange:

- Queries the Exchange server using Microsoft PowerShell commands and standard APIs for information related to the ActiveSync-enabled devices. Using PowerShell and related APIs allows for abstraction from the specifics of the Exchange server implementation and allows the Cloud Extender to support multiple mailbox servers and clustered/resilient Exchange server configurations.
- Processes device and policy information, and transmits it to the MaaS360 Portal for reporting and management functions.
- Retrieves ActiveSync policy information from the ActiveSync Server.
- Receives ActiveSync policies, actions and policy assignments, and carries out the relevant actions on the ActiveSync server.
- The device and policy information collected is uploaded to MaaS360 to facilitate reporting and management workflows.
- At predetermined intervals, the Cloud Extender looks for changes in the data and policies on the ActiveSync server and any new data is provided to MaaS360.

When the administrator requests a device action be performed on the ActiveSync server (Wipe, Policy Change, Block Approve, Remove), the action request is sent to the appropriate customer instance of the Cloud Extender and the Cloud Extender executes the requested commands on the server and returns the status to MaaS360.

Important: It is important to note that our Integration with ActiveSync is not an email proxy. In other words, the Cloud Extender does not sit between email and devices. This integration is simply for visibility into your ActiveSync environment to give you the ability to take actions upon devices that are connected to ActiveSync as well as apply compliance rules and remediation to those devices that may not be enrolled in MaaS360 but are enrolled in ActiveSync.

Scaling Requirements Overview

The following tables provide guidance on how to size the machine that the Cloud Extender(s) requires to operate effectively and how many instances of the Cloud Extender are required to service large and complex Exchange/ActiveSync environments.

In large environments the following guidelines should be followed:

- The number of mailboxes and connected devices should be balanced across mailbox servers.
- Device data gather times should not exceed 60 minutes and should average between 25 and 40 minutes for 5000 devices. Current and average gather times are available on the Cloud Extender Status page within the MaaS360 portal.

- A rule of thumb to determine the number of Cloud extender instances required to effectively service the environment is to divide the potential number of ActiveSync connected devices by 5000 and the number of Mailboxes by 10,000 and use the higher of the two values to arrive at the number of Cloud Extenders instances required.

For example, an Exchange 2010 environment with 30,000 Mailboxes and 20,000 Connected Devices that does not have Auto-Quarantine enabled would require: Greater of (30,000/10,000 or 20,000/5000) = 4 Cloud Extender instances.

Important: Gather times should be closely monitored. If they start to consistently exceed 60 minutes, additional Cloud Extenders should be considered.

Exchange 2007 using Exchange Management Tools

Mailboxes	< 5000	5000-10000	> 10000 mailboxes
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Devices	< 2500	2500-5000	> 5000 devices
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Exchange 2010/13 using PowerShell

Mailboxes	< 5000	5000-10000	> 10000 mailboxes
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Devices	< 2500	2500-5000	> 5000 devices
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Exchange 2010/13 using PowerShell with Auto-Quarantine

Mailboxes	< 2500	2500-5000	> 5000 mailboxes
CPU	2 Cores	2 cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Devices	< 1250	1250-2500	> 2500 devices
CPU	2 Cores	2 cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Office365 using Remote PowerShell

	All Devices
CPU	2 cores
Memory	8 GB

Network Traffic

Traffic between Exchange server and MaaS360 Cloud Extender:

- First time upload data usage: 3.35 MB
- Steady state data usage per month: 8872.75 MB

Traffic between MaaS360 Cloud Extender and MaaS360:

- First time upload data usage: 1 MB
- Steady state data usage per month: 95.75 MB

Test Metrics:

- 1000 devices
 - Incremental Data upload frequency = 15 mins
 - Heartbeat frequency = 1 hour
 - Full Data upload frequency = 1 week
- Environment Change
 - On every incremental query, 1% of device have attribute changes
 - All the devices are online; all devices heartbeat every hour
- Data packet size
 - 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 & compression of data uploaded to MaaS360 = 70%

Permission Requirements

Item	Meets Requirement
Exchange Server 2007, 2010, or 2013; Office 365; BPOS-D	
Domain User and Local Admin access is required on the machine the Cloud Extender is installed on	
Exchange Organization Administrator (2007), Organization Management (2010/2013)	
Office 365 Only: One Global Administrator Account per 1000 devices	
Exchange 2007 Only: Exchange Management Tools (The tools version must match the service pack version of the Exchange server itself).	

Item	Meets Requirement
PowerShell 3.0+	

About Exchange Administrator Roles

To perform various functions against an exchange server environment, the user account being used to execute actions must have the proper access rights defined within the Active Directory domain. Microsoft has pre-defined 4 access role groups to delegate these rights:

- Exchange Organization Administrators – The highest access group, which grants full rights over the Exchange organization.
- Exchange Recipient Administrators – Allows full access mailbox level rights for the assigned users, while restricting access to organization level settings
- Exchange View-Only Administrators – Allows full view (read-only) access at both the organization and recipient levels.
- Exchange Server Administrators – Allows full access rights at the Exchange server level, while restricting the access to read-only at an organization level

With Exchange 2007, it is not possible to grant a subset of the rights associated with each of these roles to a particular user account. Therefore, in order to have any of the rights associated with Exchange Organization Administrators, the user account must have all rights associated with that role.

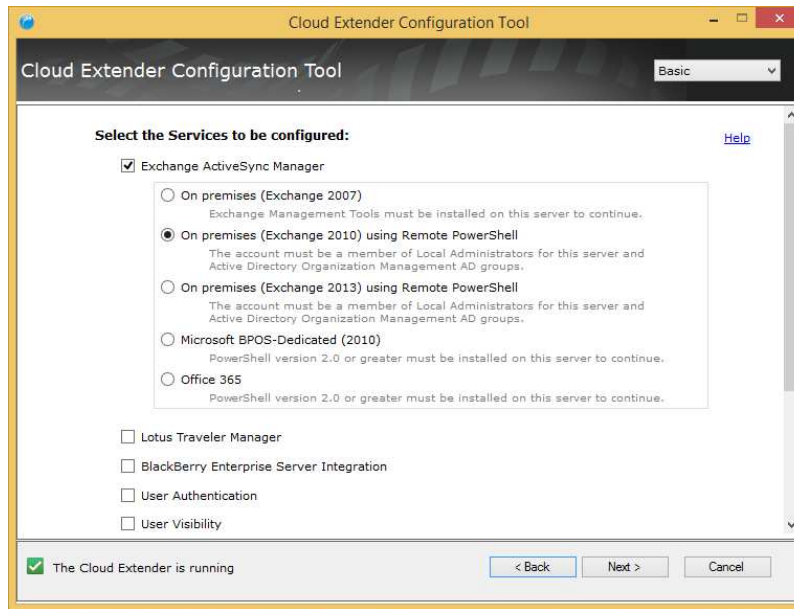
In Microsoft Exchange Server 2010, Microsoft has added a Role Based Access Control (RBAC) feature that allows for the creation of customized Exchange Access Roles. These custom roles can be limited to specific subsets of commands and functionality from the various pre-defined roles. Unfortunately, this level of granularity has not been implemented with Exchange 2007.

There are several functions performed by the MaaS360 Cloud Extender that require the rights associated with the Exchange Organization Administrator's role. These functions include creating, editing, and deleting ActiveSync policies, wiping of ActiveSync devices, and removing ActiveSync devices from the exchange server.

Configure Exchange Integration

Procedure

1. Open the Cloud Extender Configuration Tool and enable the Exchange ActiveSync Manager.
2. Choose your integration server type you use for Exchange integration, click **Next**.

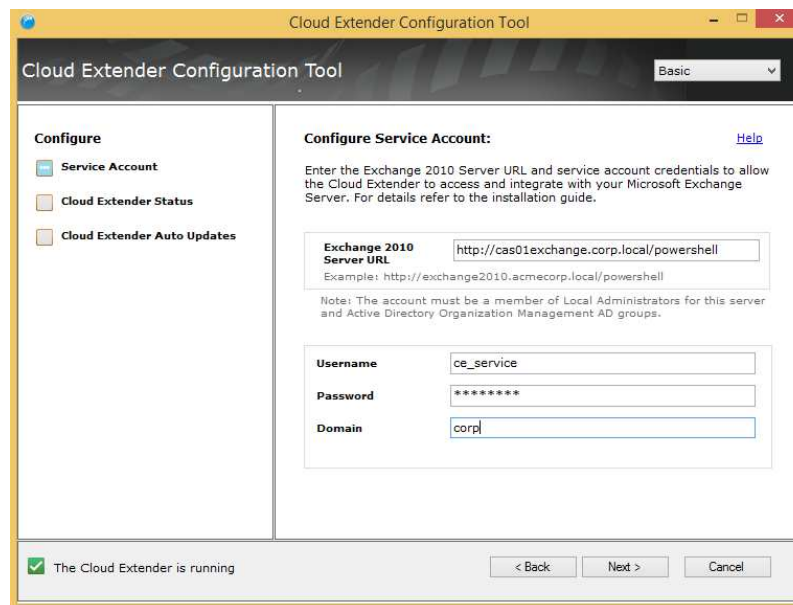


3. The tool checks to see if the necessary applications are installed. If they are, click **Next**.
4. If you are configuring Exchange 2007, 2010, and 2013, do the following.
 - a. Enter your Remote PowerShell URL: `http://<CAS_SERVER_FQDN>/PowerShell`.

Note: Do not use your ActiveSync URL here or a CAS Array. You must use a single CAS server.

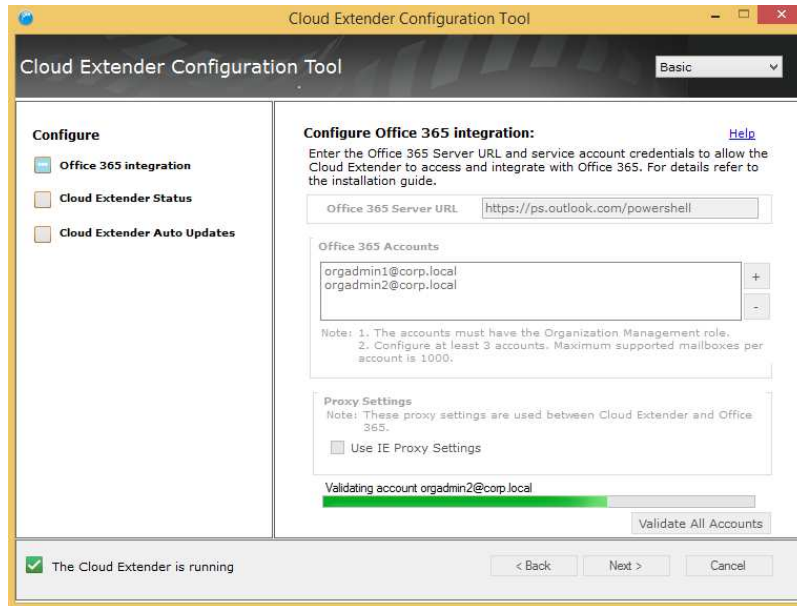
- b. Enter your MDM Service account credentials.

Note: Org Admin user created for Exchange 2007+ or Global Admin for O365



- c. Click **Next** to validate the configuration.
5. If you are configuring Office 365, do the following.

- a. Click the (+) sign to add your global administrator accounts to the Cloud Extender.
- b. Click “Validate All Accounts” at the bottom right corner of the window.



6. Click **Next** to complete the configuration and view the connection summary.
7. Click **Next** to make adjustments to Automatic Updates if necessary.
8. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

Note: Expect devices to start importing into your MaaS360 portal within a few hours depending on the size of your environment. Watch the Cloud Extender logs to view this in real-time.

About Auto-Discovery Configuration

The MaaS360 integration with Exchange/ActiveSync provides auto-discovery of devices within the ActiveSync environment. This includes all connected devices within the environment with no limit on when the last sync occurred. Devices are imported into the portal as they are discovered. Access the Auto-Discovery settings in the portal by navigating to **Setup > Cloud Extender Settings**. Make adjustments as needed and use the list below to make your decisions.

Data Collection Frequency

Device Data Query Frequency*
Frequency at which Exchange Server is queried to determine changes to Device data. Every 15 minutes

Device Heartbeat Query Frequency*
Frequency at which Exchange Server is queried to determine changes to Last Reported date of devices into Exchange Server. Every hour

Full Data Refresh Day*
Day of the week on which all device and policy data is uploaded from Exchange Server to ensure all data is in sync. The Refresh will start at a random time on the specified day. Sunday

Full Data Refresh Frequency*
Frequency at which all device and policy data is uploaded from Exchange Server. Every week

Device Data Query Frequency

Frequency at which Exchange Server is queried to determine changes to Device data.

Available Options:

- Every 15 minutes, Every hour, Every 4 hours, Every 8 hours, Every day

Tip: In larger environments, increase the amount of time between data queries for better server performance.

Device Heartbeat Query Frequency

Frequency at which Exchange Server is queried to determine changes to Last Reported date of devices into Exchange Server.

Available Options:

- Every hour, Every 4 hours, Every 8 hours, Every day

Full Data Refresh Day

Day of the week on which all device and policy data is uploaded from Exchange Server to ensure all data is in sync. The Refresh starts at a random time on the specified day.

Available Options:

- Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Full Data Refresh Frequency

Frequency at which all device and policy data is uploaded from Exchange Server. This is coupled with the Full Data Refresh Day option (ie. Every alternate week on Sunday).

Available Options:

- Every week, Every alternate week, Every 4th week

Enable Auto-Removal with Exchange

About this task

ActiveSync may not be setup to remove old records from its database and users generally do not clear their old device associations after configuring new devices. Customers should turn this feature on to have MaaS360 automatically remove records of devices that have not synced in a certain time frame to maintain a clean environment.

It is recommended to enable Auto-Removal before enabling Auto-Quarantine and/or applying compliance rules to enforce enrollment.

Automated removal of old ActiveSync records

Time Period for automated removal*
Automatically remove ActiveSync devices not reported in this specified period. Last 90 days

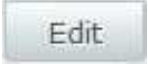
Frequency of running the automated removal job*
Every week

Day of week on which automated removal job is initiated*
Friday

Time to start automated removal job
Time specified in server timezone. If not specified, the process will start at a random time on the specified day. 05:00

Find additional troubleshooting information at <http://knowledge.fiberlink.com/display/visibility/FAQ+++CE+Exchange+ActiveSync+module>.

Procedure

1. Log into the portal as an administrator.
2. Go to **Setup > Cloud Extender Settings**.
3. Choose **Exchange ActiveSync** and click  at the upper right.
4. Check the box at the bottom of the screen labeled “Enabled Automated removal of old ActiveSync records”.

Enable Automated removal of old ActiveSync records

You are given a few options to configure the removal process

- Time Period for automated removal
 - Last 30 days
 - Last 60 days
 - Last 90 days (most common)
 - Last 180 days
 - Frequency of running the automated removal job
 - Every week (most common)
 - Every alternate week
 - Every 4th week
 - Day of week on which automated removal job is initiated
 - Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
 - Time to start automated removal job
 - Hour in GMT +0 time (hh:mm)
5. To view the last time the automated removal command ran on the server, go to **SETUP > Cloud Extenders**, then select your Cloud Extender with Exchange Integration implemented.
 6. Click **Summary > Exchange ActiveSync**. Under the Automated Removal Settings section, you see the last time the Cloud Extender ran the removal command and how many devices were deleted at that time.

Automated Removal Settings			
Automated Removal of old ActiveSync records	Yes	Last Automated Removal execution date/time	07/17/2015 06:49 EDT
Devices removed	60		


Enable Auto-Quarantine for Exchange

About this task

The Auto-Quarantine feature allows MaaS360 to automatically block newly discovered devices on your ActiveSync server if those devices are not enrolled in MaaS360. When the discovery module of the Cloud Extender finds a new device with ActiveSync configured and not enrolled in MaaS360, that device's mailbox is immediately quarantined.

Note: Once this is saved and published, your settings take effect immediately and any new device discovered is blocked if not enrolled in MaaS360. Enable Auto-Quarantine only when ready.

Procedure

1. Log in to the Portal with Administrator credentials.
2. Go to **Setup > Cloud Extender Settings**.
3. Choose Exchange ActiveSync and click  at the upper right.
4. Under the Auto-Quarantine Settings section, change the "Auto-Quarantine any new device discovered" selection to "Enable".



Best Practices for Exchange Auto-Quarantine


Communicate

Customers are advised to communicate when Auto-Quarantine is enabled. Provide help desk FAQs and emails to company workforce to be notified that on a certain date, users can no longer connect to ActiveSync by any other means other than through MaaS360. Communicate to users that they need to remove their Native Mail or other MDM and enroll in MaaS360. Let them know that on the migration day, they would be out of compliance. This can be done in waves as well as by operating system (if you want to migrate all iOS devices first, and another OS second). Wave deployments are a good idea to give the company's help desk a chance to work on one Operating System at a time.

Once communication has been performed, set up the infrastructure to handle the migration.

Create an Unenrolled ActiveSync Device Group

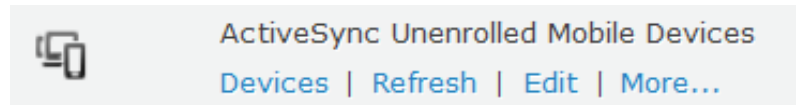
It is important to isolate devices that are not MaaS360 managed and connected to ActiveSync.

1. Go to **Devices > Groups** and click  at the upper right.
2. Within the advanced search, choose:
 - Active Devices

- Last reported in (Last 90 days)

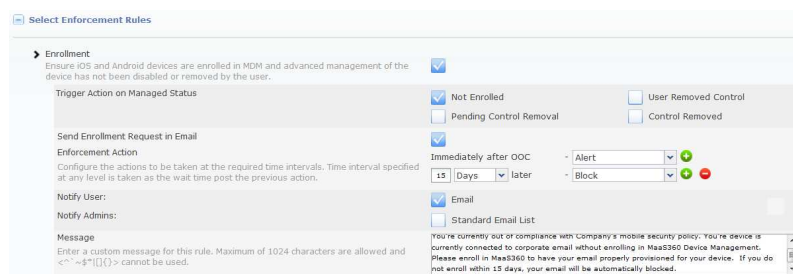
Note: Make this setting equal to the setting that is set in “Time Period for automated removal” in the Cloud Extender Settings.

3. **Device Type:** Smartphones and Tablets checked
1. **Condition 1:** Hardware Inventory > Managed status > Equal To > Not Enrolled
2. **Condition 2:** Hardware Inventory > Mailbox Managed > Equal To > ActiveSync Managed
3. **Condition 3:** Operating System > OS Name > Contains > Android (If enrolling Android)
4. **Condition 4:** Operating System > OS Name > Contains > iOS (If enrolling iOS)
5. **Condition 4:** Operating System > OS Name > Contains > Windows Phone (If enrolling Windows Phones)
6. **Apply Advanced Criteria:** 1 AND 2 AND (3 or 4 or 5)
If you're not enrolling a certain OS, remove that condition from the advanced criteria.



Use Compliance Configuration

Create a compliance rule specifically for devices that are unenrolled in MaaS360 but are ActiveSync Managed. It is advised to create this group before creating this policy. Enable Enrollment Enforcement within the compliance rule and select the following options:



Assign Compliance Rule to Group

When ready, assign the compliance rule to the group created before and immediately your devices are notified that they must enroll their device within a certain time-frame or their devices are blocked from using corporate email.

Exchange Integration for Real-Time Mail Notifications

Overview

As a part of the MaaS360 Secure Productivity Suite, MaaS360 Secure Mail delivers an office productivity app with email, calendar and contacts to allow employees to securely collaborate with colleagues while preserving the mobile experience on their corporate or personal devices.

Through authentication and authorization, only approved, valid users can access sensitive emails and data. With 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.

The one challenge for MaaS360 Secure Mail is, iOS does not allow any app to continuously run in the background. Due to this design in iOS, MaaS360 Secure Mail on iOS doesn't notify end users on new email availability in their Inbox, thereby limiting functionality that end users are used to. MaaS360 Cloud Extender solves this limitation by leveraging Exchange Web Services to subscribe for Email Notifications for users and delivering notifications via the MaaS360 Cloud to enrolled iOS devices configured with MaaS360 Secure Mail.

Requirements and Scaling

The Mail Notification module receives information from the MaaS360 portal and uses this information Email Subscription:

- User Name
- Device ID
- Email Address

The Cloud Extender uses Microsoft Exchange Web Services (EWS) to register for notifications for user's mailbox. Processes notification information and transmits it to the MaaS360 backend to device notification.

Scaling

Exchange 2007 (must have at least Update Rollup 4 for Service Pack 3 applied)

Exchange 2010 (must have at least Update Rollup 4 for Service Pack 2 applied)

Exchange 2013 (must have AutoDiscovery configured)

Mailboxes	< 15000	> 15000 mailboxes
CPU	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	

Network Traffic

MaaS360 requires outbound communication access from the Cloud Extender to the SaaS Cloud or On-Premise servers. Use the network table from the Networking section of this document to identify which URLs need to be allowed through the firewall.

The MaaS360 Cloud Extender module interacts with Exchange as if the iOS device were connected via Native Mail. In this sense, there would be no additional load to Exchange outside of the normal scope. Please ensure that your Exchange Environment is able to handle these sort of requests.

About Service Accounts

Listener accounts are the accounts that subscribe to notifications on behalf of users against Exchange Web Services (EWS) in order to detect new mail/calendar invites.

These accounts need to have specific impersonation rights in order to accomplish this integration. This section provides details on how to setup your listener accounts.

Each listener account can monitor up to 1250 mailboxes.

Each Cloud Extender allows you to configure a maximum of 12 listener accounts. This equates to a max of 15000 mailboxes monitored per Cloud Extender.

Each listener account must have the following permissions:

Item	Meets Requirement
Member of Domain Users	
Local Admin access on Cloud Extender server	
Impersonation permissions on your CAS server	

Auto Discovery in Exchange 2013

Auto Discovery is used to determine the CAS URL associated with a specific email address. This is the default mode in Exchange 2013.

The Email Notification module performs an auto discovery during the subscription process for an email address. After subscribing this URL is then cached, for this user/mailbox, and another auto discovery only occurs if the subscription fails. Caching the URL greatly speeds up the subscription process.

If auto discovery is configured correctly in your environment, it should only take a few seconds to resolve the CAS URL for a specific email address. For more details on Auto Discovery, refer to the following documentation: <http://technet.microsoft.com/en-us/library/bb124251%28v=exchg.150%29.aspx>

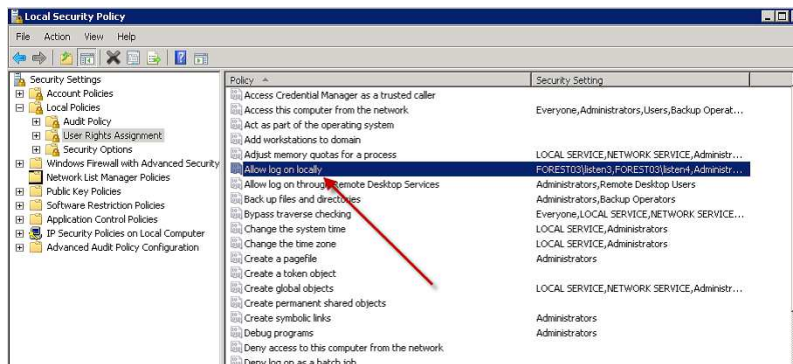
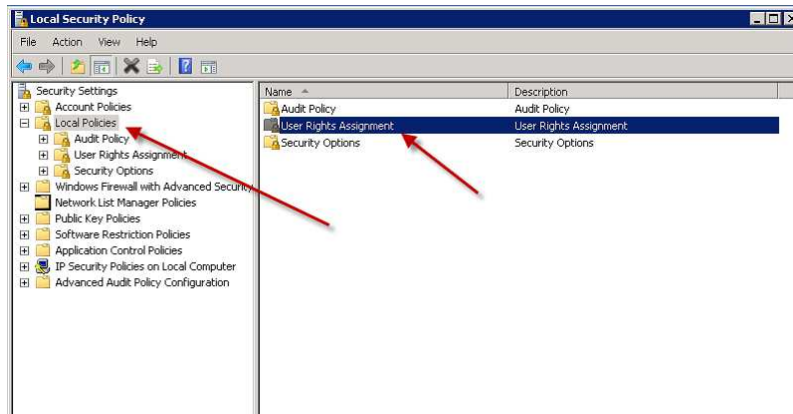
Set up Exchange 2007

About this task

Use the following recommendations for setting up your listener accounts.

Procedure

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



Set Up Exchange 2010 and 2013

Procedure

Use the following PowerShell command to enable Impersonation rights for your listener account. This command needs to be run from Exchange Shell.

```
New-ManagementRoleAssignment -Role:ApplicationImpersonation -User:<userid>
```

For additional detail on Impersonation rights, refer to Microsoft's documentation here: <http://msdn.microsoft.com/en-us/library/bb204095.aspx>

About Throttling Policies

If you have throttling policies in your environment, the listener accounts can be subjected to these policies and Email Notifications might not reliably work in your environment. In order to avoid issues due to Throttling Policies, you are required to create a new Throttling policy that does not enforce any limits on the Listener accounts.

This section highlights the steps you need to take in order to associate a new Throttling policy for your Listener Accounts that does not enforce any restrictions.

Note: This must be done for all of the Listener accounts.

Enable Throttling Policies for Exchange 2010

Procedure

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

```
New-ThrottlingPolicy MaaS360ThrottlingPolicy -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -
```

3. Type the following command to disable policy enforcement.

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

Enable Throttling Policies for Exchange 2013

Procedure

1. Log in to the Exchange Server as the administrator, and open the Exchange Management Shell.
2. At the 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 Unli
```

4. Type the following command to disable policy enforcement.

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

Configure Exchange Notifications

Before you begin

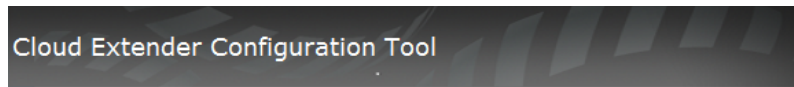
Secure Mail feature should have been enabled on your account. If this has not been enabled, please contact your IBM MaaS360 representative.

Procedure

1. Enable Email Notifications for iOS Devices in the MaaS360 portal by navigating to **Setup > Services** and expanding Secure Mail and checking the box besides the message.



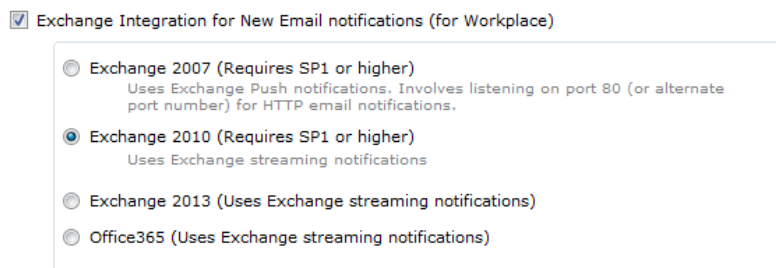
2. Open the Cloud Extender Configuration Tool and in the list of available modules, you should see “Exchange Integration for New Email Notification (for Workplace)”.



Select the Services to be configured:

- Exchange ActiveSync Manager
- Exchange Integration for New Email notifications (for Workplace)
- Lotus Traveler Manager
- BlackBerry Enterprise Server Integration
- User Authentication
- User Visibility
- Certificates Integration
- Enterprise Gateway

3. Choose your version of Exchange and click **Next**.



This screen verifies you have all the necessary pre-requisites to connect to your version of Exchange

Check Prerequisites

All prerequisites have been met. Please click "Next" to continue.

Exchange Integration for New Email notifications (Exchange 2010)

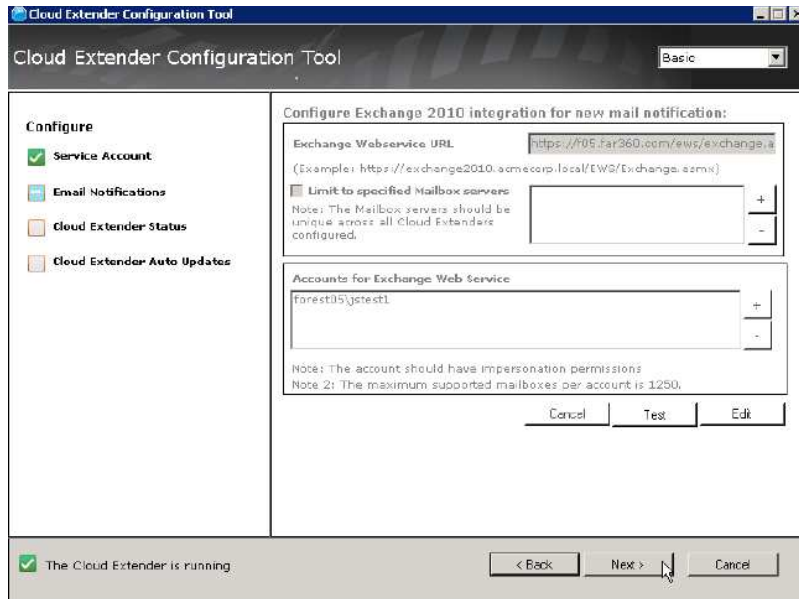
- PowerShell installed (Detected: PowerShell Version 2.0)
Required: PowerShell version 2.0 or above
- Microsoft .NET Framework installed (Detected .NET 3.5)
Required: Microsoft .NET Framework 3.5
- Exchange Web Service module loaded successfully

4. If your environment uses Exchange 2007, do the following.

The screenshot shows the 'Cloud Extender Configuration Tool' window. The title bar reads 'Cloud Extender Configuration Tool'. Below the title bar, there is a 'Basic' dropdown menu. The main area is divided into two panes. The left pane, titled 'Configure', has four items: 'Service Account' (checked), 'Email Notifications' (unchecked), 'Cloud Extender Status' (unchecked), and 'Cloud Extender Auto Updates' (unchecked). The right pane is titled 'Configure Exchange 2007 integration for new mail notification:'. It contains the following fields and controls: 'Exchange Webservice URL' with the value 'https://f01.far360.com/ews/exchange.o' and a note '(Example: https://exchange2010.acmecorp.local/EWS/Exchange.asmx)'; 'Port to listen for push notifications' with the value '8080'; a checkbox for 'Limit to specified Mailbox servers' which is checked, with a note 'Note: The Mailbox servers should be unique across all Cloud Extenders configured.' and a list box containing 'forest01\jstest1'; and a section for 'Accounts for Exchange Web Service' with a list box containing 'forest01\jstest1'. Below these fields are 'Cancel', 'Test', and 'Edit' buttons. At the bottom of the window, there is a status bar with a checked box and the text 'The Cloud Extender is running', and navigation buttons '< Back', 'Next >', and 'Cancel'.

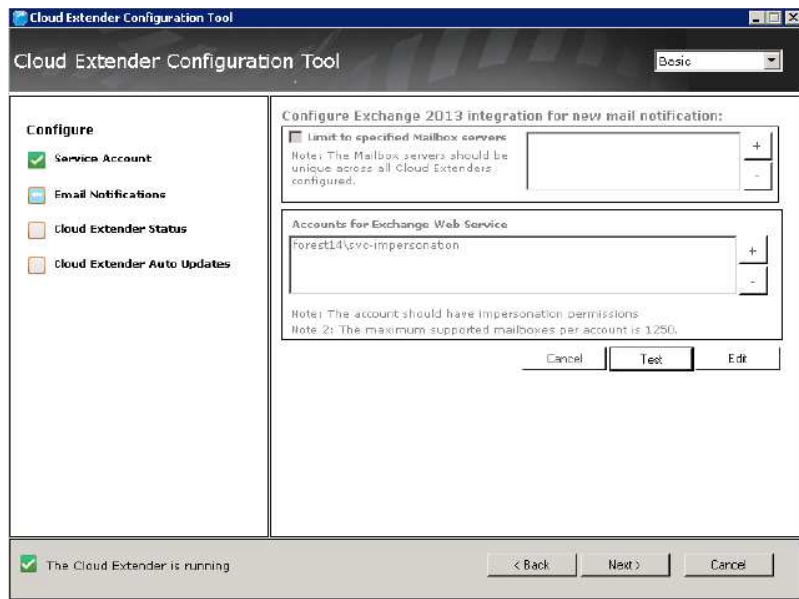
- a. Add the Exchange Web Services URL. This is the URL for your EWS service (typically, the Internal URL is used). You can use the following command on your Exchange Management Shell to determine your Web Service URL:

```
Get-WebServicesVirtualDirectory | Select name,*url* | fl
```
 - b. Set the port to Listen to push notifications. In 2007, Exchange Web Services uses Push Notifications to notify a listener service on new email availability. This requires you to open up a port on the Cloud Extender server. Specify this port number for this field.
 - c. Optionally, limit notification to specified Mailbox servers. Limit subscription of email notifications to only mailboxes on the specified list of mailbox servers.
 - d. Specify accounts for Exchange Web Services. These are the listener accounts created before this step. Each listener account can subscribe to a maximum of 1250 mailboxes. One Cloud Extender accepts up to 12 such listener accounts.
5. If your environment uses Exchange 2010, do the following.



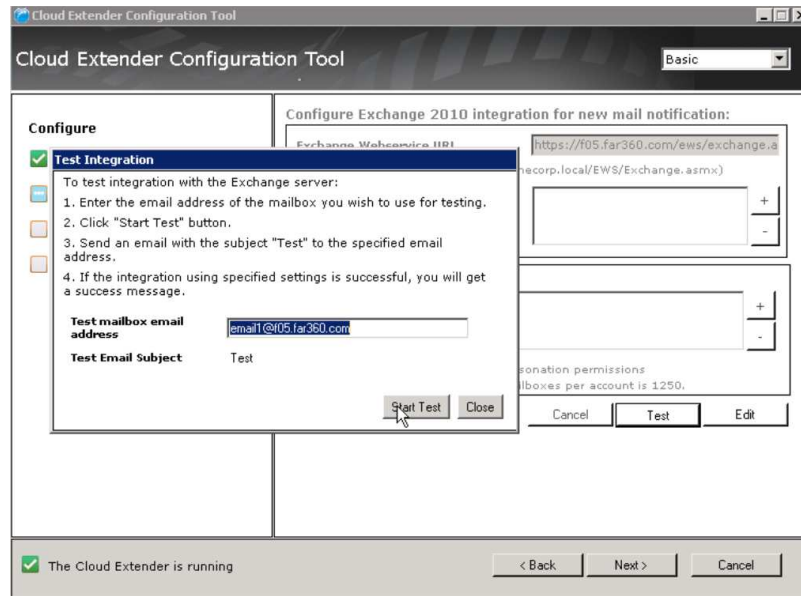
- a. Add the Exchange Web Services URL. This is the URL for your EWS service (typically, the Internal URL is used). You can use the following command on your Exchange Management Shell to determine your Web Service URL:

```
Get-WebServicesVirtualDirectory | Select name,*url* | fl
```
 - b. Optionally, limit notification to specified Mailbox servers. Limit subscription of email notifications to only mailboxes on the specified list of mailbox servers.
 - c. Specify accounts for Exchange Web Services. These are the listener accounts created before this step. Each listener account can subscribe to a maximum of 1250 mailboxes. One Cloud Extender accepts up to 12 such listener accounts.
6. If your environment uses Exchange 2010, do the following.



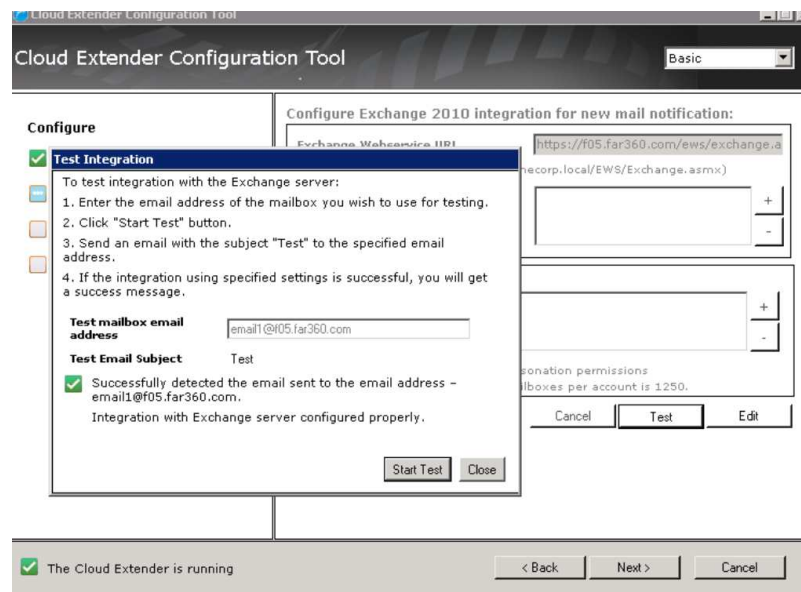
- a. Add the Exchange Web Services URL. Note required since AutoDiscovery is enabled in Exchange 2013

- b. Optionally, limit notification to specified Mailbox servers. Limit subscription of email notifications to only mailboxes on the specified list of mailbox servers.
 - c. Specify accounts for Exchange Web Services. These are the listener accounts created before this step. Each listener account can subscribe to a maximum of 1250 mailboxes. One Cloud Extender accepts up to 12 such listener accounts.
7. Test email notification integration.
- a. Once the setup is complete, click the **Test** button.
 - b. On the pop-up window, provide the email that you want to listen to.



- c. From your corporate email, send an email with **Subject** as **Test** to email address that is provided above.

Once it is succeeded, you'll get an integration message that indicates that the integration is successful.



Configure Exchange Policies

About this task

Once the Email notification module is successfully setup and tested on your Cloud Extender, in order for iOS users to subscribe for notifications for Secure Mail, a policy setting needs to be turned ON in your WorkPlace Persona policy.

Procedure

1. Login to your MaaS360 portal.
2. Under **Security > Policies**, click **Edit** on your WorkPlace Persona policy.
3. Under **Email > Configuration**, enable Real-time Notifications by checking the box to the right.
4. For **New Mail Notifications**, you can set it to All, None or Favorite contacts.



5. Save and publish the policy.
6. Assign the policy to your users or devices.

Once the users get the policy and configure Secure Mail, the MaaS360 app initiates email notification subscription by the user

The portal broadcasts the subscription request to all Cloud Extenders running Email Notification and completes a successful subscription

Troubleshooting Exchange Integration

Why aren't the devices getting notifications?

The most common issue that one might run into is that email notifications are not being sent to the device. Troubleshooting steps are below:

1. Ensure that your EWS URL has a valid certificate (if using SSL) and the certificate is installed on the Cloud Extender server
2. Ensure that your EWS URL is reachable from the Cloud Extender server (use a web browser to confirm reachability)
3. Ensure that the listener accounts are not locked out or passwords have expired
4. Run the Test Action on the Cloud Extender for the affected mailbox to check if the integration is working >as expected.
5. Watch the logs from C:\%ProgramData%\MaaS360\Cloud Extender\logs\EWSNotifications_YYYY_MM_DD.log
6. Run Cloud Extender Diagnostic Logs collection Tool:
 - a. Login to the Cloud Extender server
 - b. Browse to C:\Program Files(x86)\MaaS360\Cloud Extender
 - c. Double click DiagnosticCmd.exe. This generates a zip file on your desktop.
 - d. Contact IBM Support to diagnose the issue.

Why isn't the Config Tool's Email Notifications test working?

If the Config Tool's test returns failure almost immediately, check the EWSNotificationsConfig log files for the following text:

```
"[ListenerThreadManager::AssignSubscriptionsToConnections] ERROR! Got exception trying to assign s
```

If you find the above text, it means the customer does not have .NET version 3.5 installed. Solution: install it. It can be installed without removing other versions that may already be in place. It can be downloaded at <http://www.microsoft.com/en-us/download/details.aspx?id=21>

Chapter 6. Lotus Traveler Integration Module Configuration

Overview

The Cloud Extender provides visibility into all existing devices connected to the mail system. The Cloud Extender performs a number of functions on behalf of the MaaS360 Cloud to provide visibility and management of Traveler-connected devices:

- Queries Lotus Traveler server using APIs for information related to the ActiveSync-enabled devices.
- Collects and accesses device information and transmits it to the MaaS360 Portal for reporting and management functions.
- Device information is collected and uploaded to MaaS360 to facilitate reporting and management workflows.
- Receives actions and carries out the relevant actions on the Traveler server.
- At predetermined intervals, the Cloud Extender looks for changes in the data and on the Traveler server, and provides any new data to MaaS360.

Important: Integration with Traveler is not an email proxy. The Cloud Extender does not sit between email and devices. This integration is simply for visibility into your Traveler environment to give you the ability to take actions upon devices that are connected to Traveler as well as apply compliance rules and remediation to those devices that may not be enrolled in MaaS360 but are enrolled in Traveler.

System Requirements

The MaaS360 Cloud Extender requires that it be configured with an account with sufficient rights to run as a service and to access Traveler Servers.

Before beginning the installation, make sure the following requirements are met:

Item	Meets Requirement
IBM SmartCloud Notes or Lotus Domino 8.5.2 or greater	
The Cloud Extender must be installed on a machine that has the Notes client installed	
.NET 3.5 or higher	

Scaling Requirements

The following tables provide guidance on how to size the machine that the Cloud Extender(s) requires to operate effectively and how many instances of the Cloud Extender are required to service large and complex Lotus Traveler environments.

In large environments the following guidelines should be followed:

- The number of mailboxes and connected devices should be balanced across mailbox servers.
- Device data gather times should not exceed 60 minutes and should average between 25 and 40 minutes for 5000 devices. Current and average gather times are available on the Cloud Extender Status page within the MaaS360 portal.

- A rule of thumb to determine the number of Cloud extender instances required to effectively service the environment is to divide the potential number of ActiveSync connected devices by 5000 and the number of Mailboxes by 10,000 and use the higher of the two values to arrive at the number of Cloud Extenders instances required.

Important: Gather times should be closely monitored. If they start to consistently exceed 60 minutes, additional Cloud Extenders should be considered.

Mailboxes	< 5000	5000-10000	> 10000 mailboxes
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

Devices	< 2500	2500-5000	> 5000 devices
CPU	2 Cores	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	8 GB	

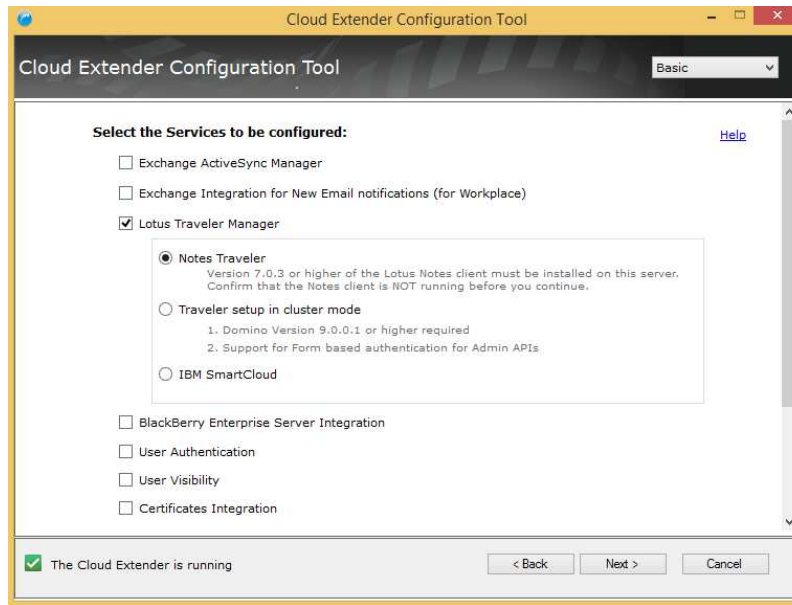
Permission Requirements

Item	Meets Requirement
Lotus Notes 8.5.2+ A Domino account and credentials with sufficient rights to perform Domino/Traveler Admin functions. You should have at least access level of Server Remote Admin, Manager w/ delete access to Traveler.nsf	
SmartCloud Notes Account with Administrator rights on SmartCloud Notes	

Configure Lotus Traveler Integration

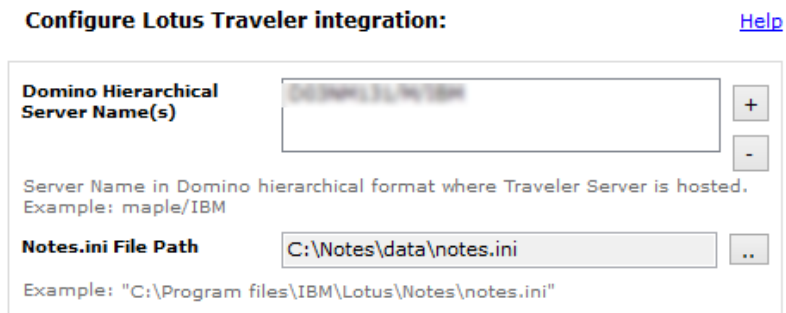
Procedure

1. Open the Cloud Extender Configuration Tool and enable the Lotus Traveler Manager.
2. Choose your integration server type you use for Traveler integration, click **Next**.



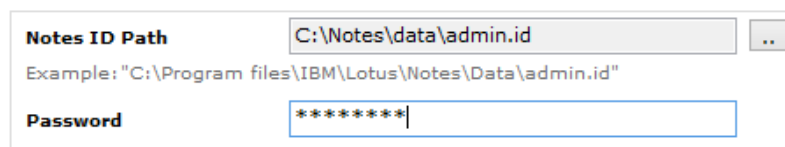
The tool checks to see if the necessary applications are installed. If they are, click **Next**.

3. If your environment is Notes Traveler, do the following.
 - a. Stop the Notes Client before continuing.
 - b. Click the (+) icon at the upper right to add in your Domino Hierarchical Server Names.
 - c. Find your Notes.ini file path to include it in this configuration.



- d. Find the Notes ID for your Notes Administrator and enter the password.

Note: The Notes ID file should have Administrator access rights for all the above Domino Servers.



- e. When complete, press **Next** to verify your servers and credentials.
4. If your environment is Traveler in Clustered Mode, do the following.
 - a. Enter your Traveler Server URL in the box at top.

Configure Lotus Traveler integration:

[Help](#)

Enter the Traveler Server URL and Administrator account credentials to allow MaaS360 to access and integrate with Traveler server.

Traveler Server URL	<input type="text" value="https://traveler.us.ibm.com"/>
Example:	https://traveler.abc.com

Note: The account must have the Traveler Administrator role.

Username	<input type="text" value="travelerAdmin"/>
Password	<input type="password" value="*****"/>

- b. Enter your user name and password that can be used to administer devices within traveler.
 - c. When complete, press **Next** to verify your servers and credentials.
5. If your environment is SmartCloud Notes, do the following.
- a. Choose your SmartCloud server from the pop-up listed at top.

Configure IBM SmartCloud Integration

[Help](#)

Enter the IBM SmartCloud Server URL and Administrator account credentials to allow MaaS360 to access and integrate with IBM SmartCloud.

IBM SmartCloud Server URL	<input type="text" value="https://api.notes.na.collabserv.com"/>
---------------------------	--

Note: The account must have the Traveler Administrator role.

Username	<input type="text" value="travelerAdmin"/>
Password	<input type="password" value="*****"/>

- b. Enter your user name and password that can be used to administer devices within SmartCloud Notes.
 - c. When complete, press **Next** to verify your servers and credentials.
6. Click **Next** to complete the configuration and view the connection summary.
 7. Click **Next** to make adjustments to Automatic Updates if necessary.
 8. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool. Expect devices to start importing into your MaaS360 portal within a few hours depending on the size of your environment. Watch the Cloud Extender logs to view this in real-time.

Lotus Traveler Configuration Options

Auto-Approve Based on Policy

Enabling Auto-Approve based on policy is recommended when trying to limit devices from accessing Traveler outside of MaaS360. This policy blocks devices that

are not assigned a policy within MaaS360. This is similar to Auto-Quarantine within Exchange but because Traveler does not have such APIs available, we have to perform the quarantine on our own.

Auto-Approve Settings	
Auto Approve based on policies Select this option if you would want to auto-approve devices based on the assigned policy.	No

Auto-Discovery Configuration

The MaaS360 integration with Lotus Traveler provides auto-discovery of devices within the Traveler environment. This includes all connected devices within the environment with no limit on when the last sync occurred. Devices are imported into the portal as they are discovered. Access the Auto-Discovery settings in the portal by navigating to **Setup > Cloud Extender Settings**. Make adjustments as needed and use the list below to make your decisions.

Data Collection Frequency	
Device Data Query Frequency Frequency at which Notes Traveler is queried to determine changes to Device data.	Every hour
Device Heartbeat Query Frequency Frequency at which Notes Traveler is queried to determine changes to Last Reported date of devices into Traveler.	Every hour
Full Data Refresh Day Day of the week on which all device and policy data is uploaded from Notes Traveler to ensure all data is in sync. The Refresh will start at a random time on the specified day.	Sunday
Full Data Refresh Frequency Frequency at which all device and policy data is uploaded from Notes Traveler.	Every week

Device Data Query Frequency

Frequency at which Traveler Server is queried to determine changes to Device data.

Available Options:

- Every 15 minutes, Every hour, Every 4 hours, Every 8 hours, Every day

Tip: In larger environments, increase the amount of time between data queries for better server performance.

Device Heartbeat Query Frequency

Frequency at which Traveler Server is queried to determine changes to Last Reported date of devices into Traveler Server.

Available Options:

- Every hour, Every 4 hours, Every 8 hours, Every day

Full Data Refresh Day

Day of the week on which all device and policy data is uploaded from Traveler Server to ensure all data is in sync. The Refresh starts at a random time on the specified day.

Available Options:

- Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Full Data Refresh Frequency

Frequency at which all device and policy data is uploaded from Traveler Server. This is coupled with the Full Data Refresh Day option (ie. Every alternate week on Sunday).

Available Options:

- Every week, Every alternate week, Every 4th week


Best Practices for Lotus Traveler Auto-Quarantine

Communicate

Customers are advised to communicate when Auto-Approve/Block is turned on. Provide help desk FAQs and emails to company workforce to be notified that on a certain date, users can no longer connect to Traveler by any other means other than through MaaS360. Communicate to users that they need to remove their Native Mail or other MDM and enroll in MaaS360. Let them know that on the migration day, they would be out of compliance. This can be done in waves as well as by operating system (if you want to migrate all iOS devices first, and another OS second). Wave deployments are a good idea to give the company's help desk a chance to work on one Operating System at a time.

Create an Unenrolled Traveler Device Group

It is important to isolate devices that are not MaaS360 managed and connected to Traveler.

1. Go to **Devices > Groups** and click  at the upper right.
2. Within the advanced search, choose:
 - Active Devices
 - Last reported = "All Records"
3. **Device Type:** Smartphones and Tablets checked
4. **Condition 1: Hardware Inventory > Managed status > Equal To > Not Enrolled**
5. **Condition 2: Hardware Inventory > Mailbox Managed > Equal To > Traveler Managed**
6. **Condition 3: Operating System > OS Name > Contains > Android (If enrolling Android)**
7. **Condition 4: Operating System > OS Name > Contains > iOS (If enrolling iOS)**
8. **Condition 5: Operating System > OS Name > Contains > Windows Phone (If enrolling Windows Phones)**

9. **Apply Advanced Criteria:** 1 AND 2 AND (3 or 4 or 5)
10. If not enrolling a certain OS, remove that condition from the advanced criteria.

Use Compliance Configuration

Create a compliance rule specifically for devices that are unenrolled in MaaS360 but are Traveler Managed. It is advised to create this group before creating this policy. Enable Enrollment Enforcement within the compliance rule and select the following options:

Select Enforcement Rules

Enrollment
Ensure iOS and Android devices are enrolled in MDM and advanced management of the device has not been disabled or removed by the user.

Trigger Action on Managed Status

<input checked="" type="checkbox"/> Not Enrolled	<input type="checkbox"/> User Removed Control
<input type="checkbox"/> Pending Control Removal	<input type="checkbox"/> Control Removed

Send Enrollment Request in Email

Enforcement Action
Configure the actions to be taken at the required time intervals. Time interval specified at any level is taken as the wait time post the previous action.

Immediately after OOC - Alert

15 Days later - Block

Notify User: Email

Notify Admins: Standard Email List

Message
Enter a custom message for this rule. Maximum of 1024 characters are allowed and <^~*~\$*~()~> cannot be used.

You're currently out of compliance with Company's mobile security policy. You're device is currently connected to corporate email without enrolling in MaaS360 Device Management. Please enroll in MaaS360 to have your email properly provisioned for your device. If you do not enroll within 15 days, your email will be automatically blocked.

Assign a Compliance Rule to the Group

When ready, assign the compliance rule to the previously created group and immediately your devices are notified that they must enroll their device within a certain time-frame or their devices are blocked from using corporate email.

Enable Auto-Approval in the Cloud Extender Settings

Enable the Auto-Approval based on Device Policy within the Cloud Extender policy settings.

Auto-Approve Settings

Auto Approve based on policies

Select this option if you would want to auto-approve devices based on the assigned policy.

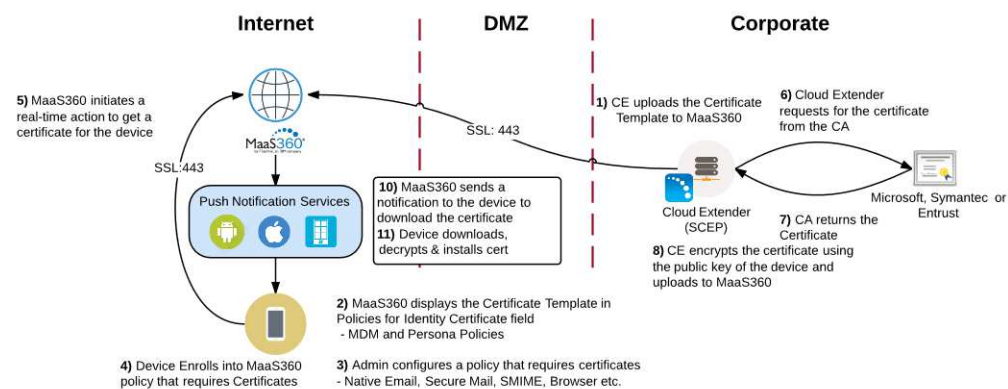
Chapter 7. Certificate Authority Integration (SCEP) Overview

MaaS360 Certificate Services Integration provides customers with the ability to leverage their existing Certificate Authority (CA) and auto-provision User Certificates to enrolled iOS Devices. Administrators can create E-mail, Wi-Fi, and VPN policies & profiles that can use User based Certificates for authentication.

The Cloud Extender interacts with CA, and pushes the issued certificates down to enrolled iOS devices. It performs the following functions:

- Processes User Certificate requests from MaaS360 when the users enroll their iOS devices against a policy that requires User Certificates
- Authenticates against the CA / Registration Authority (RA) before requesting for Certificates
- Requests User Certificates on behalf of enrolled iOS devices
- Encrypts the issued User Certificates and uploads the same to MaaS360
- MaaS360 then pushes these certificates to these devices
- Cloud Extender can integrate with Microsoft CA installed on 2003, 2008R2, or 2012R2, Symantec Managed PKI, and Entrust

The MaaS360 Cloud Extender requires that it be configured with a Certificate Template with information regarding the CA server, and administrative credentials to authenticate and request device certificates.



System Requirements for SCEP integration

Before beginning the installation, make sure the following requirements are met:

Item	Meets Requirement
Microsoft Windows 2008+	
.NET 3.5 or higher	
Entrust Only:	
<ul style="list-style-type: none"> • Entrust IdentityGuard Server v10.1, v10.2 • Entrust Admin Services v8.2 SP1, v8.3 	

Scaling

The Cloud Extender with Certificate Integration requires minimal specifications to function properly. In most cases, the Certificate Integration module can be coupled with other modules in order to limit the amount of managed resources. However, it is recommended to have more than one Cloud Extender configured with Certificate Integration if the device count tops 10,000 devices.

Devices	< 10000	> 10000 devices
CPU	2 Cores	Use Additional Cloud Extenders
Memory	4 GB	

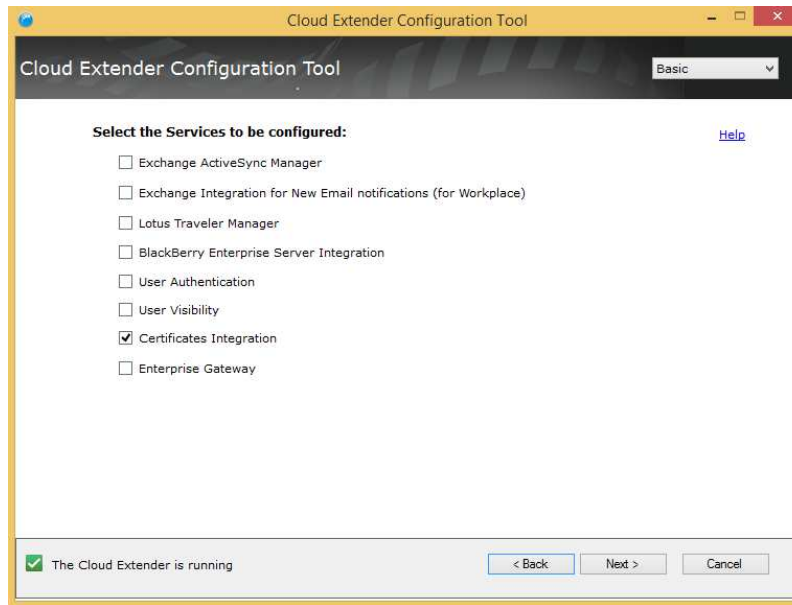
Permission Requirements

Item	Meets Requirement
Microsoft: Administrative Access to Microsoft CA Server Symantec: Administrative Access to Symantec MPKI environment (Web URL)	
Microsoft: Administrative Access to a server on which Network Device Enrollment Service (NDES) can be installed. Could be 2003 or 2008R2 Enterprise or Data Center editions. Can be enabled on either the Cloud Extender server or the CA server itself. Symantec: Administrative Access to Symantec MPKI environment with admin access to get an RA certificate.	
Microsoft: Administrator credentials for the NDES environment Symantec: Administrative credentials on Symantec MPKI environment	

Configure for SCEP Integration

Procedure

1. Open the Cloud Extender Configuration Tool and enable the Certificate Integration.



2. Click **Next** and you are brought to a page that says “Add New Template”.
3. Click the button to add a new Certificate Template.

Configure Certificate Templates

Add New Template

Template Name

4. Choose whether you want this template to be a User based certificate or a Device based certificate.

Template Configuration [Help](#)

Create New Template
 Device Certificate
For Device Identity Certificates

User Certificate
For User Certificates or S/MIME Encryption and Signature Certificates

Import Certificate Template ...

5. Give your certificate template a name that represents what it is you are providing.

Template Name

6. Continue through the next steps after choosing your certificate authority type.

Use a Microsoft CA

Before you begin

If no Microsoft NDES server has been set up, please see “About Microsoft NDES for Certificate Integration” on page 74.

About this task

In the template configuration, the administrator provides the necessary information to request a certificate from the Microsoft NDES server. This includes a configurable subject and alternative subject name, including wildcard options that are replaced with user or device information. When the information is saved the template is automatically uploaded to MaaS360. It appears in the list of available policies, and includes the name that the administrator entered during the template configuration.


Device Certificate

Procedure

1. Fill out the following fields below to set up the certificate integration.

Template Name	<input type="text" value="Company - Email Cert Auth"/>
Type	<input type="text" value="SCEP (Microsoft)"/>
SCEP Server (Distinguished Name)	<input type="text" value="scep1.america.company.local"/>
SCEP Default Template (Optional)	<input type="text"/>
Challenge UserName	<input type="text" value="user@scep1.america.company.local"/>
Challenge Password	<input type="password" value="*****"/> <input type="button" value="Continue"/>

2. Click **Continu**next to the Challenge Password area to validate credentials and to proceed.
3. The fields below should now become active and you can make adjustments as needed to the CA Name, URL, etc.

URL	<input type="text" value="http://scep1.customer.local/certsrv/"/>
Certificate Authority (CA)	<input type="text" value="Exchange CA"/>
Subject Name 	<input type="text" value="/CN=%uname%/emailAddress=%e"/>
Subject Alternative Name Type	<input type="text" value="UPN and Email"/>
Save generated certificates	<input type="checkbox"/>
Certificate Storage Path	<input type="text" value="C:\Certificates"/>


4. Lastly, you have the option to cache all certificates generated for backup, validation, and troubleshooting.



Save generated certificates	<input checked="" type="checkbox"/>
Certificate Storage Path	<input type="text" value="C:\Certificates"/> <input type="button" value="..."/>

5. Click **Next** to continue and validate the configuration.
6. Once complete, you should be directed back to the certificate template list.

Configure Certificate Templates


Template Name		
Email Device Auth	✖	✎

- If you do not see a  icon next to your template, complete the Cloud Extender configuration, close the Cloud Extender Configuration Tool and relaunch the tool.
- Once you make your way back to the certificate list, you should see two more

icons that may have not been there before.  

The gear icon allows you test the certificate

The ribbon icon allows you to export your template for backup as well as configuring other cloud extenders with the same credentials

- Click the  icon to test the issuing of certificates.

Test Certificate

Certificate Details

Certificate Name

Username

Domain

Email Address

- Click **OK** to test the issuance of the certificate and if successful you should see a screen like the one below.

Test Certificate

Certificate generated and validated successfully.

Subject: CN=company.local@company.local

Issuer: CN=COMPANY-CA

Valid from: Jul 28 22:03:51 2015 GMT

Valid to: Jul 28 22:13:51 2016 GMT

You can download the Certificate for use on a mobile device from
<C:\Certificates\Certificates\PKICerts\CE2015P07k28116E23X33T09\test2.p12>

User Certificate

Procedure

1. Fill out the following fields below to set up the certificate integration.

Template Name	<input type="text" value="Exchange SMIME"/>
Type	<input type="text" value="Microsoft"/>
FQDN of Certificate Authority (CA)	<input type="text" value="scep1.company.local"/>
FQDN of Active Directory (AD)	<input type="text" value="ad.company.local"/>
Mandatory Key Usage	<input checked="" type="checkbox"/> S/MIME Encryption <input checked="" type="checkbox"/> S/MIME Signature <input checked="" type="checkbox"/> Identity (Client Authentication)

2. Click **Next** to continue and validate the configuration.

Use a Symantec CA

About this task

In the template configuration, the administrator provides the necessary information to request a certificate from the Symantec service. This includes a configurable subject and alternative subject name, including wildcard options that are replaced with user or device information. When the information is saved the template is automatically uploaded to MaaS360. It appears in the list of available policies, and includes the name that the administrator entered during the template configuration. The process to create a Symantec template is similar to the one to create Microsoft template, but there are a few more steps.

Device certificates are the only option available.

Procedure

1. Give your template a Template Name and select the Type of template being created. Select the Symantec SCEP (Symantec/VeriSign) option from the **Type** pop-up list.

Template Configuration [Help](#)

Create New Template

Device Certificate
For Device Identity Certificates

User Certificate
For User Certificates or S/MIME Encryption and Signature Certificates

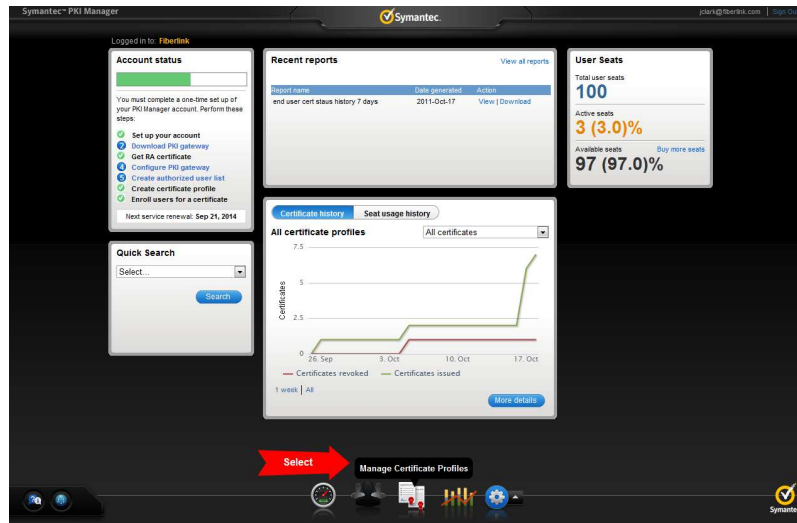
Import Certificate Template

Template Name

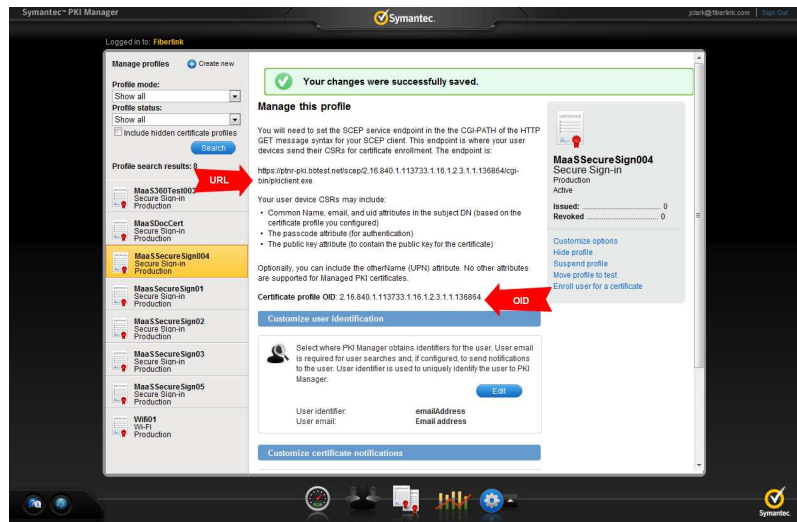
Type

2. Use your browser to log in to your Symantec PKI Manager account.
3. From your PKI Manager dashboard, select the option to Manage Certificate Profiles.

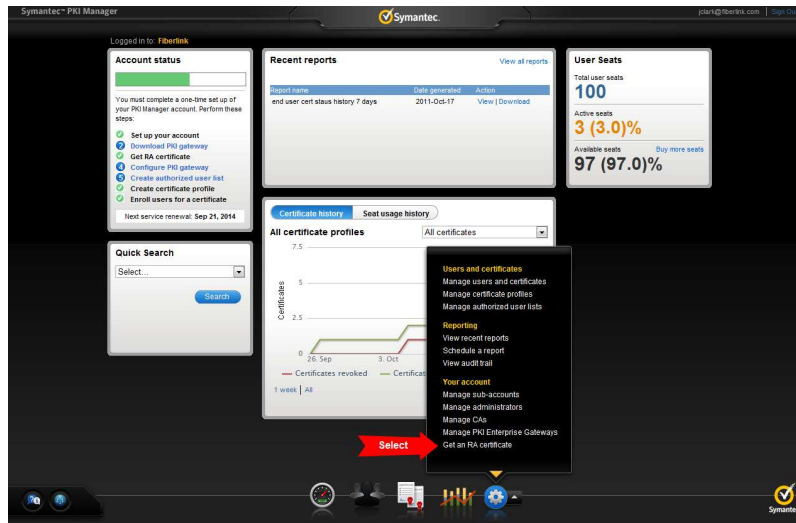
To perform this step, the certificate profile must already exist.



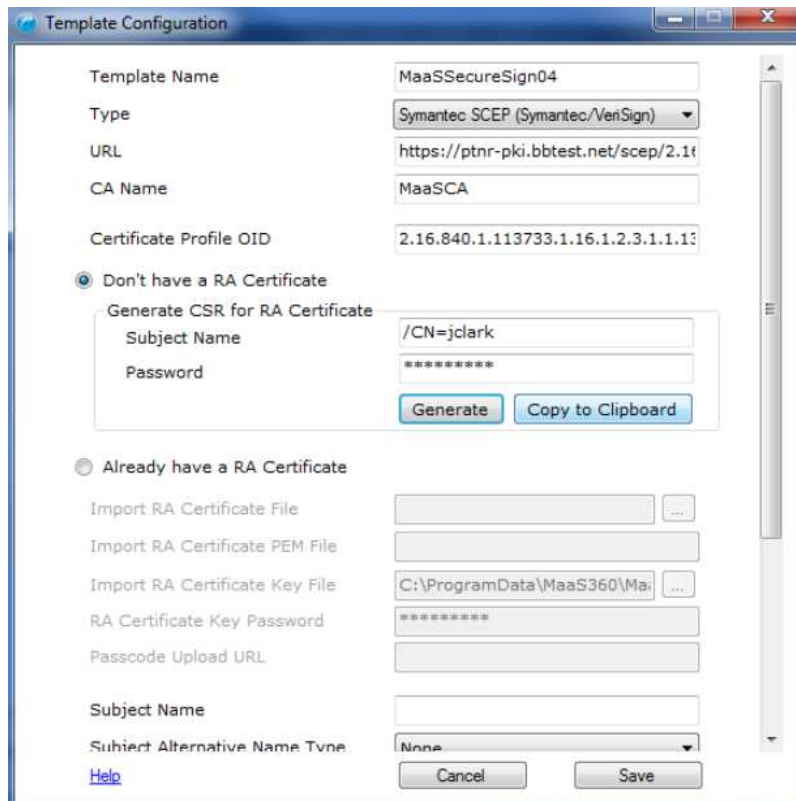
- From the Manage profiles screen, highlight the certificate profile for which you are creating this template. You see a display similar to the one displayed below. You need the URL and Certificate profile OID values on this page to complete your template configuration. Cut and paste these two values into the URL and Certificate Profile OID boxes on your Template Configuration screen.



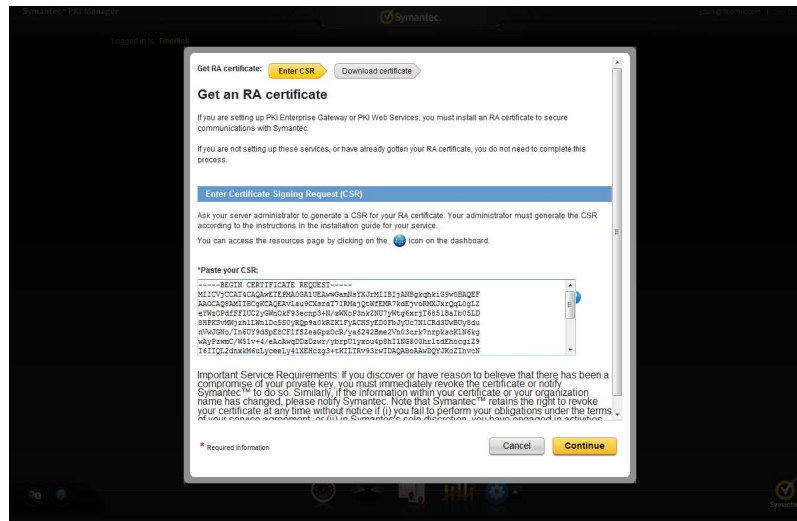
- If you do not already have an RA certificate from Symantec, you need to log in to your Symantec PKI Manager account to obtain one. From your PKI Manager Dashboard, choose the option to Get an RA certificate.



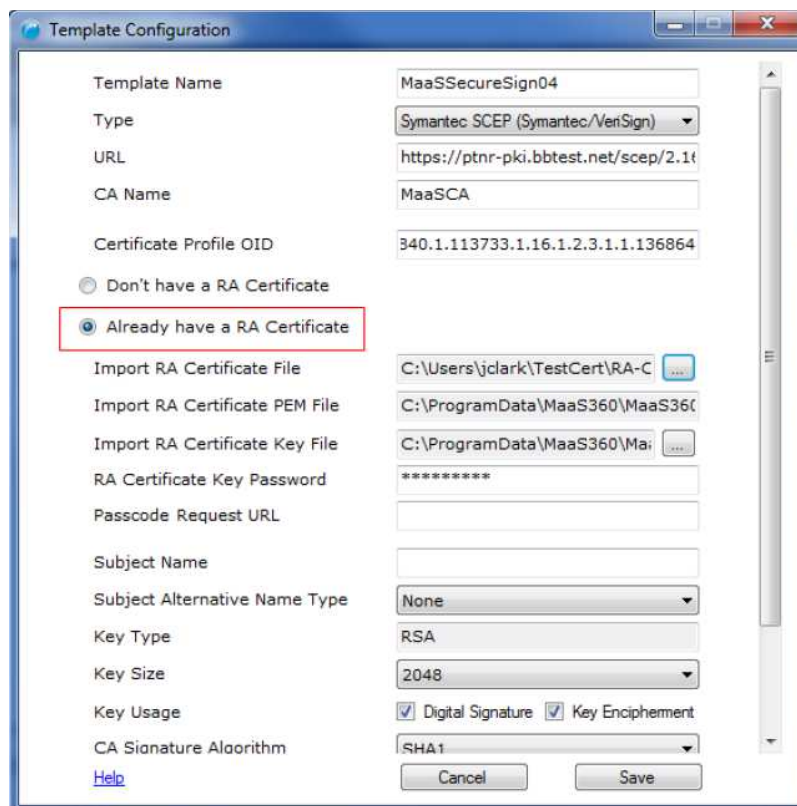
6. On the Template Configuration screen, enter a Subject Name and a Password in the **Generate CSR for RA Certificate** box.
7. Click the **Generate** button on the Template Configuration screen. This generates a CSR (Certificate Signing Request) that you can use to obtain your RA certificate from Symantec.



8. Go back to the PKI Manager Get an RA certificate screen, where you can enter the CSR that you copied to the clipboard.
9. Now, paste the CSR into the text box under Paste your CSR.
10. Click the Continue button and your RA certificate is generated and you are guided through the process of downloading your RA certificate file.

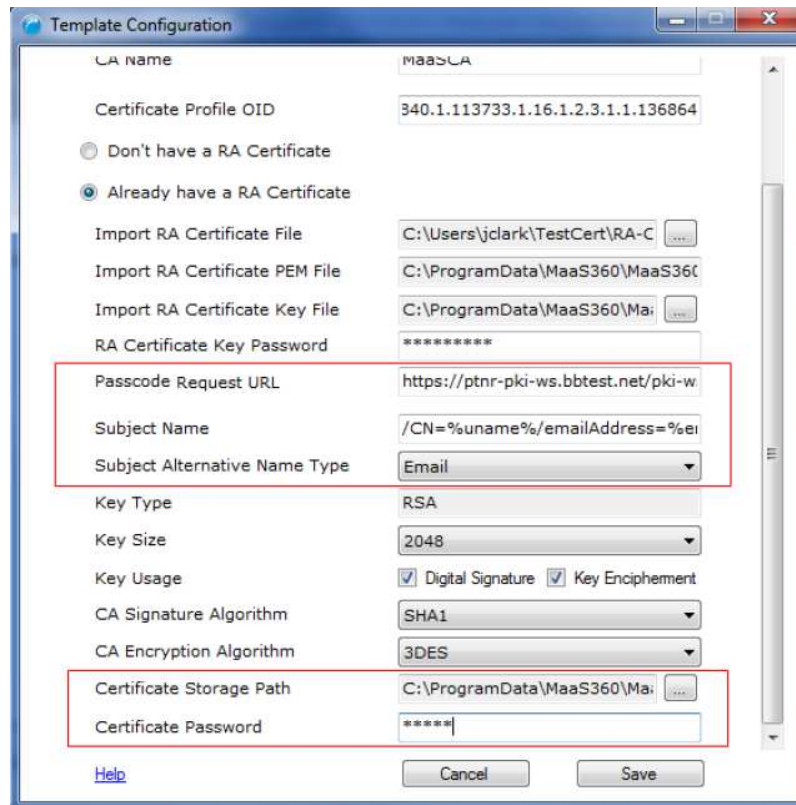



11. Now that you have an RA certificate, you can select the **Already have a RA Certificate** radio button on the **Template Configuration** screen.
12. Use the **Import RA Certificate File** browse button to go to the location of your downloaded RA certificate. After selecting the RA certificate file, the configuration tool populates the *Import RA Certificate PEM File*, *Import RA certificate Key File* and *RA Certificate Key Password* values.



13. Enter the Passcode Request URL. This value should have been provided to you by Symantec as part of the customer enrollment process. Typically this URL looks like the following: `https://ptnr-pki-ws.bbtest.net/pki-ws/`
14. Enter the Subject Name. The syntax is important for this value, for example: `/CN=%uname%/emailAddress=%email%/O=Fiberlink Communications/`

15. Select **Email** for the Subject Alternative Name Type from the drop-down list.
16. Use the Certificate Storage Path browse button to find the download folder. Typically this value is something like the following: C:\%ProgramData%\MaaS360\MaaS360 Visibility Service\Certs
17. Enter the Certificate Password for the certificate store into which the device certificates are placed.




18. Click **Save** to continue and validate the configuration.
19. Once complete, you should be directed back to the certificate template list.
20. If you do not see a  icon next to your template, complete the Cloud Extender configuration, close the Cloud Extender Configuration Tool and relaunch the tool.
21. Once you make your way back to the certificate list, you should see two more icons that may have not been there before.

The gear icon allows you test the certificate

The ribbon icon allows you to export your template for backup as well as configuring other cloud extenders with the same credentials



22. Click the  icon to test the issuing of certificates.

23. Click **OK** to test the issuance of the certificate and if successful you should see a screen like the one below.

Use an Entrust CA

Step 1: Obtain a Digital ID from Entrust Before you begin

Please contact your Entrust Administrator to create the Digital ID suitable for your environment.

About this task

A Digital ID in the Entrust world is a Certificate Template that lets you define the format of the certificate that the Entrust CA needs to issue. MaaS360 Cloud Extender leverages Web Service API's to get a certificate from a selected Digital ID. Cloud Extender can provide values for Subject Name / Subject Alternate Name from the MaaS360 system for the Identity Certificates.

Example

Here is a sample Digital ID from Entrust IdentityGuard. This Digital ID expects:

- Subject Name with a user name, a group name and a device type. Any supported MaaS360 attribute can be passed to Entrust for these fields.
- Subject Alternate Name with UPN and Email

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=enrust, c=ca
Certificate Type	fl_skp_dualusage
User Type	Person
Role	End User
RDN Format	cn=<igusername> <lggroup> <devicetype>
Directory Mode	Perform Operation
Security Manager Group Membership	All Security Manager Groups
Variables	✓ cn: <igusername> → User Type sn: <lggroup> <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](#)

Step 2: Configure the Cloud Extender for Entrust Procedure

1. Open the MaaS360 Cloud Extender Configuration Tool and go to the Certificate Template screen.
2. Click **Add New Template > Create New Template > Device Certificate**.
3. Under the Type, select Entrust.
4. Fill out the template with the following variables.

- a. Any Template Name
 - b. Type: Entrust
 - c. Web Service URL for the Entrust CA
 - d. Admin User Name
 - e. Administrator User Name
 - f. Administrator Password
 - g. Entrust Group Name
5. Click Continue. The Cloud Extender makes a Web Service call to the Entrust CA and gets the list of all defined Digital IDs.
 6. Choose the required Digital ID. This automatically populates the RDN Format for the selected Digital ID.

Digital ID Config Name	FiberLink Mobile Enrollment for iC
RDN Format	FiberLink Mobile Enrollment for Netw FiberLink Mobile Enrollment for iOS M
RDN Variables	Demo ID Test Mobile FiberLink Mobile Enrollment for iOS M


REPLACE with supported RDN variables.



7. Fill out the remaining fields.

Digital ID Config Name	FiberLink Mobile Enrollment for iC
RDN Format	cn=<igusername> <iggroup> <dev
RDN Variables	<igusername>=%username%; <iggroup
	Substitute each occurrence of REPLACE with supported RDN variables.
Subject Alternative Name Type	UPN and Email
Renewal Period (Days)	14
	<input checked="" type="checkbox"/> Search for Entrust User by CN

- a. Select the Digital ID
 - b. Read-only RDN Format for the Digital ID
 - c. RDN Variables used as Subject Name
 - d. Subject Alternate Name
 - e. Renewal Period: Days before expiry when a renewal is attempted
 - f. Search Entrust User by CN. Default is search by user name
8. Replace the %REPLACE% with supported variables for the Subject Name of the certificate for each of the RDN values. Supported Subject Name and Alternate Subject Name substitutions in MaaS360 Cloud Extender include: %udid%, %csn%, %uname%, %domain%, %email%, %imei%, %model%, %sim%, %phnumber%, %ou%, %cn%, %dc%, %dn%


Note: Usage of these attributes require User Visibility module to be implemented (not necessarily on this Cloud Extender)

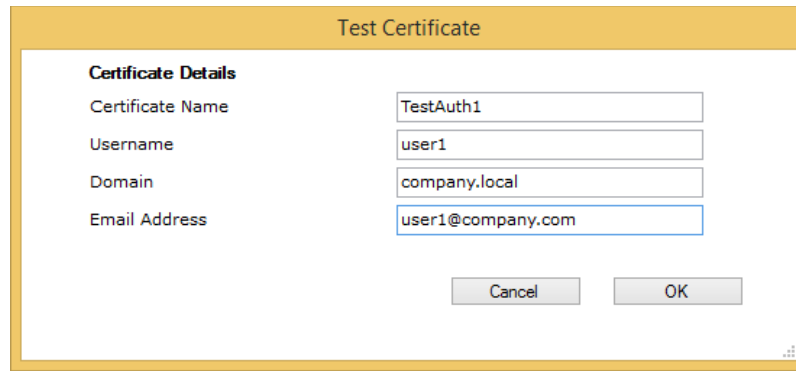
9. Save the Certificate Template. Once complete, you should be directed back to the certificate template list
10. If you do not see a  icon next to your template, complete the Cloud Extender configuration, close the Cloud Extender Configuration Tool and relaunch the tool.
11. Once you make your way back to the certificate list, you should see two more

icons that may have not been there before.  

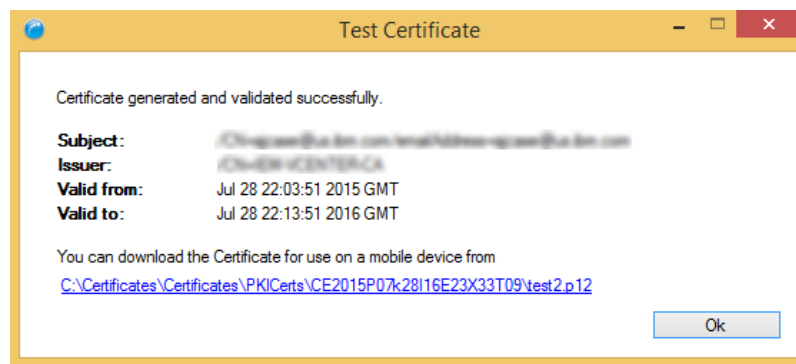
The gear icon allows you test the certificate

The ribbon icon allows you to export your template for backup as well as configuring other cloud extenders with the same credentials

12. Click the  icon to test the issuing of certificates.



13. Click **OK** to test the issuance of the certificate and if successful you should see a screen like the one below.



14. Click **Next** to complete the configuration and view the connection summary.
15. Click **Next** to make adjustments to Automatic Updates if necessary.
16. Click **Finish** to complete the setup and exit the Cloud Extender Configuration Tool.

About Microsoft NDES for Certificate Integration

MaaS360 allows integration with Microsoft’s Active Directory Certificate Services for automatic delivery of device certificates to enrolled iOS devices. Signed certificates are generated through Microsoft’s Registration Authority (RA) known as the Network Device Enrollment Service (NDES) using the Simple Certificate Enrollment Protocol (SCEP).

This document walks you through the steps you would need to perform to 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 achieve automatic certificate delivery.

This guide assumes that an Enterprise Certificate Authority (CA) is functional on your corporate network.

This guide also assumes you have the required administrative rights on the Windows Server and the CA to accomplish certificate integration.

Certificate Server Requirements

You need to identify a Windows Server upon which you install NDES. The same server can be used for the MaaS360 Cloud Extender for certificate integration, but we recommend you install them on a different server than your CA. The supported operating systems are the following:

- 2003 (Requires optional SCEP module)
- 2008 R2 and 2012 R2 Installed via Microsoft Server Manager

The content of this document is based on a Microsoft Server 2008 R2 SCEP server and a 2008 CA.

Microsoft NDES Installation

Before you begin

If you have not installed Network Device Enrollment Service on your Windows 2008 / R2 server, the Microsoft article here provides a step-by-step guide to enable NDES on the Microsoft server.

Make sure you have the requisite permissions to set up NDES:

- **SCEP Admin** : User who logs into the server and installs NDES
 - Member of Local Administrators Group
 - Must have Enroll permission on the following templates:
 - Exchange Enrollment Agent (offline request)
 - CEP Encryption
 - Must have permissions to add templates to the selected CA
 - Must be a member of the Enterprise Administrator group
- **SCEP Service Account**: Credentials that are used to run the NDES service
 - Must be a member of the local IIS_IUSRS group
 - Must have request permission on the configured CA
 - Must be a domain user account and have Read AND Enroll permissions on the configured templates (Refer to the next section for details.)
 - Must have SPN set in Active Directory
- **Device Administrator**: User who manages the devices and should request a one-time password from the service to enable security enrollment

User must have Enroll permissions on the Certificate Template which are used by NDES to request certificates against the CA

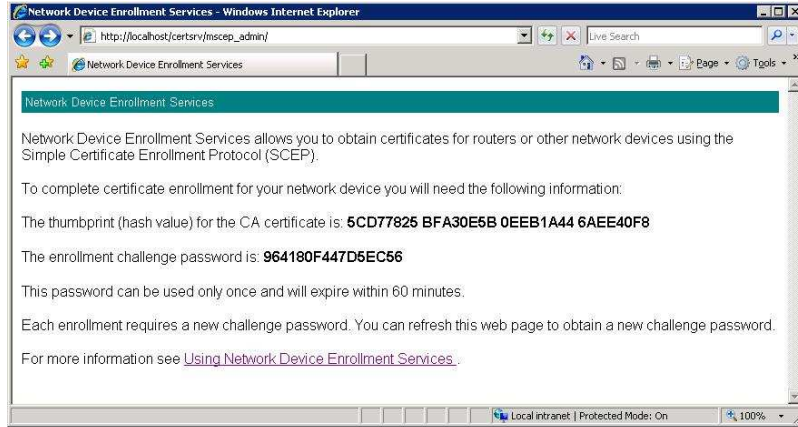
About this task

Enterprise and Datacenter Editions can enable NDES Service Role.

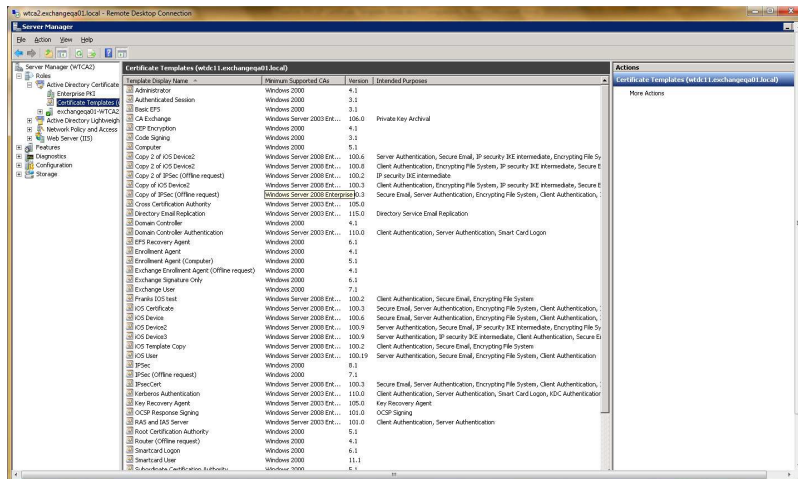
Standard Edition does not support NDES and therefore can't be used in this scenario.

Procedure

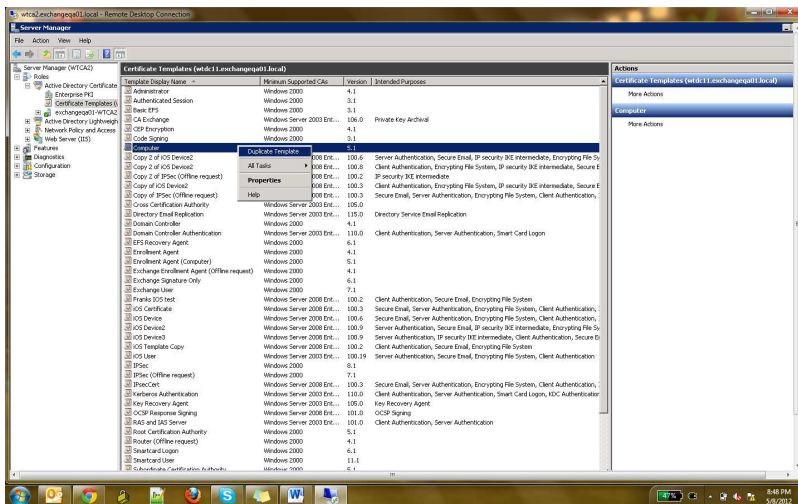
1. Make sure the SCEP is working.
 - a. Browse to the SCEP admin URL: `http://<ServerName>/certsrv/mscep_admin/`.
 - b. Enter the Device Administrator Credentials. You should see a screen like the following:



2. Configure a Certificate Template on the SCEP server that can be used with MaaS360. If you have already created a working template, compare your template properties with the details in this section.
 - a. Log on to the Microsoft SCEP server using the SCEP Admin credentials.
 - b. Open the Server Manager and select **Roles > Active Directory Certificate Services > Certificate Templates**.



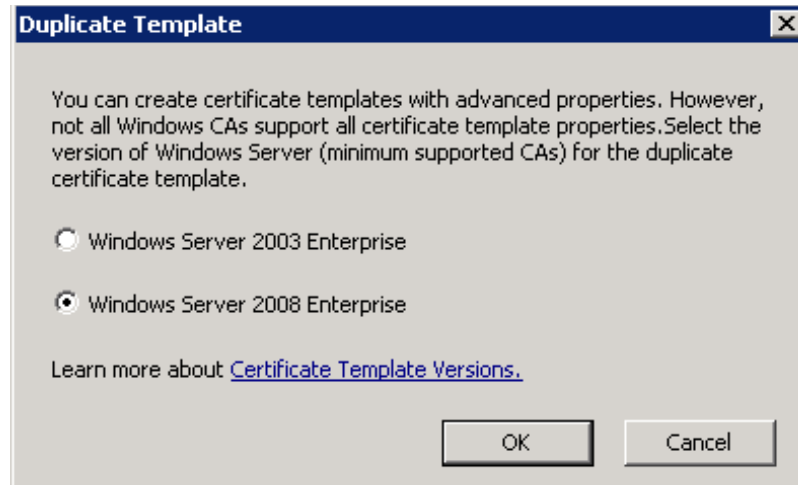
- c. Right-click **Computer** and select **Duplicate Template**.



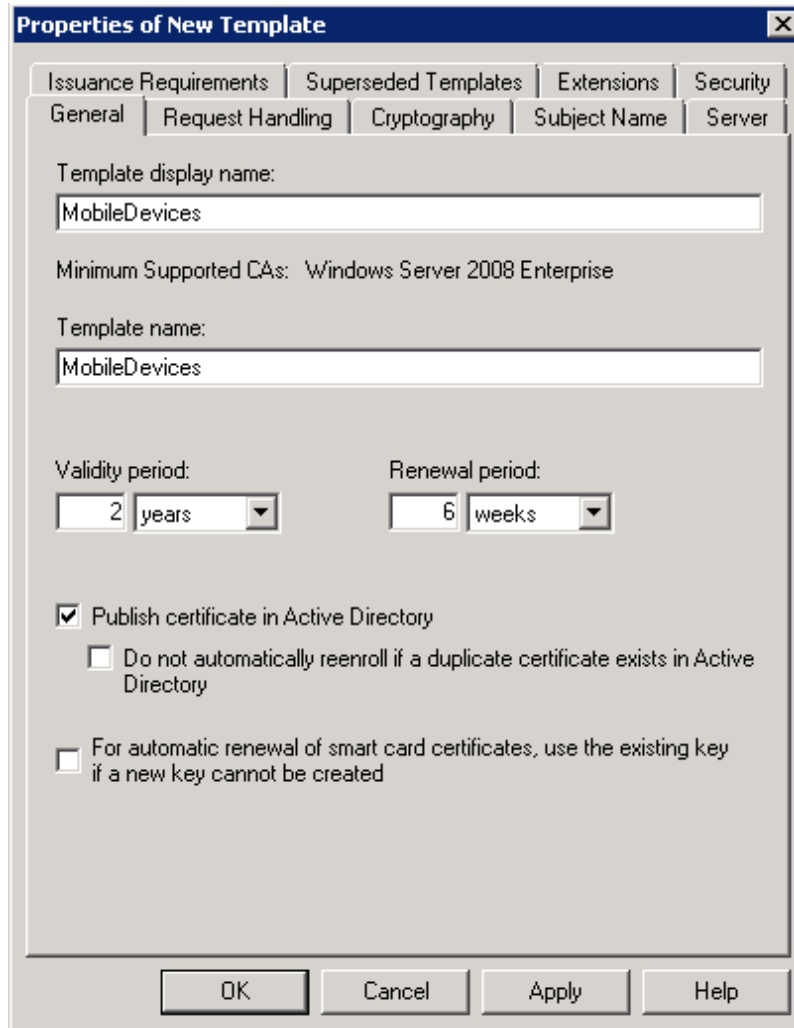
Important: Do not duplicate a user template. Microsoft SCEP does not work with user templates. If your template is based on a user template, create a new template based on the Computer template.

iOS 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.

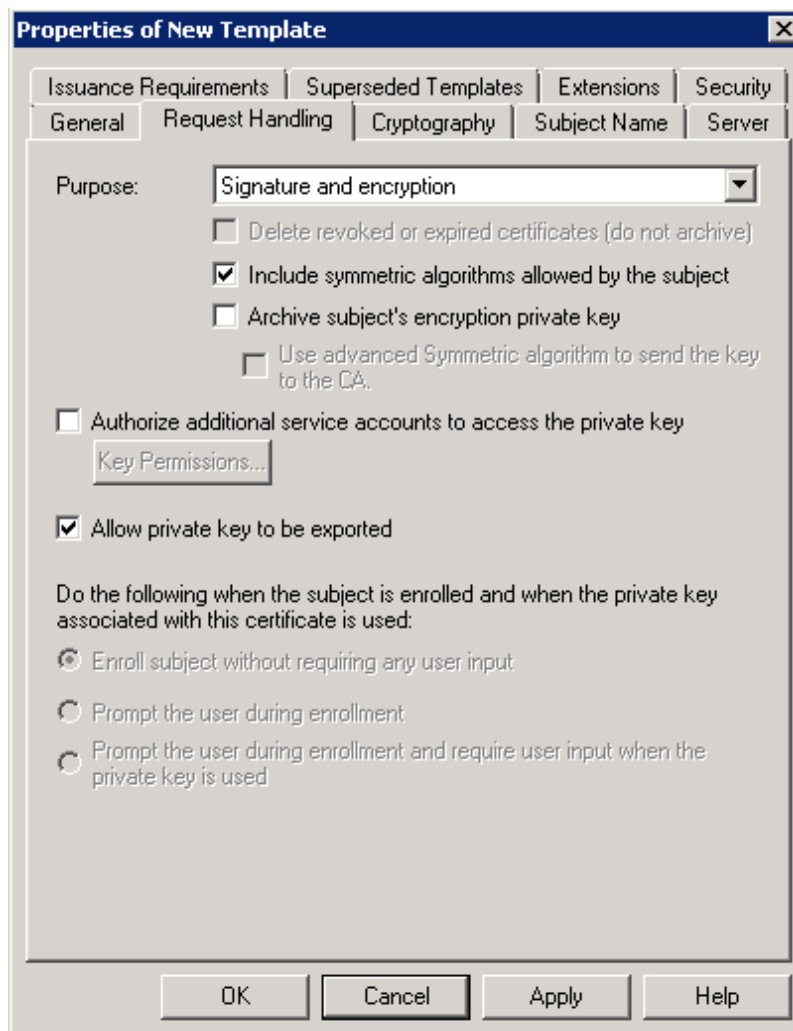
- d. Select Windows Server 2008 Enterprise as the minimum supported CA version in order to access advanced template properties.



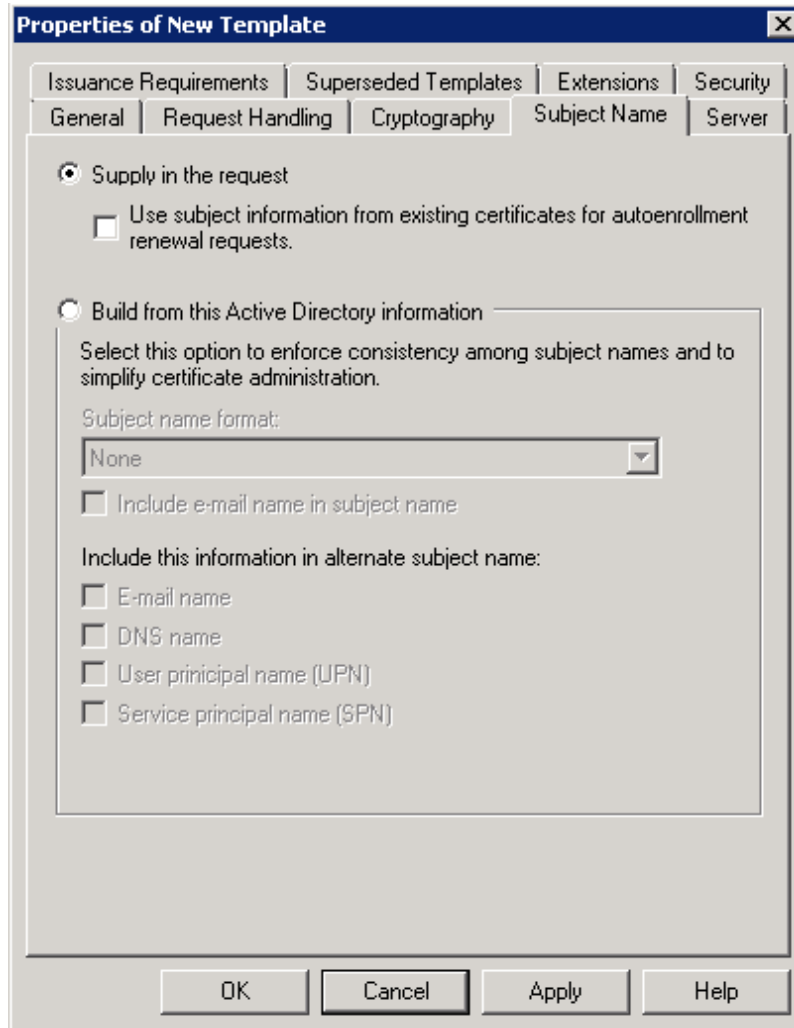
- e. Enter the following settings on the **General** tab.
 - 1) Enter a template display name.
 - 2) Copy the template name (without spaces) for later use.
 - 3) Select **Publish certificate in Active Directory**.



- f. Enter the following settings on the **Request Handling** tab.
- 1) Include symmetric algorithms allowed by the subject
 - 2) Allow private key to be exported



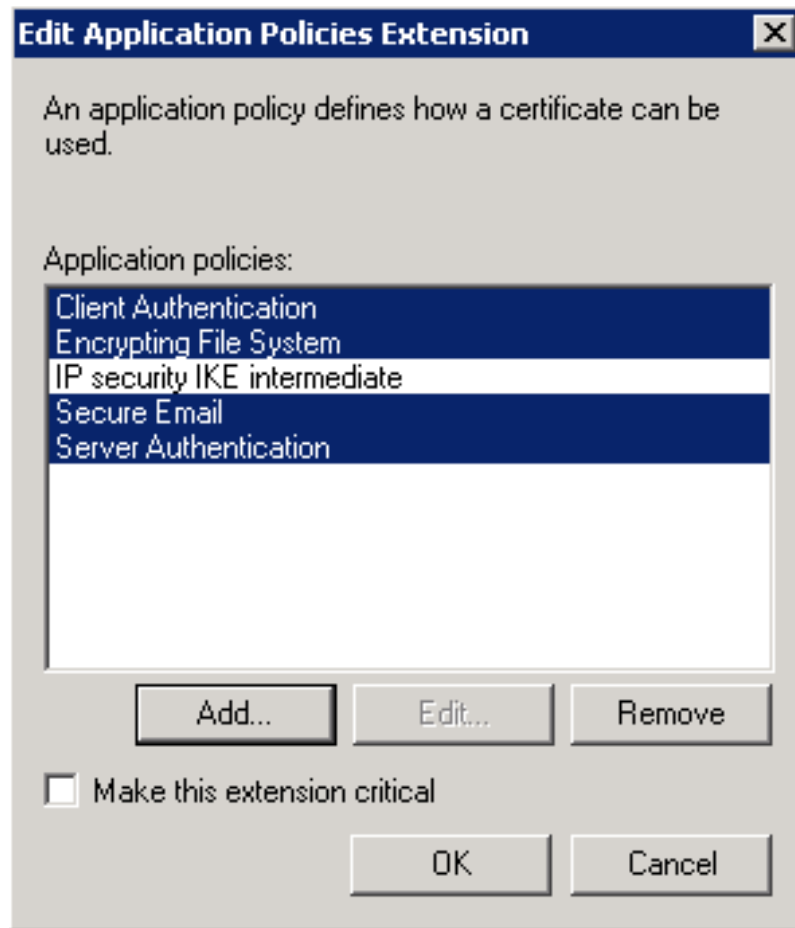
- g. Enter the following settings on the **Subject Name** tab.
Supply in Request: The Subject is supplied from the Cloud Extender template (discussed in a later section)



- h. Enter the following settings on the **Security** tab, make sure the following accounts exist and have corresponding permissions. Add them if necessary. This is the most important section in the template configuration.

Account	Permissions
Authenticated Users	Read
SCEP Service Account (from Step 1)	Read, Enroll
Domain Admins	Read, Write, Enroll
Enterprise Admins	Read, Write, Enroll
Device Administrator (from Step 1)	Read, Enroll

- i. In the **Extensions** tab, add the following for **Applications policies**.
Client Authentication
Server Authentication
- j. Optionally, in the **Extensions** tab, add the following.
Encrypting File System
Secure Email



- k. In the **Extensions** tab, confirm that the *Subject Type = Computer* for **Certificate Template Information**.
- l. Click **Apply** and close the template.

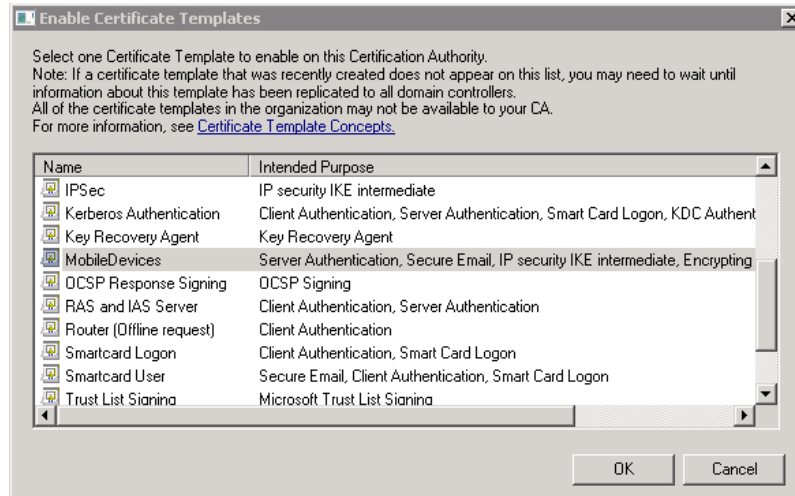
What to do next

Now go to “Enable the New Certificate Template on the Certificate Authority.”

Enable the New Certificate Template on the Certificate Authority

Procedure

1. Log on to the certificate authority server with administrative credentials.
2. Start Server Manager and open **Roles > Active Directory Certificate Services > Your CA > Certificate Templates**.
3. Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.
4. Select the newly created Certificate Template and click **OK**.



After this process, it might take some time for the published Certificate Template to be available on all Domain Controllers.

Set up the Default Certificate Template on NDES

About this task

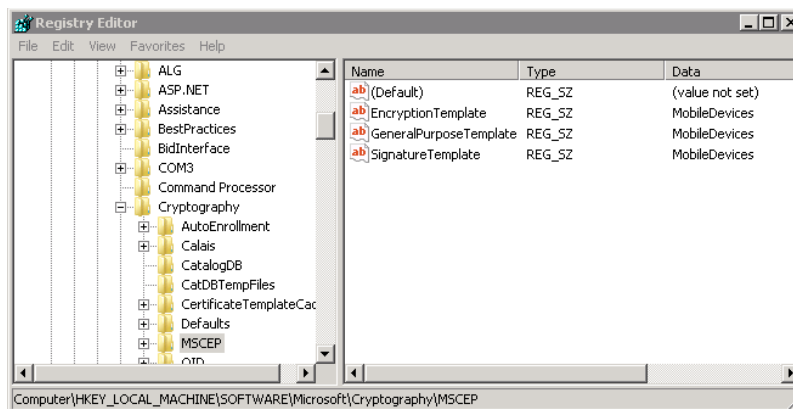
The registration authority (NDES Service) needs to specify the default template to use when requesting certificates on behalf of mobile devices.

This is done via the Windows Registry on the NDES server. This section describes the steps to set the newly created certificate template on Steps 2 and 3 as the default template on the NDES server.

Procedure

1. Log in to the NDES service with Administrative credentials.
2. Open the registry (**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.
 - EncryptionTemplate
 - GeneralPurposeTemplate
 - SignatureTemplate

You need to set these registry keys with the value in *Template Name*. Do not use the *Template Display Name*. The value in the *Template Name* field does not have any spaces.



5. “Restart IIS on NDES” on page 84.

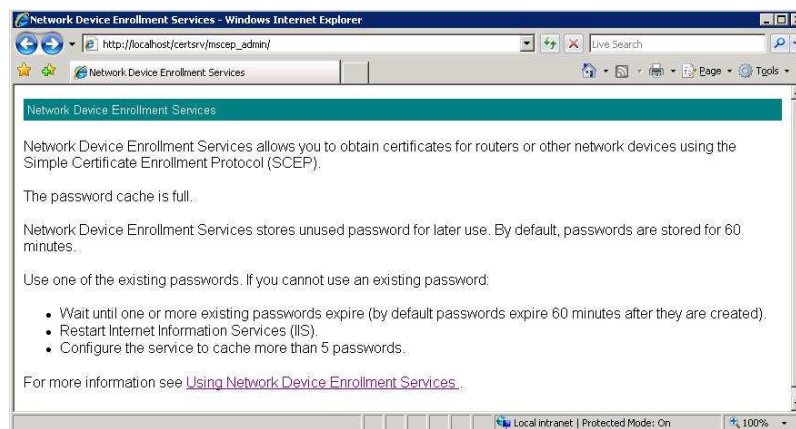
Increase the Password Cache Limit on NDES

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 have been used for certificate requests.

The default setting on the NDES server is 5 cached passwords.

If you load the SCEP Admin URL 5 times to test, and then request a challenge password the sixth time, the NDES server displays the following error:

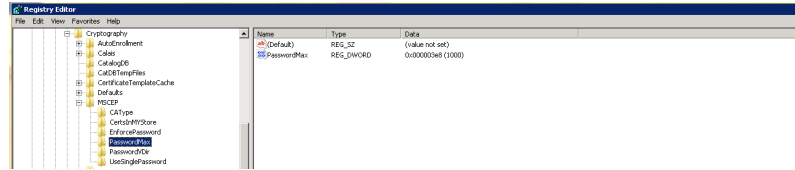


To work around this issue, consider configuring NDES to cache more than 5 passwords.

Procedure

1. Log in to the NDES server using administrative credentials.
2. Open the registry (**Start > Run > regedit.exe**).
3. Go to HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP.
4. Create a new key called PasswordMax.

- Under the **PasswordMax** key, create a new DWORD key **PasswordMax** and raise its value to perhaps 50% of your total device count.



- “Restart IIS on NDES.”

Increase the Maximum Query String Size on NDES

About this task

IIS is installed by default with the Request Filtering feature enabled and the default Maximum Query String Size is set to 2048 bytes. This means that any certificate request made with a longer query string size is filtered out.

MaaS360’s Cloud Extender uses query strings during certificate requests and this size is greater than 2048 bytes. In order to enable Cloud Extender to request for certificates against NDES, you must increase this size.

To increase the Max Query String Size, perform the following steps:

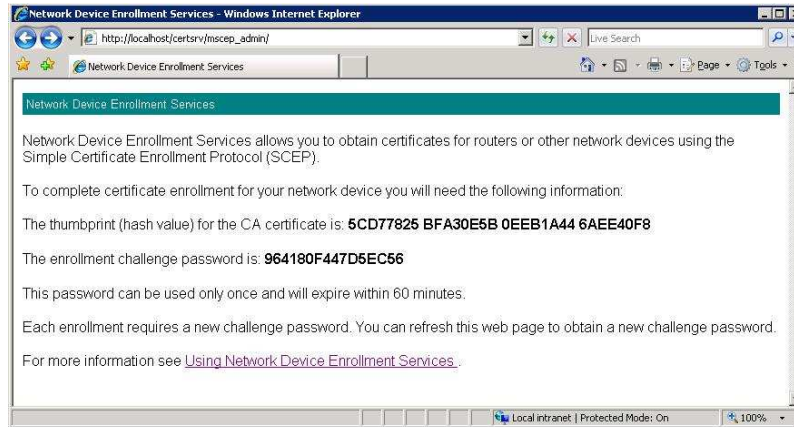
Procedure

- Log in to the NDES server with administrative credentials.
- Start a command prompt with admin privileges (**Start > Cmd > right-click > Run As Admin**).
- Copy the following command and execute this at the command prompt.
`%windir%\system32\inetsrv\appcmd set config /section:requestFiltering /requestLimits.maxQueryString:8192` This sets the max query limit to 8192 bytes.
- “Restart IIS on NDES.”

Restart IIS on NDES

Procedure

- Log in to the NDES server with administrative credentials.
- Start a command prompt with administrator privileges (**Start > Cmd > right-click > Run As Admin**).
- Enter `iisreset`.
- Confirm that the settings have been configured correctly.
 - Open a browser window and go to the SCEP Admin URL:
http://<ServerName>/certsrv/mscep_admin/.
 - Enter your device administrator credentials.
 - Confirm that the SCEP Admin URL returns a challenge password.



Assign Policies to Devices for Certificate Delivery

About this task

Once the template is created and saved on the Cloud Extender, the Template Name starts to appear in MaaS360 Device Policies for iOS under the following sections:

- **Wi-Fi > Identity Certificates**
- **VPN > Identity Certificates**
- **Exchange ActiveSync > Identity Certificates**

You can now configure email, Wi-Fi or VPN profiles to use the certificate template and publish the policies. This policy when assigned to a device triggers a certificate request and the profile delivery along with the certificate to the device.

Procedure

1. In the MaaS360 portal, select **Manage > View All Devices**.
2. Click the link for an enrolled iOS device.
3. Select **Actions > Change iOS Policies**.
4. Select the published iOS policy with the certificate template.

The device should now be associated to the certificate template policy.

Once the device has downloaded the policy, MaaS360 triggers a certificate request to the Cloud Extender for this particular device. The certificates are requested from the PKI and then delivered and installed on the iOS device.

Note: It takes about 10-15 minutes for the Email, VPN or Wi-Fi settings (that uses certificates) to appear on the device. If the settings are installed, the certificates are installed as well. MaaS360 does not push the settings to the device without getting the certificate from your CA.

5. Confirm if the certificate is installed on the device.
 - a. Select **Manage > View All Devices**.
 - b. Select the iOS device.
 - c. Choose **Summary**, then look at the **Security > Compliance** section.

Profile Name	Profile ID	Organization
ActiveSync (12)	com.maa360.mdm.ios.policies.eas	MaaS360
App Catalog	com.maa360.mdm.ios.provision.mebapp	MaaS360
Certificates, IMAP... (12)	com.maa360.mdm.ios.policies	MaaS360
MaaS360 MDM Profile	com.maa360.mdm.ios.provision	MaaS360
Passcode (12)	com.maa360.mdm.ios.policies.passcode	MaaS360
Restrictions (12)	com.maa360.mdm.ios.policies.applicationaccess	MaaS360
VPN (12)	com.maa360.mdm.ios.policies.vpn	MaaS360
Wi-Fi (12)	com.maa360.mdm.ios.policies.wifi	MaaS360

The *Configuration Profiles* section should have the profiles installed.

If the Email, VPN or Wi-Fi profile that uses certificates is listed, the certificate is installed on the device.

Update a Certificate on iOS

Procedure

1. Log in to MaaS360.
2. Go to **Manage > View All Devices**.
3. Select the iOS device that has the certificate installed.
4. Click **ACTIONS** and select **Update Device Certificate**. This action provides two possible options.
 - **Generate a new Device Certificate from certificate authority**
This option clears the existing device certificate on the Cloud Extender's cache, and requests for a new device certificate from the NDES server.
 - **Republish the existing Device Certificate to the device**
This option tells the Cloud Extender to re-send the device certificate from its local cache that can be republished and pushed to the device.

Are you sure you want to update the device certificate for "Eric Peterson - Company 3G iPad"?

Generate a new Device Certificate from Certificate Authority
 Republish the existing Device Certificate to the device

Comments (Max. 64 chars)

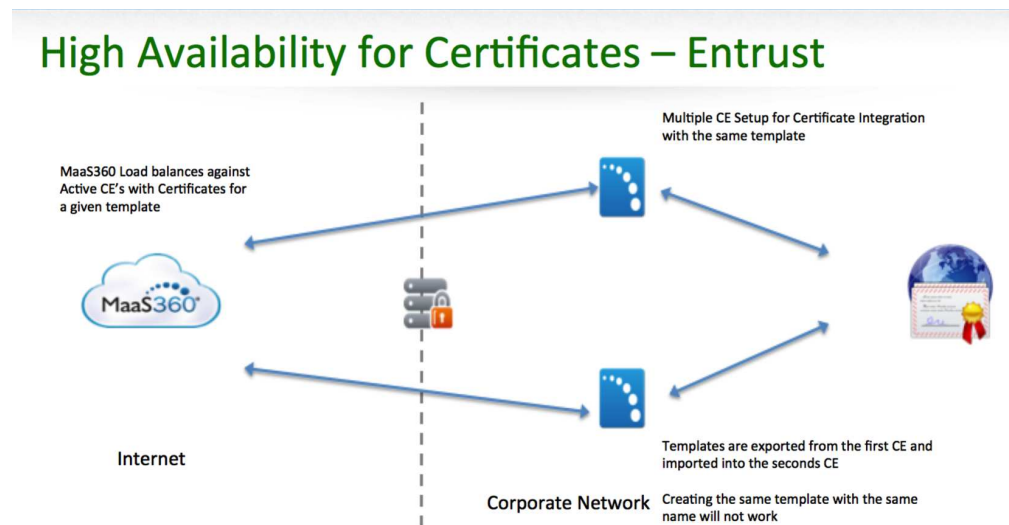
Chapter 8. High Availability (HA)

MaaS360 Cloud Extender supports High Availability configuration for the Certificate Integration module. Multiple Cloud Extenders can be spun up and configured with the same Certificate Template for Active-Active HA configuration.

High Availability (HA) Architecture

HA configuration for Certificate Integration module involves importing the same Certificate on all active Cloud Extenders in the HA Cluster.

MaaS360 portal takes care of automatically load-balancing certificate generation and renewal requests among active Cloud Extenders in a round-robin fashion. The architecture below highlights this configuration with two Cloud Extenders.



Configure for High Availability (HA)

Before you begin

Configure a Cloud Extender for Entrust CA Certificate Integration using "Use an Entrust CA" on page 71.

About this task

The assumption is that there is already a Cloud Extender configured for Entrust CA Certificate Integration as the instructions in the Stand-alone Configuration section. Steps to implement additional Cloud Extenders are highlighted below:

Procedure

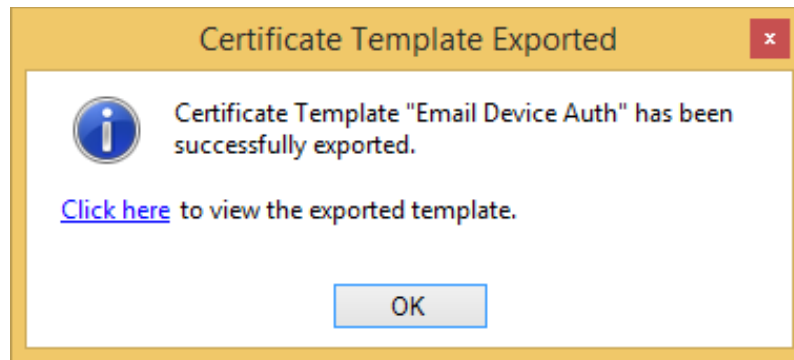
1. Export the Certificate Templates from the first Cloud Extender using the Export option against the Certificate Template on the Cloud Extender tool.

Configure Certificate Templates

[Help](#)

Template Name				
Email Device Auth	✖	✎	⚙	👤

- Once the Template is exported, the tool provides a link to the default exported location of the templates.



- Copy over the exported templates on the other Cloud Extenders in the HA cluster.
- On the next Cloud Extender server, within the Cloud Extender Configuration Tool, go to the Certificate Template screen, **click the**

button.

- Select Import Certificate Template and browse to the exported template file(s) to import the same template.

Template Configuration

[Help](#)

Create New Template

Device Certificate
For Device Identity Certificates

User Certificate
For User Certificates or S/MIME Encryption and Signature Certificates

Import Certificate Template

C:\ProgramData\MaaS360\Cloud Extender' ...

- Hit Save to save the template and run Test actions to confirm that test certificates can be issued.
- Repeat the above steps on all Cloud Extenders on the cluster.

Troubleshooting High Availability

- Watch the logs from C:\%ProgramData%\MaaS360\Cloud Extender\logs\EMSAgent_YYYY_MM_DD.log.
- Search for "PKIE-CERTACT".
- Run Cloud Extender Diagnostic Logs collection Tool:
 - Login to the Cloud Extender server
 - Browse to C:\Program Files(x86)\MaaS360\Cloud Extender.
 - Double click DiagnosticCmd.exe. (This generates a zip file on your desktop.)

4. Contact IBM Support to diagnose the issue.

Chapter 9. Mobile Enterprise Gateway Module

IBM MaaS360 Mobile Enterprise Gateway (MEG) provides simple, seamless and secure access to behind-the-firewall information resources to your mobile users. This access can be enabled for your mobile population without requiring you to implement a new VPN-like technology. IBM MaaS360 provides great user experience and usability benefits, including:

- Seamless logon
- Credential caching
- One-time logon across multiple applications
- Single sign-on to protected intranet resources that are protected by strong authentication schemes like NTLM, Kerberos, SPENGO and Identity Certificates

MaaS360 Mobile Enterprise Gateway solution provides maximum security by authenticating users and devices based on Corporate Directory credentials and MaaS360 Enrollment Identity Certificates thereby satisfying two-factor authentication requirements for intranet resources. The solution ensures that all communication between mobile devices and the Mobile Enterprise Gateway is fully encrypted and secured end-to-end – hence preventing man-in-the middle attacks.

All data on the Mobile Device is stored within the context of the MaaS360 container solution, fully encrypted and protected from data leakage that are fully controlled by MaaS360 container security policies as your security requirements. Additional security benefits include the following:

- Seamless background re-authentication of users and devices without prompting end users for credentials
- Authentication token requirements for every intranet resource
- Proxy access list validation on the gateway

Tight integration with the MaaS360 portal helps define lockout policies and provides ability to pull back access to the gateway based on automated compliance rules.

MaaS360 Mobile Enterprise Gateway helps your organization mobilize corporate resources to your ever-growing mobile population while still maintaining control over the data flow and associated data security.

Key Features

- Seamless integration with MaaS360, Easy & Simple Configuration
- Cloud Extender module integration
- Strong gateway authentication schemes
- Cross Forest / Cross Domain authentication
- Support for SSO for Gateway across multiple apps on a device
- Support for Kerberos / SPENGO & NTLM v2 authentication against sites
- Internal Proxy support for sites
- Granular proxy access list
- Seamless High Availability (HA) configuration
- High-scaling up to 100k devices

- Regional Gateway Cluster support & automatic local gateway routing
- Streaming scenarios – large files and videos
- WebDAV support for Windows File Shares
- Relay DR support

About Gateway Modes

MaaS360 Mobile Enterprise Gateway operates in 2 modes:

Relay Access Mode: In this mode, the gateway establishes an outbound access to the MaaS360 relay server. The devices talk only to the relay server and not directly to the gateway.

Important: Relay Access mode is currently not supported for IBM MaaS360 On-Premises.

Direct Access Mode: In this mode, the devices directly talk to the MaaS360 Mobile Enterprise Gateway for direct resource access and completely bypasses the MaaS360 hosted relay servers.

In addition to the two modes, the gateway can be installed as a stand-alone gateway for smaller deployments and also as a clustered gateway for High Availability.

Requirements and Scaling for Mobile Enterprise Gateway

System Requirements

Before beginning the installation, make sure the following requirements are met:

Item	Meets Requirement
Physical or Virtual Machine with Windows Server 2012 RC2, 2012, 2008 RC2, or 2008	
Supported clients: iOS 6.0 and higher Android 4.2 or later (carrier versions)	

Scaling

MaaS360 Mobile Enterprise Gateway provides the point of control for mobile access to business resources. Before beginning the installation, make sure the following requirements are met:

Devices	< 10000	> 10000 devices
CPU	2 Cores (2.8Ghz)	Use Additional Gateways in High Availability Mode
Memory	4 GB	
Storage	2 GB	

Scaling for High Availability

Device Counts	Scaling recommendation
Non-HA gateway < 10000 devices	1 gateway is sufficient No HA possible
HA gateway < 10,000	2 gateways running in clustered mode. Even if one gateway can handle the load, it is recommended to spin up another instance from a HA perspective
HA gateway > 10,000 and < 20,000	3 gateways running in clustered mode. In case of outage for one of the gateways, the other 2 gateways can handle load
For every 10,000 device increments	1 gateway per 10,000 devices plus 1 clustered gateway for handling outage load. For example: 50,000 devices would require 6 gateways.

Permission Requirements

Item	Meets Requirement
A <i>Service Account</i> that MaaS360 Mobile Enterprise Gateway can run as: <ul style="list-style-type: none"> • Member of <i>Domain User</i> group on your Active Directory • Member of <i>Local Administrator</i> group on the server 	

Networking Requirements

Access to the following URLs from the Mobile Enterprise Gateway machine:

Port 443 outbound used by the gateway to communicate with MaaS360 Backend and Web Services (see the Base Networking Requirements section for more details).

Note: If you are an on-premise customer, you must allow the Cloud Extender to communicate outbound to your MaaS360 instance within your environment.

If using Relay Mode, **Port 443** outbound used by the gateway to communicate with the Relay Services.

There is no inbound port used for the relay.

Relay Mode

US Relay		
https://us01-gw.meg.maas360.com	https://eu01-gw.meg.maas360.com	https://ap01-gw.meg.maas360.com
173.193.219.242	159.8.170.231	119.81.207.131

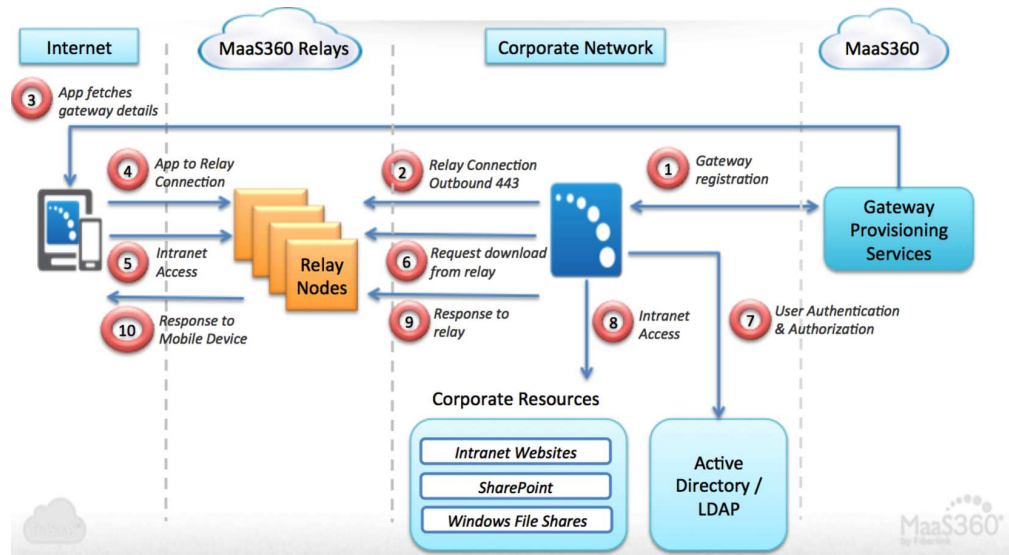
Direct Mode

Inbound connection required from Internet to the Gateway.

Port is configurable through the installation and configuration processes.

Mobile Enterprise Gateway Architecture

Relay Access Mode



Client

- The MaaS360 app for iOS and Android, MaaS360 Secure Browser and any Enterprise App wrapped within MaaS360 or integrated the MaaS360 SDK can communicate with the MaaS360 Mobile Enterprise Gateway.
- MaaS360 apps are available via iTunes or Google Play, and can also be pushed to devices through the App Catalog.
- The apps connect to the relay services via HTTPS and post requests and pick-up responses.
- In addition to the SSL connections to the relays, the payloads themselves are encrypted with AES-256 bit encryption end-to-end between the app and the gateway.
- Corporate data is secured within the context of the MaaS360 app container & enforcing policies.
- Mobile device itself is never on the organization's network, nor does the MaaS360 apps ever directly see the network. This preserves network security and isolation.

Gateway

- Windows based server software that runs on a physical host machine or Virtual Machine (VM) on your organization's internal network or DMZ.
- Packaged along with the Cloud Extender as a module.
- The gateway establishes outbound connections to the MaaS360 Relay services in the cloud over port 443.

- 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.
- Gateway authenticates users against Active Directory / LDAP servers.
- Supports Single Sign On (SSO) for upstream sites that challenge for NTLM, Kerberos, SPNEGO and Identity Certificate based authentication.

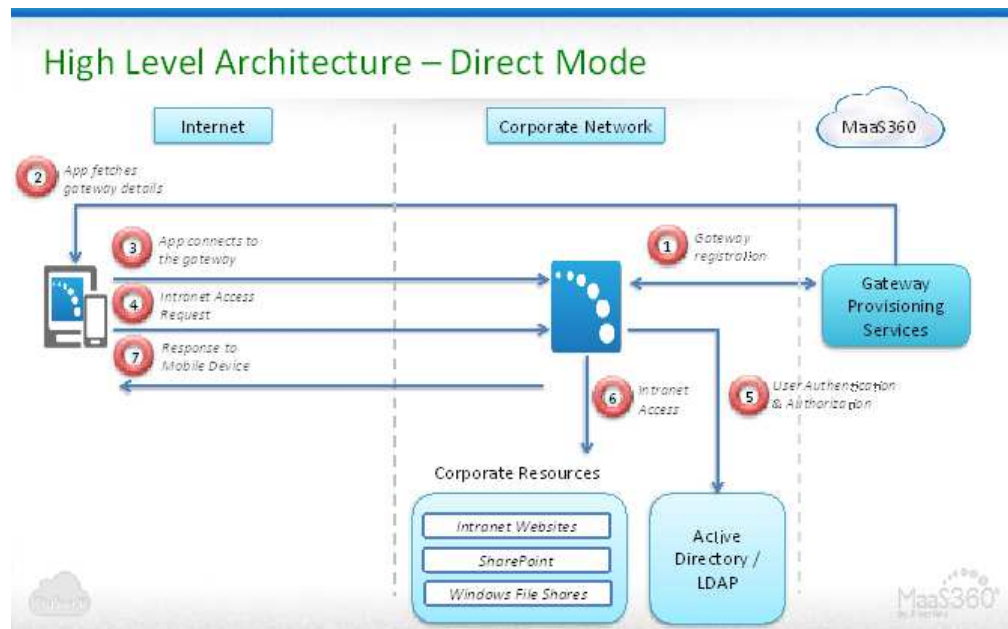
Gateway Provisioning Services

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

Relay Server

- Web services in the cloud that facilitates communications between the clients and your gateway.
- The Link service can not read the encrypted communication between the clients and the gateway.

Direct Access Mode



Client

- The MaaS360 app for iOS and Android, MaaS360 Secure Browser and any Enterprise App wrapped within MaaS360 or integrated the MaaS360 SDK can communicate with the MaaS360 Mobile Enterprise Gateway.
- MaaS360 apps are available via iTunes or Google Play, and can also be pushed to devices through the App Catalog.
- The apps connect directly to the gateway for intranet resource access.
- Access via HTTPS if SSL certificate is used.

- In addition to the SSL connections to the gateway, the payloads themselves are encrypted with AES-256 bit encryption end-to-end between the app and the gateway.
- Corporate data is secured within the context of the MaaS360 app container & enforcing policies.

Gateway

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

Install the Mobile Enterprise Gateway

Before you begin

The Enterprise Gateway feature should have been enabled on your account. If this has not been enabled, please contact your Fiberlink representative.

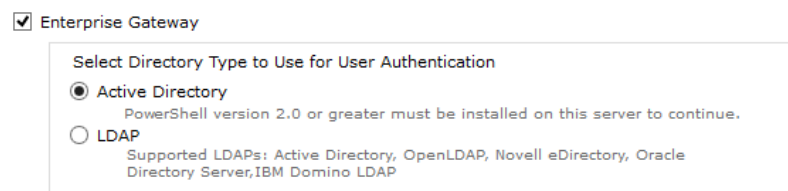
Procedure

1. Log in to MaaS360 and browse to the Services page (**Setup > Services**).

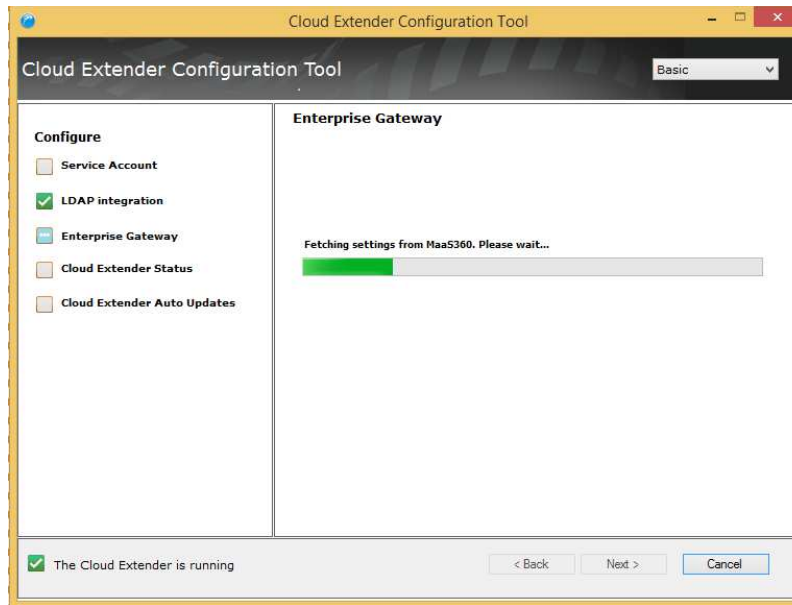


The list of available relay servers is shown on this screen (only for relay mode). The list here is just indicative and the list may differ depending on your account.

2. Install the Cloud Extender on the gateway server you have provisioned using the steps from the Basic Cloud Extender Installation section.
3. When the Cloud Extender Configuration Tool has opened, select Enterprise Gateway from the list of services.
4. Select your Directory Authentication type.



5. After LDAP/AD has been configured for User Authentication, click **Next** to move onto configuring the Enterprise Gateway.



Configure Mobile Enterprise Gateway in Standalone Mode

About this task

If you plan to setup your gateways in a High Availability (HA) cluster, skip to Gateway Configuration in HA mode section.

Important: Switching the gateway mode from standalone to HA for an already configured gateway is not supported.

Procedure

1. To configure the Gateway in Relay Mode, use the following settings.

Gateway Details

Gateway Name

Gateway Mode Relay Direct

Select Relay Server

Accept all Untrusted Certificates
Selecting this option will cause the Gateway to ignore any certificate exceptions while accessing internal resources. It is recommended not to select this option.
 If your internal resources use self-signed certificates, please add these certificates to the Gateway server's Trusted Root Certificate Store.

Configuration Setting	Description
Configuration Mode	Gateway can be configured as a standalone instance or a High Availability cluster. Select Standalone .
Gateway Name	Enter any Gateway Name . This is the name that appears in all MaaS360 portal workflows

Configuration Setting	Description
Gateway Mode	Gateway runs in Relay or Direct mode. Select Relay .
Select Relay Server	Select the Relay Server from the list of available relay servers. MaaS360 administrators provision the relay server list during service provisioning. If any regional relay is missing from your list (US, EU, APAC), please contact your Fiberlink representative
Accept all Untrusted Certificates	By selecting this option, the gateway ignores any certificate exceptions from intranet resources. For e.g., if your intranet site has a self signed certificate, then accessing this site throws a certificate exception. With this option, the exception is ignored and the request is served by the gateway. It is recommended not to check this option and ideally install the site SSL certificates to the Certificate store of the Gateway server.
Database Setup	See Database Setup section for different database configurations.

2. To configure the Gateway in Direct Mode, use the following settings.

Enterprise Gateway

Gateway Details

Gateway Name:

Gateway Mode: Relay Direct

Use Web Server/Load Balancer in front of the Gateway

Gateway External URL (including port):
Http/Https URL for Gateway direct access

Gateway Server Port:
Local port on which the gateway will listen for requests.

Enterprise Gateway

Gateway Details

Gateway Name:

Gateway Mode: Relay Direct

Use Web Server/Load Balancer in front of the Gateway

Gateway External URL (including port):
Http/Https URL for Gateway direct access

Gateway Server Port:
Local port on which the gateway will listen for requests.

Configuration Setting	Description
Configuration Mode	Gateway can be configured as a standalone instance or a High Availability cluster. Select <i>Standalone</i> .
Gateway Name	Enter any Gateway Name. This is the name that appears in all MaaS360 portal workflows.
Gateway Mode	Gateway runs in Relay or Direct mode. Select <i>Direct</i> .
Use Web Server / Load Balancer in front of the Gateway.	If selected, you are required to configure your Load Balancer to: <ul style="list-style-type: none"> Accept traffic from inbound traffic from Mobile Devices. Forward this traffic to the Gateway server.
Gateway External URL (including port)	If a Load Balancer is used in front of the gateway, the Gateway URL is the External URL (hostname) of your Load Balancer. If Load Balancer is not used, the Gateway URL is the hostname of this gateway server. This External URL should include the port, if it is different from the standard ports for HTTP or HTTPS.
Gateway Server Port	Gateway server port is the port on which gateway server runs and listens for requests. If a Load Balancer is used, then ensure that load balancer redirects traffic to this Gateway port. If Load Balancer is not used, the Gateway port is any open port on this gateway server

Configure SSL for Direct Mode

Procedure

Use the following settings.

Enterprise Gateway

Use SSL	<input checked="" type="checkbox"/>
SSL Certificate	C:\Certificates\Certificates\ <input type="button" value="Browse"/>
SSL Certificate needs to be issued by a Public Certificate Authority. Self-signed Certificate is not supported.	
SSL Certificate Private Key	C:\Certificates\Certificates\ <input type="button" value="Browse"/>

Configuration Setting	Description
Use SSL	<p>This option lets you use SSL encryption on top of the AES-256 bit end-to-end encryption to further secure communication between the mobile device and the gateway. Note that this is optional and not using SSL does not compromise the security of the MaaS360 Mobile Enterprise Gateway solution.</p> <ul style="list-style-type: none"> • If you do not use a Load Balancer, then the SSL Certificate (see below) is used by the Mobile Device to initiate an SSL session to the gateway. • If you use a Load Balancer, then the SSL Certificate (see below) is used by your Load Balancer to initiate an SSL session to the gateway. <ul style="list-style-type: none"> – Traffic between the Mobile Device and your load balancer can be secured by your Load Balancer SSL certificate. Please refer to your vendor documentation for this detail.
SSL Certificate	<p>Path to the SSL certificate (.pem) file.</p> <p>If a Load Balancer is not used, then SSL terminates on your gateway.</p> <p>In this case, it is <i>required</i> to get an SSL certificate from a public Certificate Authority (CA) and not use self-signed certificates.</p>
SSL Certificate Private Key	<p>Private key of the SSL certificate (.key) file.</p>
Accept all Untrusted Certificates	<p>By selecting this option, the gateway ignores any certificate exceptions from intranet resources. For example, if your intranet site has a self signed certificate, then accessing this site throws a certificate exception. With this option, the exception is ignored and the request is served by the gateway.</p> <p>It is recommended not to check this option and ideally install the site SSL certificates to the Certificate store of the Gateway server.</p>

About Gateway in High Availability Mode

If you have already setup your gateway in standalone mode, you can skip this section and continue to Gateway Authentication, WebDAV & Internal Proxy settings section.

Why Clustered Gateways?

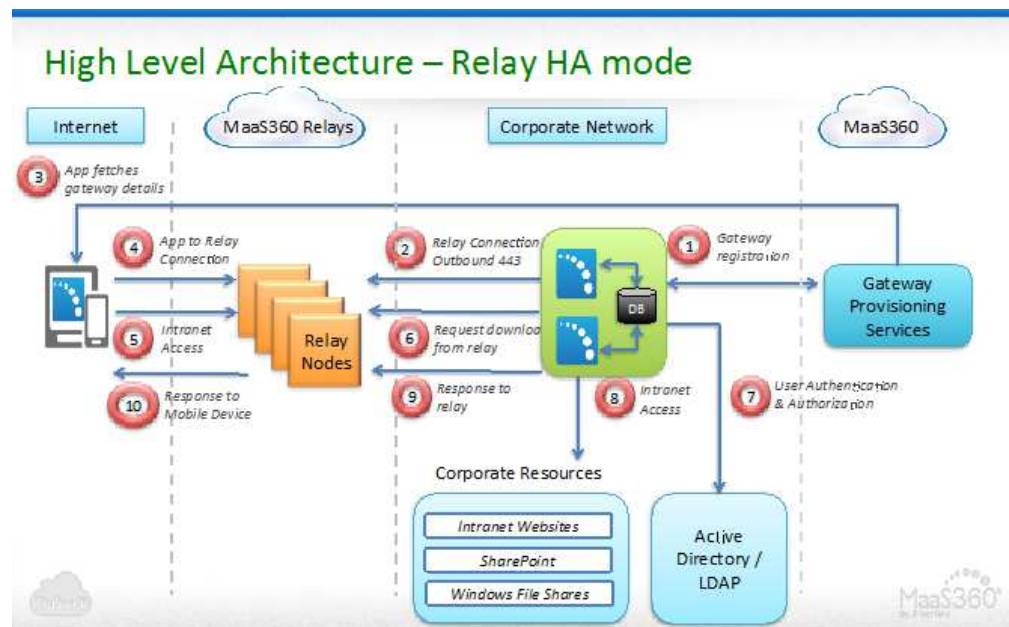
MaaS360 Mobile Enterprise Gateways, when setup in clustered High Availability (HA) configuration, the gateways run in Active-Active mode – all gateways are active and handling requests. Even if one gateway server goes down, the other gateways in the cluster can handle the traffic and prevent an outage. Hence it is always recommended to run your gateways in HA mode.

In addition to high availability, from a scaling perspective, one gateway server can handle 10,000 devices, serving up to 200 devices per second with average response size of 50KB. If you plan to make this service available to more than 10,000 devices, it is recommended to use additional gateways.

High Availability Architecture

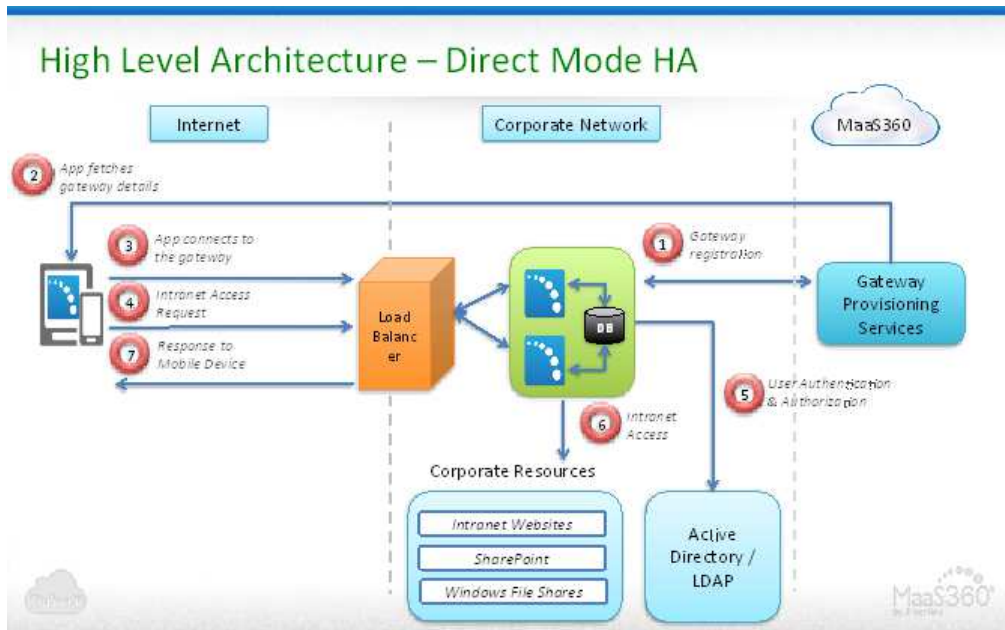
Relay Mode

- In Relay Clustered mode, all gateways talk to a shared database
- Relay Server automatically load-balances requests among the active gateways
- No load-balancer setup required on your network



Direct Mode

- In Direct Clustered mode, all gateways talk to a shared database.
- Required to implement a load-balancer in your network to actively load-balance incoming traffic among active gateways.
- May need to setup SSL certificates for device-to-load-balancer SSL communication.
- May setup SSL certificates for traffic between load-balancer and gateway. This is optional and the data packets between them are anyways encrypted, even over HTTP.



Database Requirements for High Availability

High Availability (HA) setup for MaaS360 Mobile Enterprise Gateway requires a shared database among active gateways to share configuration and authentication information. Hence setting up a database on your database server is necessary. MaaS360 Mobile Enterprise Gateway supports the following database servers:

- Microsoft SQL 2008 or higher
- MySQL 5.6.22+
- DB2 10.5.500.107

Database Integration Requirements

1. Identify and setup the database server that the gateways can integrate with.
Required - hostname and port of the database server for integration
2. Create a blank database within the database server.
Required - database name for integration
3. There needs to be either Local SQL server account or Windows NT account for database access.
Required - *create table* and *read and write permissions* on the database.

Once the gateway service starts, it automatically creates the database tables required for functioning of the Gateway.

Database Sizing Requirements

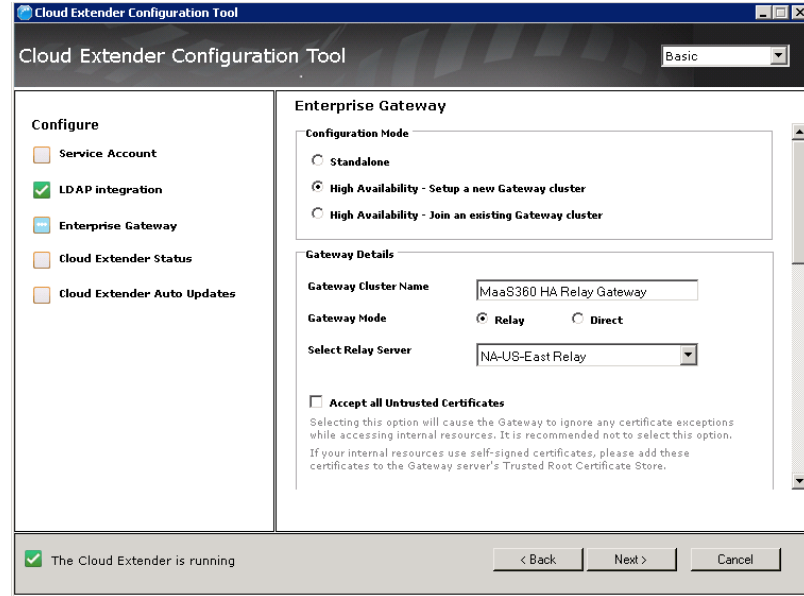
The recommended database size as 10KB per device (# of devices x 10Kb).

If your environment also has Kerberos authentication for your websites, then the database size increases significantly depending on the Kerberos token size and the number of websites that use Kerberos authentication. For sizing assume 50KB per site per user.

Configure Gateway As HA in Relay Mode

Procedure

Use the following settings.



Configuration Setting	Description
Configuration Mode	Gateway can be configured as a standalone instance or a High Availability cluster. Select <i>High Availability – Setup a New Gateway cluster</i> .
Gateway Name	Enter any Gateway Name. This is the name that appears in all MaaS360 portal workflows.
Gateway Mode	Gateway runs in Relay or Direct mode. Select <i>Relay</i> .
Select Relay Server	Select the Relay Server from the list of available relay servers. MaaS360 administrators provision the relay server list during service provisioning. If any regional relay is missing from your list (US, EU, APAC), please contact your Fiberlink representative.
Accept all Untrusted Certificates	By selecting this option, the gateway ignores any certificate exceptions from intranet resources. For example, if your intranet site has a self signed certificate, then accessing this site throws a certificate exception. With this option, the exception is ignored and the request is served by the gateway. It is recommended not to check this option and ideally install the site SSL certificates to the Certificate store of the Gateway server.

Configuration Setting	Description
Database Setup	See “Database Setup for High Availability” on page 106 for different database configurations.

Configure Gateway As HA in Direct Mode

About this task

Procedure

Use the following settings.

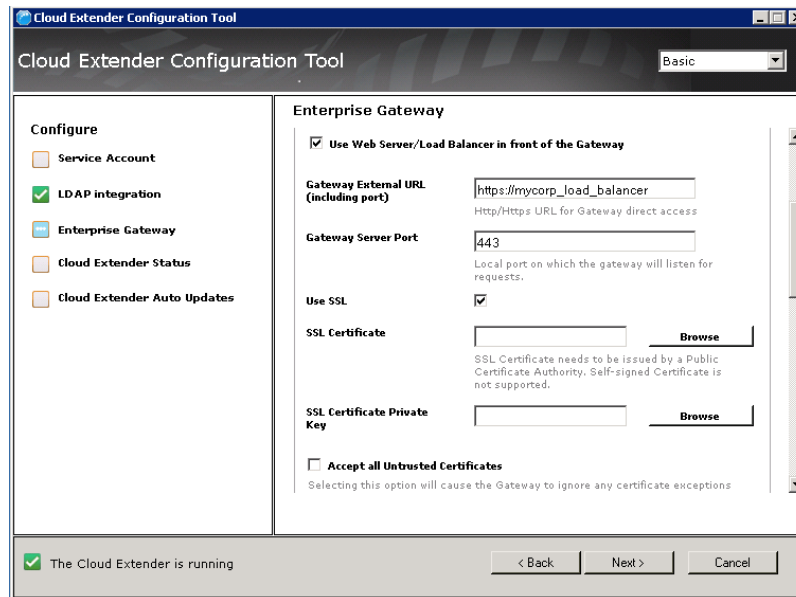
The screenshot shows the 'Cloud Extender Configuration Tool' window. On the left, there is a 'Configure' sidebar with options: Service Account (unchecked), LDAP integration (checked), Enterprise Gateway (checked), Cloud Extender Status (unchecked), and Cloud Extender Auto Updates (unchecked). The main area is titled 'Enterprise Gateway' and contains the following settings:

- Configuration Mode:**
 - Standalone
 - High Availability - Setup a new Gateway cluster
 - High Availability - Join an existing Gateway cluster
- Gateway Details:**
 - Gateway Cluster Name:** MaaS360 HA Direct Gateway
 - Gateway Mode:**
 - Relay
 - Direct
 - Use Web Server/Load Balancer in front of the Gateway
 - Gateway External URL (including port):** https://mycorp_load_balancer
Http/Https URL for Gateway direct access
 - Gateway Server Port:** 443
Local port on which the gateway will listen for requests.

At the bottom, there is a status bar with a checked box 'The Cloud Extender is running' and navigation buttons: '< Back', 'Next >', and 'Cancel'.

Configuration Setting	Description
Configuration Mode	Gateway can be configured as a standalone instance or a High Availability cluster. Select <i>High Availability – Setup a new Gateway cluster</i> .
Gateway Name	Enter any Gateway Name. This is the name that appears in all MaaS360 portal workflows
Gateway Mode	Gateway runs in Relay or Direct mode. Select <i>Direct</i> .
Use Web Server / Load Balancer in front of the Gateway	Turn On the setting. You are required to configure your Load Balancer to: Accept traffic from inbound traffic from Mobile Devices Forward this traffic to the Gateway server

Configuration Setting	Description
Gateway External URL (including port)	<p>If a Load Balancer is used in front of the gateway, the Gateway URL is the External URL (hostname) of your Load Balancer.</p> <p>If Load Balancer is not used, the Gateway URL is the hostname of this gateway server</p> <p>This External URL should include the port, if it is different from the standard ports for HTTP or HTTPS.</p>
Gateway Server Port	<p>Gateway server port is the port on which gateway server runs and listens for requests.</p> <p>If a Load Balancer is used, then ensure that load balancer redirects traffic to this Gateway port.</p> <p>If Load Balancer is not used, the Gateway port is any open port on this gateway server</p>



Configuration Setting	Description
Use SSL	<p>This option lets you use SSL encryption on top of the AES-256 bit end-to-end encryption to further secure communication between the mobile device and the gateway. Note that this is optional and not using SSL does not compromise the security of the MaaS360 Mobile Enterprise Gateway solution.</p> <p>The SSL Certificate (see below) is used by your Load Balancer to initiate an SSL session to the gateway</p> <p>Traffic between the Mobile Device and your load balancer can be secured by your Load Balancer SSL certificate. Please refer to your vendor documentation for this detail.</p>

Configuration Setting	Description
SSL Certificate	Path to the SSL certificate (.pem) file.
SSL Certificate Private Key	Private key of the SSL certificate (.key) file.
Accept all Untrusted Certificates	By selecting this option, the gateway ignores any certificate exceptions from intranet resources. For example, if your intranet site has a self signed certificate, then accessing this site throws a certificate exception. With this option, the exception is ignored and the request is served by the gateway. It is recommended not to check this option and ideally install the site SSL certificates to the Certificate store of the Gateway server.
Database Setup	See “Database Setup for High Availability” for different database configurations.

Database Setup for High Availability

In order to connect the gateways to the shared database, you need the following details:

- Hostname / IP address and port for your database server
- Database Name for Mobile Enterprise Gateway
- Service account credentials – either local or Windows NT credentials.

MySQL Database Configuration

The screenshot shows the 'Cloud Extender Configuration Tool' window. On the left, a 'Configure' sidebar has 'LDAP integration' checked and 'Enterprise Gateway' selected. The main area is titled 'Enterprise Gateway' and contains two sections: 'Shared Database for High Availability' and 'Authentication Details'. In the first section, 'Database Type' is set to 'MySQL', and the 'Database Connection String' is 'jdbc:mariadb://{HOST}:{PORT}/{DB_N}'. There are input fields for 'Username' and 'Password', and a 'Test Database Connection' button. The 'Authentication Details' section has 'Users required to authenticate every' set to '30 (days)' and a checkbox for 'Re-use user's credentials for internal resources that require Basic or Digest' which is unchecked. At the bottom, a status bar shows 'The Cloud Extender is running' with 'Back', 'Next', and 'Cancel' buttons.

Microsoft SQL Database Configuration

Active Directory Mode LDAP Mode

Cloud Extender Configuration Tool

Cloud Extender Configuration Tool Basic

Configure

- Service Account
- Enterprise Gateway
- Cloud Extender Status
- Cloud Extender Auto Updates

Enterprise Gateway

Shared Database for High Availability

Database Type: Microsoft SQL Server

Database Connection String: jdbc:sqlserver://{IP_ADDR};(PORT);da

Use Service Account

Username:

Password:

Test Database Connection

Authentication Details

Users required to authenticate every: 30 (days)
Supported values: 1 to 90

Re-use user's credentials:

The Cloud Extender is running

< Back Next > Cancel

Cloud Extender Configuration Tool

Cloud Extender Configuration Tool Basic

Configure

- Service Account
- LDAP integration
- Enterprise Gateway
- Cloud Extender Status
- Cloud Extender Auto Updates

Enterprise Gateway

Shared Database for High Availability

Database Type: Microsoft SQL Server

Database Connection String: jdbc:sqlserver://{IP_ADDR};(PORT);da

Username:

Password:

Test Database Connection

Authentication Details

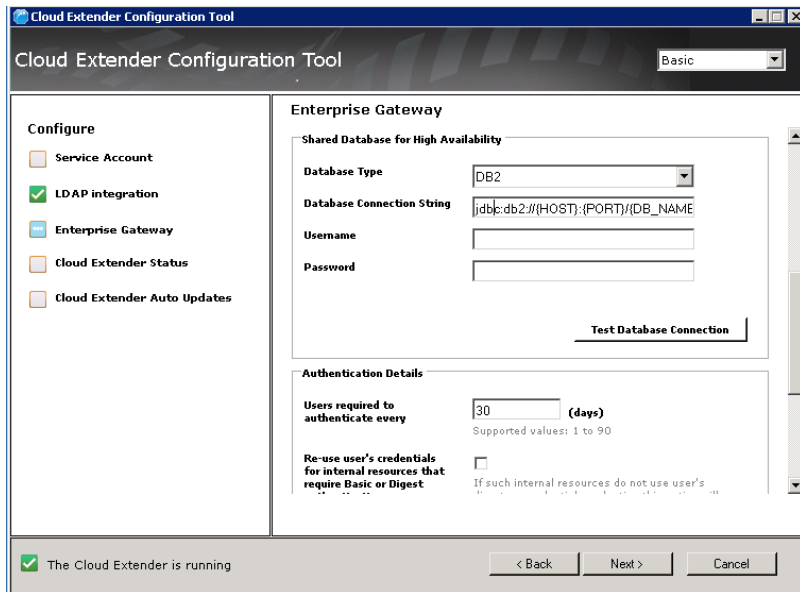
Users required to authenticate every: 30 (days)
Supported values: 1 to 90

Re-use user's credentials for internal resources that require Basic or Digest:
If such internal resources do not use user's ...

The Cloud Extender is running

< Back Next > Cancel

DB2 Database Configuration



Configuration Setting	Description
Database Type	MySQL / Microsoft SQL Server / DB2 – select one depending on your database type
Database Connection String	<p>The database connection string gets automatically populated on the gateway depending on the Database Type selection.</p> <p>You need to replace the {HOST}, {IP_ADDR}, {PORT} and {DB_NAME} with actual values from requirements. Connection strings are as follows:</p> <p>MySQL: jdbc:mariadb://{HOST}:{PORT}/{DB_NAME}</p> <p>MS SQL: jdbc:sqlserver://{IP_ADDR}:{PORT};databaseName={DB_NAME}</p> <p>DB2: jdbc:db2://{HOST}:{PORT}/{DB_NAME}</p>
User name / Password	Local credentials for Local SQL server login
Use Service Account	<p>Only available in AD authentication mode for MS SQL (not available in LDAP).</p> <p>The gateway service account should have the required rights on database.</p>
Test Database Connection	<p>Tests connection to the database using the specified hostname, port, database and service account credentials. Quick test to ensure that all settings are configured correctly.</p> <p>The Cloud Extender Configuration Tool automatically re-checks for database connectivity while saving the gateway configuration.</p>

Join the Gateway to an Existing HA Cluster

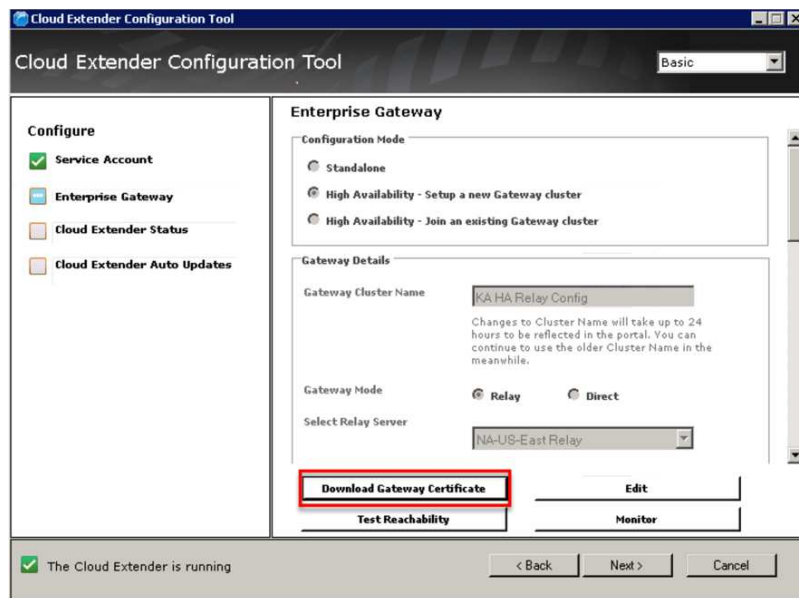
About this task

Procedure

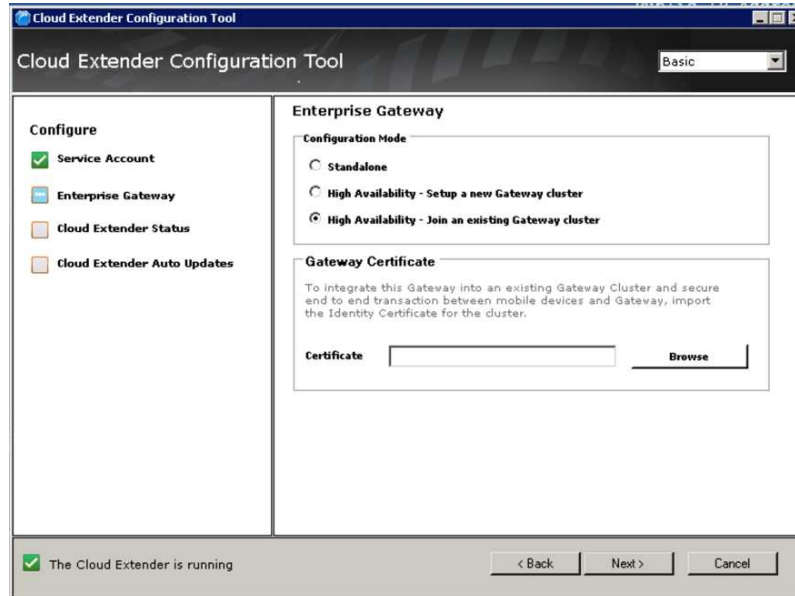
1. Once the first Mobile Enterprise Gateway of the cluster is setup, the gateway generates an encrypted Identity Certificate for the cluster configuration and prompts you to save the certificate.



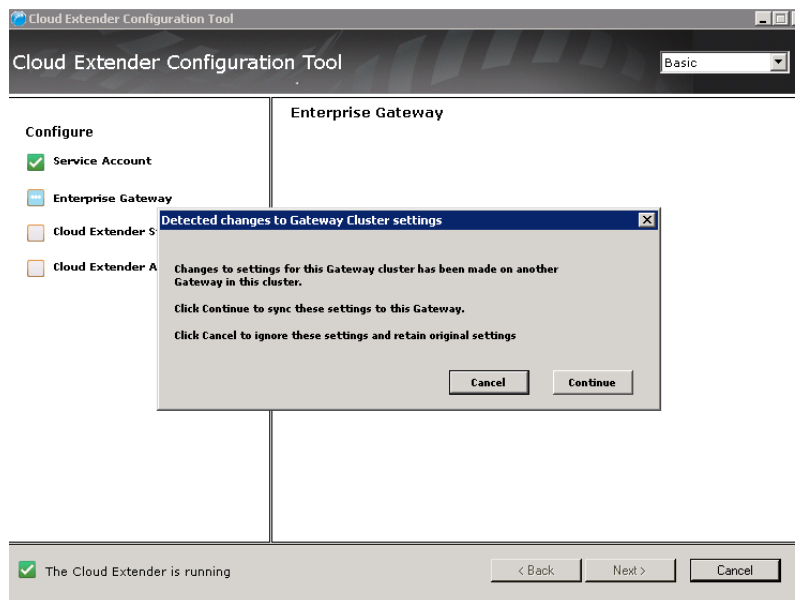
This certificate is required to join new gateways to this HA cluster. If you do not find this certificate, you can always download this certificate again from your first gateway using the **Download Gateway Certificate** button.



2. Browse to this Gateway Certificate. All the gateway settings are automatically downloaded to the new gateway node.



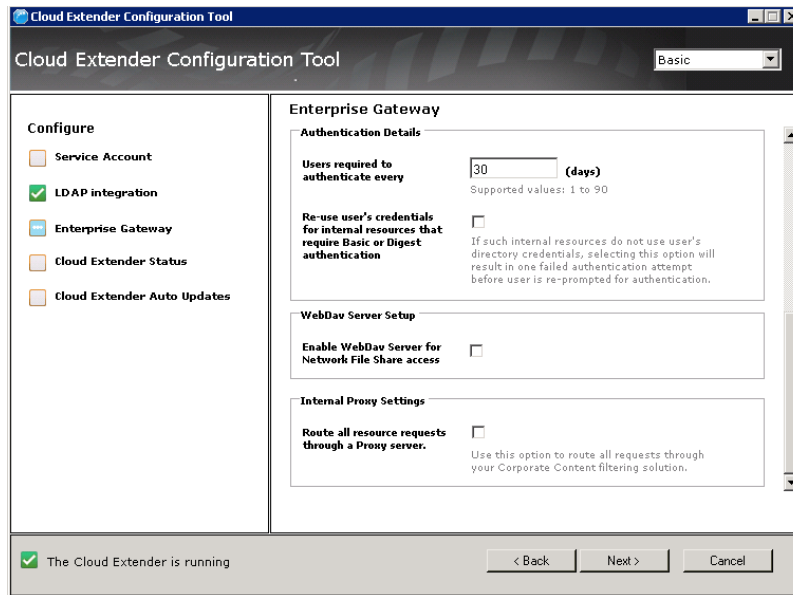
3. Once the gateways are setup in HA mode, if you make a change to the configuration on one of the nodes, you are prompted to update the gateway configuration on other nodes when you launch the Cloud Extender Configuration Tool.
4. Launch the Cloud Extender Configuration Tool on all other gateways and select **Update Configuration** on all of them so that all the gateways are in sync.



Configure Gateway Authentication Details and WebDAV

Procedure

1. Continue to scroll down through the Gateway Configuration pane to configure Authentication and WebDAV.



Configuration Setting	Description
<p>Authentication Frequency:</p> <p>Users required to authenticate every (x) days</p>	<p>This settings controls how often the gateway needs to re-authenticate users connecting to the gateway. Choose any value between 1 and 90 days.</p> <p>It is recommended to select the authentication frequency to 1 day and configure a setting on the MaaS360 portal to cache end user credentials in the MaaS360 app (covered later). This achieves both good end user experience and organizational security requirements.</p>

Configuration Setting	Description
Re-use user's credentials for intranet resources that require Basic or Digest authentication	<p>Certain intranet websites that use Basic or Digest authentication might be integrated with Corporate Credentials for authentication, although this is not very common. If you have one such configuration, use this setting:<i>If the option is checked:</i></p> <ul style="list-style-type: none"> • If an internal site challenge for Basic or Digest authentication, the Gateway provides the end user's credentials it received during gateway authentication and passes it back to the site – thereby seamlessly signing on the user on to the site. • If the authentication fails, the challenge for credentials is sent back to the user on the MaaS360 app. Once the user provides credentials, a new authentication is attempted • However, there is a failed authentication attempt for the user before the user gets a chance to authenticate. <p>If the option is unchecked, all Basic or Digest authentication challenges are propagated back to the user to enter manually</p>
Enable WebDAV server	Enable this if you require to enable access to Network File Shares

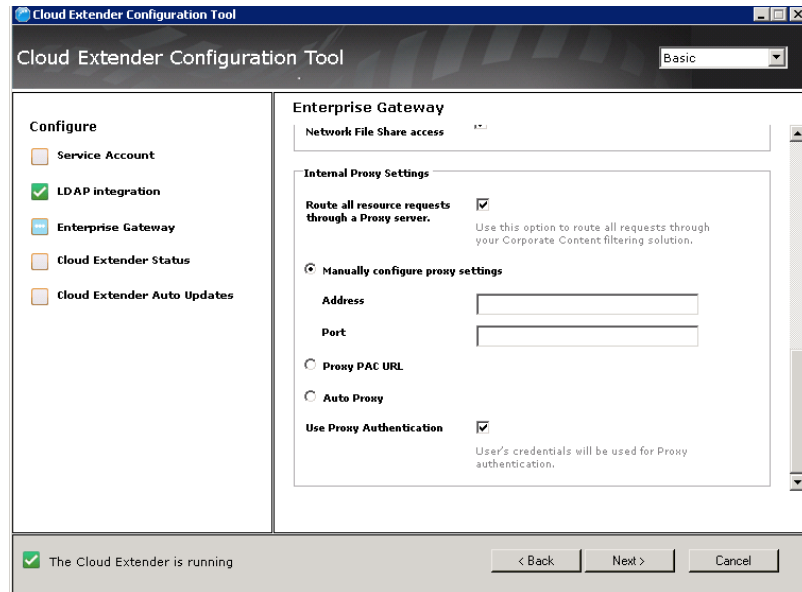
2. If you want to enable access to network file shares, in WebDAV Server Setup, select Enable WebDAV server.

Configure Intranet Proxy Settings for the Cloud Extender

About this task

If you use a proxy server for Internet access, configure proxy settings on this screen.

Cloud Extender uses these settings to reach out to MaaS360 backend services for overall configuration and management.



Procedure

1. Choose your routing method. From the Gateway, if your intranet sites are not directly accessible without going through a proxy or you require to proxy all traffic through a corporate content filtering platform, select **Route all resource requests through a Proxy server**.
2. Choose the proxy setting for your environment.
 - **Manual Proxy:** Enter the hostname/IP and port
 - **Proxy PAC URL:** URL to a PAC file hosted in your environment
 - **Auto Proxy:** PAC file is typically hosted in your DHCP or DNS server as Web Proxy Auto-Discovery Protocol (WPAD) file
 - **No Proxy:** If your network allows direct outbound connection

This proxy setting is only used for intranet resources. External proxy settings are already covered elsewhere in this document

3. If your proxy requires authentication, select the **Use Proxy Authentication** check box.

For authenticating against the proxy server, the end user's credential that is trying to access the resource is used.

All your end users can authenticate against this proxy server.

Note: This proxy setting is only used for outbound connections from the Cloud.

4. Click **Next**. The gateway makes API calls against the MaaS360 backend and gateway provisioning service and completes the gateway registration process.
5. Finish the Cloud Extender Configuration Tool workflow.

Configure Secure Browser and Docs Access

MaaS360 Secure Browser and MaaS360 Docs applications allow your users to access intranet sites through the MaaS360 Mobile Enterprise Gateway. This section provides details on the portal configuration to enable this access.

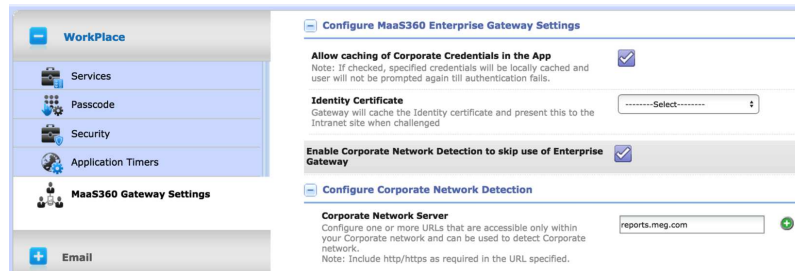
Configure Secure Browser Settings

About this task

Secure Browser configuration for intranet website access is all configured with WorkPlace Persona policies.

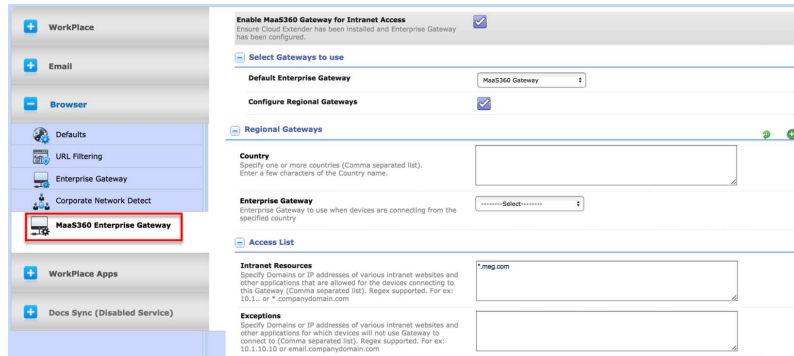
Procedure

1. Access the MaaS360 console and open the WorkPlace Persona policy.
2. Select **MaaS360 Gateway Settings** on the left side of the screen to display the following policy settings.



Policy Setting	Description
Allow caching of Corporate Credentials in the App	<p>With this setting enabled, user credentials are saved within the Secure Browser app in its encrypted database and protected overall by container security.</p> <p>With this setting enabled, the browser re-authenticates against the gateway using these credentials without prompting the user to re-enter credentials each time.</p> <p>End users are prompted for credentials only when their passwords change and the browser fails to authenticate against the gateway.</p>
Identity Certificate	<p>Choose the Identity Certificate Template (from your Cloud Extender's Certificate Integration setup).</p> <p>This Identity Certificate can be used by the gateway to authenticate against upstream intranet sites that challenge for Identity Certificate credentials for authentication</p>
<p>With this feature enabled, the browser traffic for intranet sites skips the Gateway route if any specified <i>Corporate Network Server</i> is resolvable by the browser.</p> <p>With this feature enabled, any sites that require identity certificate-based authentication does not work. Since the gateway is the one that presents the identity certificate to intranet sites that challenge for the same, and in Corporate Network use-case, the gateway route is bypassed; such site authentication does not work.</p>	

3. Click **Browser** on the left side of the screen to expand the options.
4. Select **MaaS360 Enterprise Gateway**.



Policy Setting	Description
<p>Default Gateway</p>	<p>Select one of the gateways or gateway clusters you have already setup. The Gateway Name automatically shows up on the pop-up list.</p> <p>All devices associated with this policy communicate with this Default Gateway if there are no regional gateways configured.</p>
<p>Enabling this feature allows you to route devices to regional gateways or gateway clusters based on the geography of the device.</p> <p>Specify the <i>Country</i> list and the <i>Regional Gateway</i> that the devices in that country should communicate with.</p> <p>The location (country) of the device is determined by the time zone setting on the device and device GPS location.</p> <p>This feature allows you to manage one persona policy for all devices and still achieve location awareness for all devices around the globe.</p>	
<p>Access List for Intranet Resources</p>	<p>Specify Domains or IP addresses of intranet sites that should be allowed for devices connecting to the gateway. Allows wildcards for domains like *.companydomain.com (regular expressions)</p> <p>You should restrict this access list to only intranet sites and domains and not proxy traffic to public sites.</p>

Policy Setting	Description
Exceptions	If you have your Access List set to *.companydomain.com but want certain traffic like email, OWA, etc. to be not proxied via the gateway, you can use the exception list. You would add the domain name of the mail server (email.companydomain.com) to the exception and this traffic directly connects to your server on the internet and it does not use the gateway.

Configure Secure Document for SharePoint / CMIS Access

About this task

MaaS360 Secure Document container allows users to access SharePoint/CMIS repositories and view all files in a Document View.

Procedure

1. Scroll to **Docs > Content Sources** to set up the Secure Document container.
2. Select **Add Source > Microsoft SharePoint**.

Add SharePoint Site

Site Display Name*
This is what your end user will see.

Site Visibility*
 Internal External

Select Gateway*
Select the Gateway for this File Share

Configure Regional Gateways
Enterprise Gateway to use when devices are connecting from the specified country

Browser URL *
Copy this from the browser where you access a SharePoint folder. To let users add their own SharePoint Sites, provide a URL of type
http://mysharepoint.mydomain.com/*
(supported on MaaS360 for iOS 2.90+ and MaaS360 Android 5.21+).

More..

Group Access Permissions
*Select group and set permissions. *Use Workplace Settings* is supported on iOS App 2.40+ and Android App 5.00+.

Configuration Setting	Description
Site Display Name	The name of the site that your end users see on their devices.
Site Visibility	Select Internal to route the traffic through the gateway. Select External if your SharePoint site is publicly hosted and does not require gateway access.

Configuration Setting	Description
Select Gateway	<p>Select one of the gateways or gateway clusters you have already set up. The gateway name automatically appears on the drop-down list.</p> <p>All devices associated with this distribution communicate with this gateway if there are no regional gateways configured.</p>
Configure Regional Gateway	<p>Enabling this feature allows you to route devices to regional gateways or gateway clusters based on the geography of the device.</p> <p>Specify the country and the regional gateway that the devices in that country should communicate with.</p> <p>The location (country) of the device is determined by the time zone setting on the device and device GPS location.</p> <p>This feature allows you to manage one distribution for all devices and still achieve location awareness for all devices around the globe.</p>
Browser URL	<p>URL to your SharePoint site. Access your SharePoint site from your Browser and paste the link to the site directly here.</p> <p>You need a new distribute per site.</p>
Group Access Permissions	<p>Lets you distribute the SharePoint site to a targeted device along with permissions associated with the distribution.</p>

Configure Secure Document for Windows File Share Access

About this task

MaaS360 Secure Document container allows users to access Windows File Shares on their Mobile Devices and view all files in a Document View.

Procedure

1. Scroll to **Docs > Content Sources** to set up the Secure Document container.
2. Select **Add Source > Windows File Share**.

Configuration Setting	Description
Display Name	This is the name of the Windows File Share that your end users see on their devices
Select Gateway	Select one of the gateways or gateway clusters you have already setup. The Gateway Name automatically shows up on the pop-up list as long as it has Network File Share feature enabled. All devices associated with this distribution communicate with this Default Gateway if there are no regional gateways configured.
Configure Regional Gateway	Enabling this feature allows you to route devices to regional gateways or gateway clusters based on the geography of the device. Specify the Country list and the Regional Gateway that the devices in that country should communicate with. The location (country) of the device is determined by the time zone setting on the device and device GPS location. This feature allows you to manage one distribution for all devices and still achieve location awareness for all devices around the globe.

Configuration Setting	Description
Folder Path	UNC path to your Windows File Share (\server\share\file_path) In order to use this capability, WebDAV needs to be enabled on your gateways. The %username% variables can be used to distribute user specific file shares if the folder names are the same as MaaS360 user names.
Group Access Permissions	Lets you distribute the File Shares to targeted device along with permissions associated with the distribution.

Portal Management Workflows

MaaS360 portal offers Cloud Extender Views on the portal to view your gateway installation. This view also helps confirm if your gateway is active and online or not (Cloud Extender online status).

This workflow can be accessed by navigating to **Setup > Cloud Extender** workflow.

On this workflow, you can pick your Gateway server, and once the page loads, select **Summary > Enterprise Gateway**. The page shows:

- Gateway Settings: Name, mode, relay server details, WebDAV details and related settings.
- High Availability details: Mode, Database Type and service accounts.
- Authentication mode: AD / LDAP and associated authentication settings
- Gateway Statistics
- Internal Proxy details (if configured)

Device : WIN-1CVMBDO3TJB		Configuration State: <input checked="" type="checkbox"/>	Cloud Extender Online: <input checked="" type="checkbox"/>
Enterprise Gateway Actions			
	Username	Not Available	Last Reported
	License Status	Active	Installed Date
			04/20/2015 08:17 EDT
			04/16/2015 08:36 EDT
Gateway Settings			
Gateway Name	MaaS360 Gateway	Gateway Mode	Relay
Last Cluster Configuration Modified Time	04/16/2015 17:15 UTC	Last Configuration Modified Date	04/16/2015 17:15 UTC
Relay Server	NA-US-East Relay	Direct URL	-
Use a Webservier or a Loadbalancer in Front of Gateway	No	Local Port on Which Gateway is Running	-
Accept All Untrusted Certificates	No	Enable WebDav Server for Network File Share Access	Yes
SSL Enabled	No		
High Availability Setup			
Configuration Mode	Standalone	Database Type for High Availability	-
Use Service Account for Database Access	No	Database Username	-
Database Connection String	-	Database Domain	-

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

This workflow also provides a test action to test reachability to intranet sites. Under **Actions > Test Reachability (Enterprise Gateway)** let's you specify the hostname / intranet site and confirm reachability of this site from the gateway.

Device : WIN-1CVM8DO3TJB

Enterprise Gateway

Actions

Cloud Extender Actions

- Configure Cloud Extender Settings
- Refresh Data (Enterprise Gateway)
- Test Reachability (Enterprise Gateway)**
- Mark as Inactive
- Uninstall Cloud Extender

Username

License Status

Gateway Settings

Gateway Name

Last Cluster Configuration Modified Time 04/16/2015 17:15 UTC

Relay Server NA-US-East Relay

Note: This action is sent directly from MaaS360 portal to the gateway and it does not traverse through the relays. This test cannot be used to test accessibility through the relay

Test Reachability

Enter the URL

URL

Yes No

MaaS360 also offers a new view of your gateways and clusters. You can access this workflow from **Setup > Mobile Enterprise Gateway** menu. This consolidated view shows all gateways, their configuration mode, and node counts per cluster.

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	

The detailed view also provides a summary of all the settings from a cluster point of view and details of all active nodes. See below.

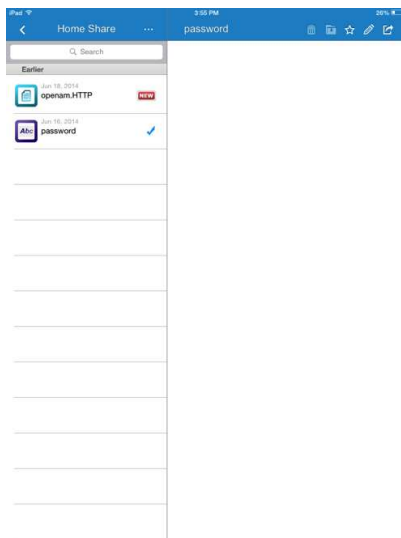
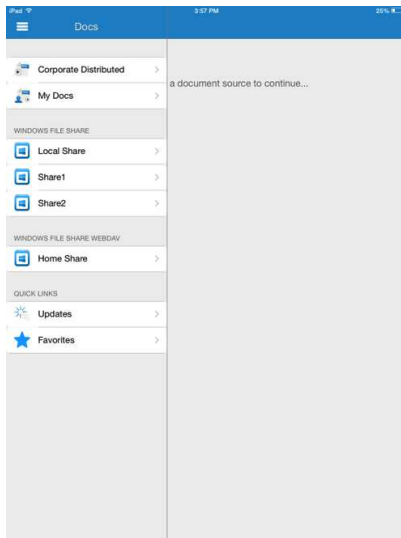
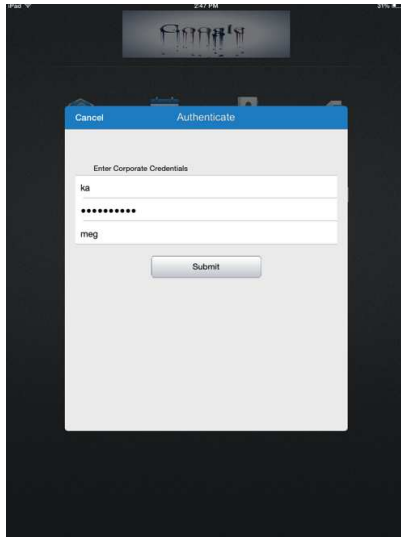
MaaS360 Gateway			
Gateway Settings			
Cluster Name	MaaS360 Gateway	Configuration	Standalone
Mode	Relay	Relay Server To Use	NA-US-East Relay
Direct URL	-	Use a Webserver or a Loadbalancer in front of Gateway	No
Local Port on which Gateway is running	0	Accept all Untrusted Certificates	No
Enable WebDav 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	-		
Authentication Setup			
Authentication Time to live (mins)	1440	Use cached credentials for websites with Basic or No Digest authentication	
Gateway Statistics			
Resources accessed (Top 10)	-		

About Mobile App Configuration

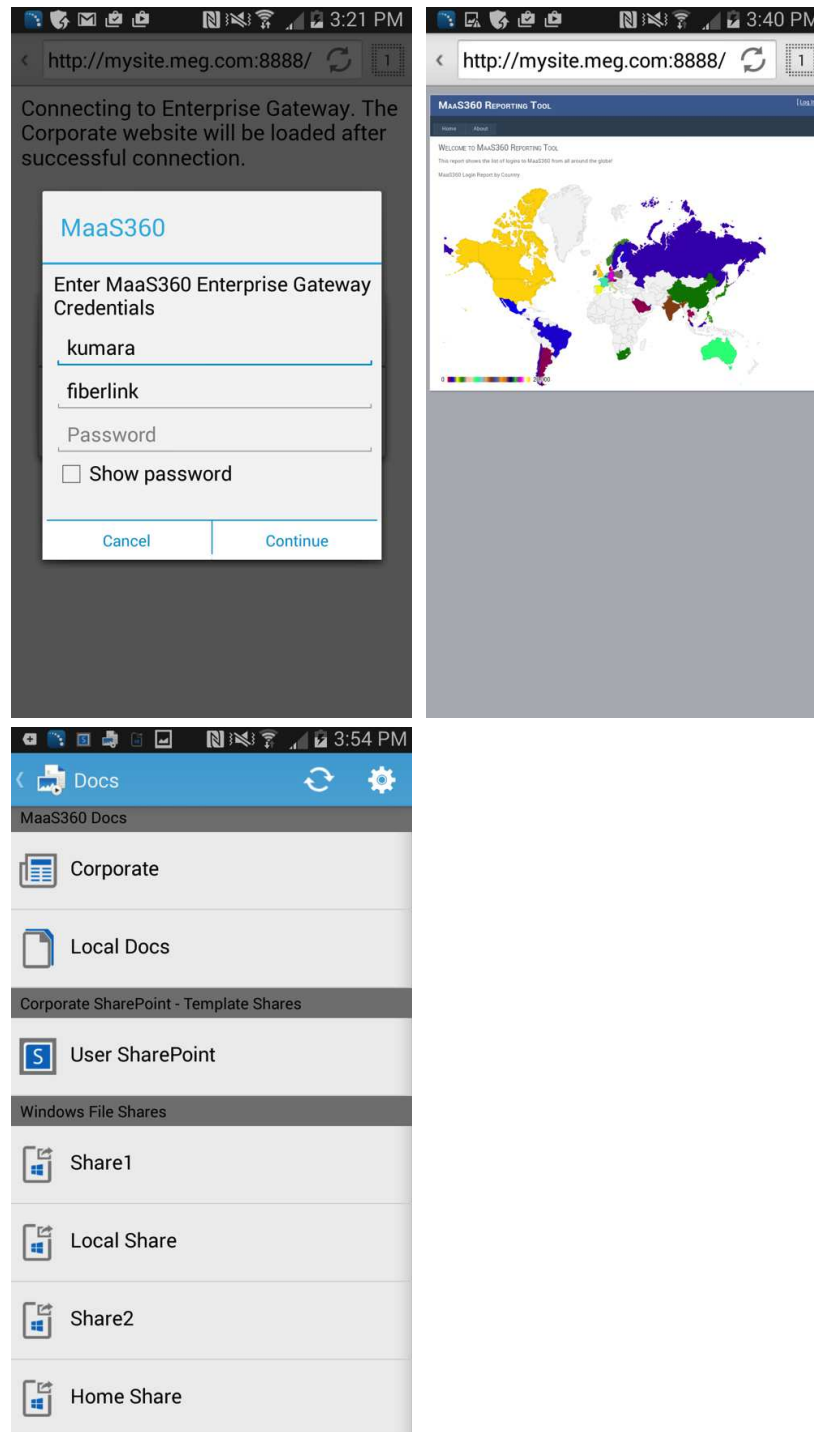
Enroll your iOS / Android device in MaaS360 and assign the persona policy that has Secure Browser features enabled.

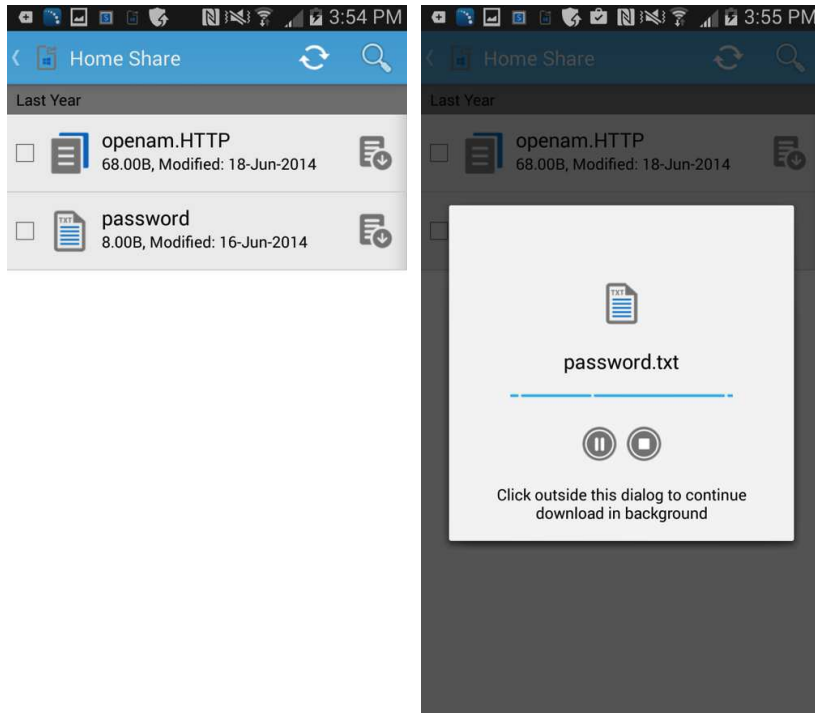
On the first launch of the browser, you are prompted for credentials. Once authenticated, you can access you intranet sites.

iOS Experience



Android Experience





Troubleshooting Mobile App Configuration

All my users are unable to access one intranet site through the Secure Browser. How can I fix this?

1. Make sure the site in question is a part of the proxy access list in persona policies.
2. Log on to the server on which the gateway is installed, open a browser and try accessing the intranet site.
3. Try connecting the device to the corporate network—either Wi-Fi or VPN—and see if the site is accessible.
4. If both (1) and (2) are not working, the intranet site might have gone down.
5. Open the browser on the gateway, use developer tools and capture logs while loading the site in question.
6. Gather Gateway logs (using procedure highlighted below) and send it to your MaaS360 contact for analysis.

None of my users are able to access ANY intranet sites through the Secure Browser. What should I do?

1. Log on to the server on which the gateway is installed, open the Services console and ensure that Cloud Extender service is running. If not, start the service.
2. With a test device, start the Secure Browser app, authenticate (if required) and confirm that you are able to access the intranet sites.
3. If it's still not working, open the browser on the gateway server and try accessing intranet sites that are published. Check to see if there have been any recent firewall/proxy changes in your internal network that might be blocking this access.
4. Gather gateway logs (using the procedure below) and send it to MaaS360 for analysis.

How can I collect gateway logs?

1. Replicate the issue in question and note down the timestamp.
2. Log on to the server on which the gateway is installed.
3. Browse to **C:\Program Files(x86)\MaaS360\Cloud Extender** folder.
4. Double click **DiagnosticCmd.exe**. The tool runs and collects all relevant logs for the gateway and places a zip file on your **Desktop**.
5. Send this zip folder to your MaaS360 contact along with detailed description and the timestamp when the issue was replicated. Please provide your account number with the logs.

How can I collect Secure Browser logs?

1. Replicate the issue in question using the Secure Browser and note the timestamp.
2. In iOS, open the **Browser** click the 3 dots after the address bar, select **Settings > Email Logs**. This launches your email client (native / secure) with a new email and logs as attachments.
3. In Android, open MaaS360 App, go to **Settings > Email Logs**. On the Secure Browser Settings menu, there is an option to enable verbose logging as well, in case of assisted troubleshooting.

Where can I find the log files on the Mobile Enterprise Gateway

1. Go to **C:\%ProgramData%\MaaS360\Cloud Extender\logs**.
 - a. **MobileGateway.log** contains all activities of the gateway
 - b. **MobileGatewayAuth.log** has all authentication attempts
 - c. **MobileGatewayAccess.log** has details of all the intranet resources accessed by end users
 - d. **MobileGatewayWebResAuth.log** contains all authentication attempts against intranet resources

How can I check the version of the Secure Browser installed on my device?

1. In iOS, go to **Settings > Browser**, and version field indicates the version of the browser.
2. In Android, go to **Settings > Application Manager > Browser** to access the version.