IBM MobileFirst Protect (MaaS360) On-Premises Mobile Enterprise Gateway 2.0 Quick Start Guide

Contents

Chapter 1. Overview

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. 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

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

All data on the Mobile Device is stored in the MaaS360 container, fully encrypted and protected from data leaks, and is protected by MaaS360 container security policies depending on 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

These benefits come without compromising a great user experience, which is typically not the case with VPN-based solutions.

Tight integration with the MaaS360 console helps define lockout policies and provides the ability to revoke 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.

What's new in MEG 2.0?

- Seamless integration with MaaS360 version 2.3.0.1 and later, with easy configuration
- Integration with the Cloud Extender module
- Strong gateway authentication schemes
- Cross Forest/Cross Domain authentication
- Support for SSO for Gateway across multiple apps on a device
- Support for Kerberos/SPENGO and 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 and automatic local gateway routing
- Streaming scenarios—large files and videos
- WebDAV support for Windows File Shares

Gateway Mode

MEG operates in Direct Access mode—devices talk directly to it for resource access.

MEG can also be installed as a standalone gateway for smaller deployments, or as a clustered gateway for HA, but it will always be in Direct Access mode.

This document describes the MEG architecture for Direct Access mode for standalone and High Availability installations, and provided detailed instruction on how to implement the solution in your environment.

Note: *Relay Access mode is currently not supported for MaaS360 On Premises.*

Important: To enable MEG 2.0 for your On Prem instance please contact IBM Support.

System Requirements

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

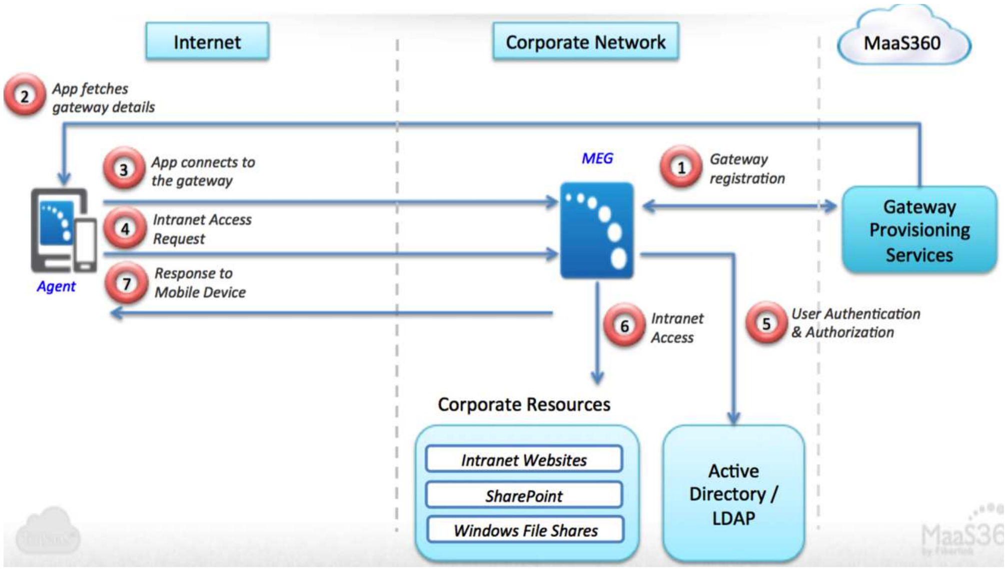
Item	Meets Requirements
IBM MobileFirst Protect (**MaaS360**) **version 2.3.0.1 or later** account (either SaaS or On-Premises installation)	
Physical or Virtual Machine with Windows Server 2012, 2008 RC2, or 2008 as an installation target for the MaaS360 Mobile Enterprise Gateway.	
A **Service Account** that MEG can run as: A member of the **Domain User** group on your Active Directory A member of the **Local Administrator** group on the server	
Memory: 4 GB	
Processor: Dual Core	
CPU: 2.8Ghz	
Disk space: 2GB	

Item	Meets Requirements
Access to the following URL from the MEG machine: Port 443 outbound used by the gateway to communicate with MaaS360 Backend and Web Services. MaaS360 Backend: Service URL for the MaaS360 On Premises instance	
Supported clients: iOS 6.0 and higher Android 4.2 or later (carrier versions)	

Direct Access Mode Architecture

Traffic through the MEG proceeds between the Internet, your corporate network and MaaS360 as follows:

1. Gateway provisioning services registers with MaaS360 On Premises.
2. The MaaS360 app on the device fetches Gateway details.
3. The app connects to the Gateway.
4. The app requests intranet access from MaaS360 On Premises.
5. MaaS360 On Premises compare the user's credentials with the Active Directory/LDAP credentials and grants access if they match.
6. The user can access corporate resources with the device.
7. Information from the content repositories can be sent to the device.


Internet
Corporate Network
MaaS360
2 App fetches gateway details
3 App connects to the gateway
4 Intranet Access Request
7 Response to Mobile Device
Agent
MEG
1 Gateway registration
Gateway Provisioning Services
6 Intranet Access
5 User Authentication & Authorization
Corporate Resources
Intranet Websites
SharePoint
Windows File Shares
Active Directory / LDAP

Architecture Components

MEG has two components, the Client and the Gateway.

Client

The MaaS360 app for iOS and Android, MaaS360 Secure Browser and any Enterprise App wrapped within MaaS360 or integrated the MaaS360 SDK will be able to communicate with MEG.

The apps connect directly to the gateway for intranet resource access.

Access is via HTTPS if an 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 protected within the context of the MaaS360 app container with 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.

It is 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.

The gateway 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.

The 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.

Chapter 2. Install the Gateway

About this task

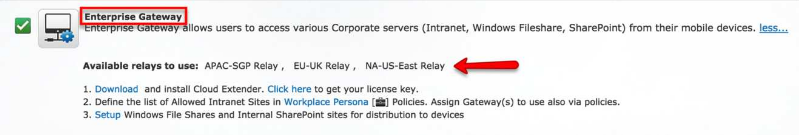
To install the Gateway, perform the following steps:

Procedure

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

   The **Enterprise Gateway** feature should have a checkmark.

   Note: If this has not been enabled, please contact your Fiberlink representative.



☑ **Enterprise Gateway**

Enterprise Gateway allows users to access various Corporate servers (Intranet, Windows Fileshare, SharePoint) from their mobile devices. less...

Available relays to use: APAC-SGP Relay , EU-UK Relay , NA-US-East Relay

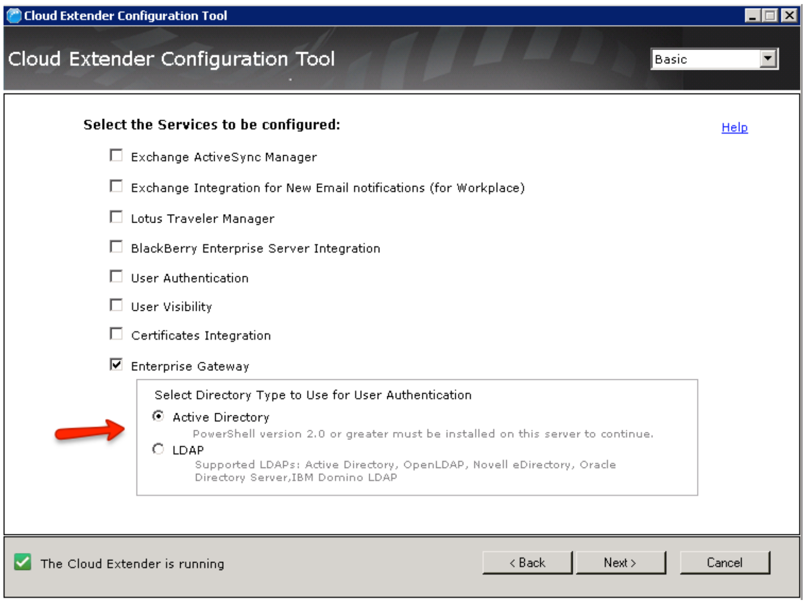
1. Download and install Cloud Extender. Click here to get your license key.
2. Define the list of Allowed Intranet Sites in Workplace Persona [💼] Policies. Assign Gateway(s) to use also via policies.
3. Setup Windows File Shares and Internal SharePoint sites for distribution to devices

2. **Download** the Cloud Extender using the download link from Step 1 in the portal.
3. Select **Click here** to send your license key to your registered email address.

Set Up the Gateway Authentication Mode

Procedure

1. On the list of available services, check **Enterprise Gateway** option. The Gateway module might take a few minutes to download after the Cloud Extender installation. If the Enterprise Gateway option is missing, close the configuration tool and reopen it in a couple of minutes.
2. Choose the **Directory Type** used for User Authentication.
3. If you choose Active Directory for the directory type, do the following:
   a. Select **Active Directory** and then click **Next**.



Cloud Extender Configuration Tool

Cloud Extender Configuration Tool

Basic

Select the Services to be configured:

Help

☐ 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

Select Directory Type to Use for User Authentication

● Active Directory

PowerShell version 2.0 or greater must be installed on this server to continue.

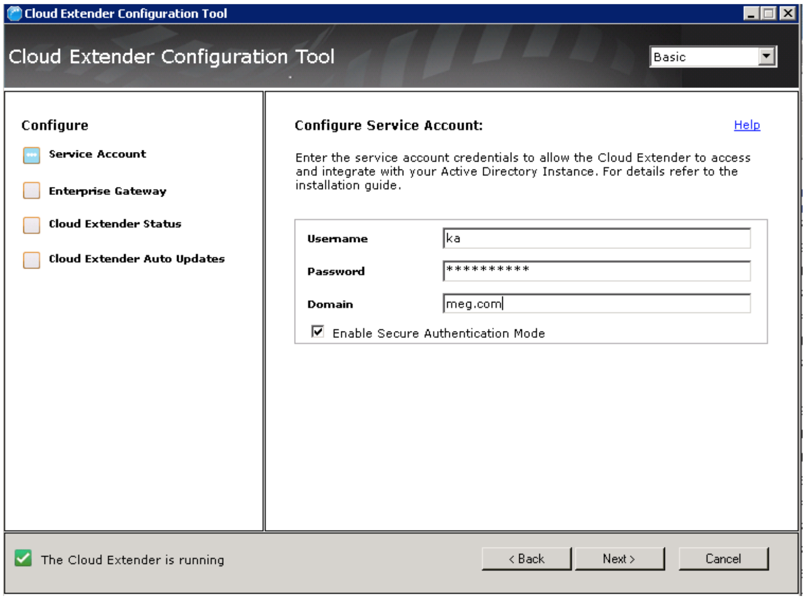
○ LDAP

Supported LDAPs: Active Directory, OpenLDAP, Novell eDirectory, Oracle Directory Server,IBM Domino LDAP

✓ The Cloud Extender is running

< Back | Next > | Cancel

b. Enter the Service Account's *Username*, *Password* and *Domain* (See Requirements). Click **Next** to receive the success message.


Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
Configure
Service Account
Enterprise Gateway
Cloud Extender Status
Cloud Extender Auto Updates
Help
‹ Back
Next ›
Cancel

Configure Service Account:

Enter the service account credentials to allow the Cloud Extender to access and integrate with your Active Directory Instance. For details refer to the installation guide.

Username: ka

Password: **********

Domain: meg.com

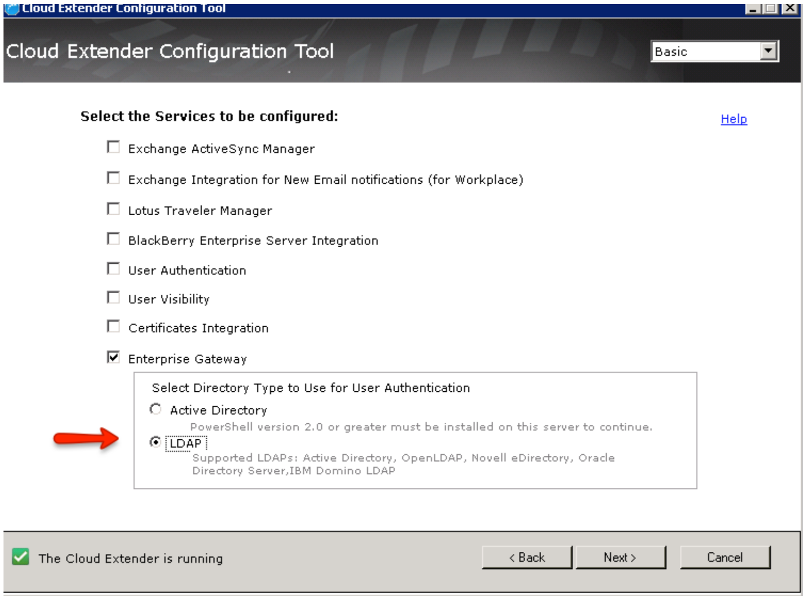
☑ Enable Secure Authentication Mode

✓ The Cloud Extender is running

c. Click **OK** to dismiss the success message, and then click **Next** to Chapter 4, "Test Gateway Authentication," on page 13.

4. If you choose LDAP for the directory type:

a. Select **LDAP** as the Enterprise Gateway


Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
Help
‹ Back
Next ›
Cancel

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

Select Directory Type to Use for User Authentication

○ Active Directory

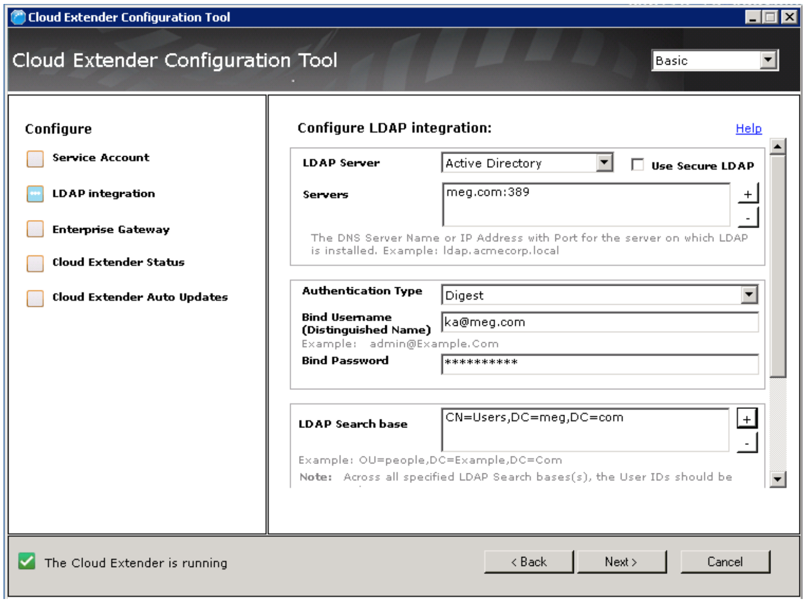
PowerShell version 2.0 or greater must be installed on this server to continue.

● LDAP

Supported LDAPs: Active Directory, OpenLDAP, Novell eDirectory, Oracle Directory Server,IBM Domino LDAP

✓ The Cloud Extender is running

b. On the **Configure LDAP Integration** screen, click **Edit**, enter the appropriate settings and then click **Next**:



Configure LDAP integration:

LDAP Server: Active Directory □ Use Secure LDAP

Servers: meg.com:389

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

Authentication Type: Digest

Bind Username (Distinguished Name): ka@meg.com

Example: admin@Example.Com

Bind Password: **********

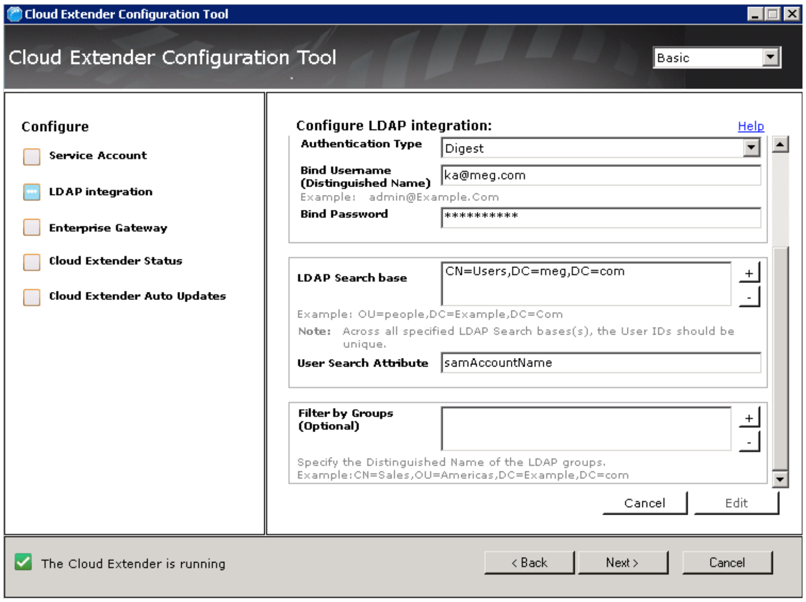
LDAP Search base: CN=Users,DC=meg,DC=com

Example: OU=people,DC=Example,DC=Com

Note: Across all specified LDAP Search bases(s), the User IDs should be

☑ The Cloud Extender is running

c. On the next configuration screen, enter the following settings and click **Next**:



Configure LDAP integration:

Authentication Type: Digest

Bind Username (Distinguished Name): ka@meg.com

Example: admin@Example.Com

Bind Password: **********

LDAP Search base: CN=Users,DC=meg,DC=com

Example: OU=people,DC=Example,DC=Com

Note: Across all specified LDAP Search bases(s), the User IDs should be unique.

User Search Attribute: samAccountName

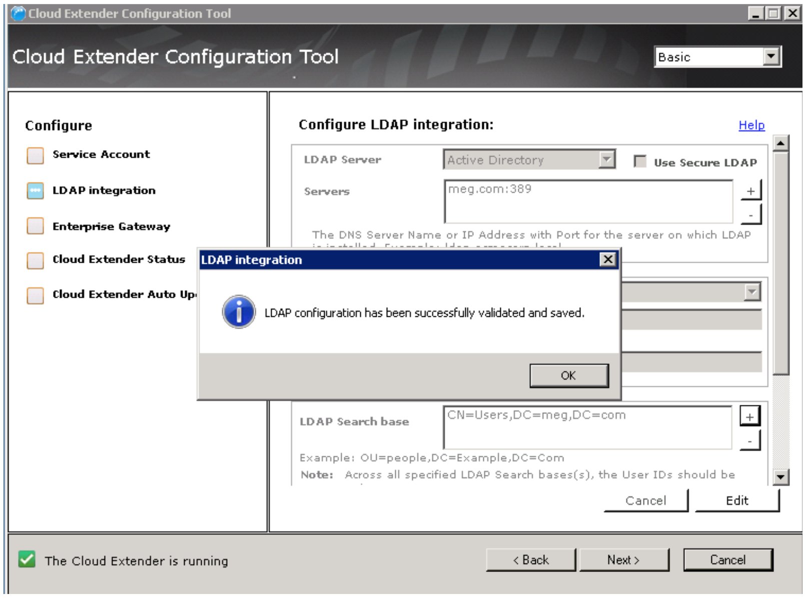
Filter by Groups (Optional):

Specify the Distinguished Name of the LDAP groups. Example:CN=Sales,OU=Americas,DC=Example,DC=com

☑ The Cloud Extender is running

Configuration Setting	Description
LDAP Server Name & Port	FQDN name of your LDAP server and port
Authentication Type	**Basic** or **Digest**
Bind Username & Password	Service account credentials
LDAP Search Base	Your search root on your LDAP
User Search Attribute	The name of the attribute that identifies the user in your LDAP server (like samAccountName in Active Directory)
Filter by Groups	Does not apply for LDAP authentication

5. When you have entered your changes, you will receive a success message. Click **OK** to dismiss the message, and then click **Next**.



LDAP Server: Active Directory

Servers: meg.com:389

The DNS Server Name or IP Address with Port for the server on which LDAP

LDAP integration: LDAP configuration has been successfully validated and saved.

LDAP Search base: CN=Users,DC=meg,DC=com

Example: OU=people,DC=Example,DC=Com

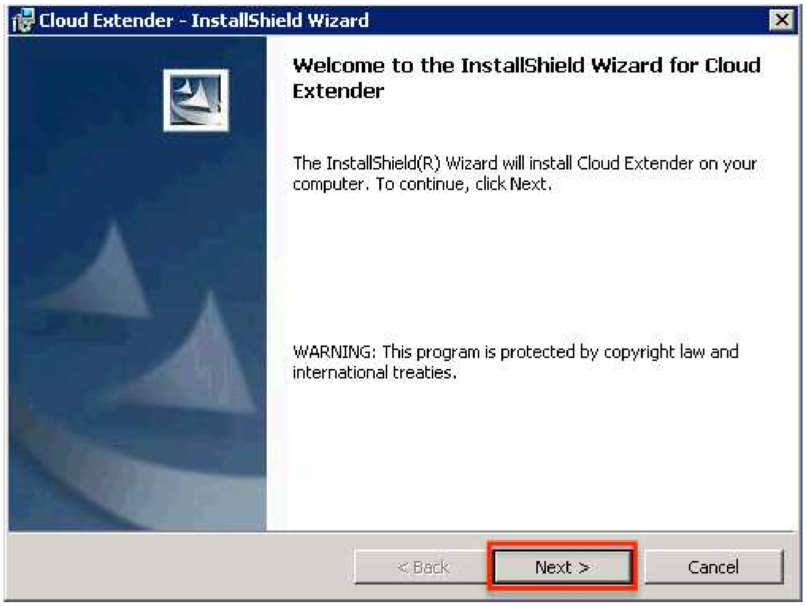
Note: Across all specified LDAP Search bases(s), the User IDs should be

The Cloud Extender is running

Install the Cloud Extender module

Procedure

1. On the **Welcome** screen, click **Next**.

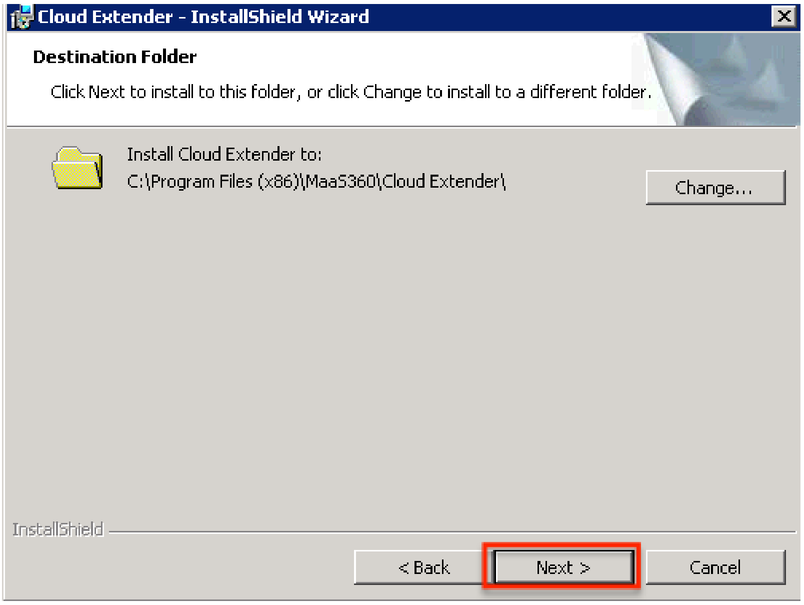


Welcome to the InstallShield Wizard for Cloud Extender

The InstallShield(R) Wizard will install Cloud Extender on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Click **Next** to install the files into the default folder.



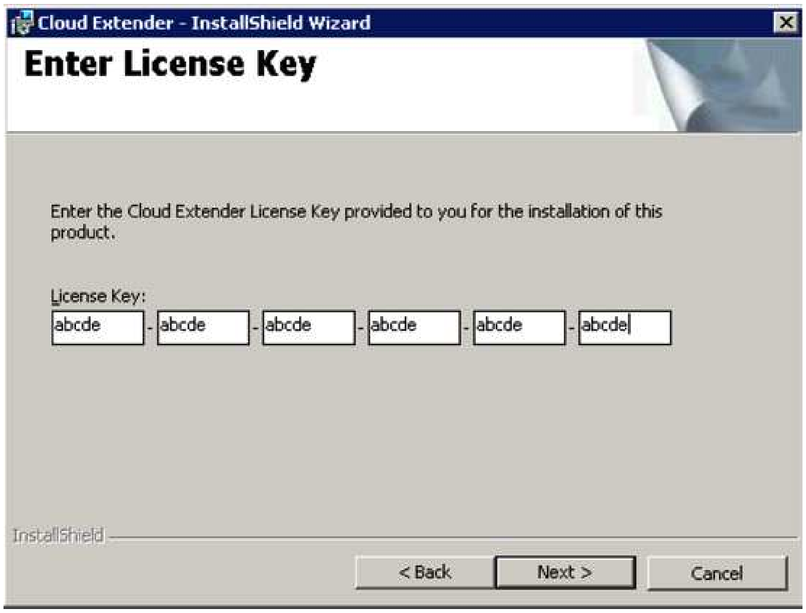
Cloud Extender - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Cloud Extender to:
C:\Program Files (x86)\MaaS360\Cloud Extender\

3. Enter the license key and click **Next**.



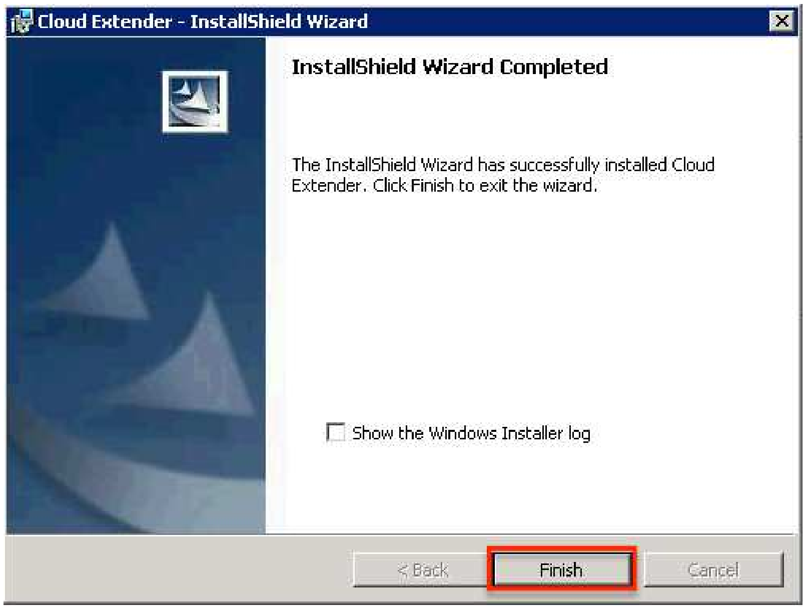
Cloud Extender - InstallShield Wizard

Enter License Key

Enter the Cloud Extender License Key provided to you for the installation of this product.

License Key:
abcde - abcde - abcde - abcde - abcde - abcde

4. When the installation has completed, click **Finish**.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Cloud Extender. Click Finish to exit the wizard.

□ Show the Windows Installer log

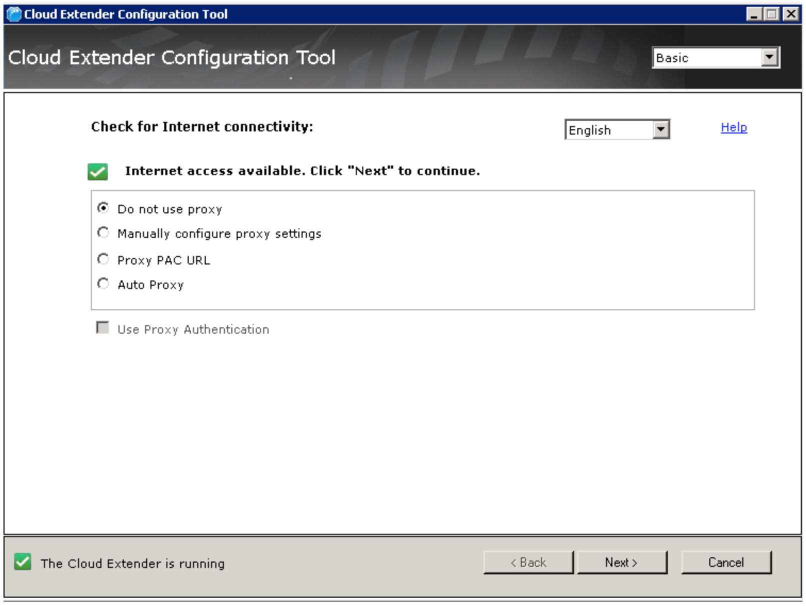
Once the Cloud Extender installation completes, the Cloud Extender Configuration Tool launches automatically.

Chapter 3. Configure Outbound Proxy Settings for the Cloud Extender

About this task

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

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


Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
English
Help
< Back
Next >
Cancel

Check for Internet connectivity:

✓ Internet access available. Click "Next" to continue.

● Do not use proxy
○ Manually configure proxy settings
○ Proxy PAC URL
○ Auto Proxy

□ Use Proxy Authentication

✓ The Cloud Extender is running

Procedure

1. 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
2. If your proxy requires authentication, select the **Use Proxy Authentication** checkbox and configure a service account credential that can be used to authenticate and traverse through the proxy.

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

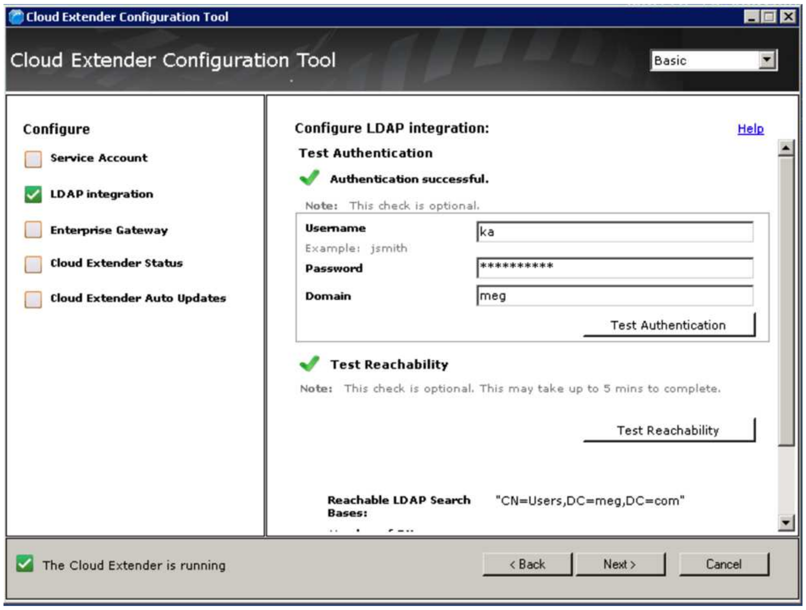
Chapter 4. Test Gateway Authentication

About this task

After the Gateway has been set up and credentials have been saved, you can test authentication against your Directory.

Procedure

When the configuration tool prompts, use the **Test Authentication** and **Test Reachability** buttons:



Configure LDAP integration:

Test Authentication

✓ Authentication successful.

Note: This check is optional.

Username Example: jsmith	ka
Password	**********
Domain	meg

✓ Test Reachability

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

Reachable LDAP Search Bases:	"CN=Users,DC=meg,DC=com"

☑ The Cloud Extender is running

Chapter 5. Configure the Gateway in Direct Mode as Standalone

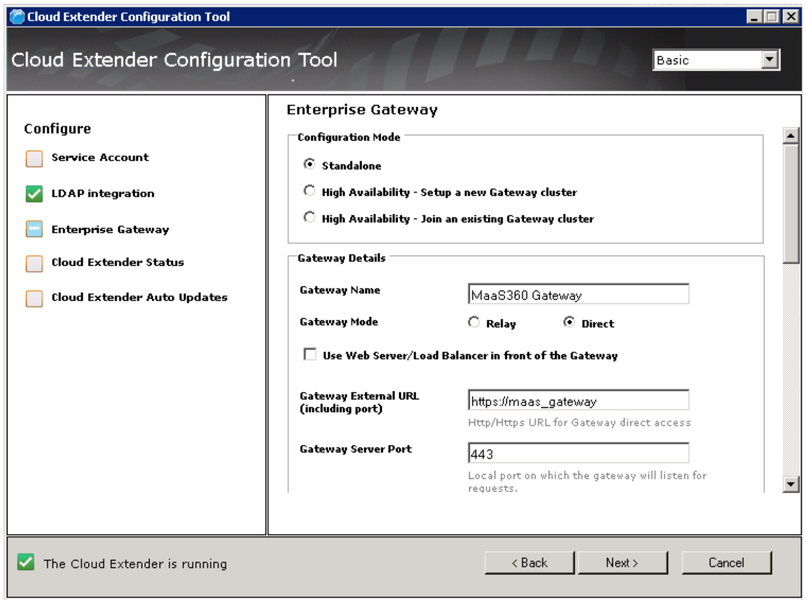
About this task

If you plan to set up your gateways in an HA cluster, skip to Gateway Configuration in HA mode.

Important: If a gateway has already been configured as standalone, you cannot switch the gateway mode to HA.

Procedure

1. In the Configuration Mode section, choose **Standalone**.



Cloud Extender Configuration Tool

Configure

□ Service Account

☑ LDAP integration

▣ Enterprise Gateway

□ Cloud Extender Status

□ Cloud Extender Auto Updates

Enterprise Gateway

Configuration Mode

● Standalone

○ High Availability - Setup a new Gateway cluster

○ High Availability - Join an existing Gateway cluster

Gateway Details

Gateway Name: MaaS360 Gateway

Gateway Mode: ○ Relay ● Direct

□ Use Web Server/Load Balancer in front of the Gateway

Gateway External URL (including port): https://maas_gateway

Http/Https URL for Gateway direct access

Gateway Server Port: 443

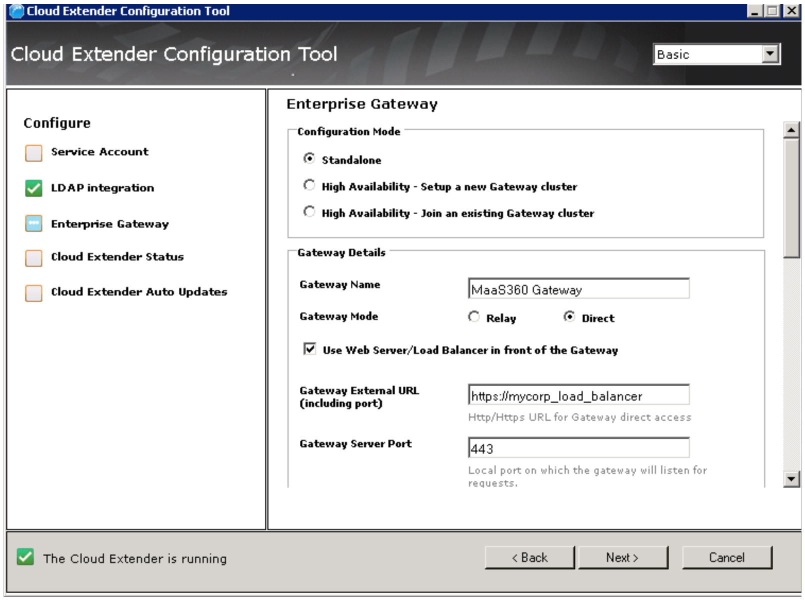
Local port on which the gateway will listen for requests.

☑ The Cloud Extender is running

2. If you want to use a web server or load balancer in front of the Gateway, enter the **Gateway External URL** and **Gateway Server Port**.

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.
Gateway Mode	Select **Direct**.
Use Web Server / Load Balancer in front of the Gateway	If selected, you will be 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)	If a Load Balancer is used in front of the gateway, the **Gateway URL** will be the **External URL** (hostname) of your Load Balancer. If Load Balancer is not used, the **Gateway URL** will be 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 will run and listen 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** will be any open port on this gateway server.



Enterprise Gateway

Configuration Mode

● Standalone

○ High Availability - Setup a new Gateway cluster

○ High Availability - Join an existing Gateway cluster

Gateway Details

Gateway Name: MaaS360 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.

☑ The Cloud Extender is running

3. Click **Next** to continue configuration.

Chapter 6. Configure SSL

About this task

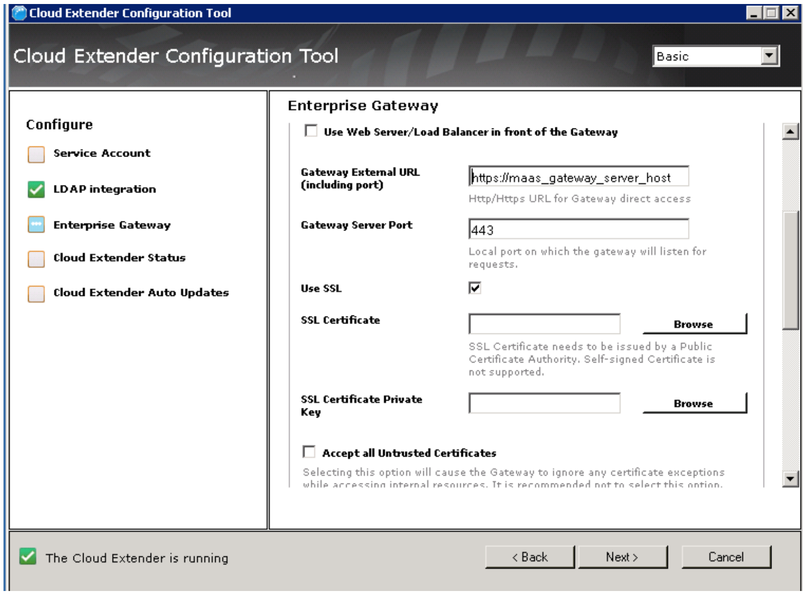
Use SSL encryption on top of the AES 256-bit end-to-end encryption to further secure communication between the mobile device and the gateway.

Note: This is optional—not using SSL will not compromise the security of the MaaS360 Mobile Enterprise Gateway.

Procedure

1. On the Enterprise Gateway configuration pane, scroll down to select **Use SSL** and fill the other configuration settings.

Configuration Setting	Description
Use SSL	• 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. • 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 details.
SSL Certificate	Path to the SSL certificate (.pem) file. If a load balancer is not used, the SSL will terminate on your gateway. In this case, you are *required* to get an SSL certificate from a public Certificate Authority (CA) and not use self-signed certificates.
SSL Certificate Private Key	Private key of the SSL certificate (.key) file.
Accept all Untrusted Certificates	By selecting this option, the gateway will ignore any certificate exceptions from intranet resources. For example, if your intranet site has a self-signed certificate, accessing this site will throw 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. You should install the site SSL certificates to the Certificate store of the Gateway server.



Enterprise Gateway

□ Use Web Server/Load Balancer in front of the Gateway

Gateway External URL (including port): https://maas_gateway_server_host

Http/Https URL for Gateway direct access

Gateway Server Port: 443

Local port on which the gateway will listen for requests.

Use SSL: ☑

SSL Certificate:

SSL Certificate needs to be issued by a Public Certificate Authority. Self-signed Certificate is not supported.

SSL Certificate Private Key:

□ 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.

✓ The Cloud Extender is running

2. When finished, click **Next** to move to the next setting.

Chapter 7. Configure the Gateway in High Availability (HA) Mode

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

Why Clustered Gateways?

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

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, you should use additional gateways.

Sample scaling recommendations:

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 will be able to handle load
For every 10,000 device increments	1 gateway per 10,000 devices, plus 1 clustered gateway for handling outage loads. For example, 50,000 devices would require 6 gateways.

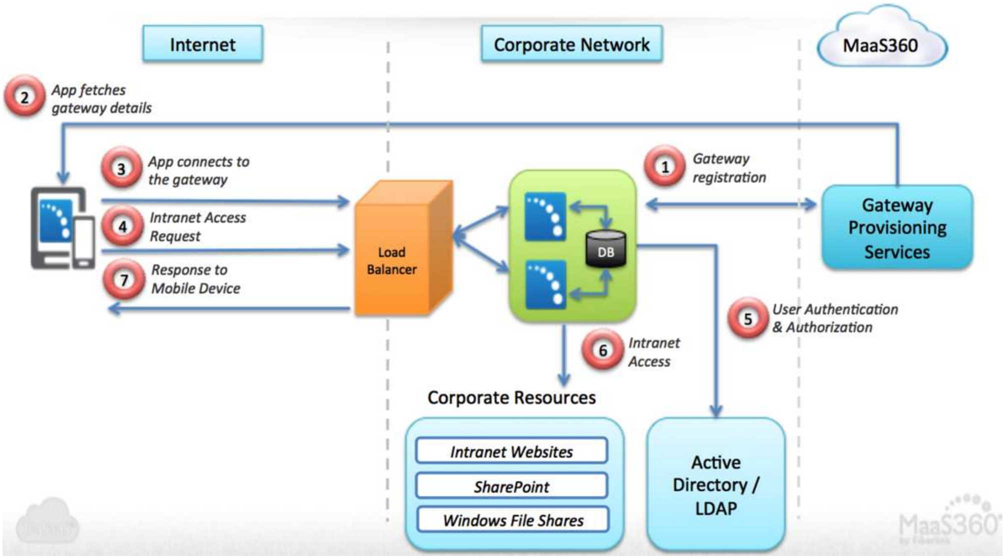
Direct Architecture in Clustered Mode

In Direct Clustered mode, all gateways talk to a shared database.

You must implement a load balancer in your network to actively balance incoming traffic among active gateways

You may need to set up SSL certificates for device-to-load balancer SSL communication.

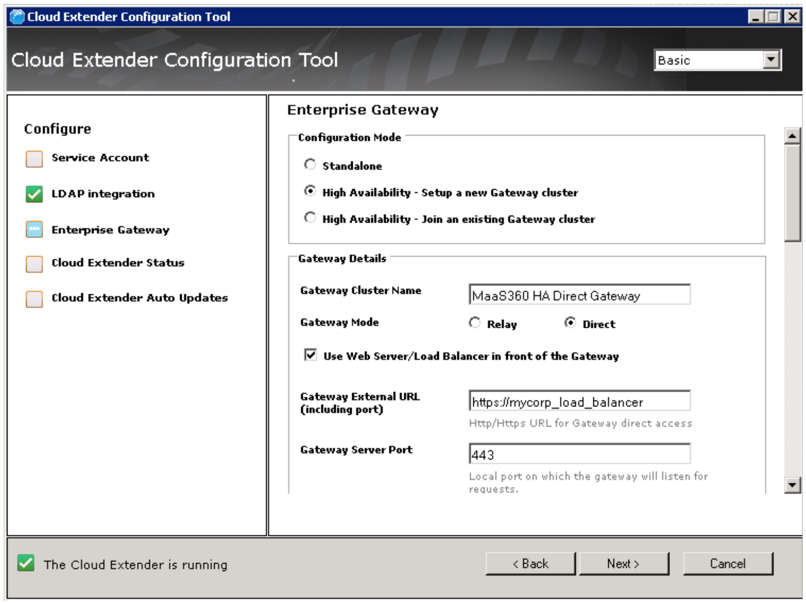
You may set up SSL certificates for traffic between load-balancer and gateway. This is optional and the data packets between them are anyways encrypted, even over HTTP.



Configure Gateway as HA in Direct Mode

Procedure

1. On the first configuration screen, enter the settings as described below:



Enterprise Gateway

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

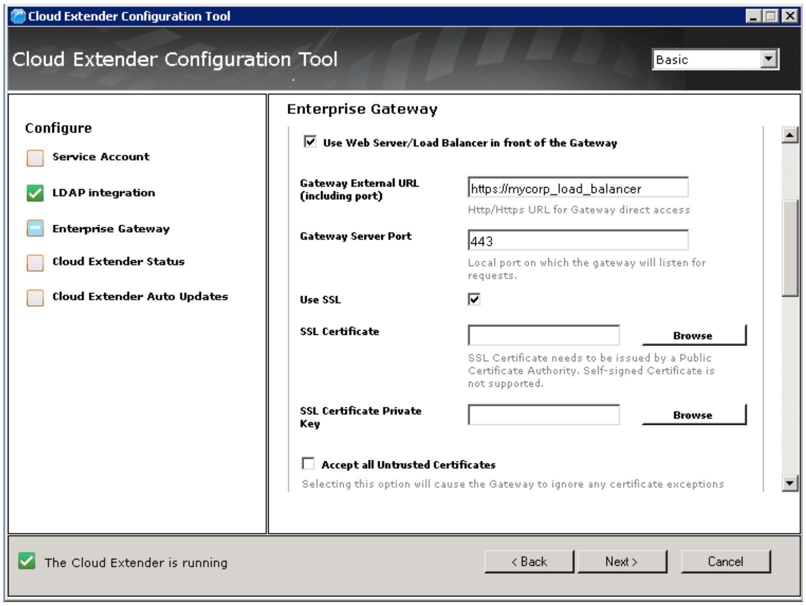
Local port on which the gateway will listen for requests.

✓ The Cloud Extender is running

Configuration Setting	Description
Configuration Mode	The gateway can be configured as a standalone instance or a High Availability cluster. Select **High Availability – Setup a new Gateway cluster**.

Configuration Setting	Description
Gateway Cluster Name	Enter any gateway name. This is the name that appears in all MaaS360 portal workflows.
Gateway Mode	Select **Direct**.
Use Web Server/Load Balancer in front of the Gateway	Select the checkbox. You will be required to configure your load balancer to: • Accept 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** will be the **External URL** (hostname) of your Load Balancer. If it is not used, the **Gateway URL** will be the **hostname** of the gateway server. The 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 the gateway server will run and listen for requests. If a load balancer is used, then ensure that it redirects traffic to this port. If it is not used, the **Gateway port** will be any open port on this gateway server.

2. Scroll down to enter the next group of settings:



Cloud Extender Configuration Tool

Enterprise Gateway

☑ 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.

Use SSL: ☑

SSL Certificate:

SSL Certificate needs to be issued by a Public Certificate Authority. Self-signed Certificate is not supported.

SSL Certificate Private Key:

☐ Accept all Untrusted Certificates

Selecting this option will cause the Gateway to ignore any certificate exceptions

✓ The Cloud Extender is running

Configuration Setting	Description
Use SSL	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. This is optional—not using SSL will not compromise the security of the MEG. • The **SSL Certificate** (see below) is used by your load balancer to initiate an SSL session to the gateway. – 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 details.
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	If you select this checkbox, the gateway will ignore any certificate exceptions from intranet resources. For example, if your intranet site has a self-signed certificate, then accessing this site will throw a certificate exception. With this option, the exception is ignored and the request is served by the gateway. It is recommended that you not select this option. Install the site SSL certificates to the Certificate store of the Gateway server instead.
Database Setup	See Database Setup for different database configurations.

Prepare a Database

About this task

Because an HA setup for MEG requires a shared database among active gateways to share configuration and authentication information, you must set up a database on your database server.

MEG supports the following database servers:

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

Sizing Requirements

The recommended database size is 10KB per device.

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

Procedure

1. Identify/set up the database server that the gateways can integrate with. The *hostname* and *port* of the database server are required for integration.
2. Create a blank database within the database server. The *database name* is required for integration.
3. Make sure there is either *Local SQL server account* or *Windows NT* account for database access.
4. Require 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.

Set Up the Database

Procedure

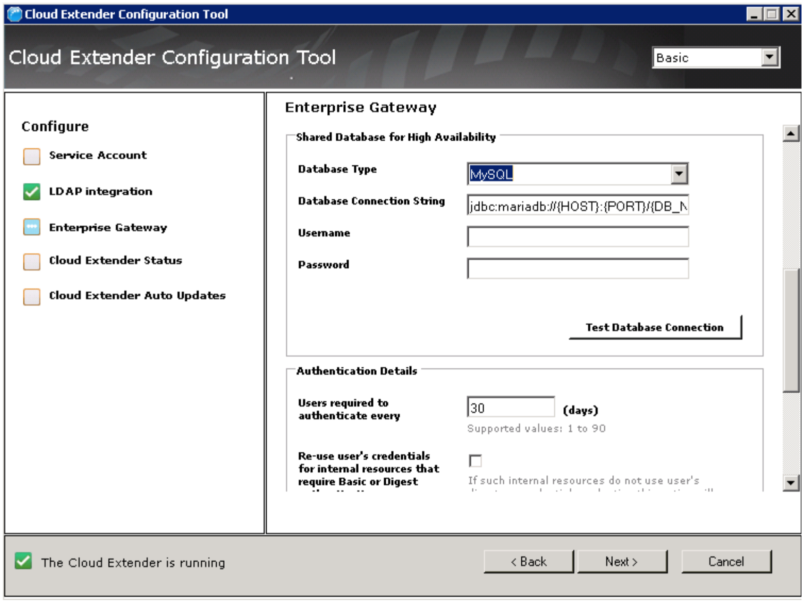
Continue scrolling down to access the next settings. To connect the gateways to the shared database, you will need the following details:

- 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

Procedure

Scroll down to enter the **Database Type**, **Database Connection String** and the authentication details.



Enterprise Gateway

Shared Database for High Availability

Database Type: MySQL

Database Connection String: jdbc:mariadb://{HOST}:{PORT}/{DB_N

Username:

Password:

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

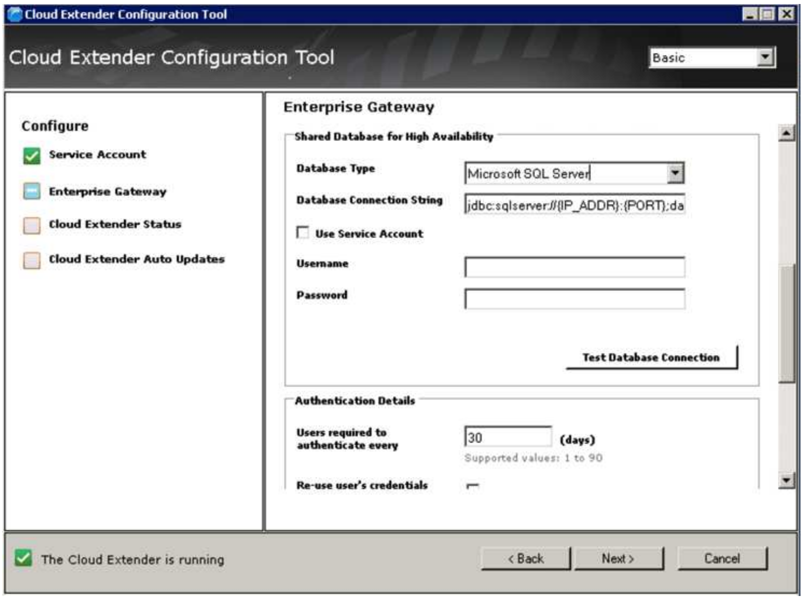
Microsoft SQL Database Configuration

About this task

There are two choices: Active Directory and LDAP.

Procedure

1. For Active Directory mode, select the **Service Account** checkbox in the left pane and enter the **Database Type**, **Database Connection String**, and the authentication details.



Cloud Extender Configuration Tool

Cloud Extender Configuration Tool

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:

Authentication Details

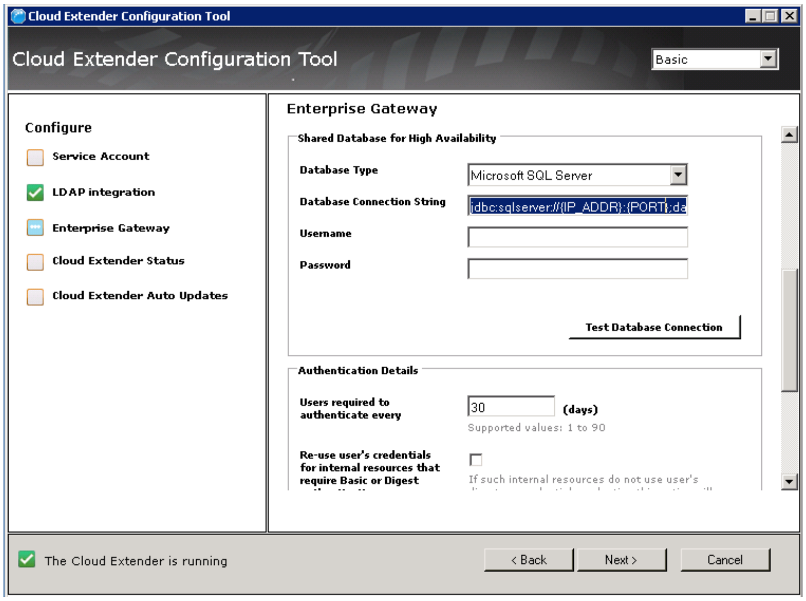
Users required to authenticate every: 30 (days)

Supported values: 1 to 90

Re-use user's credentials

☑ The Cloud Extender is running

2. For LDAP mode, select the **LDAP integration** checkbox in the left pane and enter the **Database Type**, **Database Connection String**, and the authentication details.



Cloud Extender Configuration Tool

Cloud Extender Configuration Tool

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:

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

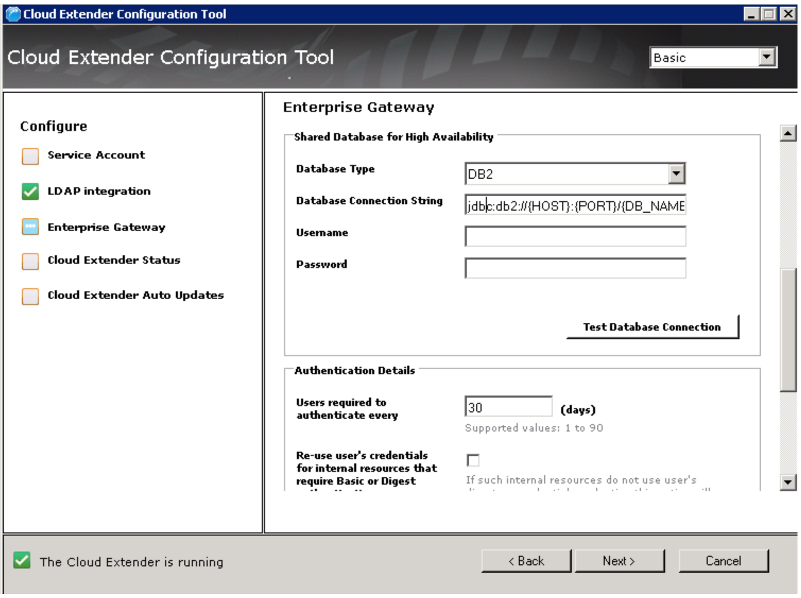
☑ The Cloud Extender is running

DB2 Configuration

About this task

Procedure

Continue scrolling down to enter the next group of settings.



Enterprise Gateway

Shared Database for High Availability

Database Type: DB2

Database Connection String: jdbc:db2://{HOST}:{PORT}/{DB_NAME

Username:

Password:

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

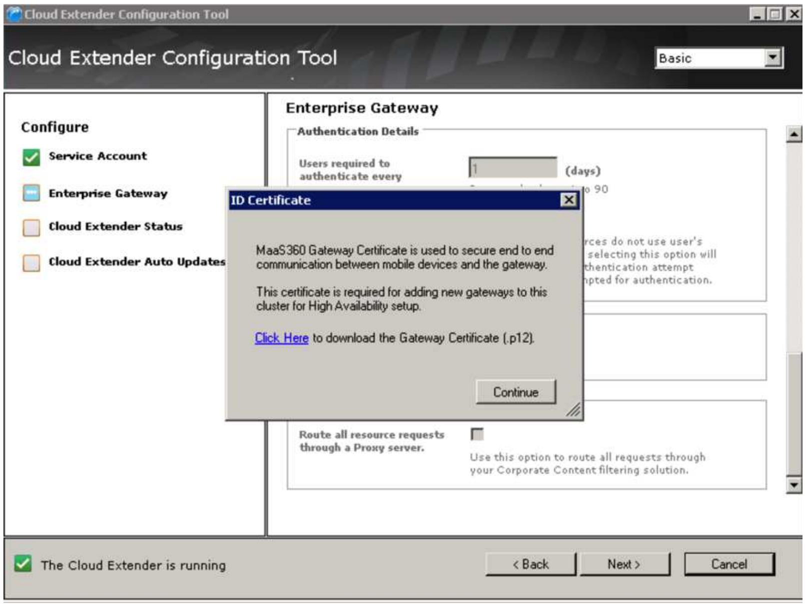
Configuration Setting	Description
Database Type	MySQL/Microsoft SQL Server/DB2 – select one depending on your database type.
Database Connection String	The database connection string gets automatically populated on the gateway depending on the Database Type selection. Replace the {HOST}, {IP_ADDR}, {PORT} and {DB_NAME} with actual values from requirements. The connection strings are as follows: • **MySQL**: jdbca:mariadb://{HOST}:{PORT}/{DB_NAME} • **MS SQL**: jdbc:sqlserver://{IP_ADDR}:{PORT};databaseName={DB_NAME} • **DB2**: jdbc:db2://{HOST}:{PORT}/{DB_NAME}
Username / Password	Local credentials for Local SQL server login.
Use Service Account	Only available in AD authentication mode for MS SQL (not available in LDAP). The gateway service account should have the required rights on database. (See Database Requirements for more information.)

Configuration Setting	Description
Test Database Connection	Tests connection to the database using the specified hostname, port, database and service account credentials. Perform a quick test to ensure that all settings are configured correctly. The Cloud Extender Configuration Tool automatically rechecks for database connectivity while saving the gateway configuration.

Join the Gateway to an Existing Cluster

Procedure

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



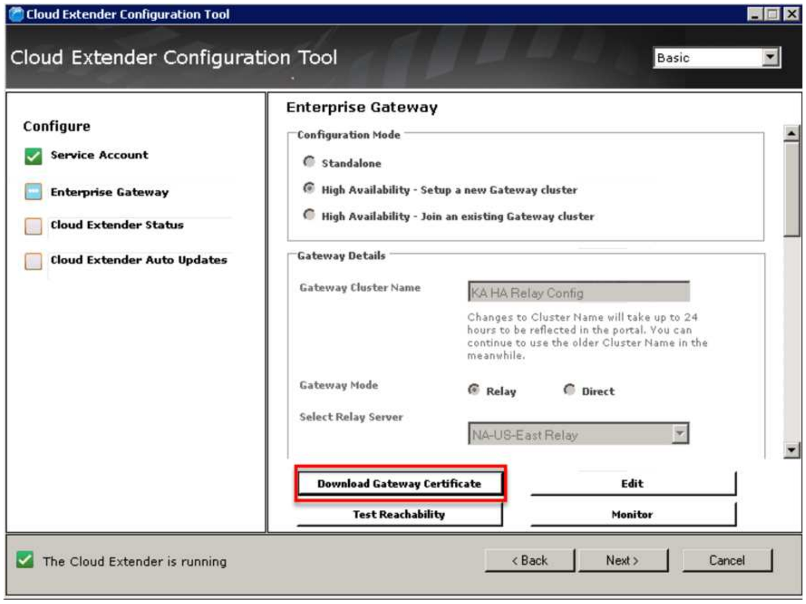
Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
Configure
☑ Service Account
Enterprise Gateway
□ Cloud Extender Status
□ Cloud Extender Auto Updates
Enterprise Gateway
Authentication Details
Users required to authenticate every
1
(days)
o 90
rces do not use user's
selecting this option will
thentication attempt
npted for authentication.
Route all resource requests through a Proxy server.
□
Use this option to route all requests through your Corporate Content filtering solution.
ID Certificate
Continue
☑ The Cloud Extender is running
< Back
Next >
Cancel

MaaS360 Gateway Certificate is used to secure end to end communication between mobile devices and the gateway.

This certificate is required for adding new gateways to this cluster for High Availability setup.

Click Here to download the Gateway Certificate (.p12).

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


Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
Configure
Service Account
Enterprise Gateway
Cloud Extender Status
Cloud Extender Auto Updates
Download Gateway Certificate
Edit
Test Reachability
Monitor
< Back
Next >
Cancel

Enterprise Gateway

Configuration Mode

○ Standalone
● High Availability - Setup a new Gateway cluster
○ High Availability - Join an existing Gateway cluster

Gateway Details

Gateway Cluster Name: KA HA Relay Config

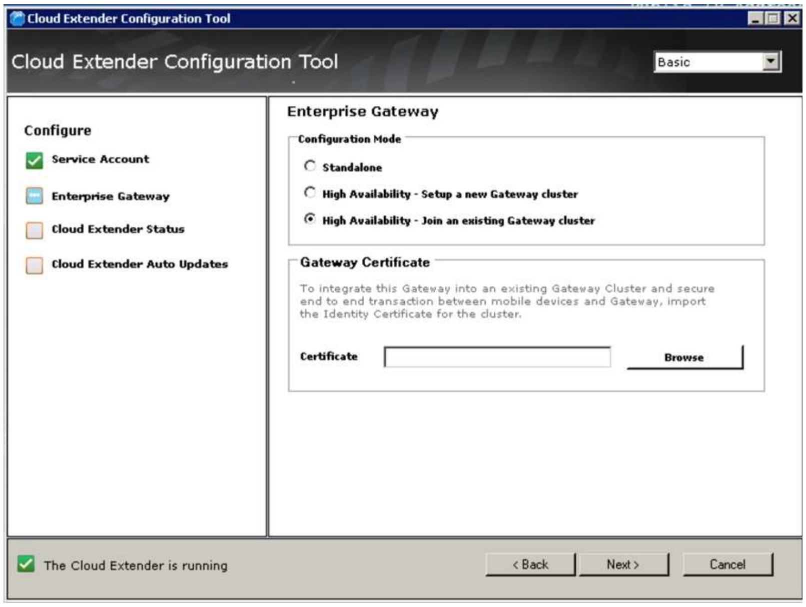
Changes to Cluster Name will take up to 24 hours to be reflected in the portal. You can continue to use the older Cluster Name in the meanwhile.

Gateway Mode: ● Relay ○ Direct

Select Relay Server: NA-US-East Relay

☑ The Cloud Extender is running

2. To add a new gateway to an existing cluster, browse to this **Gateway Certificate**. All the gateway settings are automatically downloaded to the new gateway node.


Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
Configure
Service Account
Enterprise Gateway
Cloud Extender Status
Cloud Extender Auto Updates
Browse
< Back
Next >
Cancel

Enterprise Gateway

Configuration Mode

○ Standalone
○ High Availability - Setup a new Gateway cluster
● High Availability - Join an existing Gateway cluster

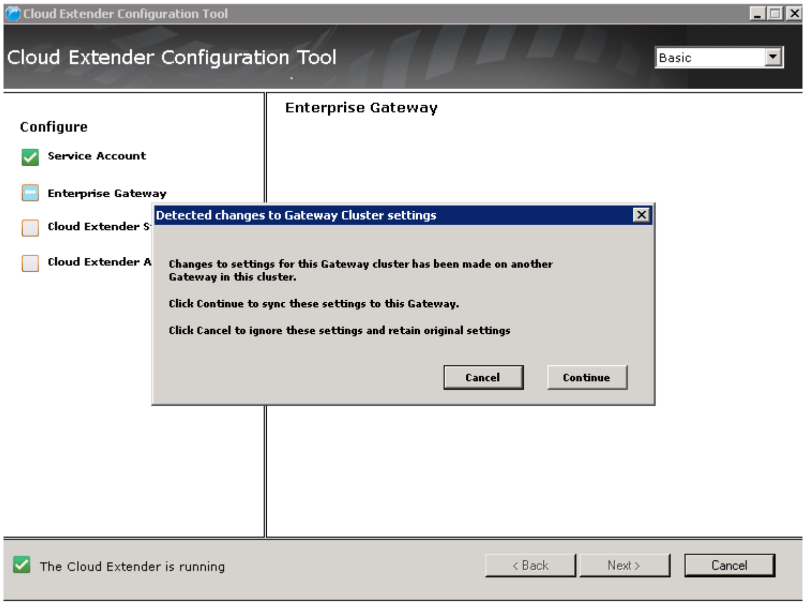
Gateway Certificate

To integrate this Gateway into an existing Gateway Cluster and secure end to end transaction between mobile devices and Gateway, import the Identity Certificate for the cluster.

Certificate:

☑ The Cloud Extender is running

3. If the gateways have been set up in HA mode and you want to change the configuration on one of the nodes, you will be prompted to update the gateway configuration on other nodes when you launch the Cloud Extender Configuration Tool.



Detected changes to Gateway Cluster settings

Changes to settings for this Gateway cluster has been made on another Gateway in this cluster.

Click Continue to sync these settings to this Gateway.

Click Cancel to ignore these settings and retain original settings

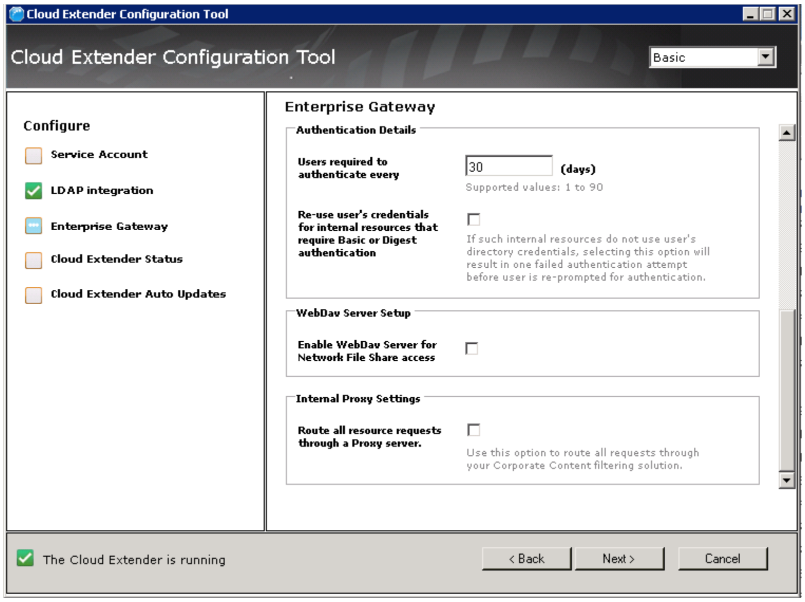
The Cloud Extender is running

4. You must 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.

Chapter 8. Configure Authentication and WebDAV

Procedure

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



Enterprise Gateway

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 authentication □
If such internal resources do not use user's directory credentials, selecting this option will result in one failed authentication attempt before user is re-prompted for authentication.

WebDav Server Setup

Enable WebDav Server for Network File Share access □

Internal Proxy Settings

Route all resource requests through a Proxy server. □
Use this option to route all requests through your Corporate Content filtering solution.

☑ The Cloud Extender is running

Configuration Setting	Description
Authentication Frequency: **Users required to authenticate every (x) days**	Specify how often the gateway needs to re-authenticate users who are connecting to the gateway. Choose any value between **1** and **90** days. The recommended authentication frequency is 1 day, with a setting on the MaaS360 portal to cache user credentials in the MaaS360 app (covered later). This provides a good user experience while meeting security requirements.

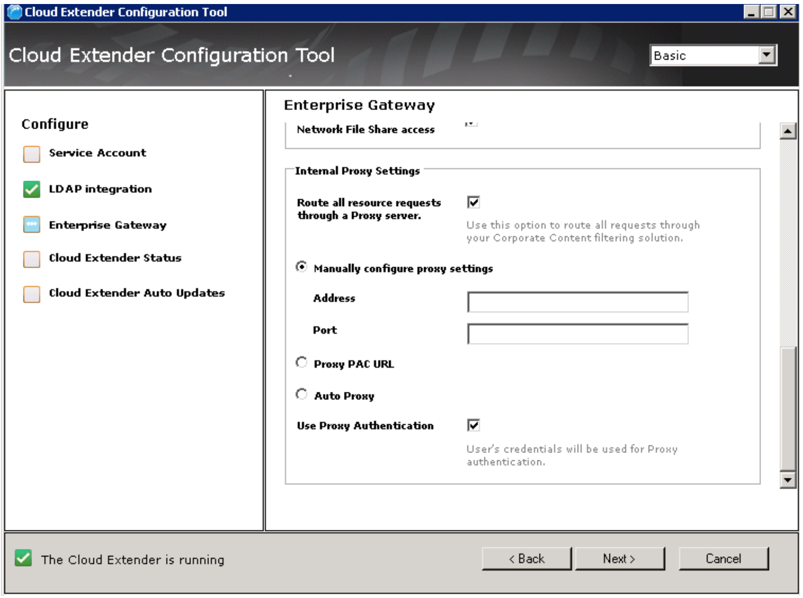
Configuration Setting	Description
Reuse user’s credentials for intranet resources that require Basic or Digest authentication	Certain intranet websites that use Basic or Digest authentication might be integrated with corporate credentials for authentication, although this is not very common. If you have this configuration: If the checkbox is selected: • If an internal site challenges for Basic or Digest authentication, the Gateway provides the user’s credentials it received during gateway authentication and passes it back to the site—thereby seamlessly signing the user on to the site. • If the authentication fails, the challenge for credentials is sent back to the user on the MaaS360 app. When the user provides credentials, a new authentication is attempted • If the credentials stored by the Gateway fail, the authentication logs for the internal site show at least one failed authentication attempt for the user. Any additional failures in the logs are due to the user's authentication failure. If the checkbox is cleared, all Basic or Digest authentication challenges are propagated back to the user to enter manually.

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

Chapter 9. Configure Intranet Proxy Settings

Procedure

1. Scroll down the Gateway configuration pane, then enter the next group of settings.



Enterprise Gateway

Network File Share access

Internal Proxy Settings

Route all resource requests through a Proxy server. ☑

Use this option to route all requests through your Corporate Content filtering solution.

● Manually configure proxy settings

Address

Port

○ Proxy PAC URL

○ Auto Proxy

Use Proxy Authentication ☑

User's credentials will be used for Proxy authentication.

☑ The Cloud Extender is running

Configuration Setting	Description
Route all resource requests through a Proxy server	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, use this setting. • **Manual Proxy:** Enter the hostname/IP and port. • **Proxy PAC URL**: URL to a PAC file hosted in your environment. • **Auto Proxy:** A PAC file is typically hosted in your DHCP or DNS server as Web Proxy Auto-Discovery Protocol (WPAD) file. • This proxy setting is only used for intranet resources. For more information about external proxy settings, see Chapter 3, "Configure Outbound Proxy Settings for the Cloud Extender," on page 11.

Use Proxy Authentication	If your proxy requires authentication, select the **Use Proxy Authentication** checkbox. For authenticating against the proxy server, the gateway uses the credentials of the user who is trying to access the resource. It is important that all of your users should be able to authenticate against this proxy server.

2. Click **Next**. The gateway makes API calls against the MaaS360 backend and completes the gateway registration process.
3. Finish the Cloud Extender Configuration Tool workflow to complete the gateway configuration.

Chapter 10. MaaS360 Portal Configuration

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.

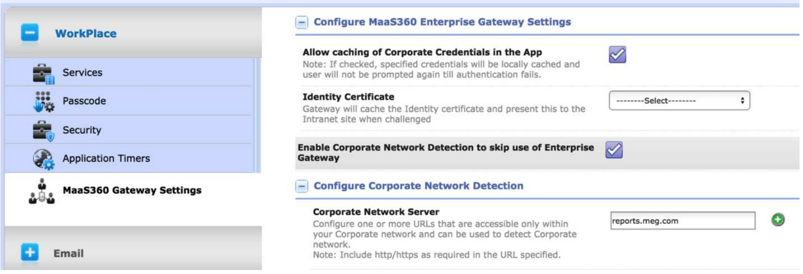
Secure Browser Configuration

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:



Configure MaaS360 Enterprise Gateway Settings

Allow caching of Corporate Credentials in the App ☑
Note: If checked, specified credentials will be locally cached and user will not be prompted again till authentication fails.

Identity Certificate: --------Select--------
Gateway will cache the Identity certificate and present this to the Intranet site when challenged

Enable Corporate Network Detection to skip use of Enterprise Gateway ☑

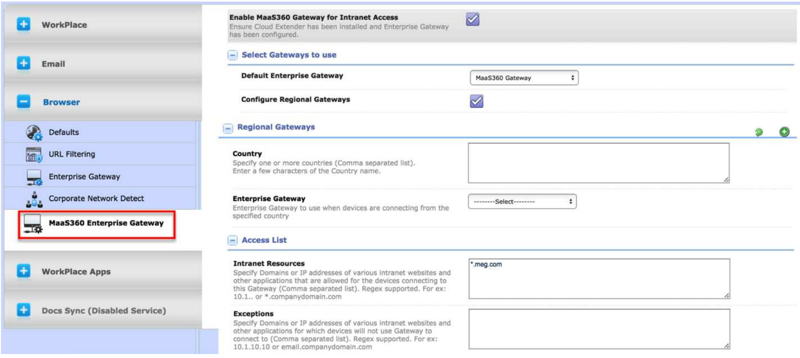
Configure Corporate Network Detection

Corporate Network Server: reports.meg.com
Configure one or more URLs that are accessible only within your Corporate network and can be used to detect Corporate network.
Note: Include http/https as required in the URL specified.

Policy Setting	Description
Allow caching of Corporate Credentials in the App	User credentials are saved within the Secure Browser app in its encrypted database, and protected overall by container security. The browser will re-authenticate against the gateway using these credentials without prompting the user to re-enter credentials each time. Users are prompted for credentials only when their passwords change and the browser fails to authenticate against the gateway.
Identity Certificate	Choose the Identity Certificate Template (from your Cloud Extender's Certificate Integration set up). This identity certificate can be used by the gateway to authenticate against upstream intranet sites that challenge for Identity Certificate credentials for authentication.

Policy Setting	Description
Enable Corporate Network Detection	The browser traffic for intranet sites will skip the Gateway route if any specified **Corporate Network Server** is resolvable by the browser. Any sites that require identity certificate-based authentication will not work. The gateway presents the identity certificate to intranet sites that challenge for them, and in the Corporate Network use case the gateway route is bypassed.

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



Enable MaaS360 Gateway for Intranet Access ☑
Ensure Cloud Extender has been installed and Enterprise Gateway has been configured.

Select Gateways to use

Default Enterprise Gateway MaaS360 Gateway

Configure Regional Gateways ☑

Regional Gateways

Country
Specify one or more countries (Comma separated list). Enter a few characters of the Country name.

Enterprise Gateway --------Select--------
Enterprise Gateway to use when devices are connecting from the specified country

Access List

Intranet Resources *.meg.com
Specify Domains or IP addresses of various intranet websites and other applications that are allowed for the devices connecting to this Gateway (Comma separated list). Regex supported. For ex: 10.1.. or *.companydomain.com

Exceptions
Specify Domains or IP addresses of various intranet websites and other applications for which devices will not use Gateway to connect to (Comma separated list). Regex supported. For ex: 10.1.10.10 or email.companydomain.com

Policy Setting	Description
Default Gateway	Select one of the gateways/gateway clusters you have already set up. The gateway name automatically appears on the drop-down list. All devices associated with this policy will communicate with this gateway if no regional gateways have been configured.
Configure Regional Gateway	Select the checkbox to route devices to regional gateways/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's GPS location. This feature allows you to manage one persona policy for all devices and still achieve location awareness for all devices around the globe.

Policy Setting	Description
Access List for Intranet Resources	Specify domains or IP addresses of intranet sites that should be allowed for devices connecting to the gateway. Use wildcards for domains like *.companydomain.com (regular expressions). It is recommended to restrict this access list to only intranet sites and domains and not to proxy traffic to public sites.
Exceptions	If you have your access list set to **.companydomain.com*, but want certain traffic like email, OWA, etc. to not be proxied via the gateway, you can use the exception list. Add *email.companydomain.com* as an exception, and the traffic will connect directly to your server on the internet without using the gateway.

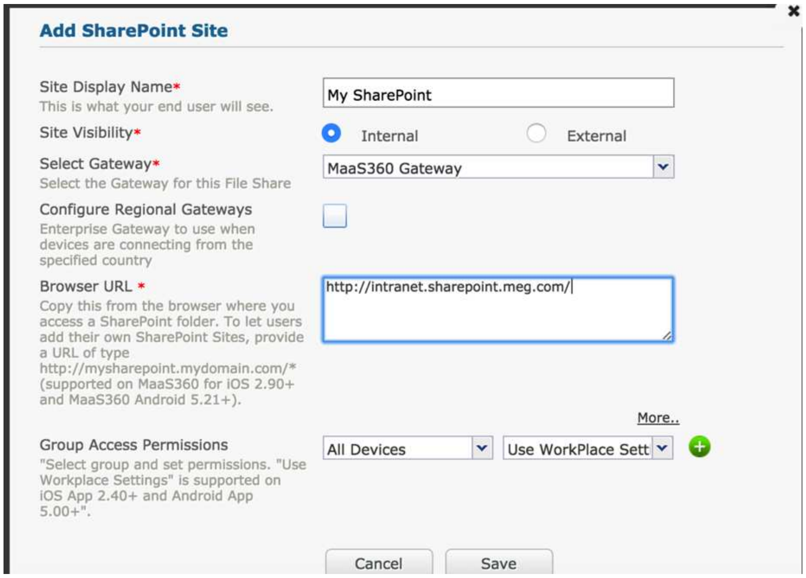
SharePoint/CMIS Configuration

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. My SharePoint

Site Visibility* ● Internal ○ External

Select Gateway* Select the Gateway for this File Share MaaS360 Gateway

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+). http://intranet.sharepoint.meg.com/

Group Access Permissions "Select group and set permissions. "Use Workplace Settings" is supported on iOS App 2.40+ and Android App 5.00+". All Devices Use WorkPlace Sett

Configuration Setting	Description
Site Display Name	The name of the site that your end users will see on their devices.

Configuration Setting	Description
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.
Select Gateway	Select one of the gateways/gateway clusters you have already set up. The gateway name automatically appears on the drop-down list. All devices associated with this distribution will communicate with this gateway if there are no regional gateways configured.
Configure Regional Gateway	Enabling this feature allows you to route devices to regional gateways/gateway clusters based on the geography of the device. Specify the country 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.
Browser URL	URL to your SharePoint site. Access your SharePoint site from your Browser and paste the link to the site directly here. You will need a new distribute per site.
Group Access Permissions	Allows you to distribute the SharePoint site to targeted device along with permissions associated with the distribution.

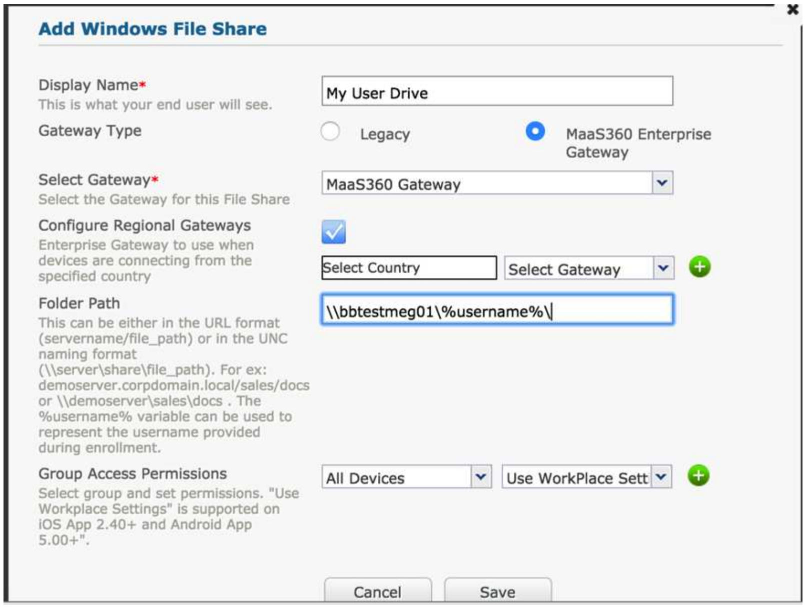
Windows File Share

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. Select **Docs>Content Sources**.
2. Select **Add Source>Windows File**.



Add Windows File Share

Display Name* — This is what your end user will see. — My User Drive

Gateway Type — ○ Legacy ● MaaS360 Enterprise Gateway

Select Gateway* — Select the Gateway for this File Share — MaaS360 Gateway

Configure Regional Gateways — Enterprise Gateway to use when devices are connecting from the specified country — ☑ — Select Country — Select Gateway

Folder Path — This can be either in the URL format (servername/file_path) or in the UNC naming format (\\server\share\file_path). For ex: demoserver.corpdomain.local/sales/docs or \\demoserver\sales\docs . The %username% variable can be used to represent the username provided during enrollment. — \\bbtestmeg01\%username%\

Group Access Permissions — Select group and set permissions. "Use Workplace Settings" is supported on iOS App 2.40+ and Android App 5.00+". — All Devices — Use WorkPlace Sett

Configuration Setting	Description
Display Name	The name of the **Windows File Share** that your end users will see on their devices.
Select Gateway	Select one of the gateways/gateway clusters you have already set up. The gateway name automatically shows up on the drop-down list as long as it has Network File Share feature enabled. All devices associated with this distribution will 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/gateway clusters based on the geography of the device. Specify the country 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). To use this feature, WebDAV needs to be enabled on your gateways. **%username%** variables can be used to distribute user specific file shares if the folder names are the same as MaaS360 usernames.
Group Access Permissions	Allows you to distribute the file shares to the targeted device along with the permissions associated with the distribution.

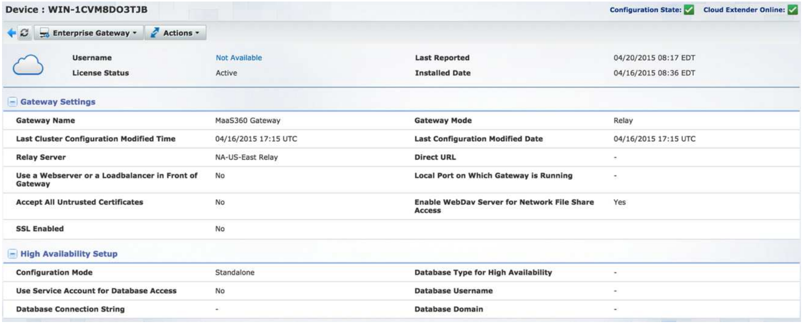
Chapter 11. Access Portal Management Workflows

About this task

MaaS360 portal offers a Cloud Extender view that shows your gateway installation. This view also helps confirm if your gateway is active, and if it is online. (The **Cloud Extender Online** indicator appears in the top right corner.)

Procedure

1. Navigate to **Setup>Cloud Extender**. On this screen, you can pick your Gateway server.
2. After the page loads, select **Summary>Enterprise Gateway**. The page shows the following details:
   - Gateway Settings: Name, Mode, 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-1CVM8DO3TJB

Configuration State: ✓ Cloud Extender Online: ✓

Username	Not Available	Last Reported	04/20/2015 08:17 EDT
License Status	Active	Installed Date	04/16/2015 08:36 EDT

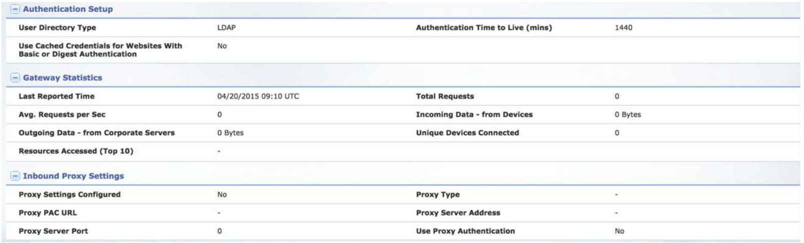
Gateway Settings

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 Webserver 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	-

3. Scroll down to see all the settings.



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)	-		

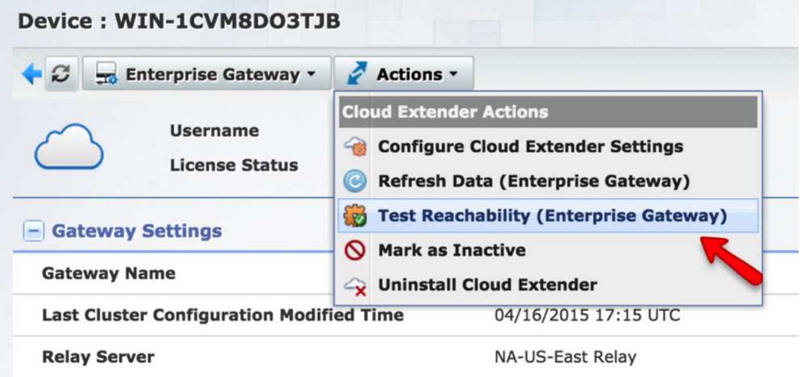
Inbound Proxy Settings

Proxy Settings Configured	No	Proxy Type	-
Proxy PAC URL	-	Proxy Server Address	-
Proxy Server Port	0	Use Proxy Authentication	No

   This view also provides a test action to test reachability to intranet sites.

4. Select the **Actions** pull-down menu, and click **Test Reachability (Enterprise Gateway)**.
5. Specify the hostname/intranet site and confirm reachability of this site from the gateway.

Note: This action is sent directly from MaaS360 portal to the gateway.


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

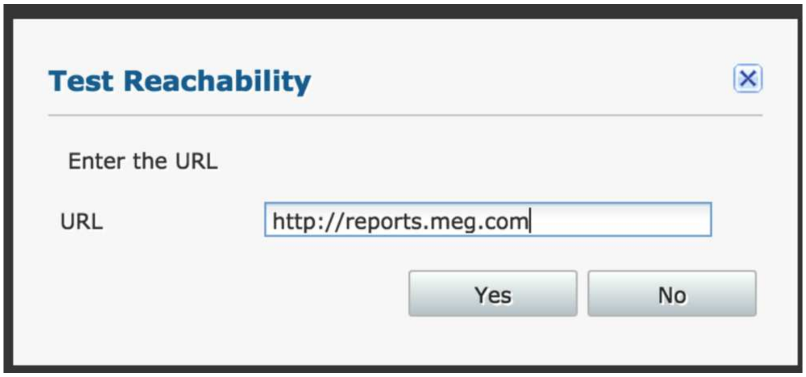
Device : WIN-1CVM8DO3TJB

Username

License Status

Gateway Settings

Gateway Name	
Last Cluster Configuration Modified Time	04/16/2015 17:15 UTC
Relay Server	NA-US-East Relay

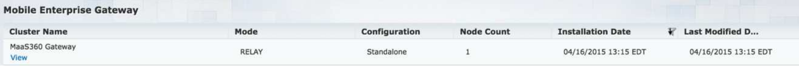


Test Reachability

Enter the URL

URL: http://reports.meg.com

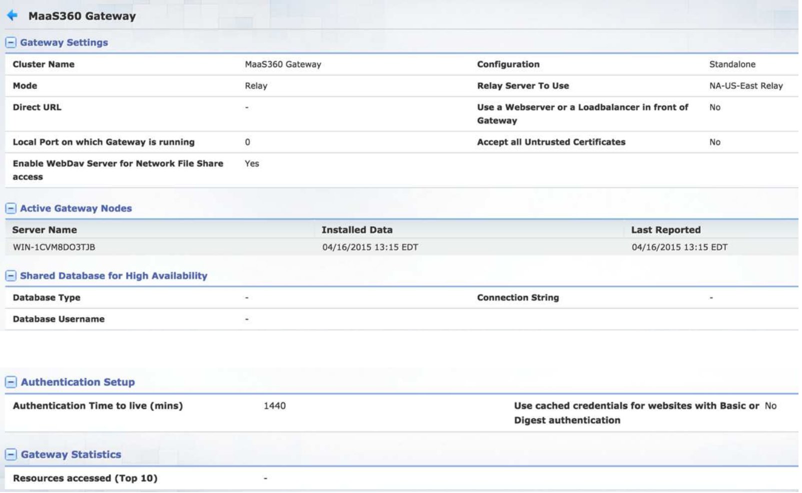
6. MaaS360 also offers a new view of your gateways and clusters. You can access this workflow from **Setup>Mobile Enterprise Gateway**. This consolidated view shows all gateways, their configuration mode, and node counts per cluster.



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

7. Select the detailed view for a summary of all the settings from a cluster point of view and details of all active nodes.



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 Digest authentication	No

Gateway Statistics

Resources accessed (Top 10)	-

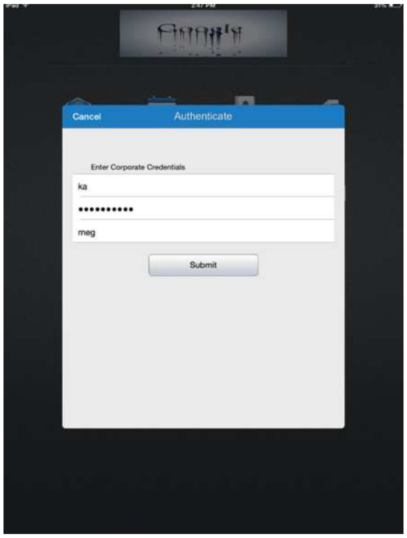
Chapter 12. Mobile App Configuration

MaaS360 provides an app for Android and iOS that will allow you to check on the status of the MEG.

Enroll your iOS or Android device in MaaS360, and assign to it the persona policy that has Secure Browser features enabled.

iOS Experience

When you first launch of the browser, you will be prompted for your credentials. Once authenticated, you will be able to access your intranet sites.



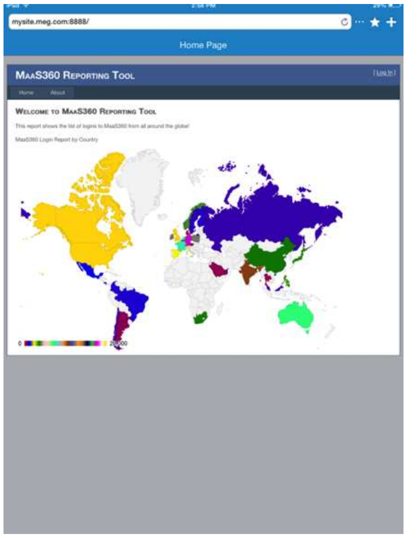
Enter Corporate Credentials

ka

••••••••••

meg

You can get access to MEG reports.

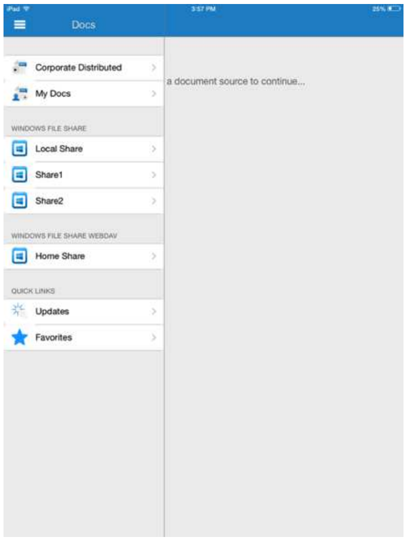


Welcome to MaaS360 Reporting Tool

This report shows the list of logins to MaaS360 from all around the globe!

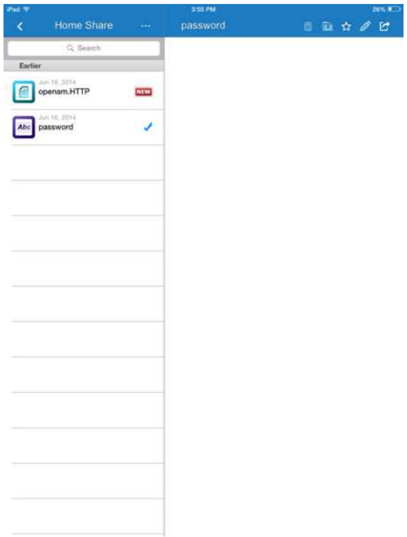
MaaS360 Login Report by Country

MaaS360 Secure Document Sharing allows you to view and update documents distributed from the MaaS360 console and from file shares.



a document source to continue...

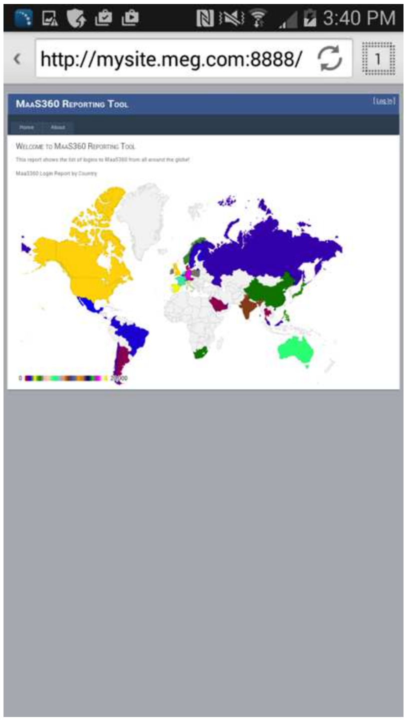
MaaS360 Secure Document Sharing lets you look at the common file types, including Word, Excel, PowerPoint and PDF. For details, refer to the product documentation.



Android Experience

When you first launch of the browser, you will be prompted for your credentials. Once authenticated, you will be able to access your intranet sites.

You can get access to MEG reports.

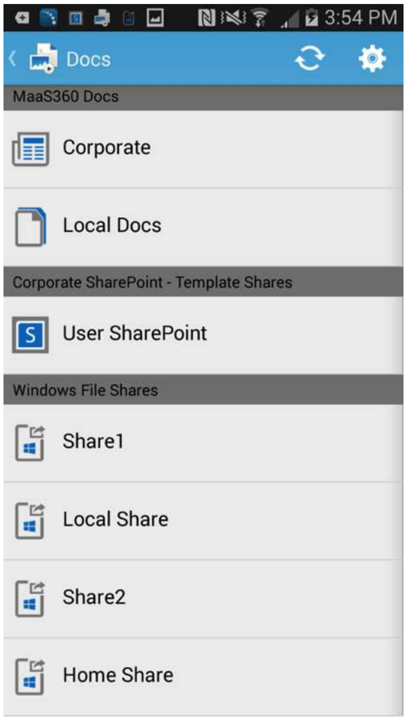


Welcome to MaaS360 Reporting Tool

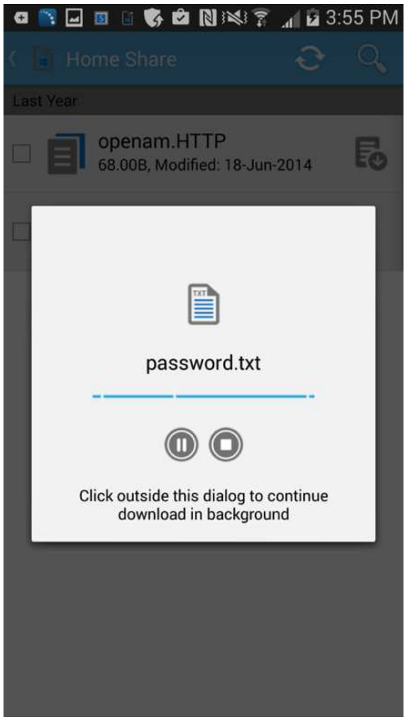
This report shows the list of logins to MaaS360 from all around the globe!

MaaS360 Login Report by Country

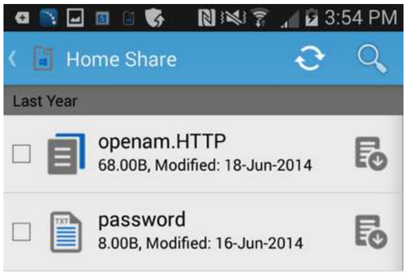
MaaS360 Secure Document Sharing allows you to view and update documents distributed from the MaaS360 console and from file shares.



MaaS360 Secure Document Sharing lets you look at the common file types, including Word, Excel, PowerPoint and PDF. For details, refer to the product documentation.



Click outside this dialog to continue download in background



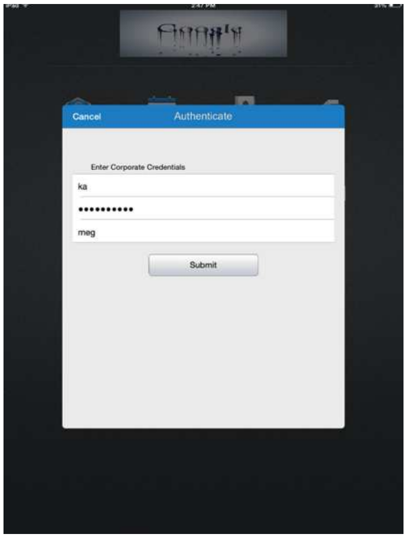
Last Year

□ openam.HTTP
68.00B, Modified: 18-Jun-2014

□ password
8.00B, Modified: 16-Jun-2014

iOS Experience

When you first launch of the browser, you will be prompted for your credentials. Once authenticated, you will be able to access your intranet sites.



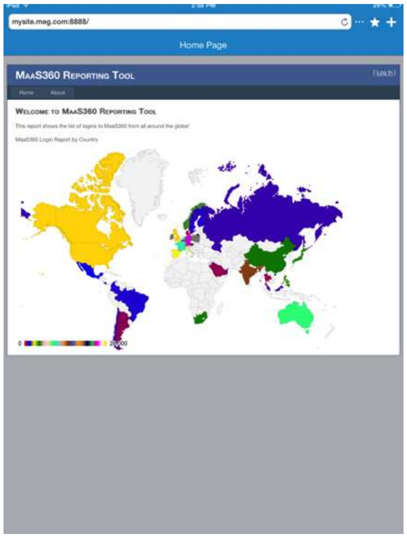
Enter Corporate Credentials

ka

••••••••••

meg

You can get access to MEG reports.

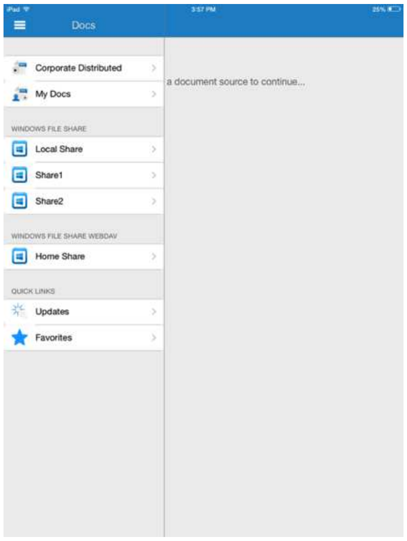


Welcome to MaaS360 Reporting Tool

This report shows the list of logins to MaaS360 from all around the globe!

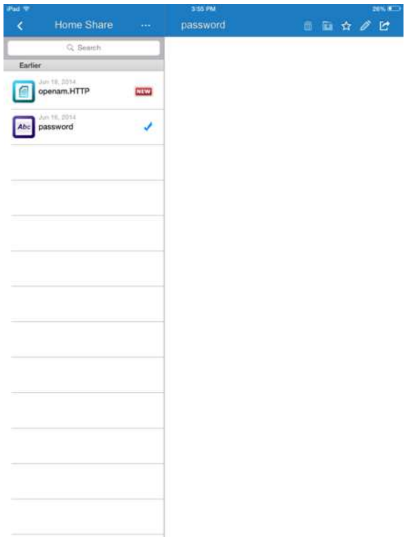
MaaS360 Login Report by Country

MaaS360 Secure Document Sharing allows you to view and update documents distributed from the MaaS360 console and from file shares.



a document source to continue...

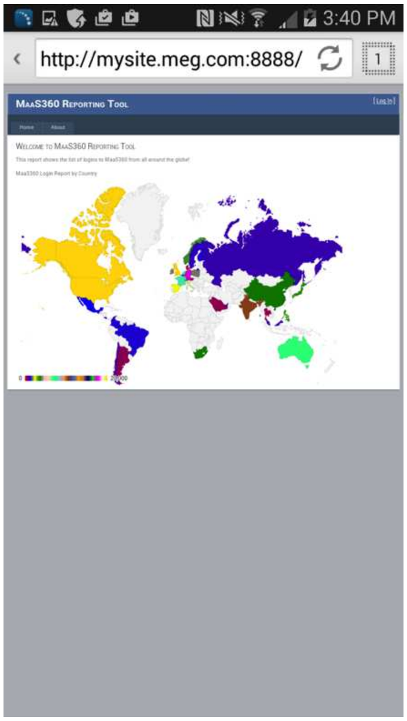
MaaS360 Secure Document Sharing lets you look at the common file types, including Word, Excel, PowerPoint and PDF. For details, refer to the product documentation.



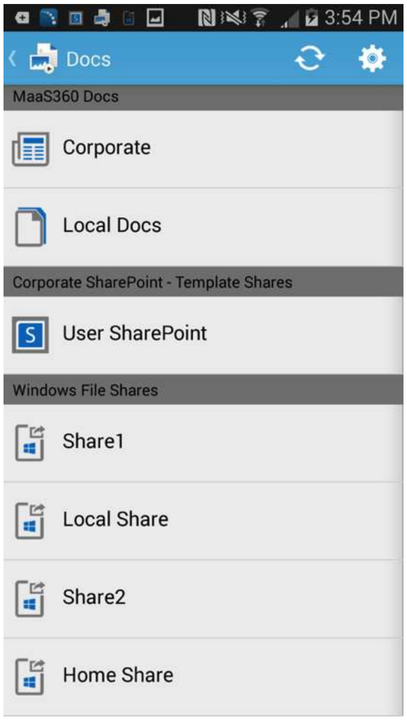
Android Experience

When you first launch of the browser, you will be prompted for your credentials. Once authenticated, you will be able to access your intranet sites.

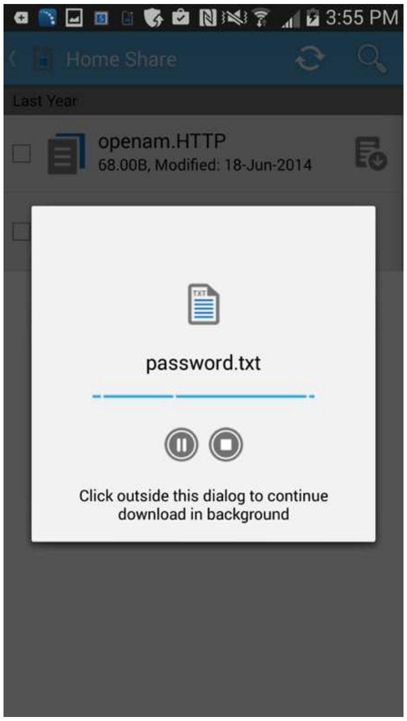
You can get access to MEG reports.


3:40 PM
http://mysite.meg.com:8888/
1
MaaS360 Reporting Tool
[Log In]
Home
About
Welcome to MaaS360 Reporting Tool
This report shows the list of logins to MaaS360 from all around the globe!
MaaS360 Login Report by Country
0
20000

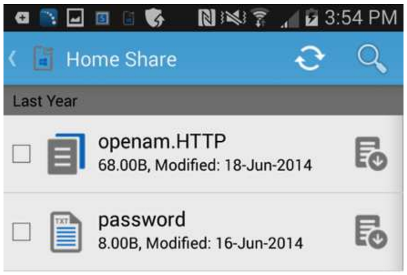
MaaS360 Secure Document Sharing allows you to view and update documents distributed from the MaaS360 console and from file shares.



MaaS360 Secure Document Sharing lets you look at the common file types, including Word, Excel, PowerPoint and PDF. For details, refer to the product documentation.



Click outside this dialog to continue download in background



□ openam.HTTP
68.00B, Modified: 18-Jun-2014

□ password
8.00B, Modified: 16-Jun-2014

Chapter 13. Frequently Asked Questions (FAQs)

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 on **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 IBM Support 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 on the 3 dots after the address bar, select **Settings > Email Logs**. This will launch your email client (native / secure) with a new email and logs as attachments.
3. In Android, open MaaS360 App, navigate 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

- Navigate to the **C:\ProgramData\MaaS360\Cloud Extender\logs** folder:

  MobileGateway.log contains all activities of the gateway

  MobileGatewayAuth.log has all authentication attempts

  MobileGatewayAccess.log has details of all the intranet resources accessed by end users

  MobileGatewayWebResAuth.log contains all authentication attempts against intranet resources

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

- In iOS, go to **Settings > Browser**. The **Version** field displays the version of the browser.
- In Android, go to **Settings > Application Manager > Browser** to access the version.

Chapter 14. Appendix A: Set Up Cross-Forest and Cross-Domain Authentication

About this task

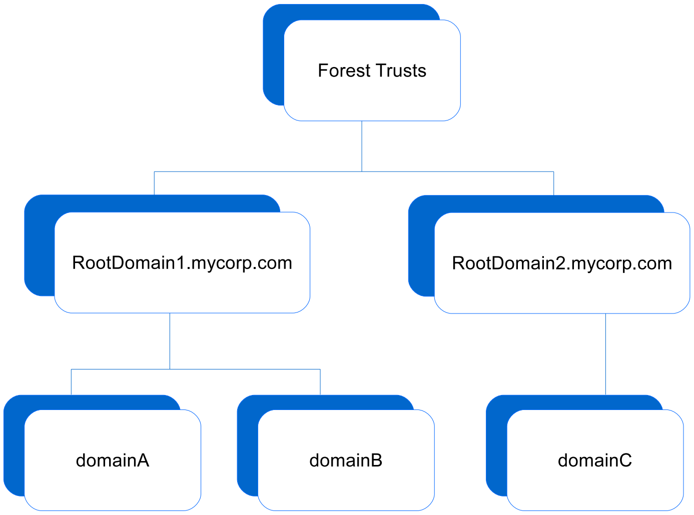
MaaS360 Mobile Enterprise Gateway requires users to authenticate against Corporate Directory Services before letting them access intranet resources. It integrates with both Active Directory and LDAP servers to achieve this form of authentication.

With respect to Active Directory integration for user authentication, the gateway needs to be configured as a Service Account that is a Domain User for a particular domain. The gateway, by default, can only authenticate users belonging to that particular domain within the forest.

If you have multiple domains in a forest and multiple forests, all these forests and domains should trust each other.

Mobile Enterprise Gateway implementation for Active Directory User Authentication can be extended to integrate with multi-domain / multi-forest environments.

This section assumes there are 2 forests and 3 domains, all trusting one another.



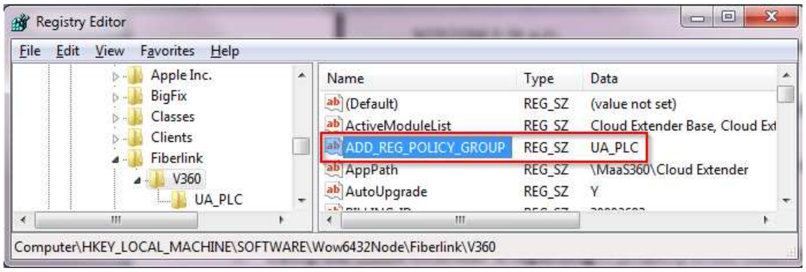
When you enable User Authentication for Active Directory, the default implementation only authenticates users within the context of the service account domain. To extend the authentication scope to all forests and domain, you will need to perform a few additional steps as shown below:

A few registry key additions/modifications are needed in order for the gateway to support multi domain/forest authentication. This must be done manually because the keys may already exist.

Procedure

1. Open Registry Editor (regedit.exe) on the Cloud Extender server.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360
3. Create a new string value in the V360 key

   ```
   ADD_REG_POLICY_GROUP=UA_PLC
   ```



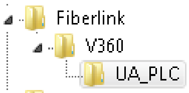
Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveModuleList	REG_SZ	Cloud Extender Base, Cloud Ext
ADD_REG_POLICY_GROUP	REG_SZ	UA_PLC
AppPath	REG_SZ	\MaaS360\Cloud Extender
AutoUpgrade	REG_SZ	Y

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360

Note: If this already exists, append UA_PLC to the list separated by a semi colon (;)

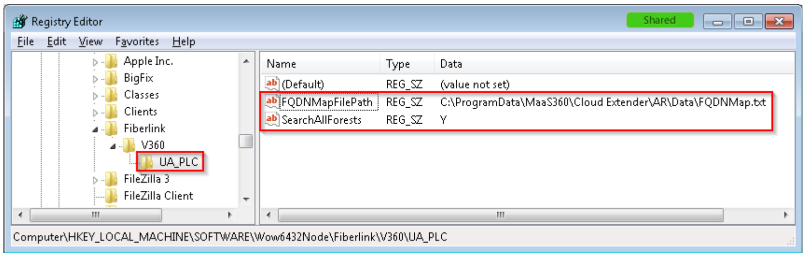
4. Create a new key under V360 named UA_PLC:

   ```
   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
   ```



Name	Type	Data
(Default)	REG_SZ	(value not set)
FQDNMapFilePath	REG_SZ	C:\ProgramData\MaaS360\Cloud Extender\AR\Data\FQDNMap.txt
SearchAllForests	REG_SZ	Y

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360\UA_PLC

6. Create a FQDNMap.txt file using any text editor The mapping file is a text file that contains one entry per line of text for each domain.

   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

   Important: Map both combinations.

   ```
   shortDomainName = FQDN
   FQDN = FQDN
   domainA = domainA.rootDomain1.mycorp.com
   domainB = domainB.rootDomain1.mycorp.com
   domainC = domainC.rootDomain2.mycorp.com
   domainA.rootDomain1.mycorp.com = domainA.rootDomain1.mycorp.com
   domainB.rootDomain1.mycorp.com = domainB.rootDomain1.mycorp.com
   domainC.rootDomain2.mycorp.com = domainC.rootDomain2.mycorp.com
   ```

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

7. Save the file as FQDNMap.txt
8. Copy the FQDN map file FQDNMap.txt to C:\ProgramData\MaaS360\Cloud Extender\AR\Data\
9. Restart the Cloud Extender Service. If multiple Gateways are implemented in an HA fashion, please implement the same steps on all gateways implementing User Authentication Service.