IBM MobileFirst Protect Mobile Enterprise Gateway

Quick Start Guide

Version 2 Release 0

IBM MobileFirst Protect Mobile Enterprise Gateway

Quick Start Guide

Version 2 Release 0

Note
Before using this information and the product it supports, read the information in "Notices" on page 57.

This edition applies to version 2, release 4, modification level 0 of IBM MobileFirst Protect (program number 5725-R11) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview 1
What's new in MEG 2.0? 1
Gateway Mode 2
System Requirements 2
Direct Access Mode Architecture. 3

Chapter 2. Installing the Gateway 5
Setting Up the Gateway Authentication Mode . . . 5
Installing the Cloud Extender module 9

Chapter 3. Configuring Outbound Proxy Settings for the IBM MobileFirst Protect Cloud Extender 11

Chapter 4. Testing Gateway Authentication 13

Chapter 5. Configuring the Gateway in Direct Mode as Standalone 15

Chapter 6. Configuring SSL 17

Chapter 7. Configuring the Gateway in High Availability (HA) Mode 19
Why Clustered Gateways? 19
Direct Architecture in Clustered Mode 19
Configuring Gateway as HA in Direct Mode . . . 20
Preparing a Database 22
Setting Up the Database 23
MySQL Database Configuration 23
Microsoft SQL Database Configuration 23
DB2 Configuration 25
Joining the Gateway to an Existing Cluster 26

Chapter 8. Configuring Authentication and WebDAV 29

Chapter 9. Configure Intranet Proxy Settings 31

Chapter 10. IBM MobileFirst Protect Administration Portal Configuration . . 33
Securing Browser Configuration 33
SharePoint/CMIS Configuration 35
Windows File Share 36

Chapter 11. Accessing Portal Management Workflows 39

Chapter 12. Mobile App Configuration 41
iOS Experience 41
Android Experience 43

Chapter 13. Frequently Asked Questions (FAQs) 51

Chapter 14. Appendix A: Setting Up Cross-Forest and Cross-Domain Authentication 53

Notices 57
Trademarks 59
Terms and conditions for product documentation. . 59

Chapter 1. Overview

IBM MobileFirst™ Protect 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 MobileFirst Protect 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, SPNEGO and Identity Certificates

MEG provides maximum security by authenticating users and devices based on Corporate Directory credentials and IBM MobileFirst Protect 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 IBM MobileFirst Protect container, fully encrypted and protected from data leaks, and is protected by IBM MobileFirst Protect 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 IBM MobileFirst Protect console helps define lockout policies and provides the ability to revoke access to the gateway based on automated compliance rules.

IBM MobileFirst Protect 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 IBM MobileFirst Protect On-Premise version 2.4 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/SPNEGO 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 IBM MobileFirst Protect On-Premise.

System Requirements

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

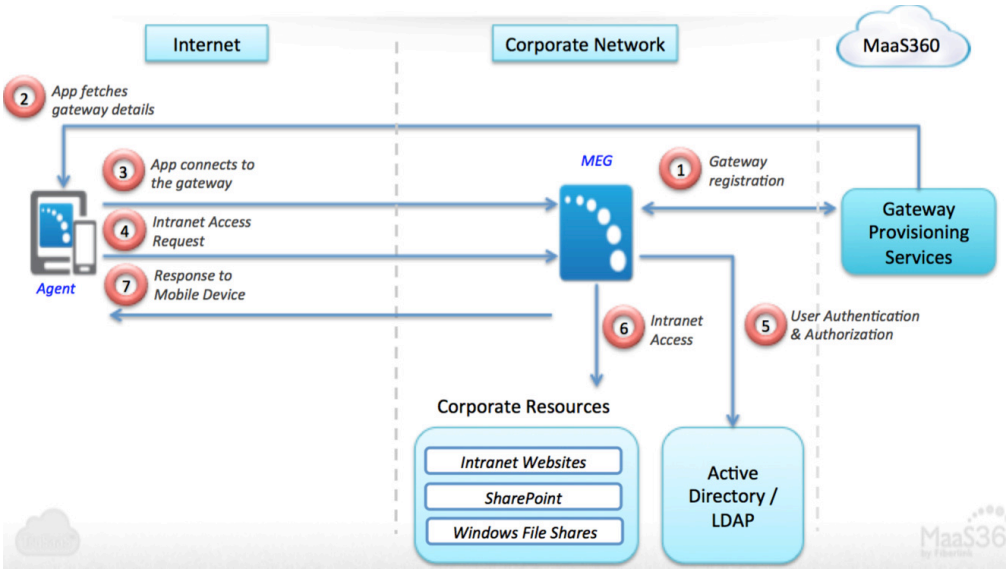
Item	Meets Requirements
IBM MobileFirst Protect version 2.4 or later account (either SaaS or On-Premise installation)	
Physical or Virtual Machine with Windows Server 2012 RC2, 2012, 2008 RC2, 2008, or 2003 as an installation target for the IBM MobileFirst Protect Mobile Enterprise Gateway.	
A **Service 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 IBM MobileFirst Protect Backend and Web Services. IBM MobileFirst Protect Backend: Service URL for the IBM MobileFirst Protect On-Premise 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 IBM MobileFirst Protect On-Premise as follows:

1. Gateway Provisioning Services registers with IBM MobileFirst Protect On-Premise.
2. The IBM MobileFirst Protect app on the device fetches Gateway details.
3. The app connects to the Gateway.
4. The app requests intranet access from IBM MobileFirst Protect On-Premises.
5. IBM MobileFirst Protect On-Premise 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.



Architecture Components

MEG has two components, the Client and the Gateway.

Client

The MaaS360 app for iOS and Android, Secure Browser and any Enterprise App wrapped within IBM MobileFirst Protect or integrated the IBM MobileFirst Protect SDK can communicate with MEG.

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

If an SSL certificate is used, access is via HTTPS

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. Installing the Gateway

About this task

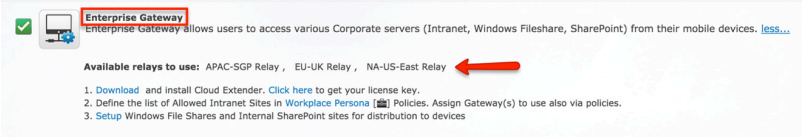
To install the Gateway, perform the following steps:

Procedure

1. Log in to IBM MobileFirst Protect and browse to the Services page (**Setup** > **Services.**).

   The **Enterprise Gateway** feature has a checkmark.

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

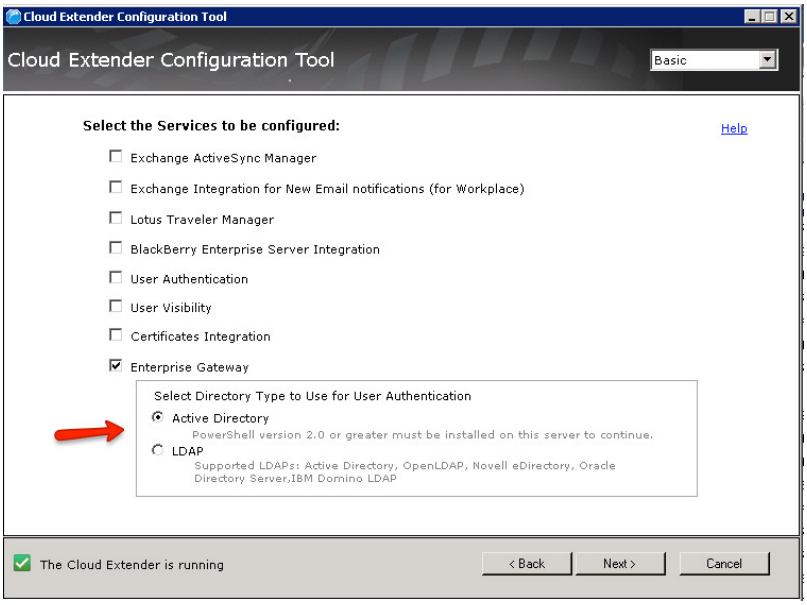


2. **Download** the Cloud Extender using the download link from Step 1 in the portal.
3. Select **Click here** to send your license key to your registered email address.

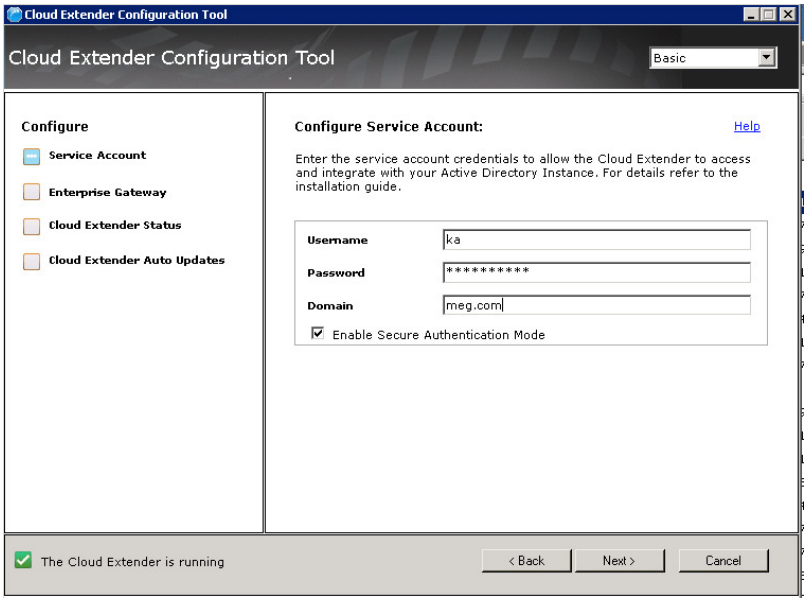
Setting Up the Gateway Authentication Mode

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**.

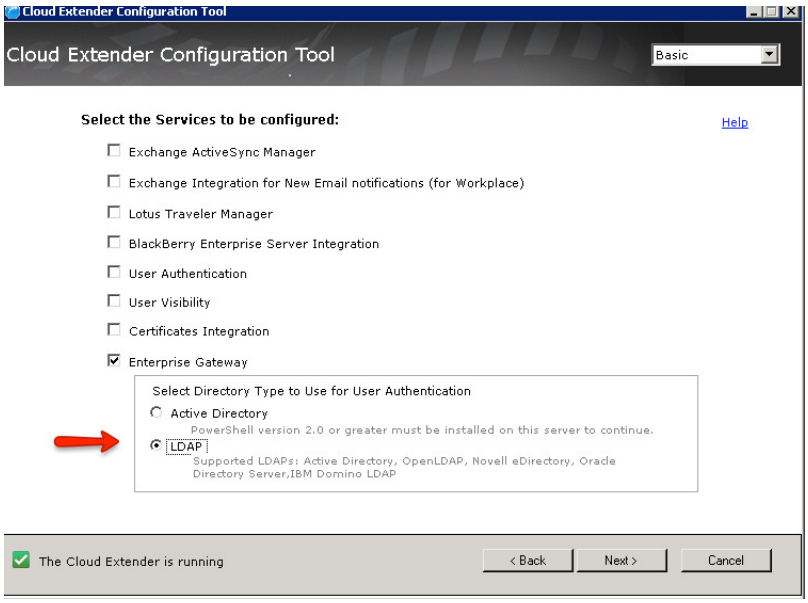


b. Enter the Service Account's *Username*, *Password* and *Domain* (See Requirements). Click **Next** to receive the success message.

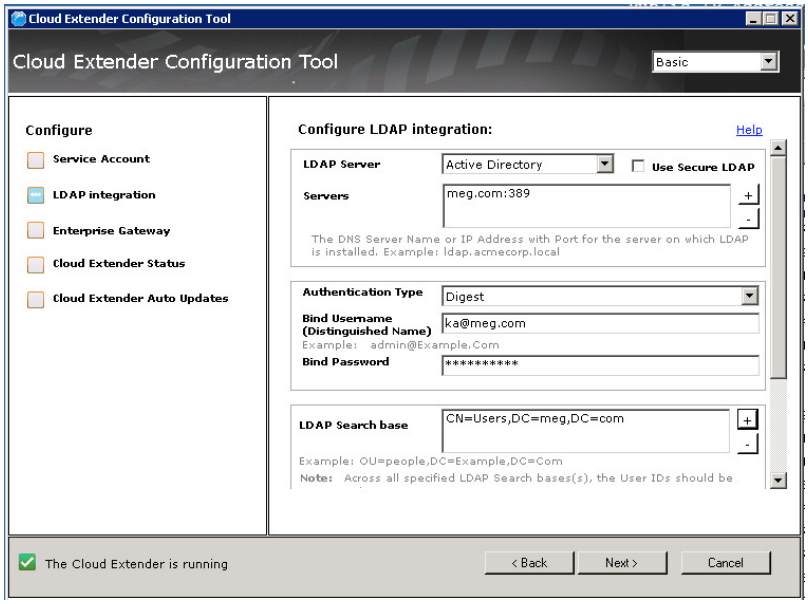


c. Click **OK** to dismiss the success message, and then click **Next** to Chapter 4, "Testing Gateway Authentication," on page 13.

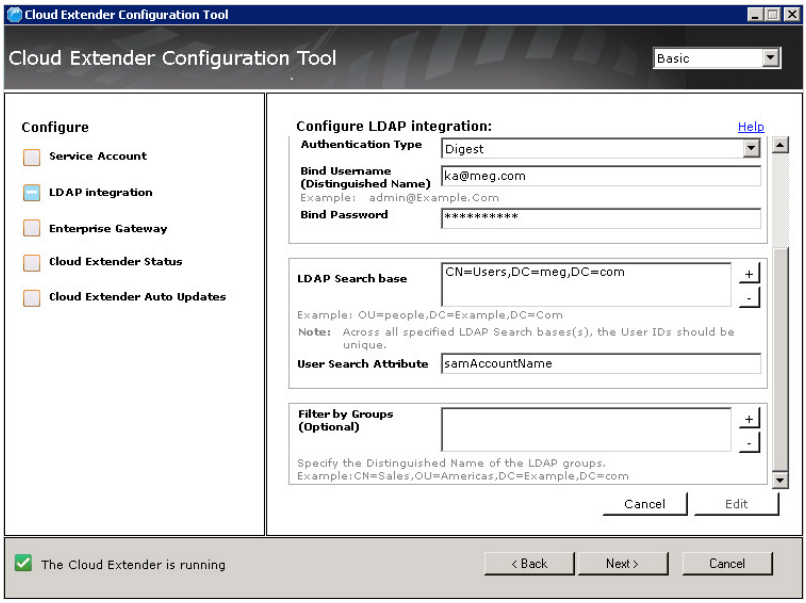
4. If you choose LDAP for the directory type:
   a. Select **LDAP** as the Enterprise Gateway



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

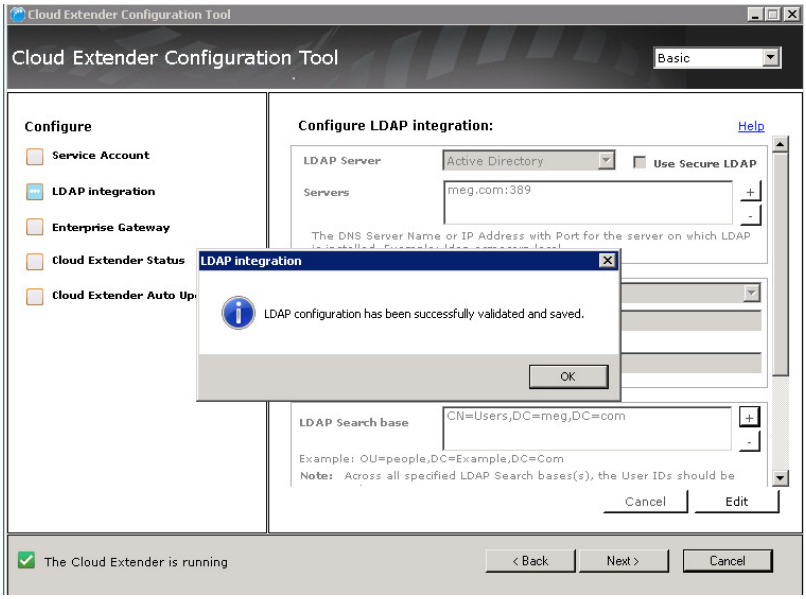


c. On the next configuration screen, enter the following settings and click **Next**:



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

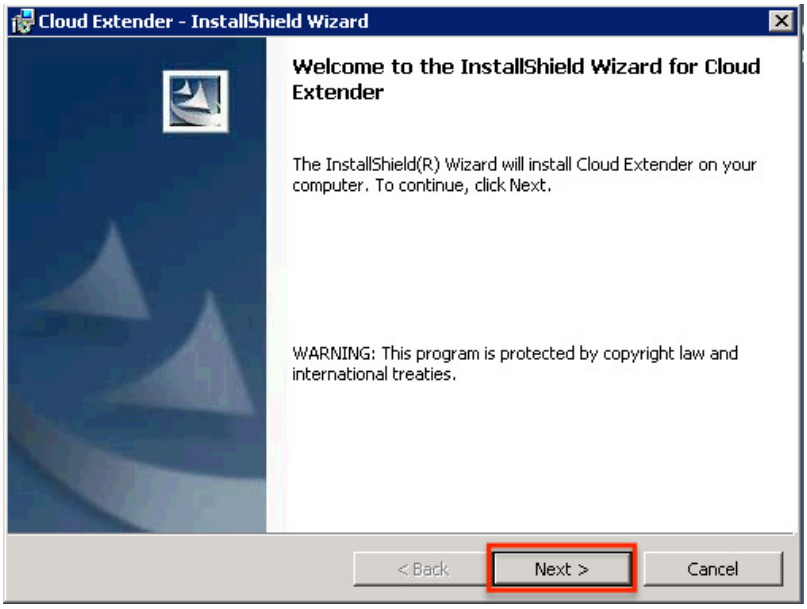
5. When you have entered your changes, you will receive a success message. Click **OK** to dismiss the message, and then click **Next**.



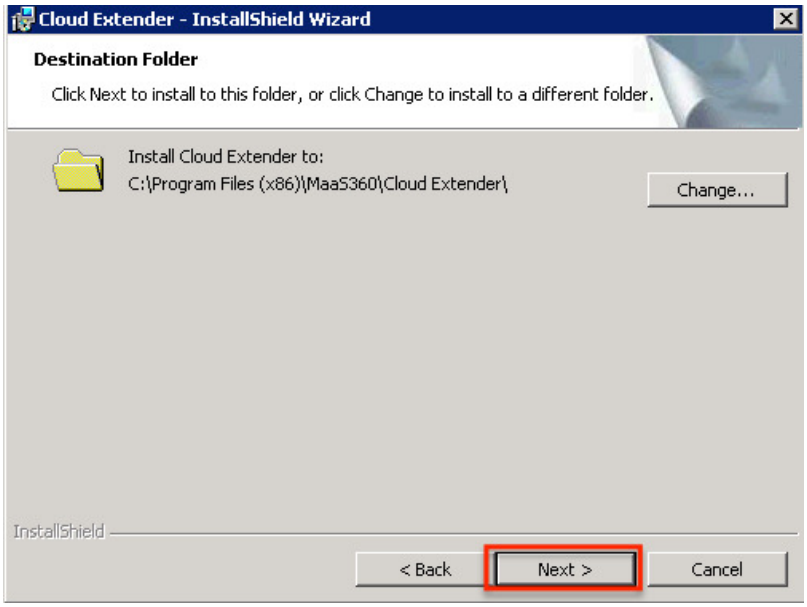
Installing the Cloud Extender module

Procedure

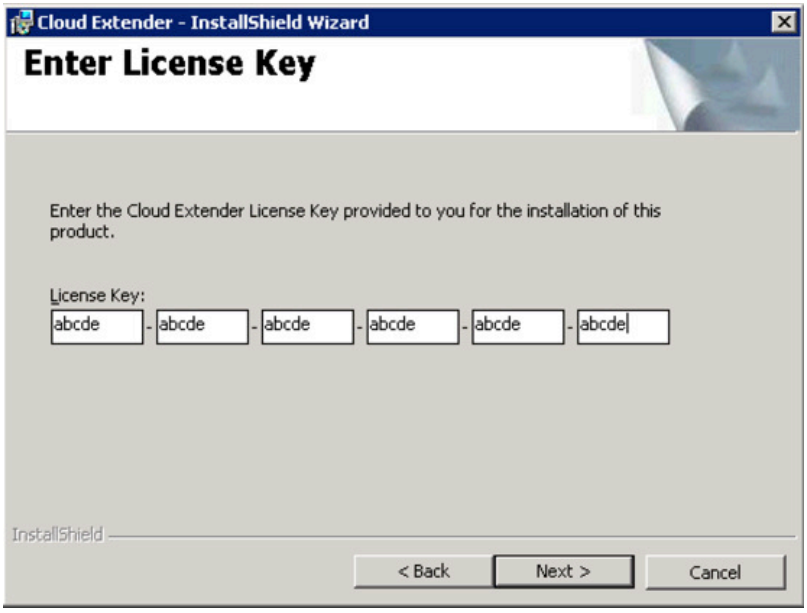
1. On the **Welcome** screen, click **Next**.



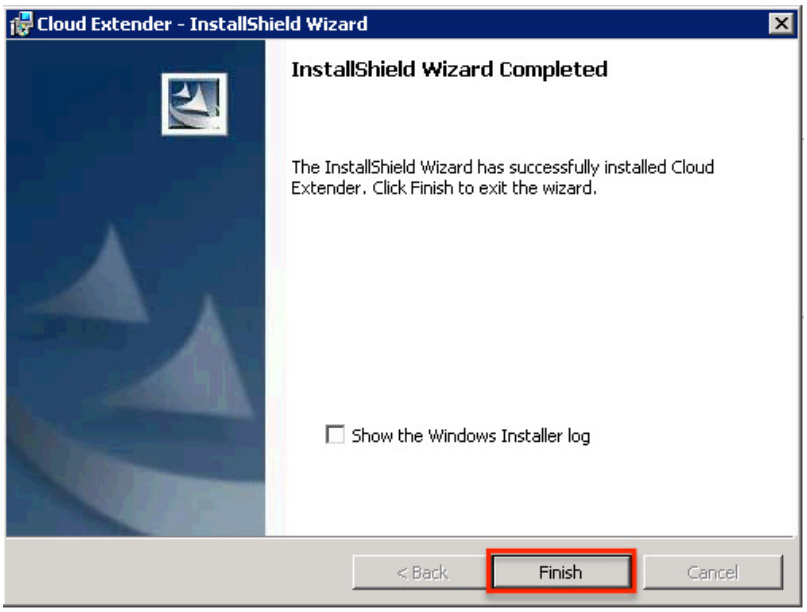
2. Click **Next** to install the files into the default folder.



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



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



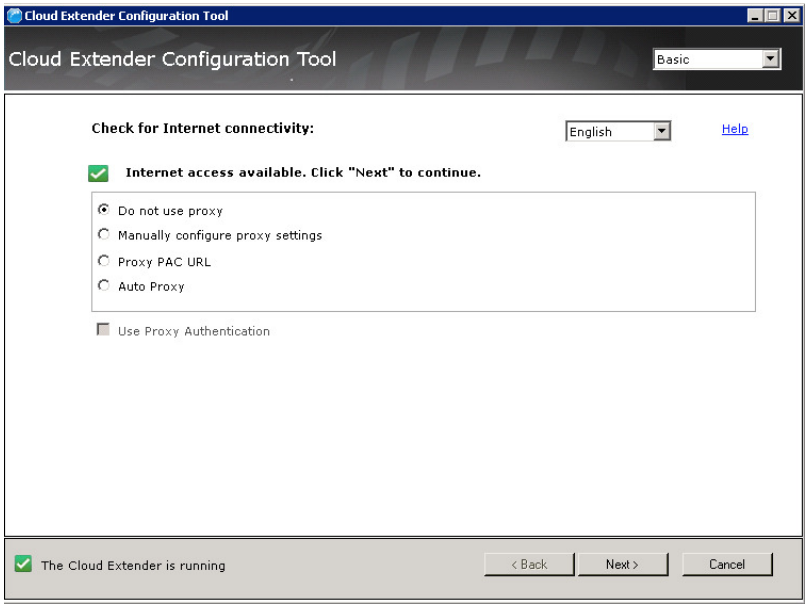
Once the Cloud Extender installation completes, the Cloud Extender Configuration Tool launches automatically.

Chapter 3. Configuring Outbound Proxy Settings for the IBM MobileFirst Protect 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 IBM MobileFirst Protect backend services for overall configuration and management.



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.

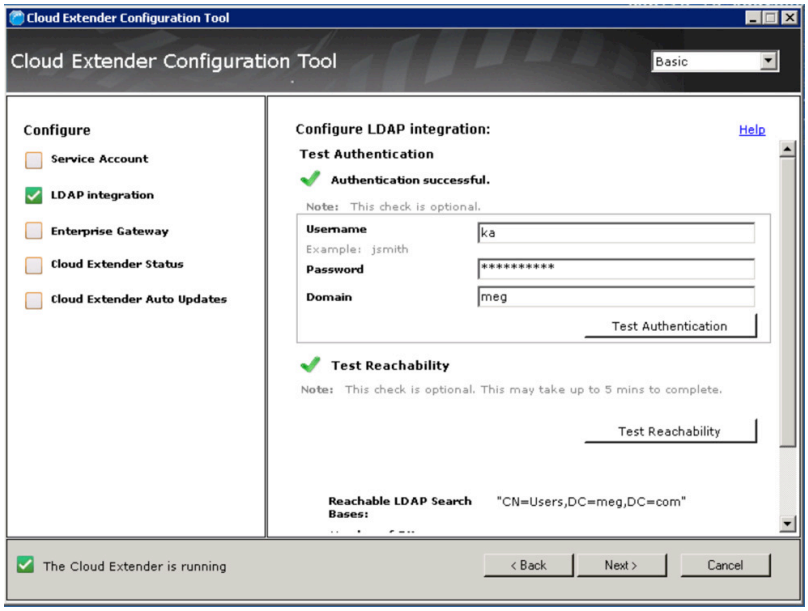
Chapter 4. Testing Gateway Authentication

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:



Chapter 5. Configuring the Gateway in Direct Mode as Standalone

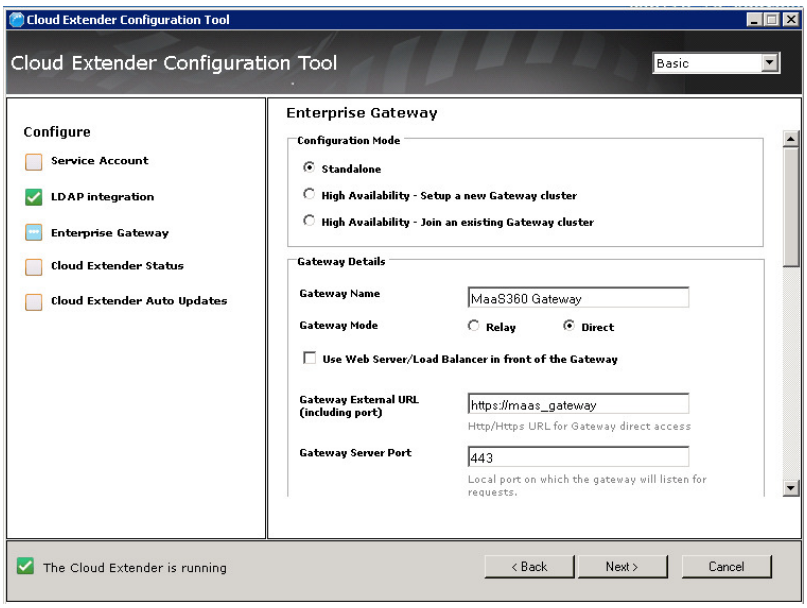
About this task

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

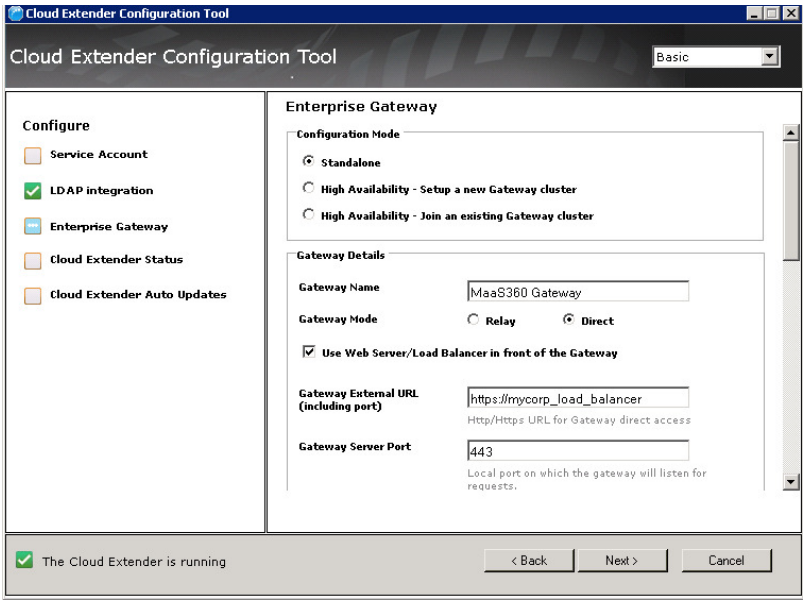
1. In the Configuration Mode section, choose **Standalone**.



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 IBM MobileFirst Protect Administration Portal workflows.
Gateway Mode	Select **Direct**.
Use Web Server / Load Balancer in front of the Gateway	If selected, 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)	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 includes the port.
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** is any open port on this gateway server.



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

Chapter 6. Configuring SSL

About this task

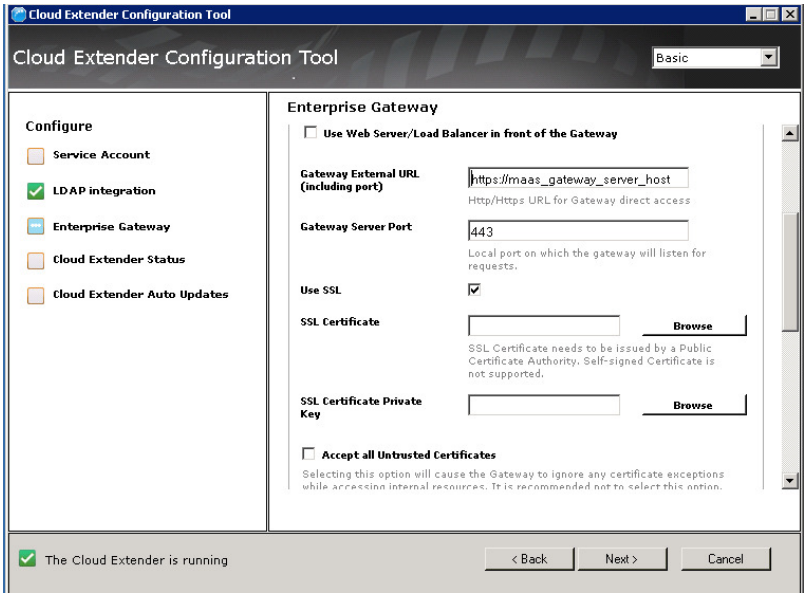
Use SSL encryption on top of the AES 256-bit end-to-end encryption to further secure communication between the mobile device and the gateway.

Note: This is optional—not using SSL will not compromise the security of the IBM MobileFirst Protect 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 is used by the mobile device to initiate an SSL session to the gateway. • If you use a load balancer, then the SSL Certificate 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. Refer to your vendor documentation for details. If you are using intermediate CAs, you must have a complete certificate chain in the .pem file.
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 must install the site SSL certificates to the Certificate store of the Gateway server.



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

Chapter 7. Configuring 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?

Multiple instances of IBM MobileFirst Protect Mobile Enterprise Gateway, 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, 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 can 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.

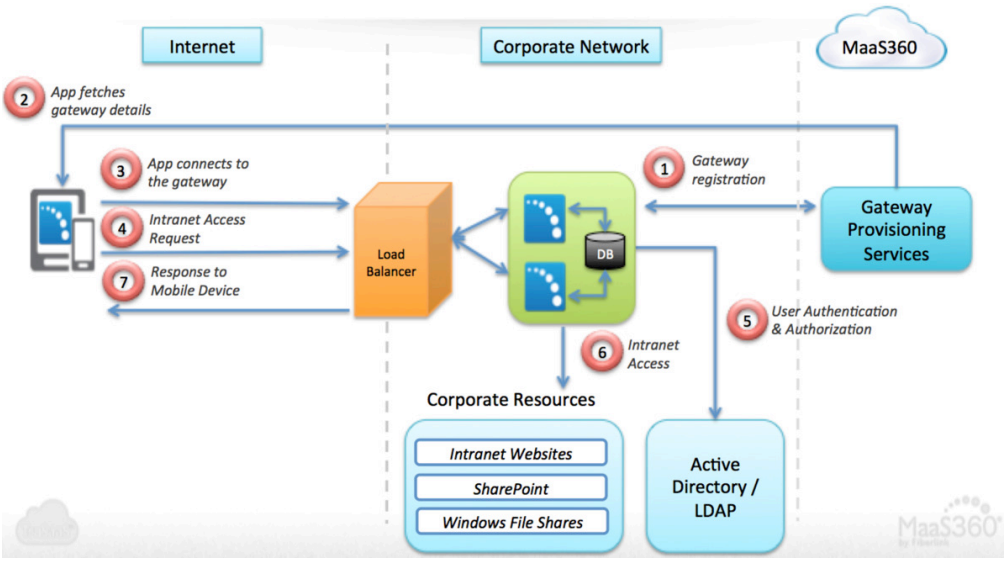
Direct Architecture in Clustered Mode

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.

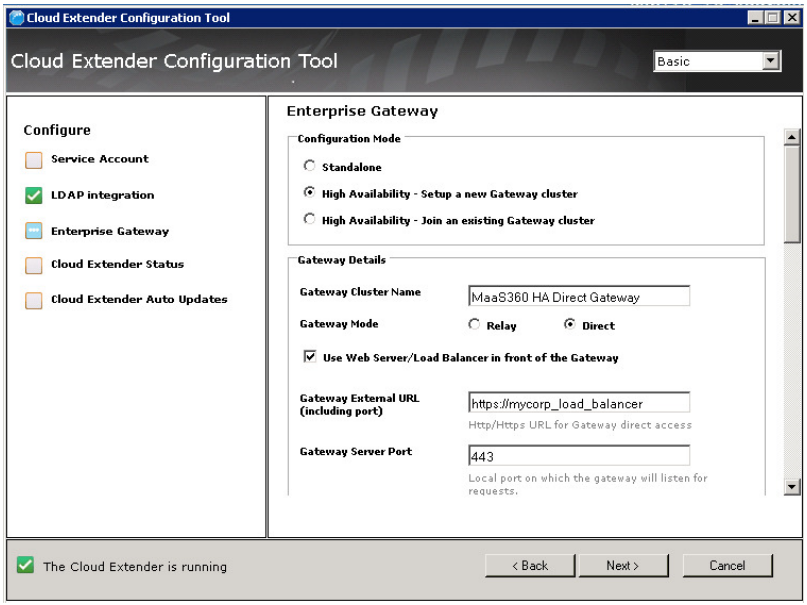
You may set up SSL certificates for traffic between load-balancer and gateway. This is optional and the data packets between them are anyways encrypted, even over HTTP.



Configuring Gateway as HA in Direct Mode

Procedure

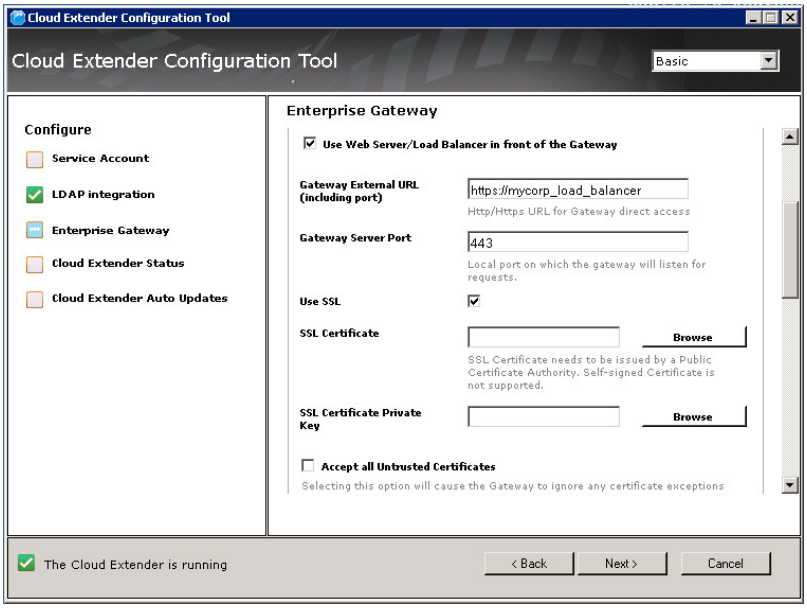
1. On the first configuration screen, enter the settings as neede:



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 IBM MobileFirst Protect Administration Portal workflows.
Gateway Mode	Select **Direct**.
Use Web Server/Load Balancer in front of the Gateway	Select the checkbox. You are 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** is the **External URL** (hostname) of your Load Balancer. If it is not used, the **Gateway URL** is the **hostname** of the gateway server. The external URL includes the port.
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** is any open port on this gateway server.

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



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** 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. 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.

Preparing 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.

Setting Up the Database

Procedure

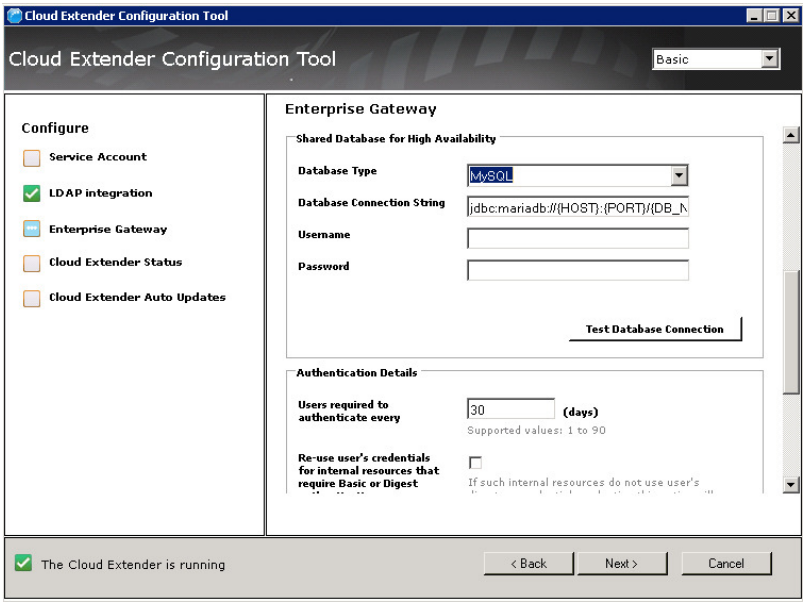
Continue scrolling down to access the next settings. To connect the gateways to the shared database, you will need the following details:

- 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.



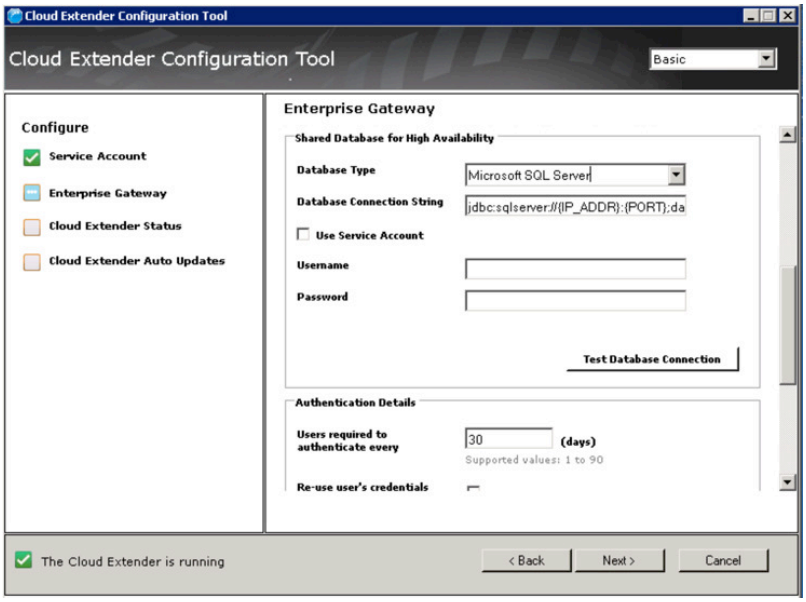
Microsoft SQL Database Configuration

About this task

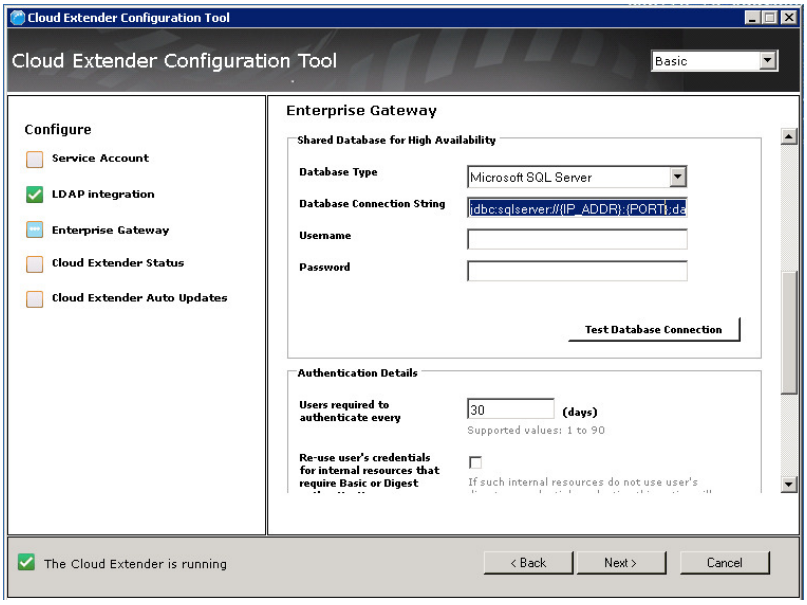
There are two choices: Active Directory and LDAP.

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.



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.

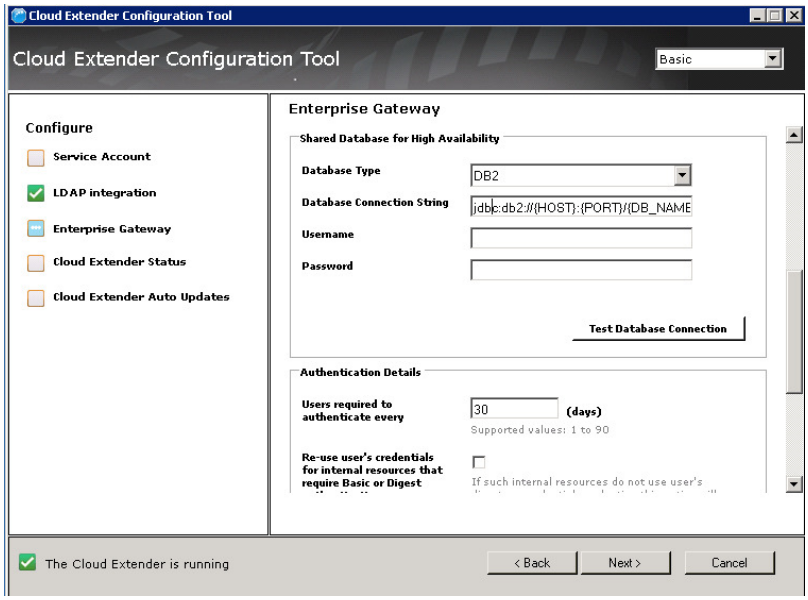


DB2 Configuration

About this task

Procedure

Continue scrolling down to enter the next group of settings.



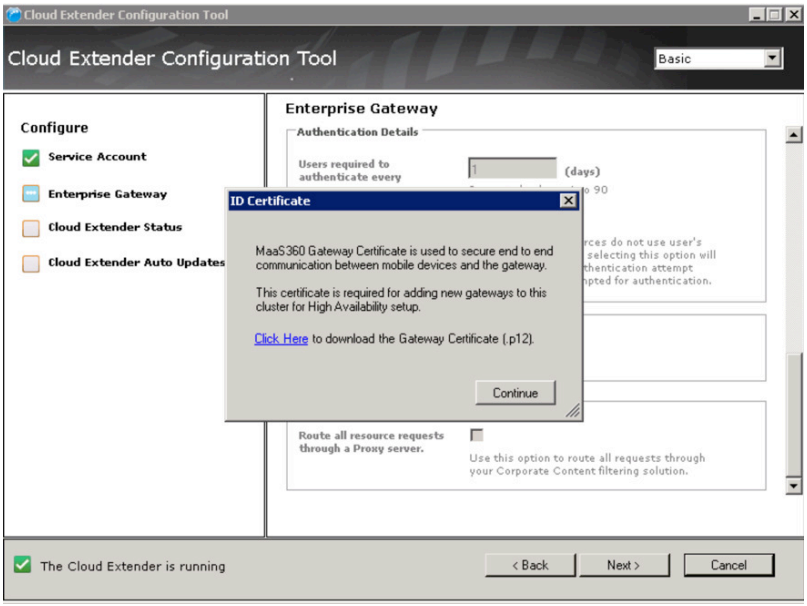
Configuration Setting	Description
Database Type	MySQL/Microsoft SQL Server/DB2 – select one depending on your database type.
Database Connection String	The database connection string gets automatically populated on the gateway depending on the Database Type selection. Replace the {HOST}, {IP_ADDR}, {PORT} 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 must 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.

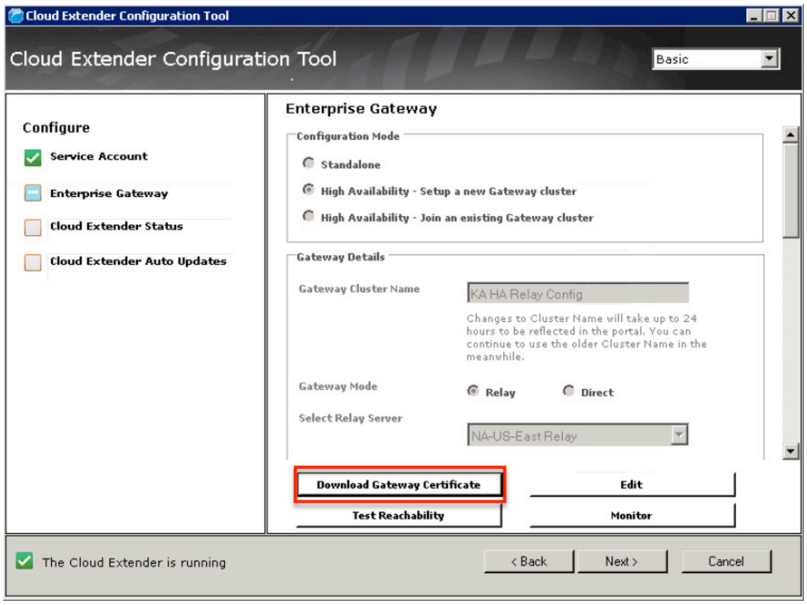
Joining the Gateway to an Existing Cluster

Procedure

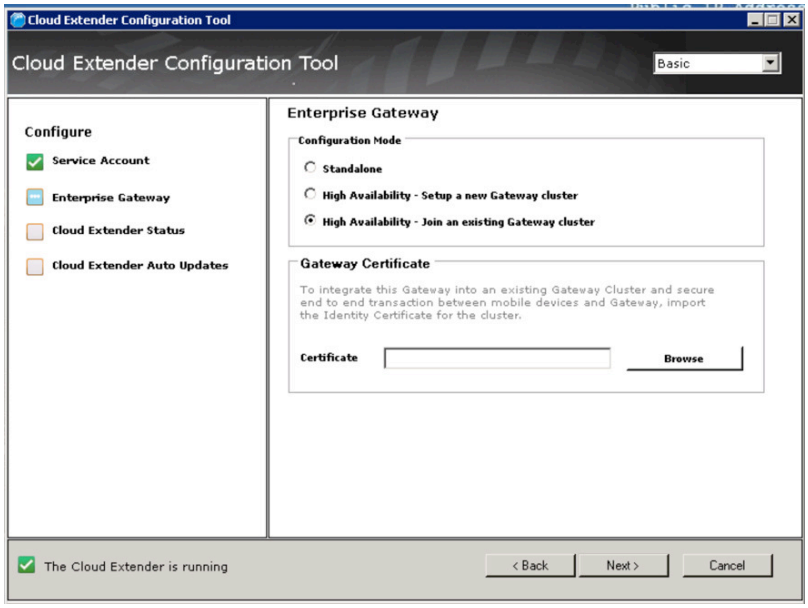
1. Once the first Mobile Enterprise Gateway of the cluster is set up, the gateway generates an encrypted Identity Certificate for the cluster configuration and prompts you to save the certificate.



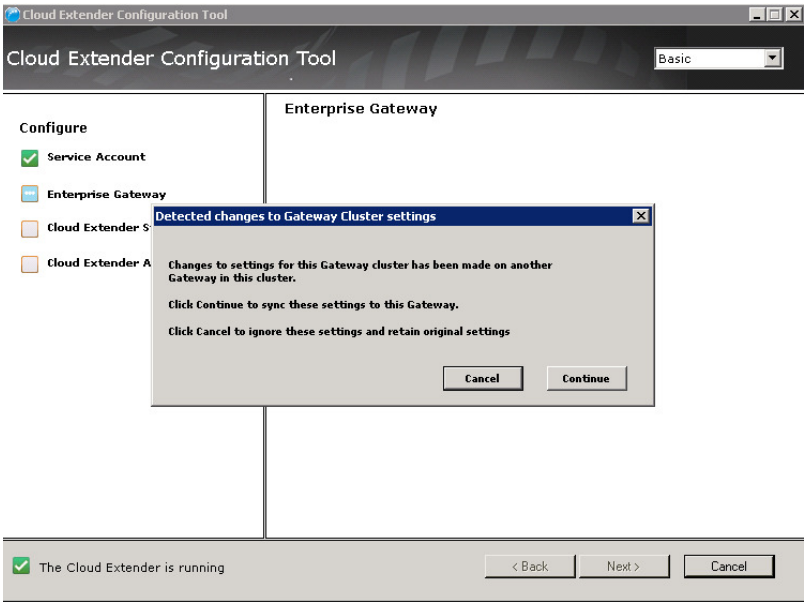
This certificate is required to join new gateways to this HA cluster. If you do not find this certificate, you can always download it again from your first gateway clicking **Download Gateway Certificate**.



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.



3. If the gateways have been set up in HA mode and you want to change 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.

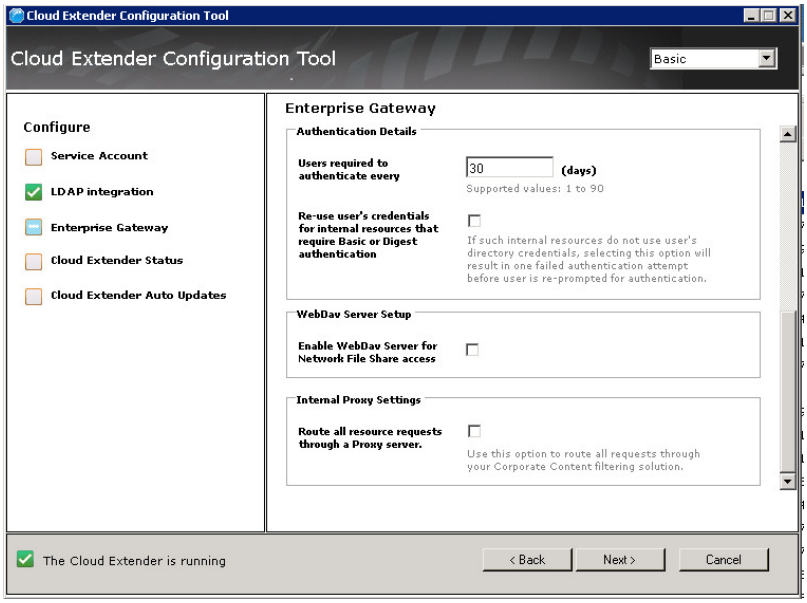


4. You must launch the Cloud Extender Configuration Tool on all other gateways and Select Update Configuration on all of them so that all the gateways are in sync.

Chapter 8. Configuring Authentication and WebDAV

Procedure

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



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 IBM MobileFirst Protect Administration Portal to cache user credentials in the MaaS360 app (covered later). This provides a good user experience while meeting security requirements.

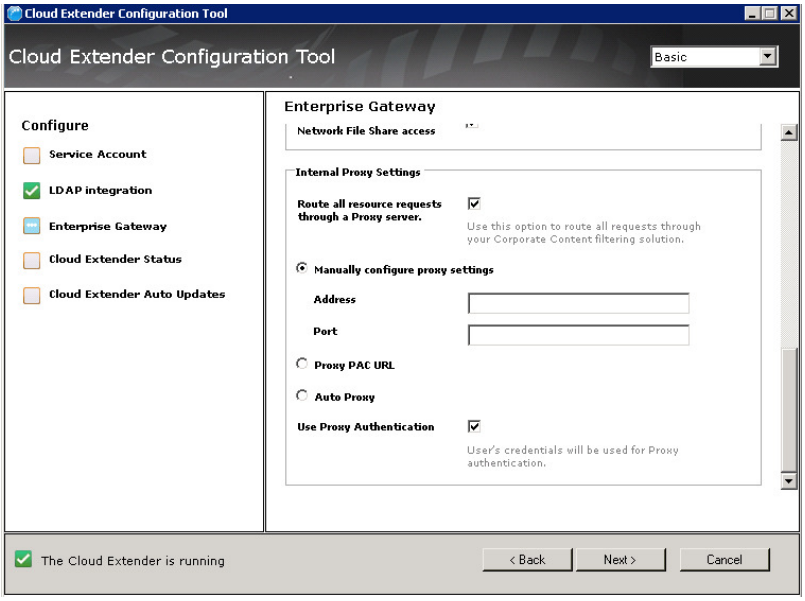
Configuration Setting	Description
Reuse user's credentials for intranet resources that require Basic or Digest authentication	Certain intranet websites that use Basic or Digest authentication might be integrated with corporate credentials for authentication, although this is not very common. If you have 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 • There is a failed authentication attempt for the user before the user gets a chance to authenticate. 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.



Configuration Setting	Description
Route all resource requests though 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, "Configuring Outbound Proxy Settings for the IBM MobileFirst Protect 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 can authenticate to this proxy server.

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

Chapter 10. IBM MobileFirst Protect Administration Portal Configuration

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

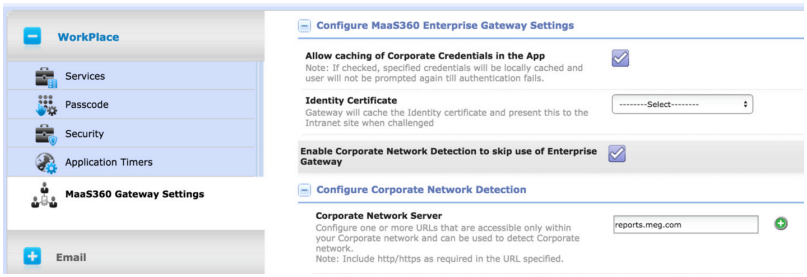
Securing Browser Configuration

About this task

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

Procedure

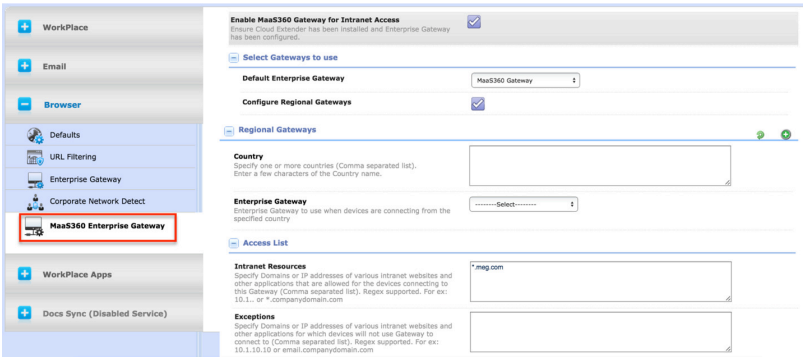
1. Access the IBM MobileFirst Protect console and open the WorkPlace Persona policy.
2. Select **MaaS360 Gateway Settings** on the left side of the screen to display the following policy settings:



Policy Setting	Description
Allow caching of Corporate Credentials in the App	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	If any specified **Corporate Network Server** is resolvable by the browser, the browser traffic for intranet sites will skip the Gateway route. 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**.



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. If no regional gateways have been configured, all devices associated with this policy will communicate with this gateway.
Configure Regional Gateway	Select the check box 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 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 are 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.

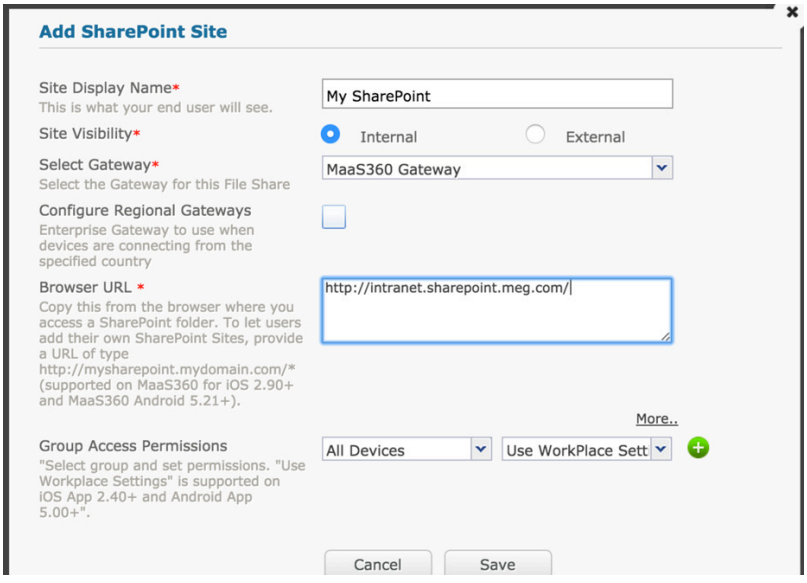
SharePoint/CMIS Configuration

About this task

The Secure Docs 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**.



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. If your SharePoint site is publicly hosted and does not require gateway access, select **External**.
Select Gateway	Select one of the gateways/gateway clusters you have already set up. The gateway name automatically appears on the drop-down list. If there are no regional gateways configured, all devices associated with this distribution will communicate with this gateway.
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 can 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.

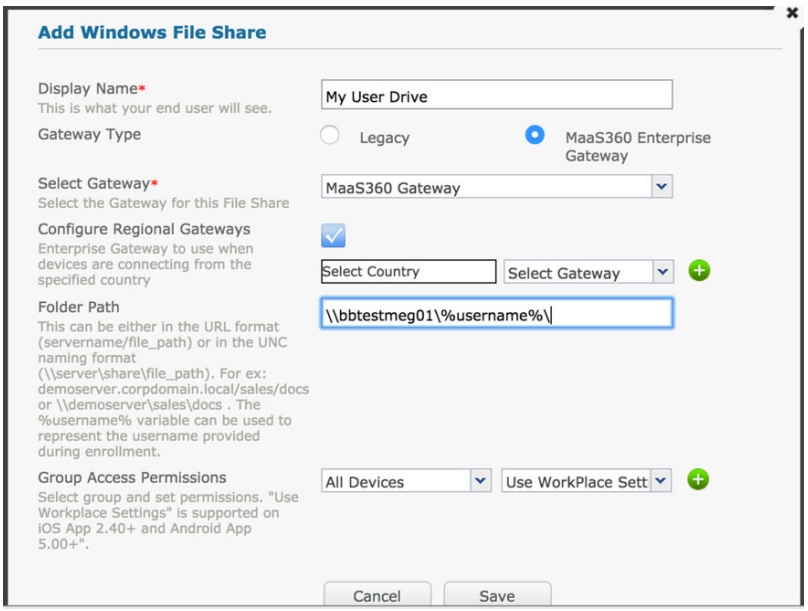
Windows File Share

About this task

The Secure Docs 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**.



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. If there are no regional gateways configured, all devices associated with this distribution will communicate with this default gateway.
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 can 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. If the folder names are the same as IBM MobileFirst Protect usernames, **%username%** variables can be used to distribute user specific file shares.
Group Access Permissions	Allows you to distribute the file shares to the targeted device along with the permissions associated with the distribution.

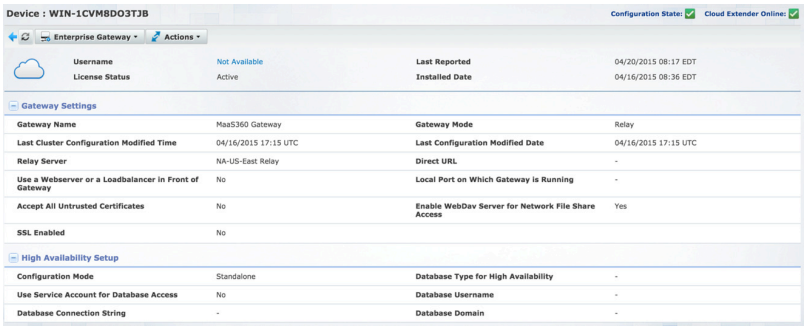
Chapter 11. Accessing Portal Management Workflows

About this task

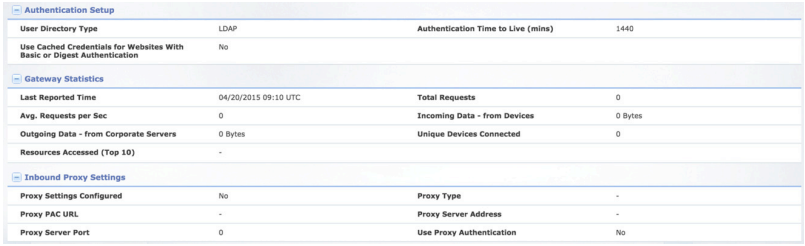
IBM MobileFirst Protect Administration Portal offers a Cloud Extender view that shows your gateway installation. This view also helps confirm if your gateway is active, and if it is online. (The **Cloud Extender Online** indicator appears in the top right corner.)

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).

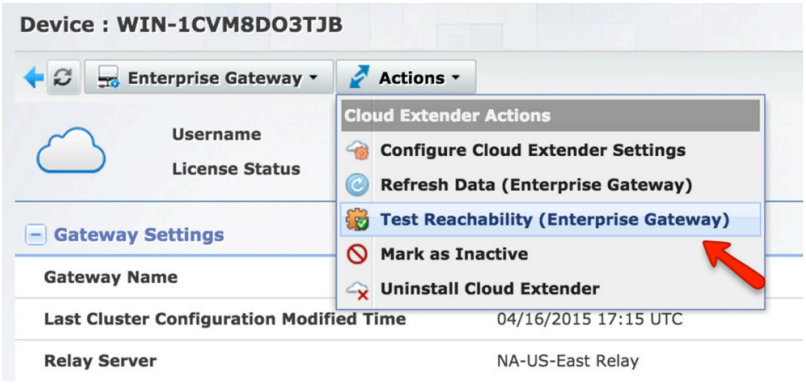


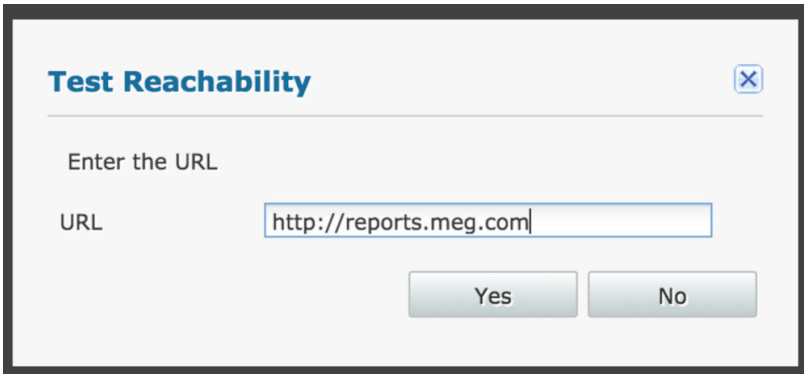
3. Scroll down to see all the settings.



   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.

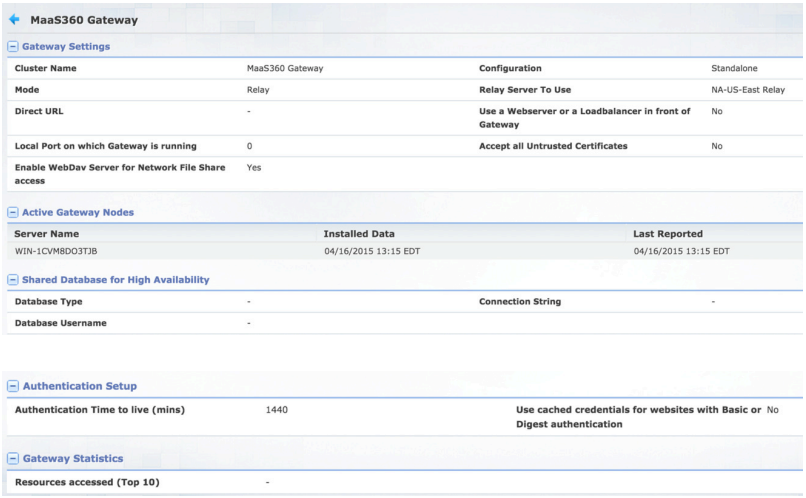
   Note: This action is sent directly from IBM MobileFirst Protect Administration Portal to the gateway.





6. IBM MobileFirst Protect 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.

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



Chapter 12. Mobile App Configuration

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

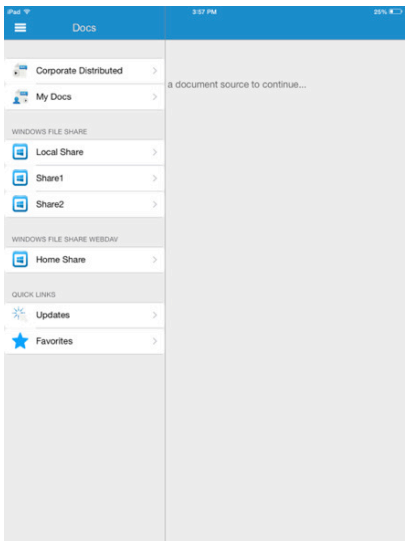
Enroll your iOS or Android device inIBM MobileFirst Protect, and assign to it the persona policy that has Secure Browser features enabled.

iOS Experience

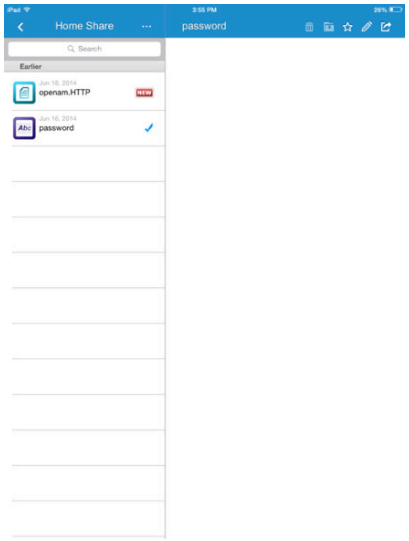
When you first launch of the browser, you are prompted for your credentials. Once authenticated, you can access your intranet sites.

You can get access to MEG reports.

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



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

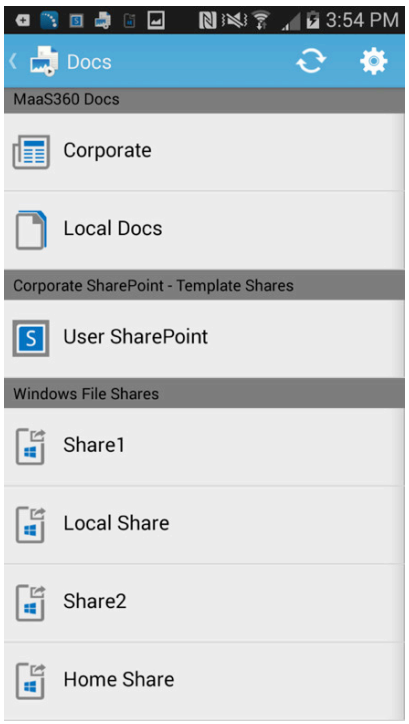


Android Experience

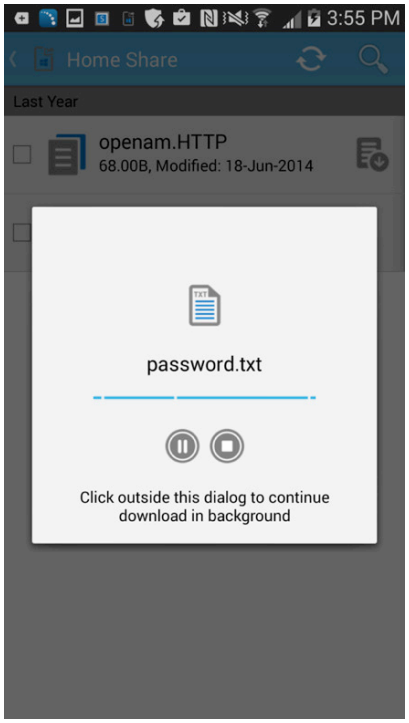
When you first launch of the browser, you are prompted for your credentials. Once authenticated, you can access your intranet sites.

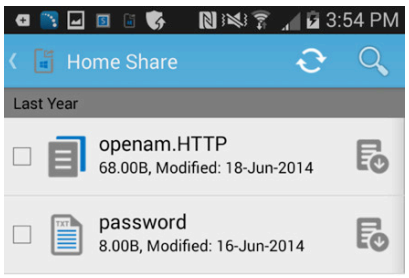
You can get access to MEG reports.

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



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



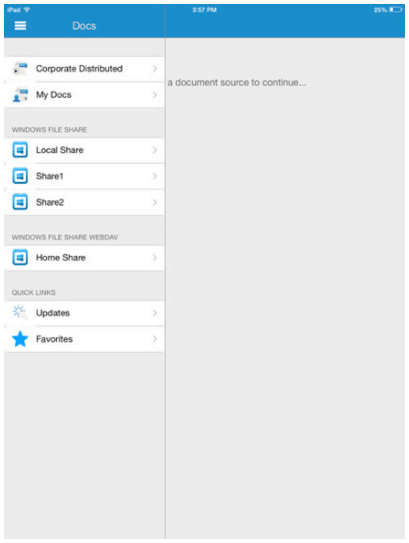


iOS Experience

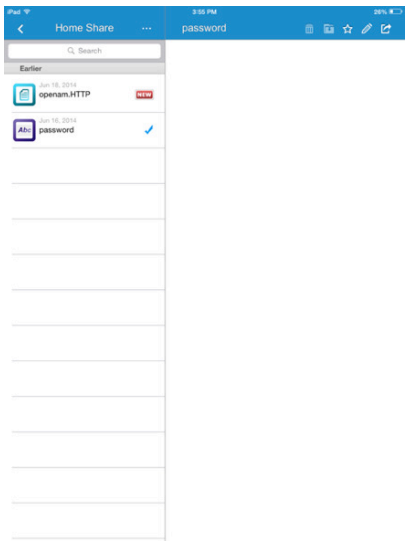
When you first launch of the browser, you are prompted for your credentials. Once authenticated, you can access your intranet sites.

You can get access to MEG reports.

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



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

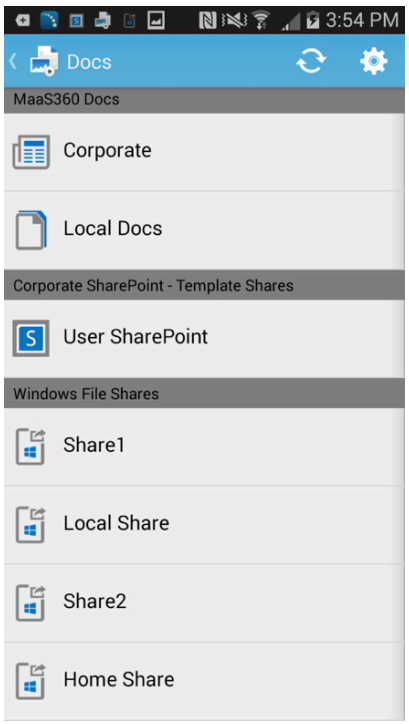


Android Experience

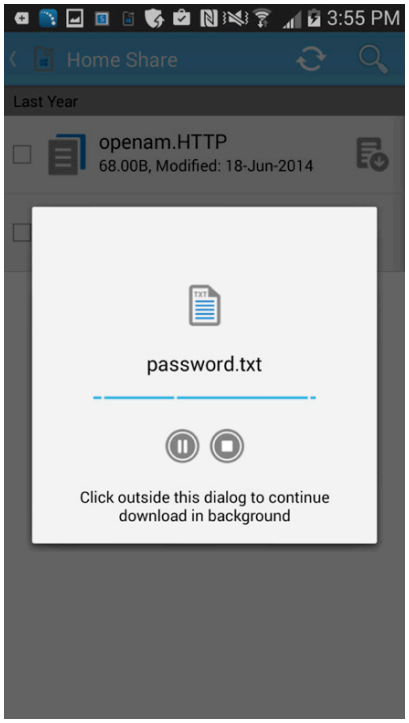
When you first launch of the browser, you are prompted for your credentials. Once authenticated, you can access your intranet sites.

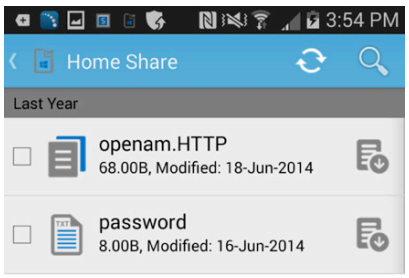
You can get access to MEG reports.

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



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




3:54 PM
Home Share
Last Year
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 and send it to your IBM MobileFirst Protect 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 and send it to IBM MobileFirst Protect 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. 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® for Android, 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: Setting Up Cross-Forest and Cross-Domain Authentication

About this task

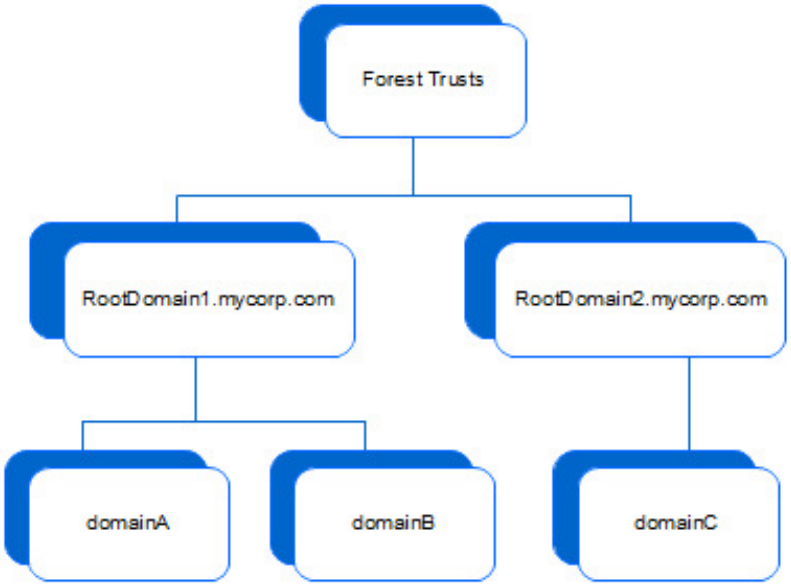
IBM MobileFirst Protect Mobile Enterprise Gateway requires users to authenticate against Corporate Directory Services before letting them access intranet resources. It integrates with both Active Directory and LDAP servers to achieve this form of authentication.

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 must 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.



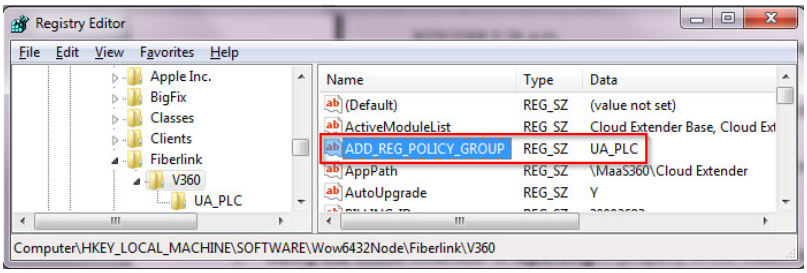
When you enable User Authentication for Active Directory, the default implementation only authenticates users within the context of the service account domain. To extend the authentication scope to all forests and domain, you will need to perform a few additional steps.

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
   ```



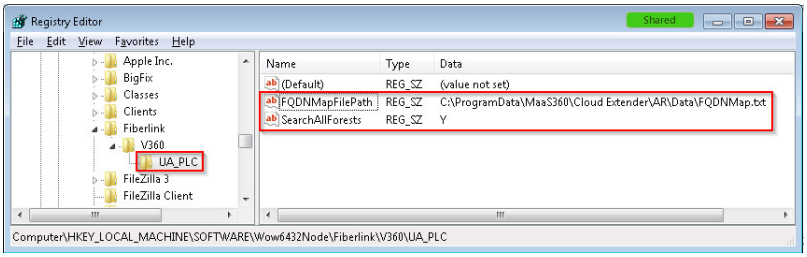
   Note: If this already exists, append UA_PLC to the list separated by a semi colon (;)

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
   ```



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 example, the file contents looks 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, implement the same steps on all gateways implementing User Authentication Service.

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360™, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM® Company.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Product Number: 5725-R11

Printed in USA