

IBM® Security Access Manager
for Versions 6.1.1, 7.0, 8.0 and 9.0

IBM MaaS360 Integration Guide



Note

Before using this information and the product it supports, read the information in 'Notices' on page 51

This edition applies to Version 3.1 release of the IBM Security Access Manager Integration with IBM MaaS360 and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2016.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

PREFACE	5
Access to publications and terminology	5
Publication Library	5
IBM Terminology website	6
Accessibility	6
Technical Training	6
Support information.....	6
Statement of Good Security Practices.....	6
Product name updates	7
INTRODUCING THE INTEGRATION	8
Introduction	8
Single Sign On to IBM Security Access Manager for Web.....	8
Email Access Gateway.....	9
Conditional Access using IBM Security Access Manager Advanced Access Control	9
Federated Single Sign On using IBM Security Access Manager Federation	10
Integration Architecture	11
Integration Product Version Information.....	13
Integration Product Contents	13
Before you start.....	13
IBM MAAS360 CONFIGURATION	14
Mobile Enterprise Gateway	14
Cloud Extender Configuration Tool.....	14
Secure Browser	19
Enable Secure Browser	19
Secure Email.....	20
Enable Secure Mail and Email Access Gateway	20
Mobile Application Management	21
Enable Mobile Application Management	21
MaaS360 SDK App Code Updates	21
Web Services	22
Enable Web Services.....	22
Create Administrator account for Web Services	22
Workplace Persona Policy	23
DNS and Intranet Host access	26

IBM SECURITY ACCESS MANAGER CONFIGURATION	27
Web Reverse Proxy Configuration	27
Authentication Mechanism	27
Authentication Challenge Type	28
Junction Management	30
WebSEAL Configuration	30
Authentication Mechanism	30
Authentication Challenge Type	30
Junction Creation	32
Advanced Access Control Appliance Configuration	32
Custom Fiberlink MaaS360 Attributes	34
Mobile Authorization Decision Point Configuration	35
Importing the MaaS360 SSL Certificate	35
Creating the Fiberlink MaaS360 Policy Information Point	36
Populating Device ID from the MaaS360 component	37
Populating Device ID using the Attribute Collection Service	37
RUNNING THE SAMPLE APPLICATION	40
Before you start	40
Security Access Manager for Web configuration	40
User Account Creation	40
Junction Management	41
MaaS360 Configuration	41
Security Access Manager Advanced Access Control Configuration	42
Create an Access Control Policy	42
Attach and publish the Access Control Policy	43
Validating Single Sign On	44
Validating Conditional Access	45
Simulating Conditional Access	45
TROUBLESHOOTING	47
Collecting Support Data	47
Security Access Manager for Web	47
Security Access Manager Advanced Access Control	48
MaaS360 Web Service API validation	49
NOTICES	51
TRADEMARKS	53

Preface

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM® Security® Access Manager Base Installation Guide*
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Security Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the pdadmin command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Security Access Manager WebSEAL Administrator's Guide*
Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.
- *IBM Security Access Manager WebSEAL Developer's Reference*
Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Reverse Proxy Appliance Information

- *IBM Security Access Manager Web Reverse Proxy Administration Guide*
Provides information about configuring and maintaining a Security Access Manager environment.
- *IBM Security Web Reverse Proxy Configuration Guide*
Provides configuration procedures and technical reference information for the Web Reverse Proxy.

- *IBM Security Web Reverse Proxy Stanza Reference*

Provides a complete stanza reference for the Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager Advanced Access Control Administration Guide*

Describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

- *IBM Security Access Manager Advanced Access Control Configuration Guide*

Explains how to complete the initial configuration of IBM Security Access Manager Advanced Access Control.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at

<http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical Training

For technical training information, see the following IBM Education website at

<http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at

<http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Additionally, this publication was first established for Fiberlink MaaS360. Fiberlink MaaS360 has since been superseded by IBM MobileFirst Protect and then IBM MaaS360.

Wherever in this guide, any figures and graphics that contain or refer to Fiberlink MaaS360, the use of IBM MaaS360 is implied. There are no functionality discrepancies between Fiberlink MaaS360, IBM MobileFirst Protect and IBM MaaS360.

Introducing the Integration

Introduction

The IBM Security Access Manager for IBM MaaS360 (formerly IBM Fiberlink MaaS360) integration enables Single Sign On, Conditional Access and Federation from a mobile device to on premise and Cloud protected resources using the MaaS360 Secure Browser, MaaS360 Software Development Kit (SDK) and limited support for native browsers running on MaaS360 registered devices.

Connections from the mobile device through the Mobile Enterprise Gateway (MEG) are authenticated to Security Access Manager for Web. Once authenticated to Security Access Manager for Web, downstream SSO to protected resources is achieved using a broad range of authentication mechanisms including existing Single Sign On patterns and integration adapters such as Trust Association Interceptor (TAI), Lightweight Third-Party Authentication (LTPA), Basic Authentication (GSO, -B, etc.), HTTP header (Kerberos, iv-creds, etc.) and Federation (using Tivoli Federated Identity Manager).

When configured as a secure email gateway, authentication and authorization of the device and user can be performed by Security Access Manager for Web before any requests are proxied to the Exchange Server; the MEG is not required to support this scenario.

When configured with Security Access Manager Advanced Access Control, fine grained authorization using Context Based Access (CBA) and Risk Based Access (RBA) provides policy driven access control and multi factor authentication. A range of attributes may be using in the access policy, including MaaS360 device data by enabling the Fiberlink MaaS360 Policy Information Point (PIP).

When configured with IBM Security Access Manager Federation, Federated Single Sign On (FSSO) to a range of on premise and Cloud services is enabled using standards based federation protocols for authentication.

Single Sign On to IBM Security Access Manager for Web

User authentication data from the Mobile Enterprise Gateway (MEG) is passed to Security Access Manager for Web to create an authenticated user session. This is achieved by configuring the MEG and ISAM against the same or replica LDAP or Active Directory.

A dedicated Security Access Manager for Web instance for inbound MaaS360 MEG connections is recommended but not mandatory.

Single Sign On to IBM Security Access Manager for Web using the MEG

The IBM Security Access Manager for Web instance can be Internet or Intranet facing. This allows access for existing direct (Internet based) connections as well as MaaS360 (Intranet based) connections. The instance must be configured to allow an authentication mechanism that the MEG can provide based on a HTTP status code 401 challenge/response.

Refer to *Table 1: Recommended IBM Security Access Manager for Web Authentication Mechanism* to determine which Security Access Manager for Web authentication mechanism is used based on the user directory configured in the MEG for the User Visibility and User Authentication services.

User Directory	Authentication Mechanism
Active Directory	SPNEGO (Kerberos)
LDAP	Basic Authentication

Table 1: Recommended IBM Security Access Manager for Web Authentication Mechanisms

Following successful authentication from the MEG to Security Access Manager for Web, features such as downstream SSO, CBA, RBA and Federation can be configured.

Single Sign On to IBM Security Access Manager for Web for SDK apps without the MEG

MaaS360 SDK based apps can authenticate to directly to Security Access Manager without establishing a connection the MEG. Using this pattern the application developer implements the required HTTP flows to enable Strong Authentication with Security Access Manager, such as OAuth 2.0.

Using this pattern, a Native or Hybrid Mobile application is authored using the MaaS360 SDK and includes the user interface prompts required to collect a user credential such as an OAuth 2.0 Authorization Code or Resource Owner Password Credentials flow; or the OAuth 2.0 registration requests are connected via the MEG enabling the use of the Gateway Credentials to SSO to Security Access Manager for Web.

Upon successful authentication to Security Access Manager the app continues to use the access token on requests directly to Security Access Manager for Web. The refresh token is encrypted and stored on the device using the MaaS360 APIs. Retrieval of the refresh token requires the `IMaaS360SDKPolicyAutoEnforceInfo.shouldAutoEnforceSSO()` API call to require the user to enter their MaaS360 device PIN to “unlock” the storage and therefor the refresh token. The MaaS360 device PIN replaces the PIN which would normally be assigned when configuring the Security Access Manager Advanced Access Control API Protection Definition.

An alternate pattern is to store the Security Access Manager OAuth 2.0 refresh token in a custom device attribute in the MaaS360 inventory and require the app to retrieve this value by reporting back to MaaS360 and retrieving from the device data. Whilst this can be seen as a more secure solution to locally storing the refresh token, it introduces token management complexity and additional Security Access Manager Mobile extension code to perform the updates in MaaS360.

Email Access Gateway

Security Access Manager can be used to provide secure and conditional access to a hosted Microsoft Exchange Server using the MaaS360 Secure Mail client.

When only the Web Reverse Proxy is used, static authorization checks including device enrolment and managed status plus restricting to only the Secure Mail client can be achieved. Supported authentication mechanisms include Basic Authentication and Certificate authentication.

Real-time Conditional Access enforcement can also be achieved by configuring the IBM Security Access Manager Advanced Access Control feature. When the Access Control Policy is applied to the ActiveSync URI paths, MaaS360 device attributes can be used to control email access on the device.

Refer to the IBM MaaS360 Email Access Gateway documentation for supported scenarios and configuration.

Conditional Access using IBM Security Access Manager Advanced Access Control

When IBM Security Access Manager Advanced Access Control is enabled, fine grained authorization using Context Based Access (CBA) and Risk Based Access (RBA) provides policy driven access control and multi factor authentication using a range of attributes.

The Security Access Manager Policy Information Point (PIP) for Fiberlink MaaS360 enables the use of device attributes from registered devices in MaaS360 in access policy and risk profiles configured

in Security Access Manager Advanced Access Control and enforced by Security Access Manager for Web.

MaaS360 device attributes available for use in access policy include device ownership, corporate policy and security compliance state and when the device last reported.

The PIP calls the MaaS360 Web Services to retrieve the device attributes from the device inventory using either the MaaS360 Device ID directly or Security Access Manager Advanced Access Control Attribute Collection Service to match a corresponding device.

MaaS360 Device ID

When a MaaS360 based app provides the Device ID to Security Access Manager Advanced Access Control, the PIP can extract the value and perform a direct lookup into the MaaS360 device inventory.

The MaaS360 Secure Browser and Secure Mail can be configured to insert the Device ID as a custom HTTP request header.

MaaS360 SDK based apps can be coded to retrieve the device ID using the MaaS360 APIs and insert a HTTP request header containing this value. Security Access Manager for Web extracts the device ID from the HTTP request header and assigns the value of the MaaS360 Device ID attribute

IBM Security Access Manager Advanced Access Control Attribute Collection Service

When the MaaS360 Device ID is unable to be inserted into the HTTP request, if the application is able to execute client side JavaScript, the Security Access Manager Advanced Access Control Attribute Collection Service can be used.

By including the *info.js* JavaScript typically into the Security Access Manager for Web login page reference and configuring a Risk Profile with those attributes, the device is fingerprinted by extracting a number of device characteristics such as screen resolution, colour depth and platform.

The PIP retrieves a list of all devices in the MaaS360 inventory for the current authenticated user and performs a 'best match' comparison for the retrieved devices against the fingerprint data that is has collected. If a match is found, the MaaS360 Device ID is cached for the remainder of that session and the corresponding MaaS360 device data can be used in access control policy.

Federated Single Sign On using IBM Security Access Manager Federation

When IBM Security Access Manager Federation is configured with Security Access Manager for Web, Federated Single Sign On (FSSO) to on premise and Cloud based Software as a Service (SaaS) providers is enabled.

Both Service Provider (SP) and Identity Provider (IdP) initiated FSSO is supported. The Point of Contact for Security Access Manager Federation Module should be the same Security Access Manager for Web that is configured for SSO when using the MEG. When the MaaS360 Secure Browser is redirected to the IdP login page, protected by Security Access Manager for Web, SSO is achieved from the device to the Federation partner without any additional authentication challenges.

No additional configuration is required in MaaS360 to use FSSO following successful SSO from the MEG to Security Access Manager for Web.

Refer to [Connectors available for SAML 2.0](#) for a list of supported Quick Connect Templates in addition to generic SAML 2.0 and Open ID Connect (OIDC) support.

Integration Architecture

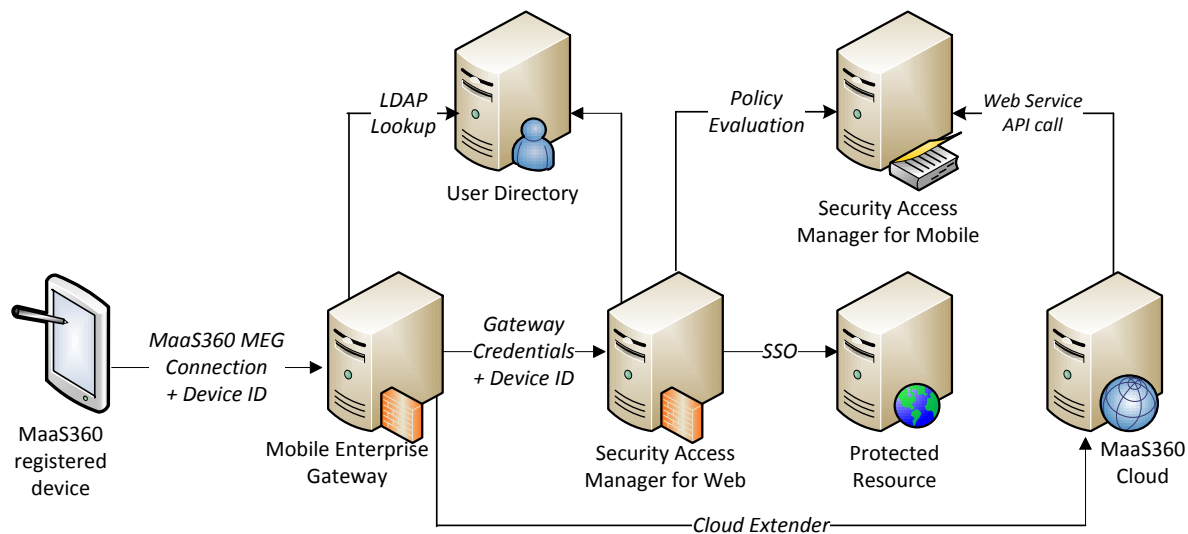


Figure 1: IBM MaaS360 Integration Architecture

Figure 1 shows the integration architecture with the following process for Single Sign On with the MEG and resource protection where Context Based Access policy is attached:

1. The user requests content from a protected resource using the Secure Browser or MaaS360 SDK based app for a resource protected by IBM Security Access Manager. The Device ID is inserted as an additional HTTP Request header or as part of the User Agent.
2. The Mobile Enterprise Gateway collects the Gateway Credentials from the user and optionally caches them.
3. The MEG forwards the request to Security Access Manager for Web passing the Device ID.
4. Security Access Manager for Web detects the request from the MEG and sends a 401 WWW-Authenticate response (Basic or Negotiate) to the MEG.
5. The MEG reissues the request passing the Gateway Credentials for the user and the Device ID.
6. Security Access Manager for Web validates the user credentials and establishes a user session.
7. Security Access Manager for Web calls Security Access Manager Advanced Access Control to authorize the request against the Access Control policy and passes all available context including the Device ID.
8. Security Access Manager Advanced Access Control identifies the device using either:
 - a. Device ID (x-fl-device-id) in an HTTP request header; or
 - b. IBM Security Access Manager attribute collection service
9. Security Access Manager Advanced Access Control invokes the Fiberlink MaaS360 PIP which calls the MaaS360 Web Service API. The API called is dependent on the attribute evaluated in the policy.
10. The MaaS360 Web Service API returns the registered device data for the authenticated user.
11. Security Access Manager Advanced Access Control parses the response from the MaaS360 Web Service API and assigns attribute values from the available device data.

12. Security Access Manager Advanced Access Control evaluates the Access Control Policy and provides the decision to Security Access Manager for Web.
13. After successful authentication, the policy attached to the resource is evaluated.
14. If the user is *permitted* to access the resource, Security Access Manager for Web forwards the request and optional SSO's to the protected resource.
15. The protected resource processes the request and returns the content to Security Access Manager for Web.
16. Security Access Manager for Web returns the content to the MEG.
17. The MEG returns the requested content to the user.

Integration Product Version Information

See the Release Notes for supported versions.

Integration Product Contents

The integration solution is packaged as a compressed file. The package contains the following files:

File Name	Description
isam_maas360_integration_guide.pdf	This integration guide.
X.X-ISAM-MAAS360.README	Readme file containing supported versions, enhancements and update history.
MaaS360MEGUserAgentRequestTransformation.xslt	Request HTTP Transformation Rule to rewrite the User Agent from the Secure Browser removing the meg20 identifier and Device ID and adds Device ID as a new HTTP request header.

Table 2: Integration Package contents

Before you start

This integration guide details the steps that are required to achieve this integration at a high level in your environment. To run the sample applications with your own infrastructure, edit the sample application code.

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

- IBM Security Access Manager
 - IBM Security Access Manager for Web Reverse Proxy or WebSEAL
 - IBM Security Access Manager Advanced Access Control
 - IBM Security Access Manager Federation
- IBM MaaS360
 - Mobile Device Management
 - Mobile Application Management
 - Mobile Content Management
 - Secure Browser
 - Secure Email
 - Email Access Gateway
 - Mobile Enterprise Gateway
 - Web Services
- User Repository Synchronization
 - Use the Cloud Extender to integrate with your Corporate User Directory ensuring the Gateway Credential User ID exactly matches the Security Access Manager User ID.

IBM MaaS360 Configuration

End to end integration between MaaS360 and Security Access Manager requires configuration of MaaS360 components in the Mobile Enterprise Gateway, Administration Portal and minor application code updates for MaaS360 SDK based apps.

The Mobile Enterprise Gateway is used to provide the user Gateway Credentials to SSO to Security Access Manager for Web and is configured against the same Corporate Directory as Security Access Manager.

Workplace Persona Policy is used to control the Device ID data that is provided to Security Access Manager and to control which requests from the Secure Browser or SDK are accessed through Security Access Manager.

Ensure you are licenced for the MaaS360 components listed in *Before you start* on page 13.

Mobile Enterprise Gateway

Install and configure a Mobile Enterprise Gateway instance that can access the Security Access Manager for Web instance.

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Services & Settings** sub-menu.
4. Expand the **Enterprise Gateway** service.
5. Download the Cloud Extender installer.
6. Retrieve the license key for Cloud Extender for MDM (Email Notification module, Mobile Enterprise Gateway, User Authentication).
7. Install the Cloud Extender.

less...'. Under the heading 'Available relays to use:', it lists 'APAC-SGP Relay', 'EU-UK Relay', and 'NA-US-East Relay'. At the bottom, there are three numbered steps: 1. Download and install Cloud Extender. Click here to get your license key. 2. Define the list of Allowed Intranet Sites in Workplace Persona [icon] Policies. Assign Gateway(s) to use also via policies. 3. Setup Windows File Shares and Internal SharePoint sites for distribution to devices." data-bbox="116 526 872 718"/>

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

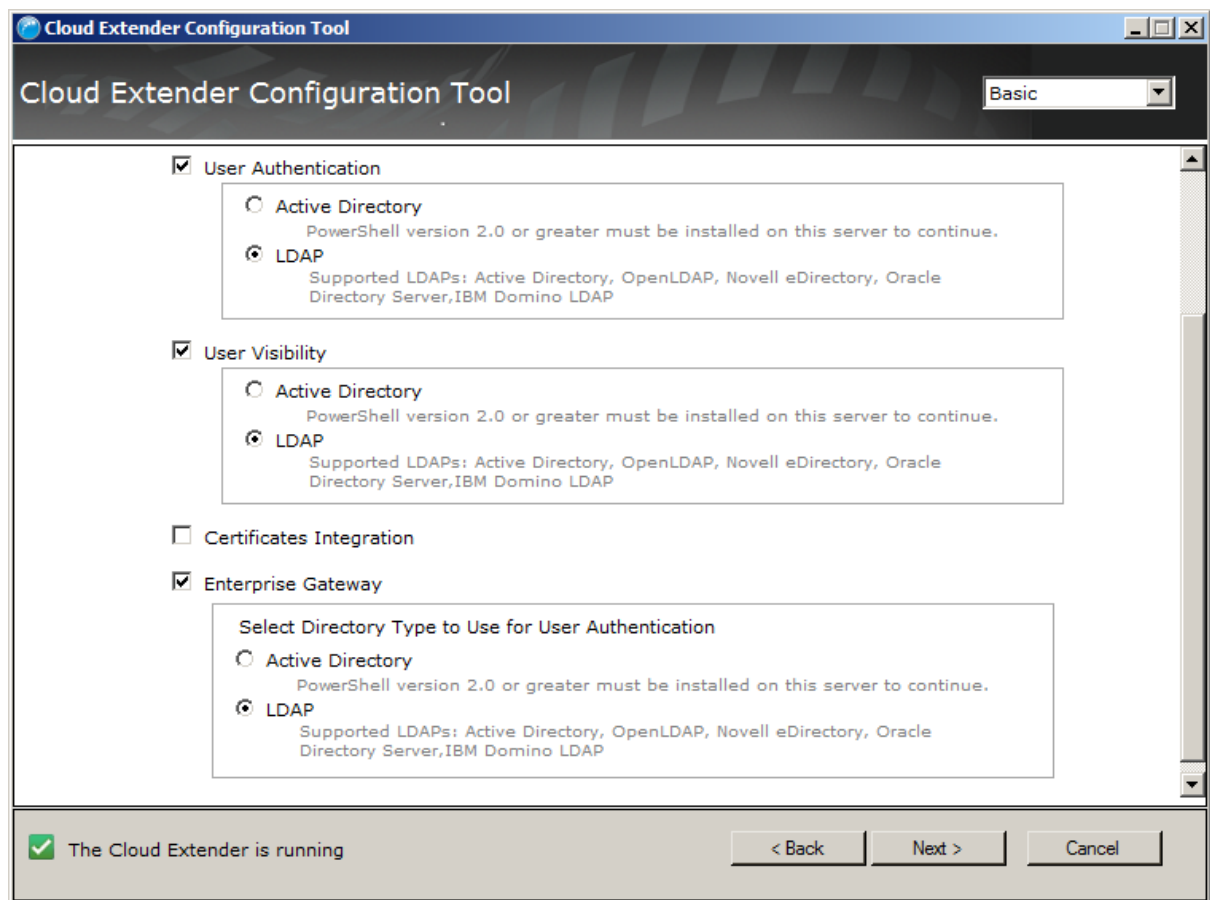
1. [Download](#) and install Cloud Extender. [Click here](#) to get your license key.
2. Define the list of Allowed Intranet Sites in [Workplace Persona](#) [icon] Policies. Assign Gateway(s) to use also via policies.
3. [Setup](#) Windows File Shares and Internal SharePoint sites for distribution to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

Cloud Extender Configuration Tool

Launch the Cloud Extender Configuration Tool to begin the integration with Security Access Manager. Once completed, the Security Access Manager user accounts from the Corporate Directory will be imported into the MaaS360 User Directory allowing devices to be provisioned to those accounts.

After installing the Cloud Extender, you may need to wait up to 10 minutes before running the configuration to allow the entitlements to be retrieved from the MaaS360 Administration portal and for the Enterprise Gateway component is downloaded.

1. Launch the Cloud Extender Configuration Tool
2. Verify the Internet connectivity and click **Next**.
3. Select **User Authentication**
 - a. Select the directory where you users are provisioned. Ensure Security Access Manager is configured against the same directory or replica. For example: **LDAP**
4. Select **User Visibility**
 - a. Select the directory where you users are provisioned. Ensure Security Access Manager is configured against the same directory or replica. For example: **LDAP**
5. Select **Enterprise Gateway**
 - a. Select the directory where you users are provisioned. Ensure Security Access Manager is configured against the same directory or replica. For example: **LDAP**
6. Click **Next**.



7. Configure the Directory Integration.

For example, to use the embedded directory server of Security Access Manager:

 - a. LDAP Server: **OpenLDAP**
 - b. Tick **Use Secure LDAP**
 - c. Servers: **<isam_management_host:636>**
 - d. Authentication Type: **Basic**
 - e. Bind Username (Distinguished Name): **cn=root,secAuthority=Default**
 - f. Bind Password: **<ldap_root_password>**
 - g. LDAP Search base: **dc=iswga**
 - h. User Search Attribute: **uid**

Note: When creating user accounts, ensure the User DN is created with the **uid** prefix.

For example `uid=appuser1,dc=iswga`. If existing user accounts use an alternative prefix, such as **cn**, ensure the User Search Attribute field is updated with the correct prefix for your environment.

8. Click **Next**.

The screenshot shows the 'Cloud Extender Configuration Tool' window. The title bar says 'Cloud Extender Configuration Tool'. Below the title bar, there's a 'Basic' dropdown menu. The main area is divided into two panes. The left pane, titled 'Configure', has four options: 'LDAP integration' (selected with a blue square), 'Enterprise Gateway' (unselected), 'Cloud Extender Status' (unselected), and 'Cloud Extender Auto Updates' (unselected). The right pane, titled 'Configure LDAP integration:', contains several fields: 'LDAP Server' (OpenLDAP), 'Use Secure LDAP' (checked), 'Servers' (isam.ibm.com:636), 'Authentication Type' (Basic), 'Bind Username (Distinguished Name)' (cn=root,secAuthority=Default), 'Bind Password' (masked with asterisks), and 'LDAP Search base' (dc=iswga). There are plus and minus buttons next to the Servers and LDAP Search base fields. A note at the bottom of the right pane says: 'Note: Across all specified LDAP Search bases(s), the User IDs should be'. At the bottom of the window, there's a status bar with a green checkmark and the text 'The Cloud Extender is running', and three buttons: '< Back', 'Next >', and 'Cancel'.

9. Click **OK** to the LDAP configuration success message.
10. Optionally, Test Authentication to the LDAP server using a valid User ID and password. For example:
 - a. Username: **appuser1**
 - b. Password: **<password>**
 - c. Click **Test Authentication**
11. Click **Next**.

12. Select the Configuration Mode for the Enterprise Gateway.

For example, for a **Standalone** instance:

- a. Gateway Name: **<gateway_name>**. For example: gw-isam
- b. Gateway Mode: **Relay** or **Direct**. For example: Relay
Use Relay Mode if your MEG is not Internet facing or you do not have the required Certificates and Trust Chain to allow Direct, or you will use the MaaS360 Regional Gateways.
- c. Select Relay Server: **<closest_regional_relay>**
- d. Accept all Untrusted Certificates: **Check**.
If your enterprise certificates are managed and distributed to all devices this can be left unchecked.
- e. Authentication Details:
 - i. Users required to authenticate every **30** days (default)
 - ii. Re-use user's credentials: **Check**
Important: This setting must be enabled to configure SSO from the MEG to Security Access Manager for Web.
- f. WebDAV Server Setup: optional

13. Click **Next**.

The screenshot shows the 'Cloud Extender Configuration Tool' window. The title bar says 'Cloud Extender Configuration Tool'. The main window has a dark header with the same title and a 'Basic' dropdown menu. On the left, there is a 'Configure' sidebar with four items: 'LDAP integration' (checked with a green icon), 'Enterprise Gateway' (highlighted with an orange icon), 'Cloud Extender Status' (unchecked), and 'Cloud Extender Auto Updates' (unchecked). The main area is titled 'Enterprise Gateway' and contains several configuration fields: 'Gateway Name' (text box with 'gw-isam'), 'Gateway Mode' (radio buttons for 'Relay' and 'Direct', with 'Relay' selected), 'Select Relay Server' (dropdown menu with 'APAC-SGP Relay' selected), and a checked checkbox for 'Accept all Untrusted Certificates'. Below this, there is a section for 'Authentication Details' with a text box for 'Users required to authenticate every' (set to '30') and '(days)', with a note 'Supported values: 1 to 90'. There is also a checked checkbox for 'Re-use user's credentials for internal resources that require Basic or Digest authentication' with a note: 'If such internal resources do not use user's directory credentials, selecting this option will'. At the bottom of the window, there is a status bar with a green checkmark and the text 'The Cloud Extender is running', and three buttons: '< Back', 'Next >', and 'Cancel'.

Cloud Extender Configuration Tool

Basic

Configure

- ☒ LDAP integration
- ☒ Enterprise Gateway
- ☐ Cloud Extender Status
- ☐ Cloud Extender Auto Updates

Enterprise Gateway

Gateway Name: gw-isam

Gateway Mode: ☒ Relay ☐ Direct

Select Relay Server: APAC-SGP Relay

☒ Accept all Untrusted Certificates

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

Authentication Details

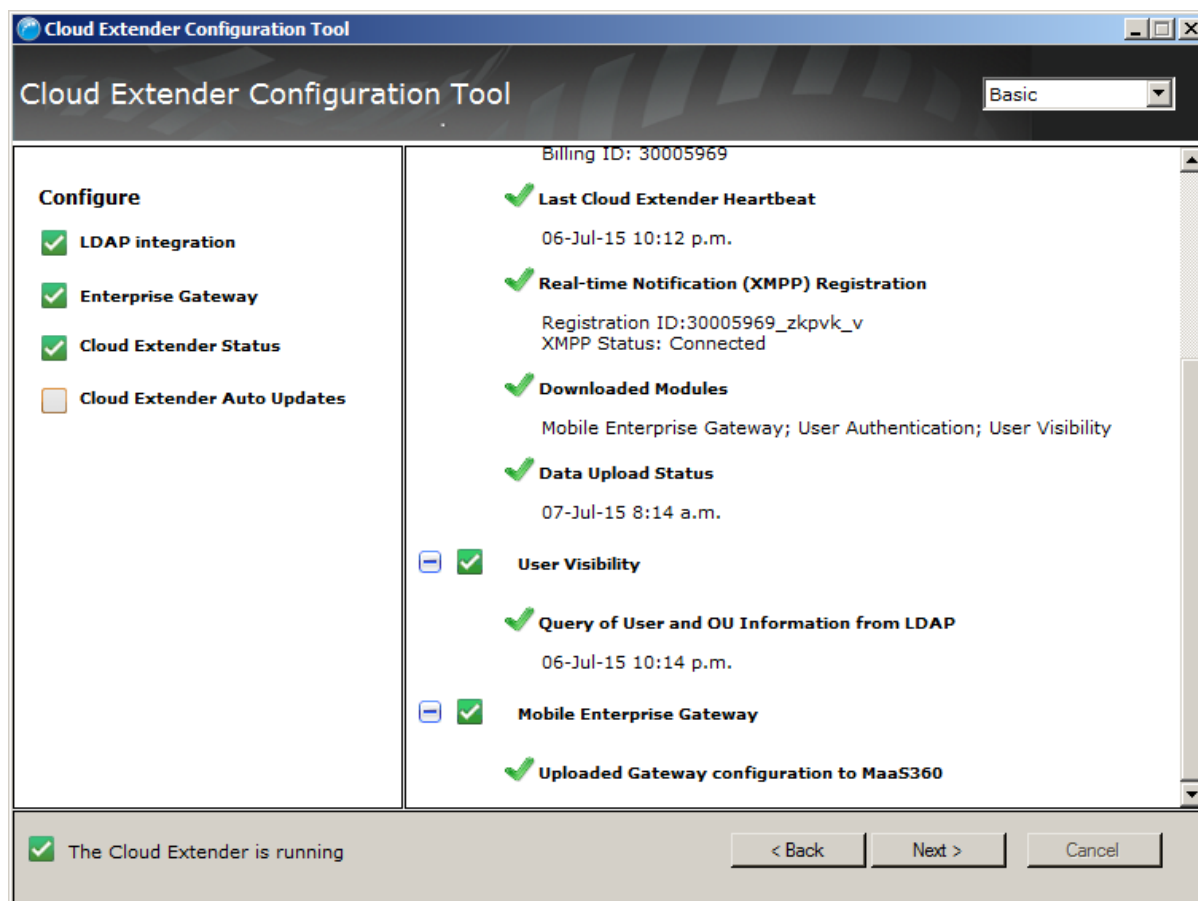
Users required to authenticate every: 30 (days)
Supported values: 1 to 90

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

☒ The Cloud Extender is running

< Back Next > Cancel

14. In the Cloud Extender Status, ensure no errors occurred.
15. Click **Next**.



16. Optionally, **Enable Automatic Software Updates**.
17. Click **Finish**.

Secure Browser

To enable SSO using Security Access Manager for Web and Conditional Access using Security Access Manager Advanced Access Control, the Secure Browser must be enabled.

Enable Secure Browser

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Services & Settings** sub-menu.
4. Enable the **Secure Browser** service.

**Secure Browser**

The Secure Browser is a full featured web browser to enable secure access to corporate intranet sites and enforce compliance of content policies. Define URL filtering and security policies, ensuring that users only access approved web content and only approved browsing controls are enabled. [less...](#)

-  URL Filtering
-  Intranet Access

Instructions

- Configure WorkPlace Persona  Policies for provisioning Secure Browser.
- Assign this policy to devices, users or groups to start enabling Secure Browser.
- [Download](#) and install the Mobile Enterprise Gateway for secure intranet access via browser.
- Ensure Cloud Extender has been installed and Enterprise Gateway has been configured.

Secure Email

To enable Security Access Manager as an Email Access Gateway the Secure Mail and Email Access Gateway must be enabled.

Refer to the MaaS360 Email Access Gateway documentation for supported scenarios and configuration detail.

Enable Secure Mail and Email Access Gateway

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Services & Settings** sub-menu.
4. Enable the **Secure Mail** service.
5. Enable the **Email Access Gateway** service.

**Secure Mail**

Secure Mail provides a separate and secure office productivity application for users to access and manage email, calendar, and contacts. Provides the ability to control emails and attachments to prevent data leakage by restricting the ability to forward or move content to other applications, enforcing authentication, restricting cut/copy/paste, and locking down email attachments for view only. [more...](#)

**Email Access Gateway**

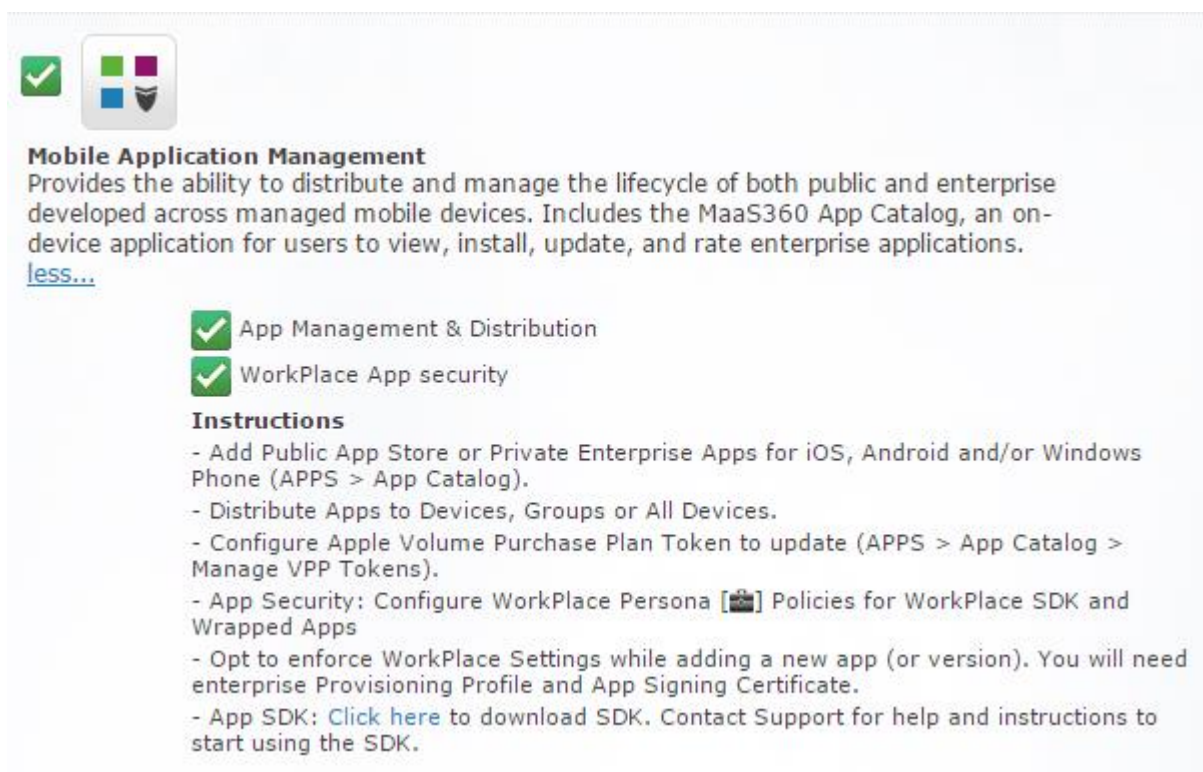
Improve security for email by setting up a reverse proxy to eliminate the need for corporate email servers to be exposed directly to the internet. Unmanaged devices and unwanted third party client access can be blocked by configuring rules on the Email Access Gateway. [more...](#)

Mobile Application Management

To enable SSO using Security Access Manager for Web and Conditional Access using Security Access Manager Advanced Access Control, for MaaS360 SDK based apps Mobile Application Management must be enabled.

Enable Mobile Application Management

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Services & Settings** sub-menu.
4. Enable the **Mobile Application Management** service.
5. Download the **App SDK** to start developing integrated applications.



Mobile Application Management
Provides the ability to distribute and manage the lifecycle of both public and enterprise developed across managed mobile devices. Includes the MaaS360 App Catalog, an on-device application for users to view, install, update, and rate enterprise applications.
[less...](#)

- ✓ App Management & Distribution
- ✓ WorkPlace App security

Instructions

- Add Public App Store or Private Enterprise Apps for iOS, Android and/or Windows Phone (APPS > App Catalog).
- Distribute Apps to Devices, Groups or All Devices.
- Configure Apple Volume Purchase Plan Token to update (APPS > App Catalog > Manage VPP Tokens).
- App Security: Configure WorkPlace Persona [👤] Policies for WorkPlace SDK and Wrapped Apps
- Opt to enforce WorkPlace Settings while adding a new app (or version). You will need enterprise Provisioning Profile and App Signing Certificate.
- App SDK: [Click here](#) to download SDK. Contact Support for help and instructions to start using the SDK.

MaaS360 SDK App Code Updates

Fiberlink MaaS360 SDK apps do not natively insert a Device ID to allow the Security Access Manager Policy Information Point (PIP) to lookup the device in the MaaS360 inventory.

Unlike the Secure Browser and Secure Mail, Workplace Person Policy cannot be used to insert it.

To use the PIP, MaaS360 SDK based apps must be updated to retrieve the Device ID and pass this to Security Access Manager for Web on all HTTP requests.

Using the MaaS360 SDK to retrieve and insert the Device ID

Update the MaaS360 SDK app to retrieve the device ID and populate an HTTP request header with the value before the request is sent.

For example:

```
public String addDeviceIdHeader(HttpServletRequest req) {
    MaaS360DeviceIdentityAttributes attrs =
    MaaS360SDKContextWrapper.getDeviceIdentityAttributes();
    String flDeviceID = attrs.getValue("maas360DeviceID");
    ...
    req.addHeader("x-fl-device-id", flDeviceID);
    ...
}
```

Note: The example code snippet provided should be modified for the language that the MaaS360 SDK app was written and inserted into the code stream where any HTTP requests are made to Security Access Manager for Web protected resources.

Ensure the app is written to handle responses from access policy evaluation which may alter the flow of execution, for example One Time Password (OTP) entry.

Web Services

To use the Security Access Manager Advanced Access Control Policy Information Point, Web Services must be enabled. This grants access to MaaS360 Web Service API's used to retrieve device attribute data.

Enable Web Services

1. Log in to the MaaS360 Administration portal. For example <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Services & Settings** sub-menu.
4. Enable the **Enterprise Gateway** service.



Create Administrator account for Web Services

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Setup** from the menu.
3. Select **Services** from the **Portal Administration** sub-menu.
4. Select **Administrators** service.
5. Click **Add Administrator**.
6. In the **Administrator Details** page, create a new account to use with the Security Access Manager Advanced Access Control PIP. For example:
 - a. Corporate Email Address: **user@domain.com**
 - b. Username: **<account_id>_webservice**
7. Click **Next**.
8. In the **Assign Roles** page, select the **Read-Only** role.
9. Click **Next**.
10. In the **Review Details** page, click **Save**.
11. In the **Security Check** window, enter your account password and click **Continue**.

12. Log out of the MaaS360 Administration portal.
13. Log in to the MaaS360 Administration portal using the new Administrator account.
14. Follow the prompts to change the password.
15. Follow the prompts to update the personal details.

Workplace Persona Policy

Update the Workplace Persona to enable features required to provide SSO between apps on the device, an indicator that SSO from the MEG is configured, the Device ID and which HTTP requests should be connected using the MEG to Security Access Manager.

1. Log in to the MaaS360 Administration portal. For example, <https://m3.maas360.com>
2. Hover over **Security** from the menu.
3. Select **Policies**.
4. Click **View** on the User Persona Policy. For example, `Default User Persona Policy`.
5. Click **Edit**.
6. Expand the **Workplace** menu.
7. Select the **Services** sub-menu.
 - a. Secure Mail: **Checked** (Optional for Secure Email)
 - b. Browser: **Checked**
 - c. Workplace App Container: **Checked** (Optional for SDK apps)

Secure Mail

Configure PIM app to provide corporate email, calendar and contacts.



Browser

Enables a fully-functional web browser to enforce compliance. Use the browser section to configure the service.



8. Select the **MaaS360 Gateway Settings** sub-menu.
 - a. Allow caching of Corporate Credentials in the App: **Checked**

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.



9. Expand the **Browser** menu.
10. Select the **Defaults** sub-menu.
 - a. Override User Agent: **Checked**
 - b. Android User Agent String: **meg20-%standard%**
 - c. iOS User Agent String: **meg20-%standard%**

Android User Agent String

Retain this blank to use the default User Agent of the browser. Supported placeholders - %deviceid%, %user%, %domain%, %email%, %upn%, %standard%

meg20-%standard%

Android Browser 1.40+

iOS User Agent String

Retain this blank to use the default User Agent of the browser. Supported placeholders - %deviceid%, %user%, %domain%, %email%, %upn%, %standard%

meg20-%standard%

iOS Browser 1.70

Note: The User Agent String meg20-%standard% indicates Security Access Manager that SSO from the MEG is configured (meg20). The original User Agent (%standard%) is inserted to ensure that integrations that require the User Agent, such as Trusteer Pinpoint Malware Detection or mobile browser optimisation continue to function.

- d. Custom headers for HTTP requests: **Checked**
- e. Encrypt Header values: **Unchecked**
- f. HTTP header field name: **x-fl-device-id**
- g. Value: **%deviceid%**
- h. Include this header for Corporate Intranet websites only: **Checked**

Note: If the Secure Browser will make direct connections to Security Access Manager for Web and Conditional is required you must enable this feature by removing the check from the box.

Custom headers for HTTP requests ☒	
Use this if you are using any Reverse proxy in front of your Mail server and need to specify HTTP headers that can be used for access control	
Encrypt Header values ☐	
This ensures data security of values and also avoids replay attacks. The Header value will be appended with a ## separator followed by device's timestamp in GMT format and will be encrypted using the specified encryption key value.	
[-]	
HTTP header field name	x-fl-device-id
Value Supported placeholders - %deviceid%, %username%, %domain%, %email%, %upn%	%deviceid%
Include this header for Corporate Intranet websites only ☒ Requires MaaS360 Enterprise Gateway	

- 11. Expand the **Email** menu.
- 12. Select the **Configuration** sub-menu.
 - a. Custom headers for HTTP requests: **Checked**
 - b. Encrypt Header values: **Unchecked**
 - c. HTTP header field name: **x-fl-device-id**

- d. Value: %deviceid%

Custom headers for HTTP requests ☒

Use this if you are using any Reverse proxy in front of your Mail server and need to specify HTTP headers that can be used for access control

Advanced Settings

Encrypt Header values ☐

This ensures data security of values and also avoid replays. The Header values will be appended with a ## separator followed by a timestamp in GMT format and will be encrypted using the encryption key specified value.

HTTP header field name	
	x-fl-device-id
Value Supported placeholders - %deviceid%, %username%, %domain%, %email%, %upn%	%deviceid%

13. Select the **MaaS360 Enterprise Gateway** sub-menu.
- Enable MaaS360 Gateway for Intranet Access: **Checked**
 - Default Enterprise Gateway: **<gateway_name>**. For example: gw-isam
 - Intranet Resources: **<intranet_hosts>**.
For example: *.poc.if, *.poc.if*, *.demos.ibm.com*

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	gw-isam ▼
Configure Regional Gateways	☐

Access List

Intranet Resources 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	*.poc.if, *.poc.if*, *.demos.ibm.com*
---	---------------------------------------

14. Expand the **Workplace Apps** menu.
15. Select the **Allowed Apps** sub-menu.

Note: This configuration item is optional. Use this field to control access to only allow distributed apps and apps that have been modified to include the Device ID as described in *MaaS360 SDK App Code Updates* on page 21.

a. Configure Apps Whitelist for Workplace Apps: **Checked**

b. iOS Apps: **<allowed_apps>**

c. Allowed Android App IDs: **<allowed_apps>**

For example to allow the Android SDK sample apps:

`com.fiberlink.maas360.android.testappsdk,com.Test521WLC`

16. Select the **MaaS360 Enterprise Gateway** sub-menu.

a. Enable MaaS360 Gateway For Workplace Apps: **Checked**

b. Default Enterprise Gateway: **<gateway_name>**. For example: `gw-isam`

c. Intranet Resources: **<intranet_hosts>**.

For example: `*.poc.if, *.poc.if*, *.demos.ibm.com*`

Enable MaaS360 Gateway For Workplace Apps ☒

Ensure Cloud Extender has been installed and Enterprise Gateway has been configured.

Select Gateways to use

Default Enterprise Gateway gw-isam ▼

Configure Regional Gateways ☐

Access List

Intranet Resources
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

*.poc.if, *.poc.if*, *.demos.ibm.com*

DNS and Intranet Host access

To achieve SSO, all hosts and domains accessed through the MEG must resolve to the Security Access Manager for Web instance.

For example, a host `https://portal.poc.if/` must be resolved by the MEG and forwarded to the Security Access Manager for Web instance, even if the host name corresponds directly to the real host with that name. If the MEG forwards directly to the real host, bypassing Security Access Manager for Web, SSO will not be completed and features such as Conditional Access and Federated Single Sign On will be unavailable.

Security Access Manager supports a number of mechanisms to allow perform the reverse proxy function. Refer to *Junction Management* on page 30.

IBM Security Access Manager Configuration

Complete the following configuration steps on Web Reverse Proxy or WebSEAL for integration with IBM MaaS360.

The **pdadmin** command-line utility can be used on the Web Reverse Proxy in addition to the graphical user interface of the Local Management Interface (LMI) for some of the integration steps.

Complete the Single Sign On configuration for either

- *Web Reverse Proxy Configuration*; or
- *WebSEAL Configuration*

For Conditional Access using MaaS360 device data, complete the steps in

- *Advanced Access Control Appliance Configuration*

Web Reverse Proxy Configuration

Complete the configuration steps on the IBM Security Access Manager for Web appliance to enable Single Sign On from the Mobile Enterprise Gateway.

Authentication Mechanism

The IBM Security Access Manager for Web Reverse Proxy instance must be configured to accept the authentication mechanism that the MEG will use to forward the Gateway Credentials on behalf of the MaaS360 user.

If the reverse proxy instance will only be used for MEG connection, all other authentication mechanisms can be disabled.

Additional authentication mechanism can be enabled, for example Forms authentication for existing direct client access and when Security Access Manager Advanced Access Control is configured, EAI authentication will be enabled.

Refer to *Table 1: Recommended IBM Security Access Manager for Web Authentication Mechanism* on page 8 to determine the authentication mechanism to enable for SSO with the MEG.

For example, when the MEG is configured using LDAP, enable Basic Authentication:

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Edit**.
5. Select the **Authentication** tab.
6. Under **Basic Authentication** → **Transport**, select **Both**.
7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Using Basic Authentication or SPNEGO/Kerberos it is not possible to sign into Security Access Manager for Web as a different user as the MEG will continue to supply SSO data.

To SSO as a different user, the MaaS360 App must disconnect from the MEG and they must resupply the Gateway Credentials of the other user when prompted.

Authentication Challenge Type

IBM Security Access Manager for Web can customize the authentication challenge that it issues to clients based on the User Agent of the HTTP request.

When multiple authentication mechanisms are enabled the Web Reverse Proxy instance must be configured to send a 401 WWW-Authenticate (Basic or Negotiate) response so that the MEG will provide the user's Gateway Credentials for requests made using the Secure Browser or SDK.

For example, when Security Access Manager Advanced Access Control has been configured for the instance, EAI Authentication will be enabled which will cause the Web Reverse Proxy to issue a login form for all unauthenticated requests which will be returned to the user and not handled by the MEG.

When checking for multiple User Agent strings separate each pattern using semi colons (;), for example:

```
auth-challenge-type = [++meg20*;++Apache*]ba, [-*meg20*;-*Apache*;++]forms
```

MaaS360 Secure Browser User Agent

Update the *auth-challenge-type* for the Secure Browser User Agent configured in *Workplace Persona* Policy on page 23.

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Configuration** → **Edit Configuration File**.
5. In the Advanced Configuration File Editor - <instance> window, locate the *auth-challenge-type* stanza.
6. Add or update the stanza to include the *meg20* pattern. For example, to enable Basic Authentication:

```
auth-challenge-type = [++meg20*]ba, [-*meg20*]forms
```
7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Although normally not required, the original standard User Agent string can be updated and passed to junctions by Security Access Manager for Web using a HTTP Transformation Rule.

The `MaaS360MEGUserAgentRequestTransformation.xslt` file shipped with the integration package is a request HTTP Transformation Rule to rewrite the User Agent from the Secure Browser. It removes the *meg20* identifier from the User Agent HTTP request header.

Refer to the [IBM Security Access Manager Knowledge Center](#) page for instructions to enable HTTP transformation rules.

MaaS360 Secure Mail User Agent

Update the *auth-challenge-type* for the MaaS360 Secure Mail User Agent. For example, the MaaS360 Android 5.21 Secure Mail client uses both *Dalvik/2.1.0 (Linux; U; Android 5.0; Android SDK built for x86_64 Build/LRX09D)* and *MaaS360-MaaS360 Mail-Android/5.45*.

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Configuration** → **Edit Configuration File**.
5. In the Advanced Configuration File Editor - <instance> window, locate the *auth-challenge-type* stanza.
6. Add or update the stanza to include the Secure Mail patterns. For example, to enable Basic Authentication (entered on a single line):
`auth-challenge-type = [+*MaaS360*;*Dalvik*]ba, [-*MaaS360*;*Dalvik*;*]forms`
Note: By returning a forms login to non Secure Mail clients, native ActiveSync clients will be unable to authenticate and therefore restrict access.
7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Verify additional User Agent strings using the reverse proxy instance *pdweb.debug* trace or *request.log*.

MaaS360 SDK User Agent

Update the *auth-challenge-type* for the MaaS360 SDK User Agent. For example, the MaaS360 Android 5.21 SDK uses the Apache HTTP client - *Apache-HttpClient/UNAVAILABLE (java 1.5)*.

10. Open the Web Reverse Proxy Web console.
11. Select **Secure Web Settings** → **Reverse Proxy**.
12. Select the reverse proxy instance to configure.
13. Select **Manage** → **Configuration** → **Edit Configuration File**.
14. In the Advanced Configuration File Editor - <instance> window, locate the *auth-challenge-type* stanza.
15. Add or update the stanza to include the Apache pattern. For example, to enable Basic Authentication:
`auth-challenge-type = [+*Apache*]ba, [-*Apache*]forms`
16. Click **Save**.
17. Deploy the pending changes.
18. Restart the reverse proxy instance.

Verify additional User Agent strings using the reverse proxy instance *pdweb.debug* trace or *request.log*.

Junction Management

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center](#) page for details of each junction type.

Once authenticated to Security Access Manager for Web, downstream SSO to protected resources is achieved using a broad range of authentication mechanisms including existing Single Sign On patterns and integration adapters such as Trust Association Interceptor (TAI), Lightweight Third-Party Authentication (LTPA), Basic Authentication (GSO, -B, etc.), HTTP header (Kerberos, iv-creds, etc.) and Federation (using Tivoli Federated Identity Manager).

WebSEAL Configuration

Complete the configuration steps on the IBM Security Access Manager WebSEAL server to enable Single Sign On from the Mobile Enterprise Gateway.

Authentication Mechanism

The IBM Security Access Manager WebSEAL instance must be configured to accept the authentication mechanism that the MEG will use to forward the Gateway Credentials on behalf of the MaaS360 user.

If the WebSEAL instance will only be used for the MEG, all other authentication mechanisms can be disabled.

Additional authentication mechanism can be enabled, for example Forms authentication for existing direct access clients.

Refer to *Table 1: Recommended IBM Security Access Manager for Web Authentication Mechanism* to determine the authentication mechanism to enable for SSO with the MEG.

For example, when the MEG is configured using LDAP, enable Basic Authentication:

1. Stop the WebSEAL server.
2. Edit the `<PDWEB_HOME>/etc/webseald-<instance-name>.conf` file. For example: `/opt/pdweb/etc/webseald-default.conf`
3. Locate the **[ba]** stanza.
4. Update `ba-auth` to **both**.
5. Save the file.
6. Restart the WebSEAL instance.

Using Basic Authentication, it is not possible to sign into WebSEAL as a different user as the MEG will continue to supply SSO data.

To SSO as a different user, the MaaS360 App must disconnect from the MEG and supply the Gateway Credentials of the other user when prompted during reconnection.

Authentication Challenge Type

IBM Security Access Manager WebSEAL can customize the authentication challenge that it issues to clients based on the User Agent of the HTTP request.

When multiple authentication mechanisms are enabled, the WebSEAL instance must be configured to send a 401 WWW-Authenticate (Basic or Negotiate) response so that the MEG will provide the user's Gateway Credentials for requests made using the Secure Browser or SDK.

For example, WebSEAL will issue a login form for all unauthenticated requests, which will be returned to the user and not handled by the MEG, when EAI Authentication is enabled.

When checking for multiple User Agent strings separate each pattern using semi colons (;). For example:

```
auth-challenge-type = [.*meg20*.*Apache*]ba, [.*meg20*.*Apache*.*]forms
```

MaaS360 Secure Browser User Agent

Update the *auth-challenge-type* for the Secure Browser User Agent configured in *Workplace Persona* Policy.

1. Stop the WebSEAL server.
2. Edit the `<PDWEB_HOME>/etc/webseald-<instance-name>.conf` file. For example: `/opt/pdweb/etc/webseald-default.conf`
3. Locate the *auth-challenge-type* stanza.
4. Add or update the stanza to include the *meg20* pattern. For example, to enable Basic Authentication:

```
auth-challenge-type = [.*meg20*]ba, [.*meg20*]forms
```
5. Save the file.
6. Restart the WebSEAL instance.

Although normally not required, the original standard User Agent string can be updated and passed to junctions by Security Access Manager WebSEAL using a HTTP Transformation Rule.

The `MaaS360MEGUserAgentRequestTransformation.xslt` file shipped with the integration package is a request HTTP Transformation Rule to rewrite the User Agent from the Secure Browser. It removes the *meg20* identifier from the User Agent HTTP request header.

Refer to the [IBM Security Access Manager Knowledge Center](#) page for instructions to enable HTTP transformation rules.

MaaS360 Secure Mail User Agent

Update the *auth-challenge-type* for the MaaS360 Secure Mail User Agent. For example, the MaaS360 Android 5.21 Secure Mail client uses both *Dalvik/2.1.0 (Linux; U; Android 5.0; Android SDK built for x86_64 Build/LRX09D)* and *MaaS360-MaaS360 Mail-Android/5.45*.

1. Stop the WebSEAL server.
2. Edit the `<PDWEB_HOME>/etc/webseald-<instance-name>.conf` file. For example: `/opt/pdweb/etc/webseald-default.conf`
3. Locate the *auth-challenge-type* stanza.
4. Add or update the stanza to include the Secure Mail patterns. For example, to enable Basic Authentication (entered on a single line):

```
auth-challenge-type = [.*MaaS360*.*Dalvik*]ba, [.*MaaS360*.*Dalvik*.*]forms
```

Note: By returning a forms login to non Secure Mail clients, native ActiveSync clients will be unable to authenticate and therefore restrict access.
5. Save the file.

6. Restart the WebSEAL instance.

Verify additional User Agent strings using the reverse proxy instance `pdweb.debug` trace or `request.log`.

MaaS360 SDK User Agent

Update the `auth-challenge-type` for the MaaS360 SDK User Agent. For example the MaaS360 Android 5.21 SDK uses the Apache HTTP client - `Apache-HttpClient/UNAVAILABLE (java 1.5)`.

1. Stop the WebSEAL server.
2. Edit the `<PDWEB_HOME>/etc/webseald-<instance-name>.conf` file. For example: `/opt/pdweb/etc/webseald-default.conf`
3. Locate the `auth-challenge-type` stanza.
4. Add or update the stanza to include the Apache pattern. For example, to enable Basic Authentication:
`auth-challenge-type = [+*Apache*]ba, [-*Apache*]forms`
5. Save the file.
6. Restart the WebSEAL instance.

Verify additional User Agent strings using the reverse proxy instance `pdweb.debug` trace or `request.log`.

Junction Creation

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Standard WebSEAL junctions](#) and [IBM Security Access Manager Knowledge Center Virtual Hosting](#) pages for details of each junction type.

Once authenticated to Security Access Manager WebSEAL, downstream SSO to protected resources is achieved using a broad range of authentication mechanisms including existing Single Sign On patterns and integration adapters such as Trust Association Interceptor (TAI), Lightweight Third-Party Authentication (LTPA), Basic Authentication (GSO, -B, etc.), HTTP header (Kerberos, iv-creds, etc.) and Federation (using Tivoli Federated Identity Manager).

Advanced Access Control Appliance Configuration

Complete the configuration steps on the IBM Security Access Manager Advanced Access Control appliance to enable Conditional Access using the MaaS360 Policy Information Point (PIP).

In addition to the existing attributes available in Security Access Manager Advanced Access Control, the Fiberlink MaaS360 Policy Information Point can be used to include MaaS360 device attributes in access control policy for that device. The PIP is able to identify the MaaS360 device using:

- *Direct mapping.*
A MaaS360 app such as the Secure Browser and Secure Mail or MaaS360 SDK app sends its Device ID as a HTTP request header.
- *Device characteristic “best effort” mapping.*

Using the Attribute Collection Service (info.js) a fingerprint of the device is collected using key device characteristics. The PIP searches for all devices registered for the authenticated user (partial username search using the Web Service APIs) and attempts to find a best match.

Once the device has been identified by the PIP, the predefined MaaS360 device attributes can be used in access control policies. Complex business rules for access to protected resources can be authored using device compliance information as well as other predefined attributes.

For example:

- When the **Managed Status** is *not (!) Enrolled* in MaaS360 or **Match Found** is *False*, **Deny with Obligation** *MaaS360 enrolment page*.
- All access to the Manager portal requires devices to be *In Compliance*. *Corporate Owned* devices may access the Manager portal at any time and afterhours and an *Employee Owned* device requires **Permit with Authentication One Time Password (OTP)**. Otherwise **Deny**.
- All devices where the **Compliance State** is *Out of Compliance* can only access the Enterprise Help portal providing them access to self-service features and instructions on how to rectify.
- All **Jail Broken** devices receive **Deny with Obligation** *Corporate Policy details page*.

Attribute	Description	Values
fiberlink.maas360.device.compliance.state	Fiberlink MaaS360 ownership indicator of the registered device.	In Compliance Out of Compliance
fiberlink.maas360.device.ownership	Fiberlink MaaS360 ownership indicator of the registered device.	Corporate Owned Corporate Shared Corporate Third Party Employee Owned Not Defined
fiberlink.maas360.device.managed.status	Fiberlink MaaS360 managed status of the registered device.	Enrolled Not Enrolled User Removed Control Control Removed Pending Control Removal
fiberlink.maas360.device.jailbroken	Fiberlink MaaS360 jailbroken state of the registered device.	Yes No
fiberlink.maas360.device.last.reported	Fiberlink MaaS360 last reported date/time of the device to the server.	YYYY-MM-DDTHH:MM:SS For example: 2014-01-30T12:00:00
fiberlink.maas360.device.match.found	Fiberlink MaaS360 derived attribute indicating a match against the attribute collection service data to a registered device.	True False

Table 3: Available attributes from MaaS360

See to [IBM Security Access Manager Knowledge Center Fiberlink MaaS360 PIP](#) and [IBM Security Access Manager Knowledge Center Predefined attributes](#) for additional information.

Custom Fiberlink MaaS360 Attributes

Custom attributes can be created in IBM Security Access Manager Advanced Access Control enabling additional Fiberlink MaaS360 *Security & Compliance Information* attributes to be evaluated in Advanced Access Control Policy. Refer to *Table 3: Available attributes from MaaS360* for predefined attribute support.

The source of additional attributes is the **Get Security & Compliance Information for a Mobile Device** Web Service API detailed in the MaaS360 Web Services Reference Guide.

For example:

```
https://m3.maas360.com/deviceapis/devices/1.0/mdSecurityCompliance/1101234?deviceId=a2e13f
```

Create any additional attributes required in Security Access Manager Advanced Access Control to represent the device *Security and Compliance Information* data.

Values will be assigned to these attributes during attribute mapping in the PIP configuration.

1. Open the Advanced Access Control Appliance Web console.
2. Select **Secure Access Control: Policy** → **Attributes**.
3. Click **New**.
4. Enter the details associated with this new attribute:

Attribute	Description
Name	Name of this attribute. E.g.: fiberlink.maas360.device.camera.present
Identifier	Identifier for this attribute. E.g.: urn:ibm:security:fiberlink:maas360:device:camera:present
Description	Description of this attribute E.g.: This attribute is used to check the presence of camera in the user's device
Issuer	urn:ibm:security:fiberlink:maas360
Category	Select one from the drop down menu. E.g.: Subject
Data Type	Select one from the drop down menu based on the data type of the attribute. E.g.: String
Matcher	Select one from the drop down menu. E.g.: exact_match.
Type	Select the type/s of this attribute. E.g.: Policy
Storage Domain	Select all that applies for this attribute E.g.:

Attribute	Description
	Device.

Table 4: Custom Attribute details for MaaS360 Security and Compliance Information

Important: The Issuer name must exactly match

`urn:ibm:security:fiberlink:maas360` to ensure the custom attribute used in access policy cause the PIP to be called.

5. Click **Save**.
6. Deploy pending changes.

Mobile Authorization Decision Point Configuration

Ensure you configure the Web Reverse Proxy to use the Advanced Access Control Appliance by executing the **isamcfg** tool.

See to [IBM Security Access Manager Knowledge Center Using the isamcfg tool](#) for instructions on performing the configuration.

Importing the MaaS360 SSL Certificate

The MaaS360 Web Services API endpoint SSL certificate must be imported to the Security Access Manager key database.

1. In a browser, navigate to the MaaS360 URL provided by Fiberlink during registration. For example `https://services.m3.maas360.com`
2. Export the certificate. Using Mozilla Firefox:
 - a. Left-click on the padlock icon to the left of the URL in the address bar
 - b. Click **More Information**.
 - c. In the **Security** panel, click View **Certificate**.
 - d. In the **Details** tab, click **Export...**
 - e. Ensure the certificate is saved with the **.crt** file extension and click **Save**.
3. Open the Advanced Access Control Appliance Web console.
4. Select **Manage System Settings** → **Secure Settings** → **SSL Certificates**.
5. Select the **rt_profile_keys** Certificate Database
6. Click **Manage** → **Edit SSL Certificate Database**.
7. Select the **Signer Certificates** tab.
8. Click **Manage** → **Import** → **Browse** and then select the **.crt** certificate file exported from MaaS360.
9. Click **Open**.
10. Type a name for the certificate in the **Certificate Label** for example *MaaS360 Web Service API*.
11. Click **Import**.
12. Deploy the pending changes.

Creating the Fiberlink MaaS360 Policy Information Point

1. Open the Advanced Access Control Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Information Points**.
3. Click the **New** button.
4. Select **Fiberlink MaaS360**.
5. Enter the PIP connection details associated with the Web Service API:

Attribute	Description
Name	urn:ibm:security:fiberlink:maas360
Description	Fiberlink MaaS360 Policy Information Point
URL	https://<maas360_host> e.g. https://services.m3.maas360.com
Username	<MaaS360_Administrator_Username>
Password	<MaaS360_Administrator_Password>
App Access Key	<MaaS360 App Access Key>
App Version	<MaaS360 App Version>
App ID	<MaaS360 App ID>
Billing ID	<MaaS360 Billing ID>
Platform ID	<MaaS360 Platform ID>
Cache Max Age	[Optional default: 600s] <MaaS360 Cache Max age>
Certificate Database	rt_profile_keys.kdb

Table 5: Fiberlink MaaS360 PIP connection details

Important: The PIP instance name must exactly match

urn:ibm:security:fiberlink:maas360 to ensure the MaaS360 attributes used in access policy cause the PIP to be called.

6. To map additional custom attributes select the **Attributes** tab.
7. Click **New**.
8. In the **New Attribute** dialog box, select the custom attribute created in *Custom Fiberlink MaaS360 Attributes* on page 34
9. Enter the Selector for the custom attribute. XPath 1.0 expressions are supported for XML selectors. Any valid XPath expression is supported.

For example:

```
//complianceAttribute[key/text()='Camera Present']/value/text()
```

10. Click **OK**.
11. Map any additional custom attributes as required.
12. Click **Save**.

13. Deploy the pending changes.

Populating Device ID from the MaaS360 component

Modify the Security Access Manager for Web configuration file to populate the `urn:ibm:security:fiberlink:maas360:device:ids` attribute from the `x-fl-device-id` HTTP request header.

Ensure you have configured the Workplace Persona Policy for Secure Browser and Secure Email to insert the `x-fl-deviceid` custom HTTP request header with the value of `%deviceid%`.

If you are using the SDK, ensure your code inserts this HTTP request header as described in *MaaS360 SDK App Code Updates* on page 21.

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Configuration** → **Edit Configuration File**.
5. Locate the **[azn-decision-info]** stanza.
6. Assign the MaaS360 Device ID to the
`urn:ibm:security:fiberlink:maas360:device:ids` attribute.

For example:

```
[azn-decision-info]
urn:ibm:security:fiberlink:maas360:device:ids = header:x-fl-device-id
```

7. Locate the **[user-attribute-definitions]** stanza.
8. Assign the datatype and category of the attribute.

For example:

```
[user-attribute-definitions]
urn:ibm:security:fiberlink:maas360:device:ids.datatype = string
urn:ibm:security:fiberlink:maas360:device:ids.category = Environment
```

9. Click **Save**.
10. Deploy the pending changes.
11. Restart the reverse proxy instance.

Populating Device ID using the Attribute Collection Service

When a native mobile browser is used no Device ID is available for use in the PIP. Security Access Manager can perform device fingerprinting to calculate a 'best match' mapping between the accessing device and the MaaS360 device inventory for the authenticated user.

Browser based access device fingerprint limitations

Partial mapping relies on the authenticated user having no more than one type of each device with the same platform and screen resolution (height or width) and a one-to-one mapping of username across both platforms.

For example, an authenticated user may have a mobile device with a resolution of 480px by 800px and a tablet with a resolution of 2560px by 1200px. These devices are able to be uniquely identified in the MaaS360 device inventory using the Security Access Manager device fingerprint.

If two devices of the same manufacturer and model are registered, the two devices cannot be uniquely identified resulting in only the first match being mapped.

Calling the Attribute Collection Service

In order to identify and fingerprint devices, the Policy Information Point requires specific device information which is obtained using the attribute collection service `info.js` script.

This must be executed before any access control policy evaluation occurs.

Include the `<script>` tag to call the attribute collection service on a page such as the Security Access Manager login page, or portal landing page.

The `info.js` script must complete before navigating away from the page and prior to accessing protected resources where access control policy is attached.

For example:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<html>
  <head>
    <title>Portal Landing Page</title>
    <script src="/mga/sps/ac/js/info.js"></script>
  </head>
  <body>
    <a href="/jctA">Click here to continue...</a>
  </body>
</html>
```

See to [IBM Security Access Manager Knowledge Center Attribute collection service](#) for additional configuration.

Modifying the risk profile

When the attribute collection service `info.js` script is executed it queries the active risk profile to determine which attributes to populate. The MaaS360 Web Service API call requires specific attributes depending on the type of search being performed in the inventory of devices.

Where device characteristic matching is used the `screenAvailableWidth`, `screenAvailableHeight` and `devicePlatform` attributes are required.

You can modify the existing active risk profile, duplicate or create a new risk profile and set it as active.

It is recommended all four attributes are added to the risk profile to cater for full and partial mapped Web Service API calls.

To create a new risk profile:

1. Open the Mobile Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Risk Profiles**.
3. Click **New Risk Profile**.

4. Specify a name, for example: **Fiberlink MaaS360 Device**
5. Select **Fiberlink MaaS360 Device** from the **Profiles** list.
6. Click **Add Attributes to Risk Profile**.
7. Check the attributes required for MaaS360 mapping and click Add.
 - `deviceName`
 - `devicePlatform`
 - `screenAvailableWidth`
 - `screenAvailableHeight`
8. Check any additional attributes to be added to your risk profile.
9. Click **Close**.
10. Specify a Weight for any of the attributes as required if using Risk Score in any access control policy.
11. Click **Save**.
12. Click **Set Active**.
13. Deploy the pending changes.

Running the Sample Application

Use the example scenario to validate SSO to Security Access Manager for Web and CBA using Security Access Advanced Access Control.

The sample environment uses the embedded directory server of Security Access Manager for Web and the Mobile Enterprise Gateway is configured to use this directory.

Before you start

This section does not cover the configuration of the entire environment. It focuses on running the test scenarios and performing the configuration with sample values.

References are made to the configuration steps provided in

- *IBM MaaS360 Configuration* on page 14
- *IBM Security Access Manager Configuration* on page 27

Security Access Manager for Web configuration

Install and configure a Security Access Manager for Web appliance:

1. When configuring the Runtime Component, use the **Embedded LDAP**.
2. Create a **Web Reverse Proxy** instance.
3. Configure **Basic Authentication** for the *Authentication Mechanism* on page 27.
4. Configure **Secure Browser¹** and **MaaS360 SDK** in *Authentication Challenge Type* on page 28.

Add the stanza entry (entered on a single line):

```
auth-challenge-type = [+*meg20*;*Apache*]ba, [-*meg20*;-  
*Apache*;*]forms
```

Note 1: The HTTP Transformation Rule is not required in this sample.

User Account Creation

Use **Policy Administration** or the **pdadmin** command-line utility to create user accounts for the tests. For example:

```
pdadmin sec_master> user create testuser1 uid=testuser1,dc=iswga Test  
User1 password1  
pdadmin sec_master> user modify testuser1 account-valid yes  
pdadmin sec_master> user create testuser2 uid=testuser2,dc=iswga Test  
User2 password2  
pdadmin sec_master> user modify testuser2 account-valid yes
```

Existing user accounts can be used in the sample. Ensure the users have a different ownership value for their registered devices in MaaS360.

Junction Management

Use **Junction Management** or the **pdadmin** command-line utility to create a standard junction to the WebSphere Liberty Profile instance on the appliance. For example:

```
pdadmin sec_master> server list
<instance-name>-webseald-<webseal-host-name>

pdadmin sec_master> server task <instance-name>-webseald-<webseal-
hostname> create -t tcp -h localhost -p 80 /maas360sample
```

Replace `<instance-name>-webseald-<webseal-host-name>` with the value output from the first command.

If Security Access Manager Advanced Access Control is not activated on the same appliance the junction creation will fail. Add the `-f` switch to the junction creation and re-execute the command to allow you to proceed with the configuration and then activate the Mobile offering.

MaaS360 Configuration

1. Register two devices and ensure different ownership for the created user accounts:
 - a. **testuser1**: Corporate Owned
 - b. **testuser2**: Employee Owned
2. Install a **HMAC OTP** app such as **Google Authenticator** on both devices.
3. Complete the installation and configuration of the *Mobile Enterprise Gateway* on page 14. Configure the MEG against the Security Access Manager embedded directory.
4. Enable *Secure Browser* on page 19.
5. Enable *Mobile Application Management* on page 20. Download the MaaS360 SDK and update the code to insert the Device ID¹. For example, using the Native Android SDK sample:
 - a. Load the **MaaS360SDKSampleApp**.
 - b. Expand `src`.
 - c. Expand `com.fiberlink.maas360.android.appSdkSampleApp` package.
 - d. Open **MainActivity.java**
 - e. Locate the line


```
MaaS360SDK.getEnterpriseGatewayService().proxy(client);
```
 - f. Immediately before this line, add:


```
//Retrieve deviceId & add to x-fl-device-id HTTP request header
String deviceId = MaaS360SDK.getContext().getDeviceCsn();
httpget.setHeader("x-fl-device-id", deviceId);
```
 - g. Save **MainActivity.java**
 - h. Build the native app sample.
 - i. Deploy the **MaaS360 SDK** app to the registered devices.
6. Enable *Web Services* on page 22.
7. Edit and distribute the *Workplace Persona Policy* on page 23. Use the same hostnames in the **Intranet Resources**².

8. Update the DNS entries of the MEG to access the Security Access Manager for Web instance in *DNS and Intranet Host access* on page 26.

The Security Access Manager host should be accessed using `isam.poc.if2`.

Note 1: If you do not have a development environment to build the sample app, this step can be simulated by crafting the equivalent HTTP request, however access must be directly to the Security Access Manager host. See *Simulating Conditional Access* on page 45.

Note 2: Different host names may be used. Ensure the host entered in the Secure Browser and SDK app matches the host added to Intranet Resources of the Workplace Persona Policy.

Security Access Manager Advanced Access Control Configuration

Install and configure a Security Access Manager Advanced Access Control appliance on the same system as the Security Access Manager for Web appliance:

1. Use the default Runtime Listening Interfaces (localhost – 80 and 443).
2. Run the **isamcfg** tool in *Advanced Access Control Appliance Configuration* on page 32.
3. Optionally complete Custom Fiberlink MaaS360 Attributes on page 34.
4. Complete *Importing the MaaS360 SSL Certificate* on page 35.
5. Complete
6. *Creating the Fiberlink MaaS360 Policy Information Point* on page 36.
7. Complete *Populating Device ID from the MaaS360* on page 37.

The Attribute Collection Service is not used in this sample.

Create an Access Control Policy

Create a simple Access Control policy where:

- If corporate owned and is in compliance, then permit;
- If employee owned, is in compliance, and is not jailbroken then permit only after supplying a One Time Password;
- All other requests are denied.

1. Open the Advanced Access Control Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Access Control**.
3. Select **Policies**.
4. Click the **Create Policy** button.
5. Author the sample policy. For example:

Property	Description
Name	MaaS360 Device Ownership

Property	Description
Description	Apply access policy based on Fiberlink MaaS360 device attributes
Precedence	First
Rules	This rule permits corporate owned devices that are in compliance: <pre>If fiberlink.maas360.device.ownership = "Corporate Owned" and fiberlink.maas360.device.compliance.state = "In Compliance" Then Permit</pre>
	This rule permits employee owned devices that are in compliance and are not jailbroken if they have entered a Time Based OTP: <pre>If authenticationTypes has member "urn:ibm:security:authentication:asf:totp" and fiberlink.maas360.device.ownership = "Employee Owned" and fiberlink.maas360.device.compliance.state = "In Compliance" and fiberlink.maas360.device.jailbroken = "No" Then Permit</pre>
	This rule permits employee owned devices that are in compliance and are not jailbroken. The user is prompted to enter a Time Based OTP: <pre>If fiberlink.maas360.device.ownership = "Employee Owned" and fiberlink.maas360.device.compliance.state = "In Compliance" and fiberlink.maas360.device.jailbroken = "No" Then Permit with Authentication TOTP One-time Password</pre>
	This rule denies access if no previous rule is matched. <pre>Deny</pre>

Table 6: Sample policy rule set

6. Click **Save**

Attach and publish the Access Control Policy

1. Open the Advanced Access Control Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Access Control**.
3. Select **Resources**.

4. Click the **Add Resource** button.
5. In the Add Resource window:
 - a. Select the **Web Container** corresponding to the IBM Security Access Manager for Web instance.
 - b. Select the `/maas360sample` **Resource** to by typing or using the **Browse** button.
 - c. Click **Save**.
6. Select the `/maas360sample` resource from the **Resources** list.
7. Click the **Attach** button.
8. Select the `MaaS360 Device Ownership` from the list of **Policies**.
9. Click **OK**.
10. Click the **Publish** button.

Validating Single Sign On

On the **Corporate Owned** device registered to **testuser1**:

1. Launch the **Secure Browser**.
2. Navigate to `https://isam.poc.if/`
3. If prompted, enter the Gateway Credentials for the user.
 - a. Username: **testuser1**
 - b. Password: **password1**
 - c. Cache Credentials: **Checked**
 - d. Click **Continue**
4. Validate the Security Access Manager for Web splash screen is displayed.

On the **Employee Owned** device registered to **testuser2**:

1. Launch the **MaaS360 SDK** app.
2. Set **Auto-Enforce SSO** check: **Yes**
3. Click **Init SDK**.
4. Enter the PIN.
5. Swipe to the **MaaS360 Gateway** heading.
6. Click **Connect Gateway**.
7. If prompted, enter the Gateway Credentials for the user.
 - a. Username: **testuser2**
 - b. Password: **password2**
 - c. Cache Credentials: **Checked**
 - d. Click **Continue**
8. Enter `https://isam.poc.if/`
9. Click **Open URL**.

10. Verify the Response: **200**

Validating Conditional Access

On the **Corporate Owned** device registered to **testuser1**:

1. Launch the **MaaS360 SDK** app.
2. Set **Auto-Enforce SSO** check: **Yes**
3. Click **Init SDK**.
4. Enter the PIN.
5. Swipe to the **MaaS360 Gateway** heading.
6. Click **Connect Gateway**.
7. Enter `https://isam.poc.if/maas360sample/`
8. Click **Open URL**.
9. Verify the Response: **200**

On the **Employee Owned** device registered to **testuser2**:

1. Launch the **Secure Browser**.
2. Navigate to `https://isam.poc.if/mga/sps/mga/user/mgmt/html/otp/otp.html`
3. Using the Google Authenticator app, scan or entry the **TOTP Secret Key**
4. Navigate to `https://isam.poc.if/maas360sample/`
5. Validate the **One-Time Password Login** entry page is displayed.
6. Retrieve the OTP from the **Google Authenticator app**.
7. Enter the **OTP** in the One-Time Password Login entry page and click **Submit**.
8. Validate the WebSphere Liberty Profile splash screen is displayed.

Simulating Conditional Access

When it is not possible to build and deploy the MaaS360 SDK sample app, CBA can be simulated by making the same HTTP requests through a browser or utility such as cURL and inserting the `Authorization` and `x-fl-device-id` HTTP request headers.

These simulated tests must be completed on the MEG system so the Intranet hostname is resolvable.

Identify the Device ID for the registered devices:

1. Log in to the MaaS360 Administration portal. For example `https://m3.maas360.com`
2. Hover over **Device** from the menu.
3. Select **Inventory**.
4. Locate the device for **testuser1**.
5. Click **View**.
6. In the Hardware Inventory pane, record **Device ID**. For example: `androidc946553034`
7. Click the Back arrow next to the device name.

8. Locate the device for **testuser2**.
9. Click **View**.
10. In the Hardware Inventory pane, record **Device ID**. For example: androidc1059620651

To simulate the **Corporate Owned** device registered to **testuser1**:

1. Use cURL or a Browser to insert the Authorization and x-fl-device-id HTTP request headers. For example:

```
curl -v -k https://isam.poc.if/ -u testuser1:password1 -H "x-fl-device-id: androidc946553034"
```
2. Verify the Response:

```
< HTTP/1.1 200 OK
```

To simulate the **Employee Owned** device registered to **testuser2**:

1. Use cURL or a Browser to insert the Authorization and x-fl-device-id HTTP request headers. For example:

```
curl -v -k https://isam.poc.if/ -u testuser2:password2 -H "x-fl-device-id: androidc1059620651"
```
2. Verify the Response:

```
< HTTP/1.1 302 ISAM for Mobile Response
```

Troubleshooting

Examine the troubleshooting and logging sections for help in resolving integration issues.

Collecting Support Data

To assist with resolution of a support issue, ensure you have collected and reviewed the trace for the components configured in this integration.

Security Access Manager for Web

pdweb.debug

The `pdweb.debug` trace will assist in identifying errors related to SSO from the MEG to Security Access Manager.

If the trace does not show a `401 Unauthorized` response to the MEG, the Gateway Credentials will not be inserted and SSO will not complete.

In this instance, ensure you have completed the steps in *Workplace Persona Policy* on page 23 and *Authentication Challenge Type* on page 28.

To enable tracing:

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Edit**.
7. In the Edit Trace Component window:
 - a. Level: **2**
 - b. Flush Interval (seconds): **5**
 - c. Rollover Size (bytes): `<default>`
 - d. Click **Save**.

To disable trace, set the Level to 0.

To review the trace file generated:

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Files**.
7. In the Manage Trace Files – `pdweb.debug` window
 - a. Select **pdweb.debug.log**
 - b. Click **View**
 - c. Number of lines to view: **1000** (depending on the number of requests)
 - d. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

pdweb.http.transformation

The `pdweb.http.transformation` trace will assist in identify errors related to the User Agent HTTP request headers and the response phrase from a Security Access Manager Advanced Access Control Access Control policy.

In this instance, ensure you have completed the steps in *MaaS360 Secure Browser User Agent* on page 28 and **Error! Reference source not found. Error! Bookmark not defined..**

To enable tracing:

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the **pdweb.http.transformation** row.
6. Click **Edit**.
7. In the Edit Trace Component window:
 - a. Level: **9**
 - b. Flush Interval (seconds): **5**
 - c. Rollover Size (bytes): <default>
 - d. Click **Save**.

To disable trace, set the Level to 0.

To review the trace file generated:

1. Open the Web Reverse Proxy Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the **pdweb.http.transformation** row.
6. Click **Files**.
7. In the Manage Trace Files – `pdweb.debug` window
 - a. Select **pdweb.http.transformation.log**
 - b. Click **View**
 - c. Number of lines to view: **10000** (depending on the number of requests)
 - d. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

Security Access Manager Advanced Access Control

Policy Information Point cache

When the cache is enabled for the PIP you must wait until the cache timeout occurs before a new call will be made to the MaaS360 Web Service APIs.

Advanced Access Control Policy may return a cached result if the device has recently been updated and reported back to MaaS360 or there is an existing cache entry.

Restart the runtime to destroy the cache if an immediate call to the MaaS360 Web Service API is required.

Policy Information Point trace

The PIP trace will assist in identifying errors related to the CBA which may be caused by an error connecting to the MaaS360 Web Service APIs or an empty value for the MaaS360 Device ID.

To enable tracing:

1. Open the Advanced Access Control Appliance Web console.
2. Select **Monitor Analysis and Diagnostics** → **Runtime Tracing**.
3. Update **Tracing Specification** to include:

```
com.tivoli.am.rba.extensions.PluginUtils=ALL:com.tivoli.am.rba.pip.FierLink
MaaS360PIP=ALL:com.ibm.security.access.httpclient.*=ALL
```

4. Click **Save**.
5. Deploy the pending changes.

To disable trace, remove the trace specification.

To review the trace file generated:

1. Open the Advanced Access Control Appliance Web console.
2. Select **Monitor Analysis and Diagnostics** → **Application Log Files**.
3. Expand **mga** → **runtime**
4. Select `trace.log`.
5. Click the **View** button.
6. Number of lines to view: **10000** (depending on the number of requests)
7. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

MaaS360 Web Service API validation

Web Service requests

The MaaS360 Web Service APIs require an authentication token to be acquired which is then used to perform the API calls such as a partial username search.

Ensure you provide the correct connection details in the PIP and if necessary, perform a manual test using a client such as cURL.

1. Acquire an authentication token:

```
curl -v -k https://services.m3.maas360.com/auth-apis/auth/1.0/authenticate/<billing_id>/ -d
"<authRequest><maas360AdminAuth><billingID>XXXXXXXX</billingID><platformID>X</platformID><appID>XXXXXXXX</appID><appVersion>X.X</appVersion><appAccessKey>XXXXXXXXXX</appAccessKey><userName>XXXXXXXX</userName><password>XXXXXXXXXX</password></maas360AdminAuth></authRequest>" -H "Accept: application/xml" -H "Content-Type: application/xml; charset=UTF-8"
```

2. Parse the response for the **<authToken>**. For example:

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><authResponse><authToken>YYYYYYYY-YYYY-YYYY-YYYY-
YYYYYYYYYYYY-YYYYYY</authToken><errorCode>0</errorCode></authResponse>
```

3. Perform a partial username search:

```
curl -v -k "https://services.m3.maas360.com/device-apis/devices/1.0/search/<billing_id>/?partialUsername=<username>&match=0" -H "Authorization: MaaS token=YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYY-YYYY" -H "Accept: application/xml" -H "Content-Type: application/xml; charset=UTF-8"
```

Note: Limits are imposed on API calls. For failed API calls, ensure you have not reached a policy threshold. Review the X-Rate-Limit-<metric> response headers for details.

Notices

This information was developed for products and services offered in the U.S.A. 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 give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.*

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 might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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
224A/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 measurement 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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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. 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 IBM's application programming interfaces.

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

© IBM 20166. Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp 2014, 20166. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.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 Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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



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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.