

IBM Security Access Manager
Version 8.0.0.5

***Fiberlink MaaS360
Integration Guide***



Note:

Before using this information and the product it supports, read the information in [Notices](#).

This edition applies to Version 1.0 release i of the IBM Security Access Manager Integration with Fiberlink MaaS360 and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2012, 2014.

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.....	7
Support information.....	7
Statement of Good Security Practices.....	7
Product name updates.....	7
Chapter 1: Introducing the integration.....	8
Introduction.....	8
Fiberlink MaaS360 PIP.....	8
Fiberlink MaaS360 JavaScript PIP rule file.....	9
Integration Architecture.....	10
Integration product version information.....	11
Integration product contents.....	11
Before you start.....	11
Chapter 2: IBM Security Access Manager Configuration.....	13
Web Gateway Appliance configuration.....	13
Junction Management.....	13
Mobile Authorization Decision Point Configuration.....	14
Mobile Appliance configuration.....	14
Adding the MaaS360 SSL Certificate.....	14
Creating an access policy.....	15
Attach and publish the access policy.....	17
Chapter 3: Browser based access using Fiberlink MaaS360 PIP.....	19
Browser based access device fingerprint limitations.....	19
Fiberlink MaaS360 configuration.....	19
Creating the ISAMDeviceID Custom Attribute.....	20
Populating the ISAMDeviceID Custom Attribute.....	20
Web Gateway Appliance configuration.....	21
Calling the Attribute Collection Service.....	21
Mobile Appliance configuration.....	22
Modifying the risk profile.....	22
Creating an instance of the Fiberlink MaaS360 Policy Information Point.....	23
Chapter 4: SDK based access using JavaScript PIP rule file.....	24
Fiberlink MaaS360 SDK app code updates.....	24
Using the MaaS360 SDK to provide the device ID.....	24
Web Gateway Appliance configuration.....	25
Configuring the Web Reverse Proxy.....	25
Mobile Appliance configuration.....	25
Creating an instance of the JavaScript PIP.....	25
Chapter 5: Running the Sample Application.....	28

Before you start.....	29
Web Gateway Appliance configuration.....	30
Sample user account creation.....	30
MaaS360 Configuration.....	30
Fiberlink MaaS360 PIP.....	30
Fiberlink MaaS360 JavaScript PIP rule file.....	31
Testing the PIP invocation and policy evaluation.....	31
Fiberlink MaaS360 PIP.....	31
Fiberlink MaaS360 JavaScript PIP rule file.....	32
Chapter 6: Troubleshooting.....	33
Notices.....	34
Trademarks.....	37

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® Tivoli® 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 Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

Provides information about configuring and maintaining a Security Access Manager environment.

- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*

Provides configuration procedures and technical reference information for the Web Gateway Appliance.

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*

Provides a complete stanza reference for the Web Gateway Appliance Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager for Mobile Administration Guide*

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

- *IBM Security Access Manager for Mobile Configuration Guide*

Explains how to complete the initial configuration of IBM Security Access Manager for Mobile.

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.

Chapter 1: Introducing the integration

Introduction

The IBM 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 on IBM Security Access Manager for Mobile, enforced by IBM Security Access Manager for Web.

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

Two PIPs are provided:

- Fiberlink MaaS360 PIP
- Fiberlink MaaS360 JavaScript PIP rule file

Note: Only one of the PIPs may be configured at any one time.

Fiberlink MaaS360 PIP

Use this PIP for traditional browser based web applications.

The PIP is provided within the appliance firmware of IBM Security Access Manager for Mobile.

When a resource is protected by IBM Security Access Manager for Web, the device can be fingerprinted and device attributes retrieved from the MaaS360 device inventory for the corresponding device by the PIP in IBM Security Access Manager for Mobile.

If the the device has been fingerprinted and is registered in IBM Security Access Manager, a corresponding device ID can be mapped to a custom attribute for the MaaS360 enrolled device.

If the device has not been registered in IBM Security Access Manager, the attribute collection service can be used to collect device data and a corresponding device can be mapped to an existing device in the MaaS360 inventory.

If the device has not been registered and no corresponding device can be matched in the MaaS360 inventory, obligations such as Consent Device Registration and Authentication Mechanisms such as HTTP Redirect can be used to fingerprint and register the device in IBM Security Access Manager and to commence the enrollment process in MaaS360.

Fiberlink MaaS360 JavaScript PIP rule file

Use this PIP for Fiberlink MaaS360 SDK applications.

The rule file is provided in the integration download.

MaaS360 SDK apps, or existing apps wrapped in the MaaS360 SDK can be coded to retrieve the device ID and insert a HTTP request header containing this value.

IBM Security Access Manager for Web extracts the device ID and adds it as an attribute available for use in the JavaScript PIP rule file in IBM Security Access Manager for Mobile which allows the exact device attributes to be queried from the MaaS360 inventory.

Integration Architecture

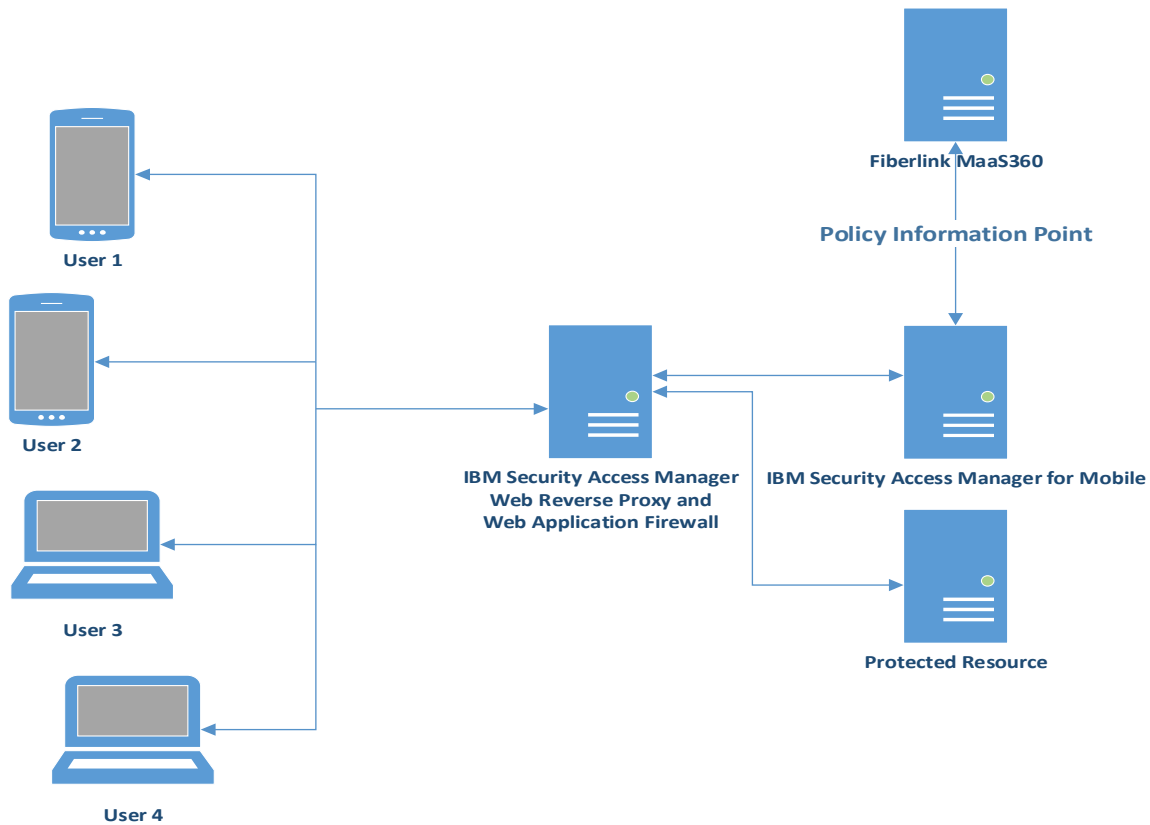


Fig. 1 MaaS360 Integration Architecture

Figure 1 above shows an integration architecture of the following processes:

1. The user requests content from the protected resource.
2. IBM Security Access Manager for Web intercepts the request and requires the user to authenticate.
3. The device is identified using either:
 - MaaS360 SDK app passing the device ID in a HTTP request header; or
 - IBM Security Access Manager attribute collection service
4. After successful authentication, the policy attached to the resource is evaluated.
5. The evaluation triggers the Policy Information Point which calls the MaaS360 Web Service API to retrieve the attribute values required by the policy. The device attributes are retrieved using either:
 - Direct search using MaaS360 device ID; or

- Partial username and hardware Web Service API calls matching the IBM Security Access Manager device fingerprint (platform, screen resolution)
- 6. The attribute values are returned to IBM Security Access Manager for Mobile and the policy evaluation is completed.
- 7. If the user is *permitted* to access the resource, IBM Security Access Manager for Web 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:

Table 1. Integration product contents

File name	Description
isam_maas360_int_guide.pdf	This integration guide
X.X-ISAM-MAAS360.README	The readme file
maas360_pip_rule.js	The JavaScript Policy Information Point rule file.

Before you start

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

IBM Security Access Manager for Mobile

Fiberlink MaaS360

Fiberlink MaaS360 Web Services enabled to grant access to MaaS360 Web Service APIs for 3rd party application integration.

Use the Cloud Extender to integrate with your Corporate User Directory to import group and associated user information, or manually provision a username in the User Directory of MaaS360 that exactly matches the IBM Security Access Manager user ID.

Chapter 2: IBM Security Access Manager Configuration

Complete the following configuration steps in the IBM Security Access Manager Local Management Interface (LMI) for integration with Fiberlink MaaS360.

Web Gateway Appliance configuration

The authentication method of the Web Reverse Proxy is not significant to the integration process but should be considered for the access type use case. For example a web browser accessing protected resources through the IBM Security Access Manager for Web hostname or a dedicated app accessing protected resources or RESTful Web Services using the hostname and dedicated URL path.

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 WebSEAL Administration Guide*](#) for details of each junction type.

The following example uses a Standard junction to a protected resource. For example, /TestApp.

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Reverse Proxy Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Junction Management**.
5. Select **New** → **Standard Junction**.
6. On the Junction tab
 - a. Add the junction name /TestApp
 - b. For Junction Type, select **TCP**.
7. On the Servers tab
 - a. Click **New** to add a target backend server.
 - b. Specify the connection details of the target server:
 - v Hostname: <test.webserver.com>
 - v TCP or SSL Port: <443>

- c. Click **Save**.
8. Click **Save**.

Mobile Authorization Decision Point Configuration

Ensure you configure Web Gateway Appliance to use the Mobile Appliance by executing the *isamcfg* tool.

Refer to: http://www-01.ibm.com/support/knowledgecenter/SSPREK_8.0.0.5/com.ibm.isamw.doc_8.0.0.5/config/task/tsk_isamcfg_appliance.html.

Mobile Appliance configuration

Configure the Mobile Appliance for integration with Fiberlink MaaS360.

Adding the MaaS360 SSL Certificate

The MaaS360 SSL certificate must be imported to the Security Access Manager key database to enable the Policy Information Point to retrieve device attributes using the Web Service API.

1. In a browser, navigate to the MaaS360 URL provided by Fiberlink during registration.
2. Export the certificate. In Mozilla Firefox this can be achieved by:
 - 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 Web Gateway Appliance Web console.
4. Select **Manage System Settings** → **Secure Settings** → **SSL Certificates**.
5. Select the **rt_profile_keys** Certificate Database and click **Manage** → **Edit SSL Certificate Database**.
6. Select the **Signer Certificates** tab.
7. Click **Manage** → **Import** → **Browse** and then select the **.crt** certificate file exported from MaaS360 and click **Open**.

8. Type a name for the certificate in the **Certificate Label** for example *MaaS360 Web Service API* and click **Import**.
9. Deploy the pending changes.

Creating an access policy

A number of predefined attributes are available in the Mobile Appliance for use in access policies.

Attribute	Description	Values
fiberlink.maas360.device.compliance.state	Fiberlink MaaS360 ownership indicator of the registered device.	In Compliance Out of Compliance
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.managed.status	Fiberlink MaaS360 managed status of the registered device.	Enrolled Not Enrolled User Removed Control Control Removed Pending Control Removal
fiberlink.maas360.device.match.found	Fiberlink MaaS360 derived attribute indicating a match against the attribute collection service data to a registered device.	True False
fiberlink.maas360.device.ownership	Fiberlink MaaS360 ownership indicator of the registered device.	Corporate Owned Corporate Shared Corporate Third Party Employee Owned Not Defined

For example, to author a sample policy where:

- If a device match is found, is corporate owned and is in compliance, then permit;
- If a device match is found, is employee owned, is in compliance, and is not jailbroken then permit;
- If a device match is not found prompt for consent to register the device in IBM Security Access Manager and enrollment in MaaS360.

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Access Control**.
3. Select **Policies**.
4. Click the **Create Policy** button.
5. Specify the necessary fields. For example:

Property	Description
Name	TestApp Policy 1
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.match.found = True and 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. <pre>If fiberlink.maas360.device.match.found = True 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 prompts for consent to register the device when it is not

	matched between IBM Security Access Manager and MaaS360. This rule could be extended with a custom Authentication Policy containing the Workflow Steps to Consent to device registration and HTTP redirect to the MaaS360 enrollment URL. <pre>If fiberlink.maas360.device.match.found = False and userConsent is missing Then Permit with Authentication Consent Register Device</pre> This rule registers the device in IBM Security Access Manager after consent. <pre>If fiberlink.maas360.device.match.found = False and userConsent is present and userConsent = "true" Then Permit with Obligation Register Device</pre> This rule denies access if no previous rule is matched. This rule is unnecessary if deny bias is used. <pre>Deny</pre>
--	---

6. Click Save.

Attach and publish the access policy

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Mobile Settings** → **Policy** → **Access Control**.
3. Select **Resources**.
4. Click **Add Resource**.
5. Select the **Web Container** corresponding to the IBM Security Access Manager for Web instance.
6. Select the **Resource** to where the policy will be attached by either typing the resource or using the Browse button.
7. Click **Save**.
8. Click the newly created resource from the **Resources** list.
9. Click the **Attach** button.
10. Select the `TestApp Policy 1` from the list of **Policies**.

11. Click **OK**.
12. Click the **Publish** button.

After creating the junction, executing the **isamcfg** tool, creating and deploying the sample policy, proceed to

[Chapter 3: Browser based access using Fiberlink MaaS360 PIP](#) or
[Chapter 4: SDK based access using JavaScript PIP rule file](#).

Chapter 3: Browser based access using Fiberlink MaaS360 PIP

The following sections detail the steps that are required to use the Fiberlink MaaS360 PIP for traditional browser based web applications including the MaaS360 Secure Browser.

Browser based access device fingerprint limitations

This integration describes a pattern of device fingerprint mapping between Fiberlink MaaS360 and IBM Security Access Manager for Mobile. Partial mapping relies on the 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, a 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 using the MaaS360 device enrollment and the IBM Security Access Manager device fingerprints. 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.

Fiberlink MaaS360 configuration

To reduce the number of Web Service API calls when mapping a device between IBM Security Access Manager and MaaS360, the custom attribute **ISAMDeviceID** can be created in the MaaS360 Administrator web console to provide direct mapping.

To use this feature, a device enrolled in MaaS360 and registered in IBM Security Access Manager must have the device name entered into the custom attribute. This mapping must be performed by an Administrator of MaaS360 and can be performed individually per device or using the Bulk Update capability for custom attributes.

The device name should not be renamed in IBM Security Access Manager once the mapping is completed.

Creating the ISAMDeviceID Custom Attribute

Create the custom attribute for device mapping in the Fiberlink MaaS360 Administrator.

1. Open the Fiberlink MaaS360 Administrator console. For example:
<https://m3.maas360.com/emc/>
2. Select **Devices** header in the navigation bar, then select **Custom Attributes** from the list.
3. Click **Manage Custom Attributes**.
4. Click **Add Custom Attribute**.
Enter **ISAMDeviceID** as the Attribute Name.
Select **Text** as the Attribute Type.
Click **Add**.
Click **Cancel** to close the dialog.

Populating the ISAMDeviceID Custom Attribute

The mapping can be completed individually per device, or using the Bulk Update feature in **Devices** → **Custom Attributes**.

The **ISAMDeviceID** attribute is accessible under the **Hardware Inventory** section of an enrolled device in MaaS360.

To populate the **ISAMDeviceID** individually:

1. Determine the device name registered in IBM Security Access Manager using either:
 - Recalling the name entered during the device registration consent; or
 - Determining the correct device using the list of devices in the **Device Selection** available from:
https://<webseal.ibm.com>/mga/sps/mga/user/mgmt/html/device/device_selection.html
2. Open the Fiberlink MaaS360 Administrator console. For example:
<https://m3.maas360.com/emc/>
3. Select **Devices** header in the navigation bar, then select **Inventory** from the list.
4. Click the **Device Name** corresponding to the device to be mapped.
5. Click the **Summary** list box and select **Hardware Inventory**.
6. Click the **Edit** button.

7. Populate the **ISAMDeviceID** field with the device name registered in IBM Security Access Manager.
8. Click **Save**.

Web Gateway Appliance configuration

Modify the IBM Security Access Manager for Web login page, or other local or junctioned page to call the attribute collection service.

Calling the Attribute Collection Service

In order to identify and fingerprint devices, the Policy Information Point requires specific device information which is obtained via the attribute collection service `info.js` script. This must be executed before the policy evaluation occurs.

Include the `<script>` tag to call the attribute collection service on a page that is accessed prior to the protected resource where the access policy is attached.

For example:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<html>
  <head>
    <title>Attribute Collection Service Caller</title>
    <script src="../../mga/sps/ac/js/info.js"></script>
  </head>
  <body>
    <a href="../../TestApp">Click here to continue...</a>
  </body>
</html>
```

Mobile Appliance configuration

Configure IBM Security Access Manager for Mobile to fingerprint devices and call the Fiberlink MaaS360 Policy Information Point.

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 the IBM Security Access Manager device name is populated in the custom attribute in MaaS360, only the *deviceName* attribute is required.
- Where device characteristic matching is used the *screenAvailableWidth*, *screenAvailableHeight* and *devicePlatform* attributes are required.

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

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 policy.
11. Click **Save**.
12. Click **Set Active**.
13. Deploy the pending changes.

Creating an instance of the Fiberlink MaaS360 Policy Information Point

1. Open the Mobile 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:

Name	urn:ibm:security:fiberlink:maas360
Description	Fiberlink MaaS360 Policy Information Point.
URL	https://<MAAS360_HOST> For example: https://services.fiberlink.com
Username	<MaaS360_Administrator_Username>
Password	<Maas360_Administrator_Password>
App Access Key	<MaaS360 App Access Key> For example: abcdef1234
App Version	<MaaS360 App Version> For example: 1
App ID	<MaaS360 App ID> For example: com.123456789.maas360
Billing ID	<MaaS360 Billing ID> For example: 123456789
Platform ID	<MaaS360 Platform ID> For example: 3
Certificate Database	rt_profile_keys.kdb

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. Click **Save**.
7. Deploy the pending changes.

After publishing the policy, proceed to [Chapter 5: Running the Sample Application](#).

Chapter 4: SDK based access using JavaScript PIP rule file

The following sections detail the steps that are required to use the Fiberlink MaaS360 JavaScript PIP rule file for MaaS360 SDK based applications or wrapped apps.

Fiberlink MaaS360 SDK app code updates

Fiberlink MaaS360 SDK apps do not natively insert a device ID to allow the PIP to lookup the device in the MaaS360 inventory.

To use the PIP, MaaS360 SDK apps or apps wrapped in the MaaS360 SDK must be updated to retrieve the device ID and pass this to IBM Security Access Manager for Web.

Using the MaaS360 SDK to provide the device ID

Update the MaaS360 SDK app, or existing app wrapped in the MaaS360 SDK to retrieve the device ID and populate a HTTP request header with the value.

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 app was written with and inserted into the code stream where any HTTP requests are made from the app which will access backend resources protected by IBM Security Access Manager for Web.

Ensure the app will handle responses from access policy evaluation which may alter the flow of execution, for example device registration or deny results.

Web Gateway Appliance configuration

Modify the IBM Security Access Manager for Web configuration file to populate the `urn:ibm:security:fiberlink:maas360:device:ids` attribute used by the PIP to retrieve the device attributes from MaaS360.

Configuring the Web Reverse Proxy

IBM Security Access Manager for Web must populate the attribute which is extracted from the HTTP request header containing the MaaS360 device ID.

1. Open the Web Gateway Appliance 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.

Mobile Appliance configuration

Configure IBM Security Access Manager for Mobile to call the Fiberlink MaaS360 JavaScript PIP rule file.

Creating an instance of the JavaScript PIP

1. Open the Mobile Appliance Web console.

2. Select **Secure Mobile Settings** → **Policy** → Information Points.
3. Click the **New** button.
4. Select **JavaScript**.
5. Enter the PIP details on the **General** tab:

Name	urn:ibm:security:fiberlink:maas360
Description	Fiberlink MaaS360 Policy Information Point.
Script	<Path-To-Integration>/maas360_pip_rule.js

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. Select the **Properties** tab.
7. Create new properties for each connection item associated with the Web Service API by clicking the **New Property** button.

MAAS_ADMIN_USERNAME	<MaaS360_Administrator_Username>
MAAS_ADMIN_PASSWORD	<MaaS360_Administrator_Password>
APP_ACCESS_KEY	<MaaS360 App Access Key> For example: abcdef1234
APP_VERSION	<MaaS360 App Version> For example: 1
APP_ID	<MaaS360 App ID> For example: com.123456789.maas360
BILLING_ID	<MaaS360 Billing ID> For example: 123456789
PLATFORM_ID	<MaaS360 Platform ID> For example: 3
MAAS_URL	<maas360host> For example: services.fiberlink.com

Note: The JavaScript PIP instance will use the `rt_profile_keys` key database.

8. Click **Save**.
9. Deploy the changes.

After updating the app, configuring the IBM Security Access Manager for Web attribute and creating the JavaScript PIP instance, proceed to [Chapter 5: Running the Sample Application](#).

Chapter 5: Running the Sample Application

The following sections detail the steps required to test this integration using a sample protected resource.

In the high level tests:

- testuser1 will not have their device registered in IBM Security Access Manager or their device enrolled in MaaS360
- testuser2 will have their device registered and enrolled.

Ensure you revert the device registration and enrollment between test scenarios.

Note: Only one of the PIPs may be configured at any one time.

The testing scenario for browser based access using the Fiberlink MaaS360 PIP is complex due to the possible combinations of device registration in IBM Security Access Manager and device enrollment in Fiberlink MaaS360.

For example:

IBM Security Access Manager registered?	Fiberlink MaaS360 enrolled?	Device lookup mechanism	Possible sample policy use cases
N	N	Partial device mapping using attribute collection service	Consent register device in IBM Security Access Manager and optional: HTTP redirect to MaaS360 enrollment.
Y	N	Partial device mapping using attribute collection service or Direct mapping using the populated custom attribute	Deny or HTTP redirect to MaaS360 enrollment.

		ISAMDeviceID in Fiberlink MaaS360.	
N	Y	Partial device mapping using attribute collection service	Consent register device in IBM Security Access Manager or Permit based on device attribute policy.
Y	Y	Partial device mapping using attribute collection service or Direct mapping using the populated custom attribute ISAMDeviceID in Fiberlink MaaS360.	Permit based on device attribute policy.

The testing scenario for SDK based access using Fiberlink MaaS360 JavaScript PIP rule file is simplified as the device does not need to be fingerprinted using the attribute collection service and registered in IBM Security Access Manager. The accessing device will identify itself to IBM Security Access Manager for Web, allowing the PIP to search the MaaS360 inventory directly for that device.

Before you start

This section does not cover the configuration of the entire environment. It focuses on running the test scenarios. References are made to the configuration steps provided in [Chapter 2: IBM Security Access Manager Configuration](#), [Chapter 3: Browser based access using Fiberlink MaaS360 PIP](#) and [Chapter 4: SDK based access using JavaScript PIP rule file](#) and suitable values are suggested where appropriate.

Ensure you have access to at least two devices with differing hardware and the ability to install and configure the MaaS360 client on those devices.

Web Gateway Appliance configuration

Complete all of the steps that are detailed in the [Chapter 2: IBM Security Access Manager Configuration](#) section.

Sample user account creation

When running the sample application, different user accounts must be tested to ensure that data is being extracted from MaaS360 and policy is being enforced correctly.

Using the **pdadmin** command-line utility, create user accounts for the tests. You must ensure that the DNs for the user accounts are appropriately matched with the Base DN configured in your LDAP server.

For example:

```
pdadmin sec_master> user create testuser1 cn=testuser1,dc=iswga test
user1 password1
pdadmin sec_master> user modify testuser1 account-valid yes
pdadmin sec_master> user create testuser2 cn=testuser2,dc=iswga test
user2 password2
pdadmin sec_master> user modify testuser2 account-valid yes
```

MaaS360 Configuration

At least one device must to be registered to successfully extract device attributes used in the sample access policy.

Ensure there is a direct username mapping from MaaS360 to the user ID in IBM Security Access Manager. Where possible, use the Cloud Extender to integrate with your Corporate User Directory to import group and associated user information.

Fiberlink MaaS360 PIP

If your are using the browser based access using the Fiberlink MaaS360 PIP, ensure the custom attribute is created.

Complete the steps in [Chapter 3: Browser based access using Fiberlink MaaS360 PIP](#).

Fiberlink MaaS360 JavaScript PIP rule file

If you are using SDK apps ensure you have updated your app code to extract the device ID and pass this as a HTTP request header where ever the app accesses a backend resource protected by IBM Security Access Manager for Web.

Complete the steps in [Chapter 4: SDK based access using JavaScript PIP rule file](#).

Testing the PIP invocation and policy evaluation

Ensure the pre-requisite steps for the desired PIP have been completed, a sample protected resource junction has been created and access policy has been authored, attached and published.

Fiberlink MaaS360 PIP

High level steps for testing the PIP functionality can be achieved by simulating the browser based access flow of device registration in IBM Security Access Manager, enrollment in Fiberlink MaaS360 and mapping of device ID by an Administrator.

For example:

1. Launch the mobile web browser accessing the protected resource.
2. Authenticate to IBM Security Access Manager for Web as `testuser1`.
3. Verify access is denied or redirected to Consent Device Registration based on the access policy.
4. Complete the Consent Device Registration steps. Take note of the device name generated, or selected.
5. Access the protected resource.
6. Verify access is denied or redirected to Fiberlink MaaS360 enrollment.
7. Install the Fiberlink MaaS360 client and enroll the device.
8. Launch the mobile web browser accessing the protected resource.
9. Authenticate to IBM Security Access Manager for Web as `testuser1`.
10. Verify access is granted based on the device attribute values referenced in the access policy.
11. Ensure the IBM Security Access Manager device name for `testuser2` has been populated in the `ISAMDeviceID` custom attribute for the corresponding device in the MaaS360 inventory.
12. Launch the mobile web browser accessing the protected resource.

13. Authenticate to IBM Security Access Manager for Web as `testuser2`.
14. Verify access is granted based on the device attribute values referenced in the access policy.

Fiberlink MaaS360 JavaScript PIP rule file

High level steps for testing the PIP functionality can be simulated using sample cURL commands if you do not have access to an MaaS360 SDK app or are unable to deploy the app into production.

For example:

1. Authenticate to IBM Security Access Manager for Web.

For example:

```
curl -kv https://<webseal.ibm.com>/pkmslogin.form -d  
"username=testuser1&password=password1&login-form-type=pwd"
```

2. Record the returned session cookie and include it in subsequent requests.
3. Access the protected resource without passing a device ID.

For example:

```
curl -kv https://<webseal.ibm.com>/TestApp -b "PD-S-SESSION-  
ID=1_2_1_3DdN+nHYIJG8aO5w9Xxe0yHQjXKVMVc6R8x1F+m9mO6wyTmH;"
```

4. Verify access is denied or a redirect to registration is returned.
5. Authenticate to IBM Security Access Manager for Web.

For example:

```
curl -kv https://<webseal.ibm.com>/pkmslogin.form -d  
"username=testuser2&password=password2&login-form-type=pwd"
```

6. Record the returned session cookie and include it in subsequent requests.
7. Access the protected resource passing a value for device ID.

For example:

```
curl -kv https://<webseal.ibm.com>/TestApp -b "PD-S-SESSION-  
ID=1_2_1_SP1Gj4xnDFWHA4MivBD6kXAC19RY3nzdO0IWkp4eU4S2eQG" -H "x-fl-  
device-id: Android363c8bf76cb6bcbf"
```

8. Verify access is granted based on the device attribute values referenced in the access policy.

Chapter 6: Troubleshooting

Enabling the PIP trace will help identify potential errors in configuration or connectivity.

To enable tracing:

1. Open the Mobile Appliance Web console.
2. Select **Monitor Analysis and Diagnostics** → **Runtime Tracing**.
3. Update **Tracing Specification** to include:
`com.tivoli.am.rba.pip.*=ALL`
4. If using the JavaScript rule file, also include:
`com.tivoli.am.rba.extensions.PluginUtils=ALL:com.ibm.security.access.httpclient.*=ALL`
5. Click **Save**.
6. Deploy the pending changes.

To review the trace file generated:

1. Open the Mobile 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.

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

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some 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:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp. _enter the year or years_. 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® 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.