IBM® MessageSight™ Virtual Appliance Configuration for MaaS360

IBM MessageSight can be configured with MaaS360 to deliver notifications to Android devices.

This can be used as an alternative to Google Cloud Messaging (GCM) notification.

Prerequisites

1. Deploy IBM MessageSight virtual appliance version 1.2 using IBM MessageSight's installation documentation.
2. Procure a trusted SSL certificate.

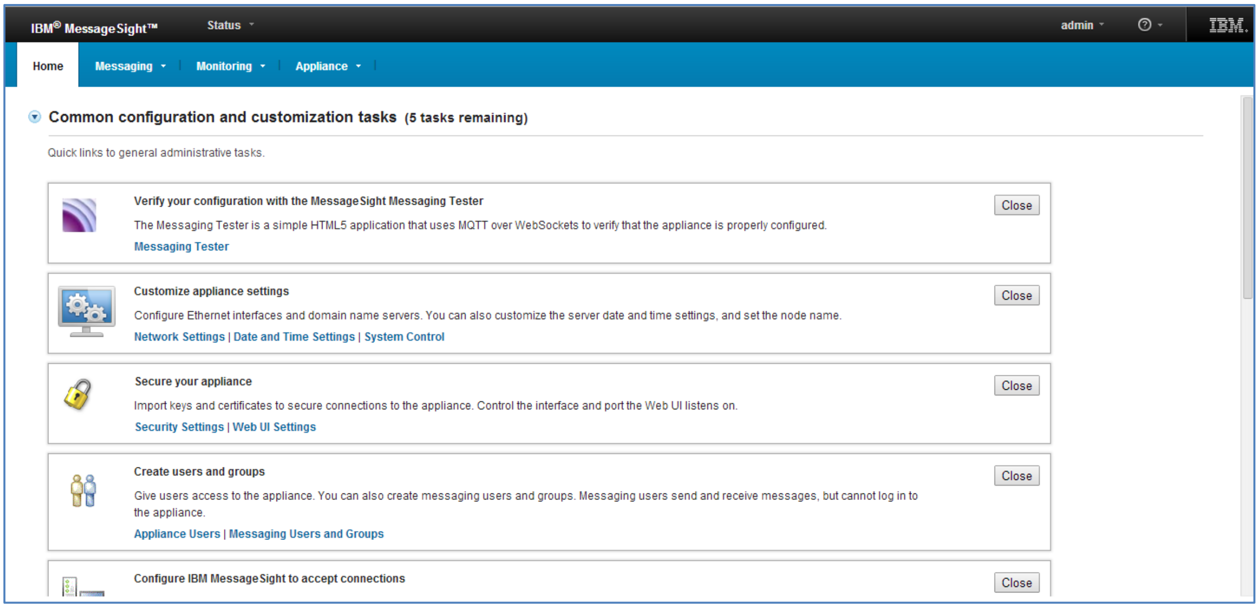
MessageSight Configuration

1. Log in to IBM MessageSight (https://xx.xx.xx.xx:9087/login.jsp , where *xx.xx.xx.xx* is the IP address set earlier).

   Username: *admin*
   Password: *admin*

   Change the port number, if it has changed.

2. After successfully logging in, the following screen appears:



Common configuration and customization tasks (5 tasks remaining)

Quick links to general administrative tasks.

Verify your configuration with the MessageSight Messaging Tester

The Messaging Tester is a simple HTML5 application that uses MQTT over WebSockets to verify that the appliance is properly configured.

Messaging Tester

Customize appliance settings

Configure Ethernet interfaces and domain name servers. You can also customize the server date and time settings, and set the node name.

Network Settings | Date and Time Settings | System Control

Secure your appliance

Import keys and certificates to secure connections to the appliance. Control the interface and port the Web UI listens on.

Security Settings | Web UI Settings

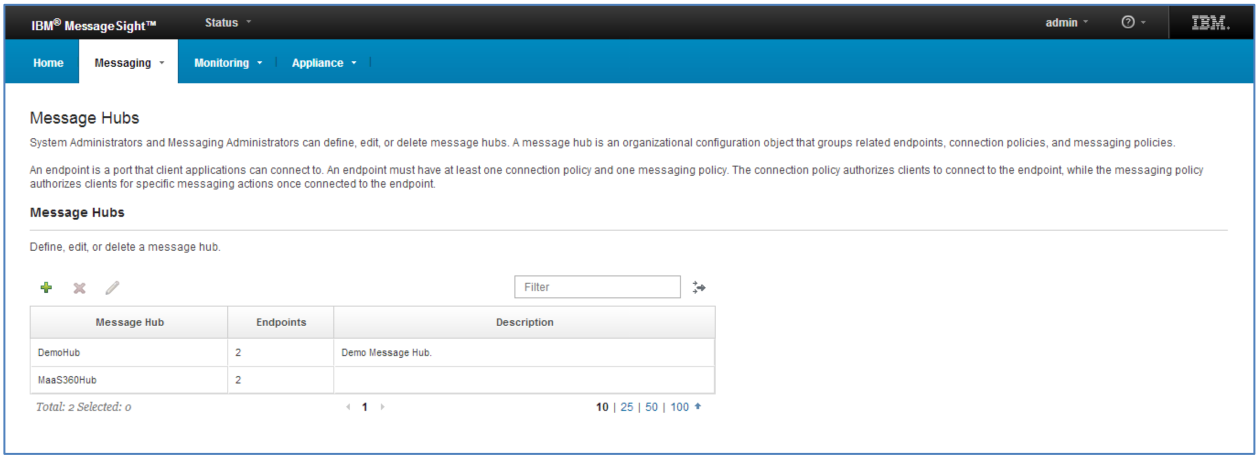
Create users and groups

Give users access to the appliance. You can also create messaging users and groups. Messaging users send and receive messages, but cannot log in to the appliance.

Appliance Users | Messaging Users and Groups

Configure IBM MessageSight to accept connections

3. Select **Messaging > Message Hub** to display a list of Message Hubs:



Message Hubs

System Administrators and Messaging Administrators can define, edit, or delete message hubs. A message hub is an organizational configuration object that groups related endpoints, connection policies, and messaging policies.

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy. The connection policy authorizes clients to connect to the endpoint, while the messaging policy authorizes clients for specific messaging actions once connected to the endpoint.

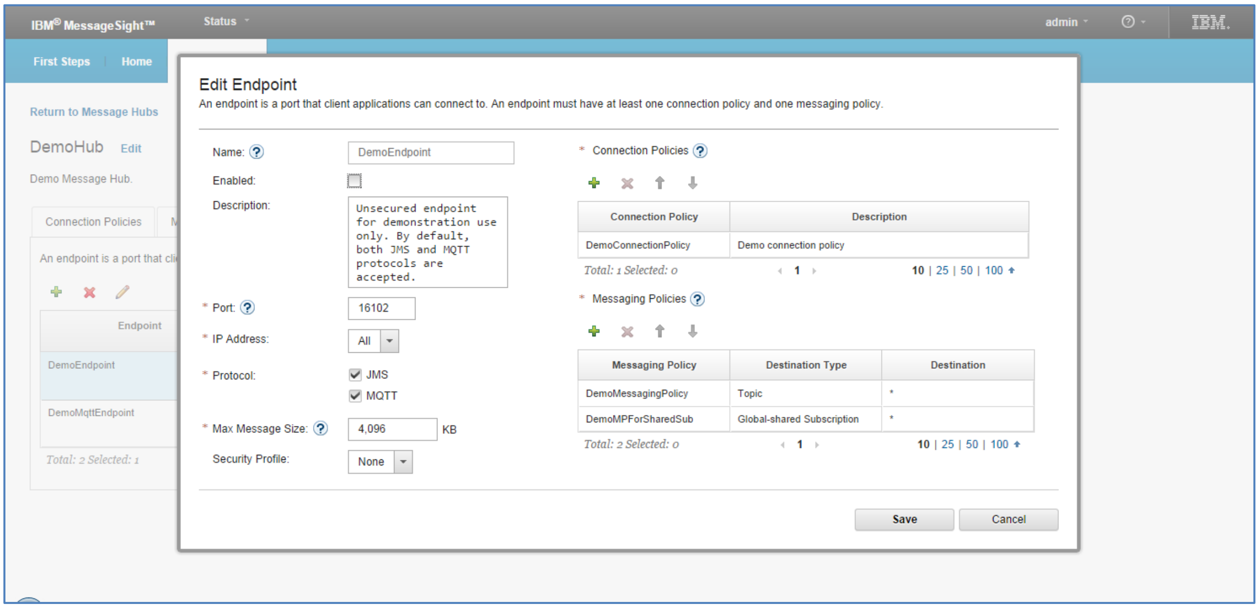
Message Hubs

Define, edit, or delete a message hub.

Message Hub	Endpoints	Description
DemoHub	2	Demo Message Hub.
MaaS360Hub	2	

Total: 2 Selected: 0

4. Open DemoHub. Clear the **Enabled** checkbox to disable both endpoints.



Edit Endpoint

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy.

Name: DemoEndpoint

Enabled: □

Description:

```
Unsecured endpoint
for demonstration use
only. By default,
both JMS and MQTT
protocols are
accepted.
```

* Port: 16102

* IP Address: All

* Protocol: ☑ JMS ☑ MQTT

* Max Message Size: 4,096 KB

Security Profile: None

* Connection Policies

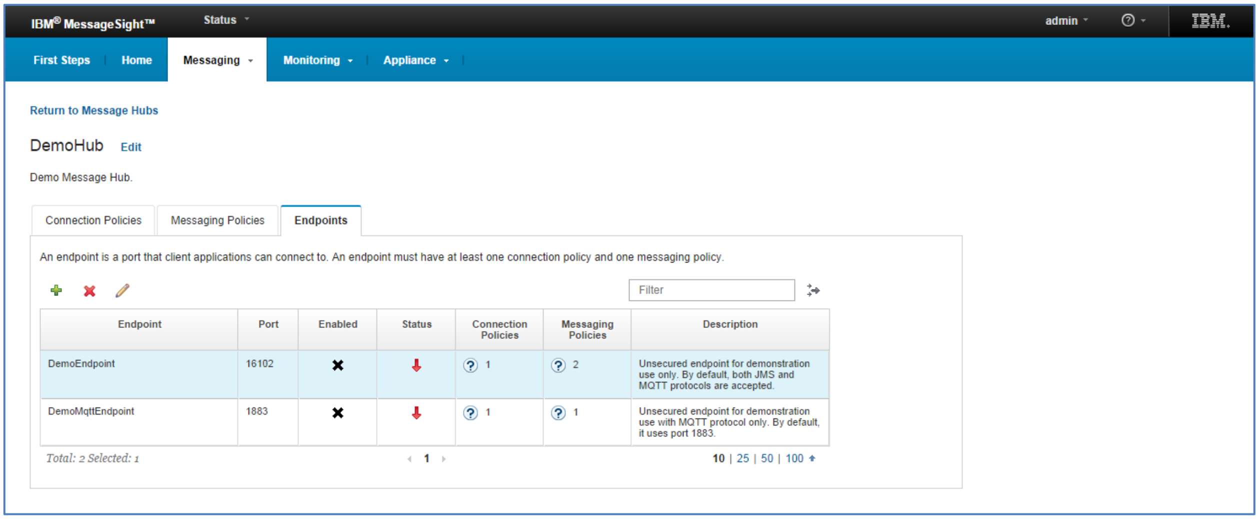
Connection Policy	Description
DemoConnectionPolicy	Demo connection policy

Total: 1 Selected: 0

* Messaging Policies

Messaging Policy	Destination Type	Destination
DemoMessagingPolicy	Topic	*
DemoMPForSharedSub	Global-shared Subscription	*

Total: 2 Selected: 0



DemoHub

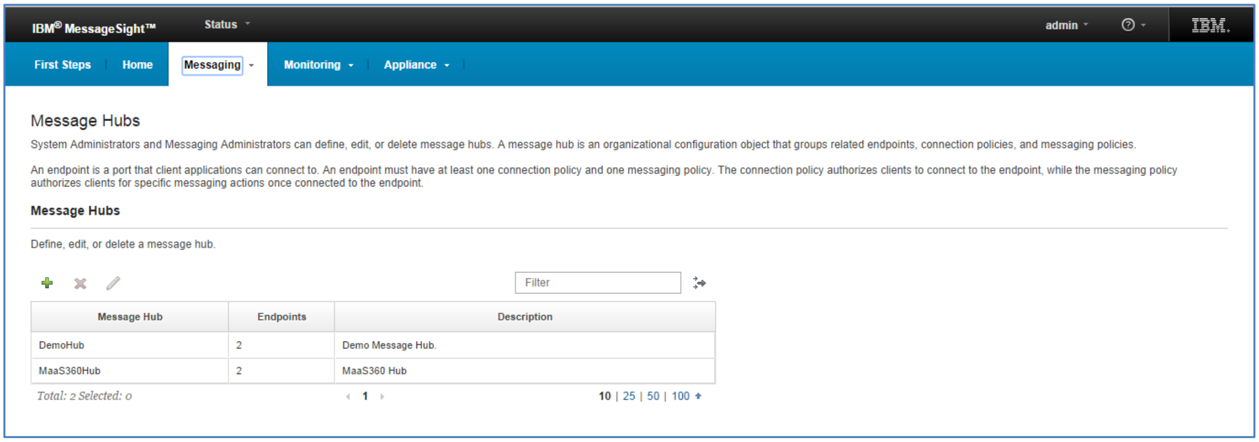
Demo Message Hub.

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy.

Endpoint	Port	Enabled	Status	Connection Policies	Messaging Policies	Description
DemoEndpoint	16102	✗	↓	? 1	? 2	Unsecured endpoint for demonstration use only. By default, both JMS and MQTT protocols are accepted.
DemoMqttEndpoint	1883	✗	↓	? 1	? 1	Unsecured endpoint for demonstration use with MQTT protocol only. By default, it uses port 1883.

Total: 2 Selected: 1　1　10 | 25 | 50 | 100

5. Add a new message hub by entering *MaaS360Hub* as the name.



Message Hubs

System Administrators and Messaging Administrators can define, edit, or delete message hubs. A message hub is an organizational configuration object that groups related endpoints, connection policies, and messaging policies.

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy. The connection policy authorizes clients to connect to the endpoint, while the messaging policy authorizes clients for specific messaging actions once connected to the endpoint.

Message Hubs

Define, edit, or delete a message hub.

Message Hub	Endpoints	Description
DemoHub	2	Demo Message Hub.
MaaS360Hub	2	MaaS360 Hub

Total: 2 Selected: 0　1　10 | 25 | 50 | 100

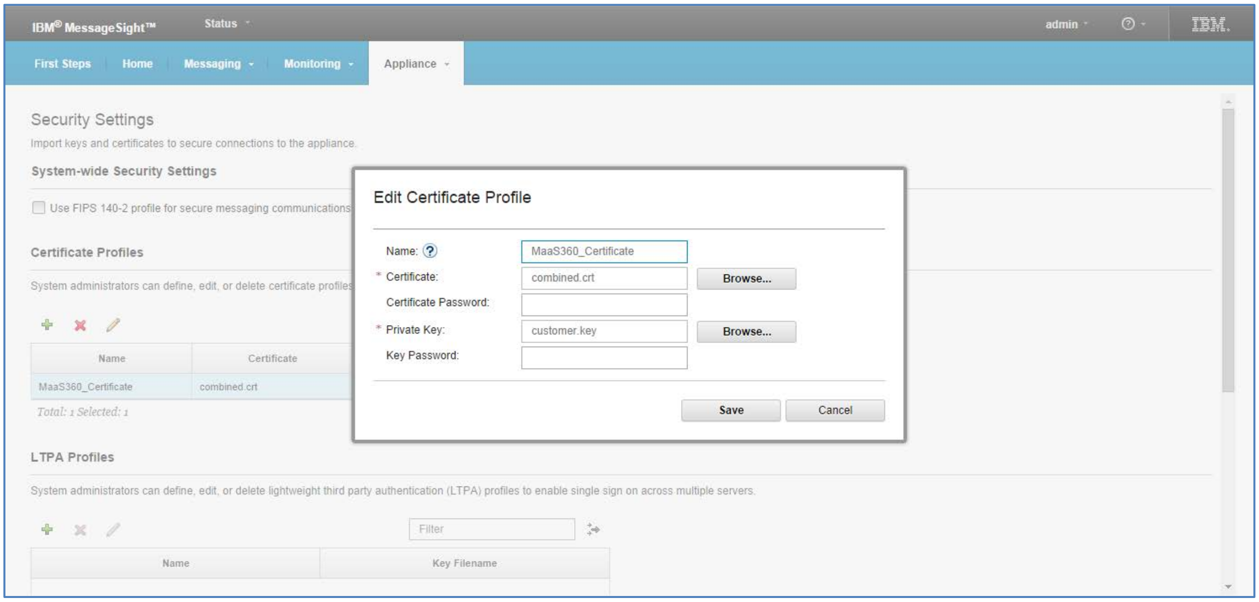
6. Configure Security Settings

    a. Navigate to Appliance > Security Settings
    b. Create a new Certificate Profile called *MaaS360_Certificate*

       A Certificate Profile is created by uploading the SSL certificate, its server certificate chain and its private key. The server certificate should be issued by a trusted CA.

Note: *You should concatenate the SSL certificate and all intermediate CAs into a single file and upload that in the Certificate prompt shown in the graphic below.*

    c. Upload the certificate chain file and the private key.



Security Settings

Import keys and certificates to secure connections to the appliance.

System-wide Security Settings

☐ Use FIPS 140-2 profile for secure messaging communications

Certificate Profiles

System administrators can define, edit, or delete certificate profiles

Name	Certificate
MaaS360_Certificate	combined.crt

Total: 1 Selected: 1

LTPA Profiles

System administrators can define, edit, or delete lightweight third party authentication (LTPA) profiles to enable single sign on across multiple servers.

Filter

Name	Key Filename

Edit Certificate Profile

Name: MaaS360_Certificate

* Certificate: combined.crt Browse...

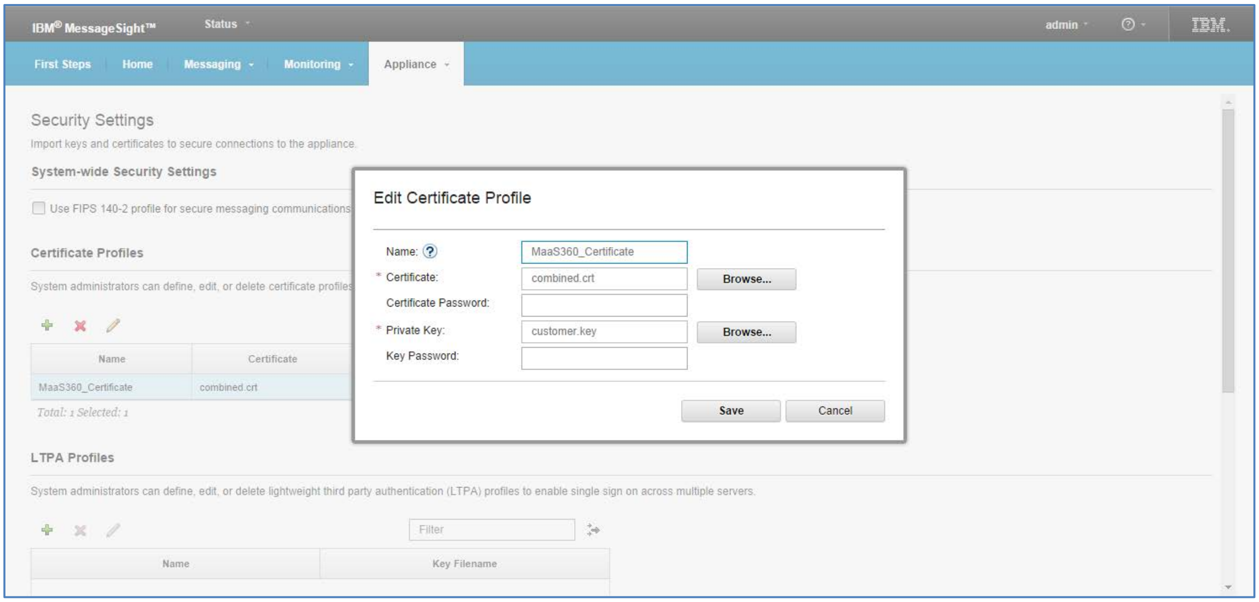
Certificate Password:

* Private Key: customer.key Browse...

Key Password:

Save Cancel

7. Configure Security Profiles:
   a. Navigate to **Appliance > Security Settings**
   b. Create a new security profile called *MaaS360Security*
   c. The security profile is created by selecting the certificate profile created previously
   d. **Minimum Protocol Method**: *TLSv1*
   e. **Ciphers**: *Medium*
   f. **Client Certificate Authentication**: Selected (enabled)
   g. **Certificate Profile**: *MaaS360_Certificate*
   h. **Use password Authentication**: Cleared (disabled)



Security Settings

Import keys and certificates to secure connections to the appliance.

System-wide Security Settings

☐ Use FIPS 140-2 profile for secure messaging communications

Certificate Profiles

System administrators can define, edit, or delete certificate profiles

Name	Certificate
MaaS360_Certificate	combined.crt

Total: 1 Selected: 1

LTPA Profiles

System administrators can define, edit, or delete lightweight third party authentication (LTPA) profiles to enable single sign on across multiple servers.

Filter

Name	Key Filename

Edit Certificate Profile

Name: MaaS360_Certificate

* Certificate: combined.crt Browse...

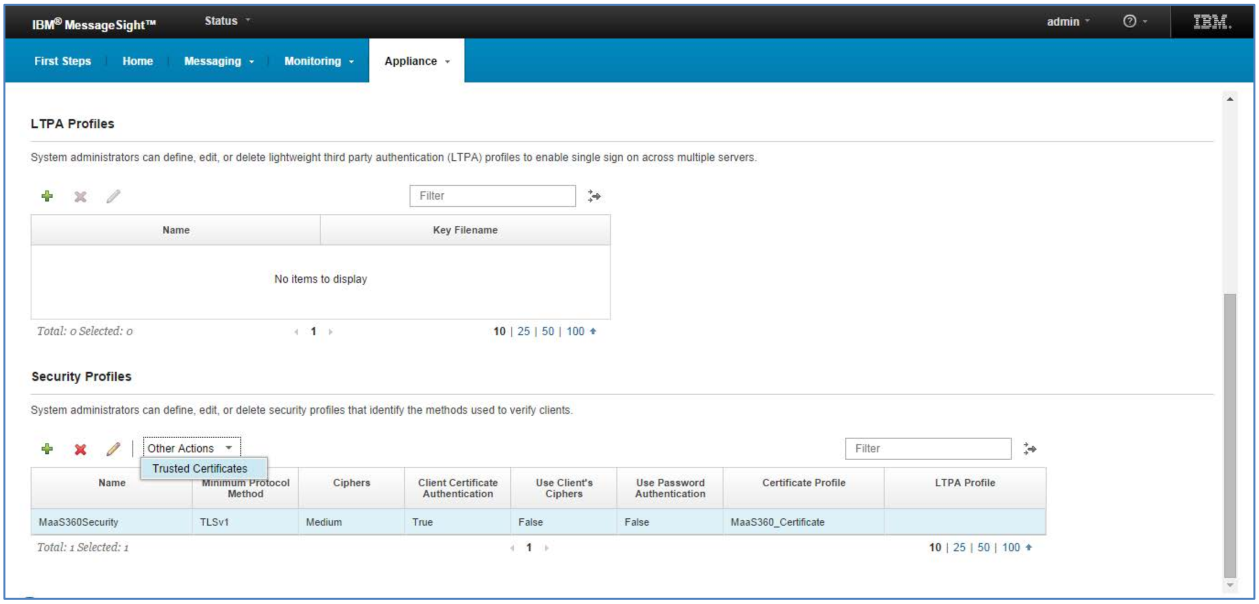
Certificate Password:

* Private Key: customer.key Browse...

Key Password:

Save Cancel

i. Add trusted certificates



LTPA Profiles

System administrators can define, edit, or delete lightweight third party authentication (LTPA) profiles to enable single sign on across multiple servers.

Name	Key Filename
No items to display	

Total: 0 Selected: 0 ‹ 1 › 10 | 25 | 50 | 100

Security Profiles

System administrators can define, edit, or delete security profiles that identify the methods used to verify clients.

Name	Minimum Protocol Method	Ciphers	Client Certificate Authentication	Use Client's Ciphers	Use Password Authentication	Certificate Profile	LTPA Profile
MaaS360Security	TLSv1	Medium	True	False	False	MaaS360_Certificate	

Total: 1 Selected: 1 ‹ 1 › 10 | 25 | 50 | 100

After selecting the security profile, the Trusted Certificates can be uploaded using **Other Actions**.

The MaaS360 Root CA and the Device Sub CA public certificates must be uploaded to this trusted certificates list.

They can be downloaded from the MaaS360 Admin Console by performing the following steps:

i. Log on to the MaaS360 Admin Console

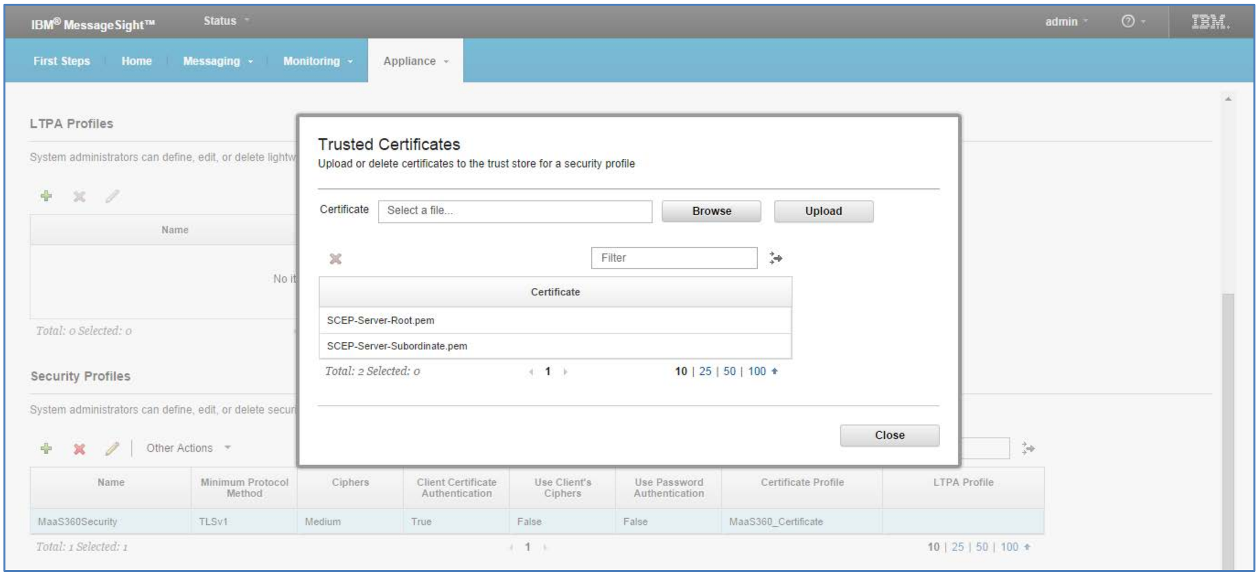
ii. Select the **Troubleshooting** tab

iii. Select **Download Certificates**

This will display a list of certificates that are available for download.

iv. Under **Scep Server Certificates** you should see *Scep_Server_Root_Certificate* and *Scep_Server_Subordinate_Certificate*

v. Download the two pem files (`scep-server-root.pem`, `scep-server-subordinate.pem`) and upload them in Trusted Certificates as shown below



LTPA Profiles

System administrators can define, edit, or delete lightw

Name
No it

Total: 0 Selected: 0

Security Profiles

System administrators can define, edit, or delete secur

Name	Minimum Protocol Method	Ciphers	Client Certificate Authentication	Use Client's Ciphers	Use Password Authentication	Certificate Profile	LTPA Profile
MaaS360Security	TLSv1	Medium	True	False	False	MaaS360_Certificate	

Total: 1 Selected: 1 1 10 | 25 | 50 | 100

Trusted Certificates

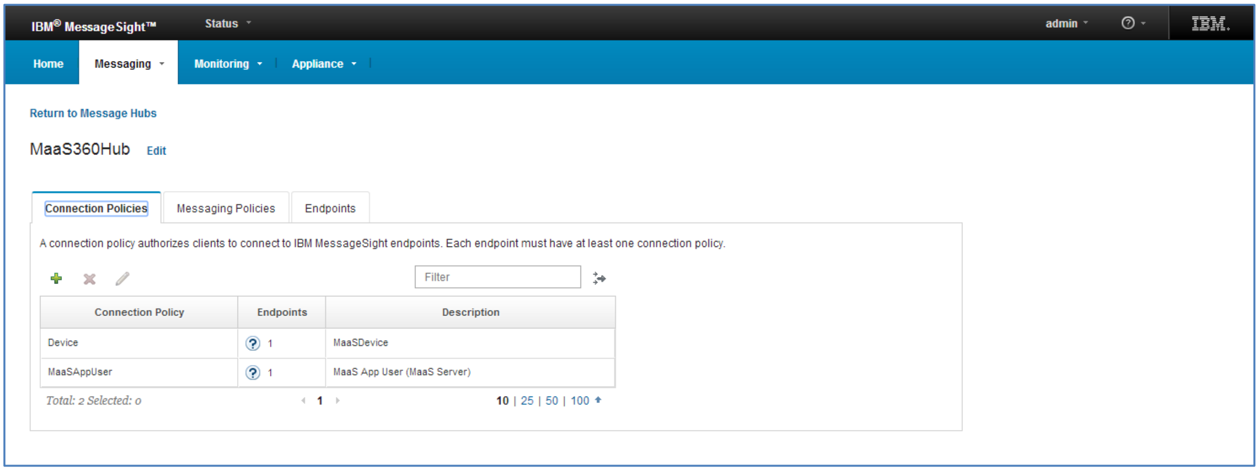
Upload or delete certificates to the trust store for a security profile

Certificate: Select a file...

Certificate
SCEP-Server-Root.pem
SCEP-Server-Subordinate.pem

Total: 2 Selected: 0 1 10 | 25 | 50 | 100

8. Double-click **MaaS360Hub**



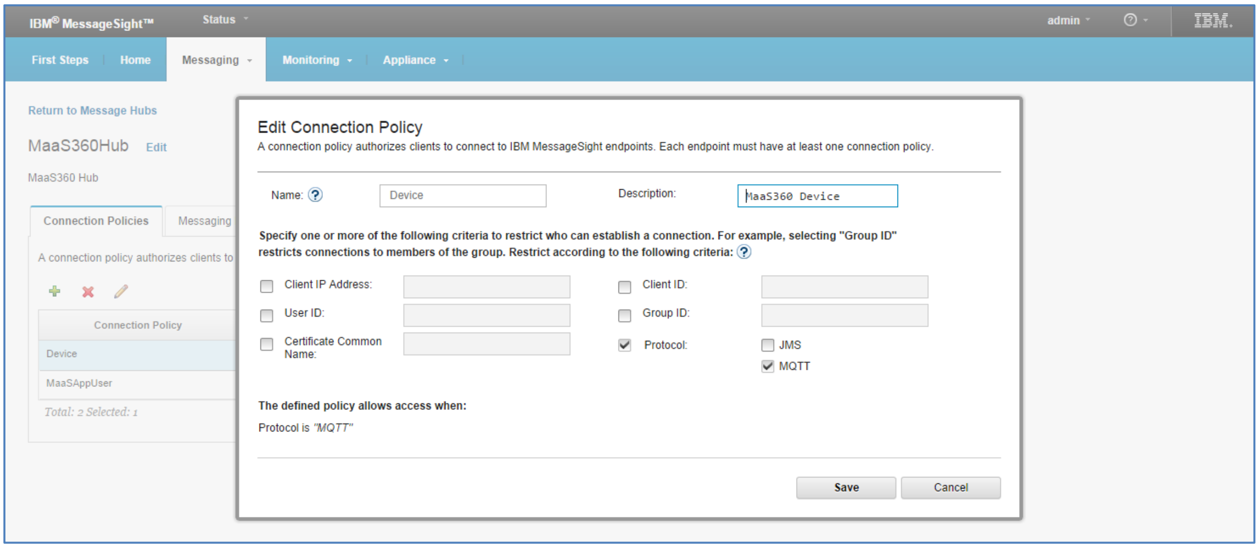
MaaS360Hub

A connection policy authorizes clients to connect to IBM MessageSight endpoints. Each endpoint must have at least one connection policy.

Connection Policy	Endpoints	Description
Device	1	MaaSDevice
MaaSAppUser	1	MaaS App User (MaaS Server)

Total: 2 Selected: 0 1 10 | 25 | 50 | 100

9. On the first tab, Connection Policies, add two connection policies for *Device* and *MaaS App User (MaaS Server)*. The protocol should be *MQTT* only.



Edit Connection Policy

A connection policy authorizes clients to connect to IBM MessageSight endpoints. Each endpoint must have at least one connection policy.

Name: Device

Description: MaaS360 Device

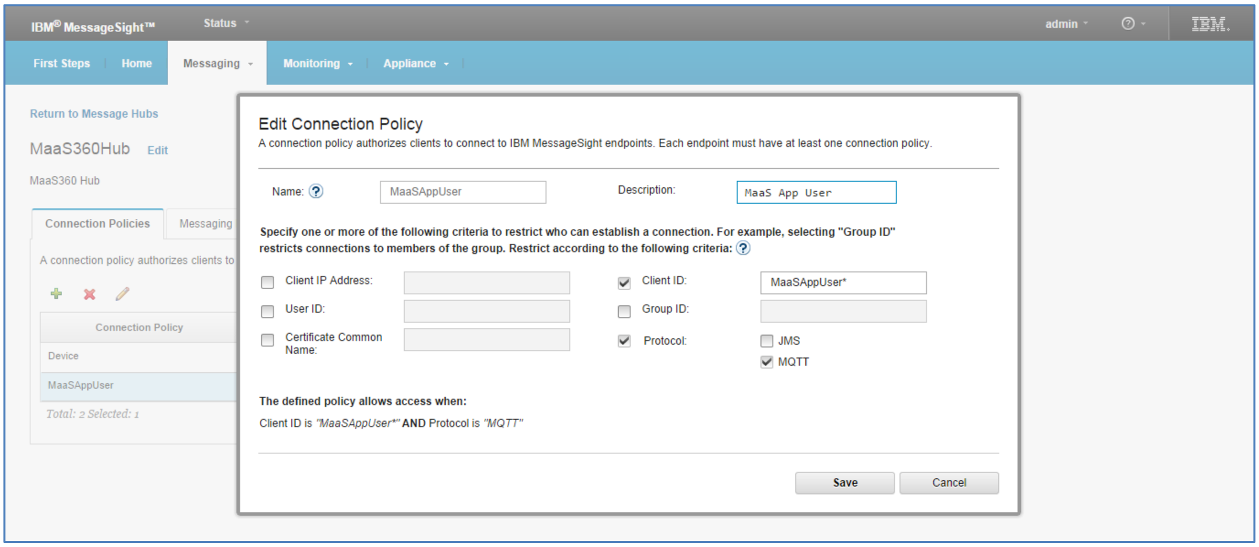
Specify one or more of the following criteria to restrict who can establish a connection. For example, selecting "Group ID" restricts connections to members of the group. Restrict according to the following criteria:

- □ Client IP Address:
- □ User ID:
- □ Certificate Common Name:
- □ Client ID:
- □ Group ID:
- ☑ Protocol: □ JMS ☑ MQTT

The defined policy allows access when:

Protocol is *"MQTT"*

For the MaaS360 App User (MaaS Server) Connection Policy, specify the Client ID as *MaaSAppUser**.



Edit Connection Policy

A connection policy authorizes clients to connect to IBM MessageSight endpoints. Each endpoint must have at least one connection policy.

Name: MaaSAppUser

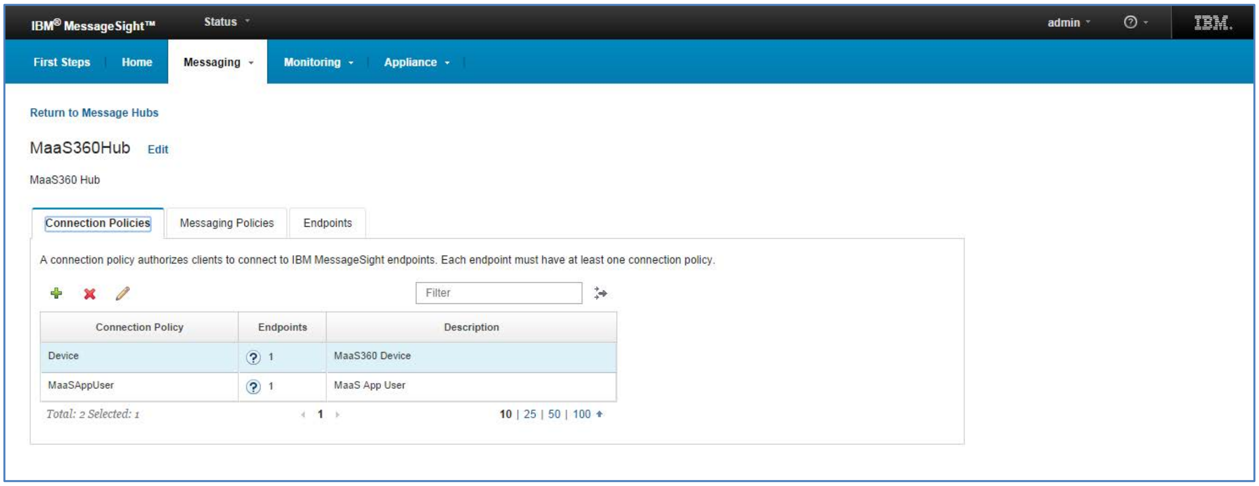
Description: MaaS App User

Specify one or more of the following criteria to restrict who can establish a connection. For example, selecting "Group ID" restricts connections to members of the group. Restrict according to the following criteria:

- □ Client IP Address:
- □ User ID:
- □ Certificate Common Name:
- ☑ Client ID: MaaSAppUser*
- □ Group ID:
- ☑ Protocol: □ JMS ☑ MQTT

The defined policy allows access when:

Client ID is *"MaaSAppUser*"* AND Protocol is *"MQTT"*



MaaS360Hub

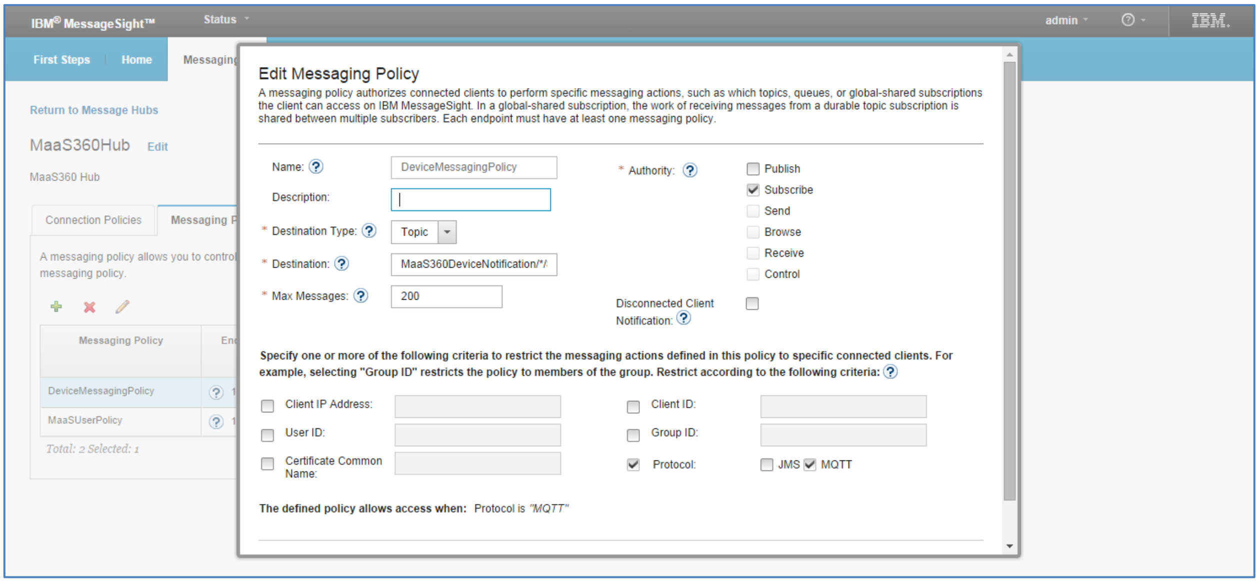
MaaS360 Hub

A connection policy authorizes clients to connect to IBM MessageSight endpoints. Each endpoint must have at least one connection policy.

Connection Policy	Endpoints	Description
Device	1	MaaS360 Device
MaaSAppUser	1	MaaS App User

Total: 2 Selected: 1 ‹ 1 › 10 | 25 | 50 | 100

10. On the next tab, Messaging Policies, add one messaging policy for Devices and another messaging policy for MaaS App User (MaaS Server):
    a. For **DeviceMessagingPolicy**:
        i. **Authority**: *Subscribe*
        ii. **Destination Type**: *Topic*
        iii. **Destination**: *MaaS360DeviceNotification/*/${CommonName}*
        iv. **Max Messages**: *200*
        v. **Protocol**: *MQTT*



Edit Messaging Policy

A messaging policy authorizes connected clients to perform specific messaging actions, such as which topics, queues, or global-shared subscriptions the client can access on IBM MessageSight. In a global-shared subscription, the work of receiving messages from a durable topic subscription is shared between multiple subscribers. Each endpoint must have at least one messaging policy.

Name: DeviceMessagingPolicy
Description:
* Destination Type: Topic
* Destination: MaaS360DeviceNotification/*/
* Max Messages: 200

* Authority: □ Publish ☑ Subscribe □ Send □ Browse □ Receive □ Control

Disconnected Client Notification: □

Specify one or more of the following criteria to restrict the messaging actions defined in this policy to specific connected clients. For example, selecting "Group ID" restricts the policy to members of the group. Restrict according to the following criteria:

□ Client IP Address:
□ User ID:
□ Certificate Common Name:
□ Client ID:
□ Group ID:
☑ Protocol: □ JMS ☑ MQTT

The defined policy allows access when: Protocol is *"MQTT"*

    b. For **MaaSUserPolicy**:

This policy should be used on a separate endpoint on a different port which can be accessed only by MaaS360.

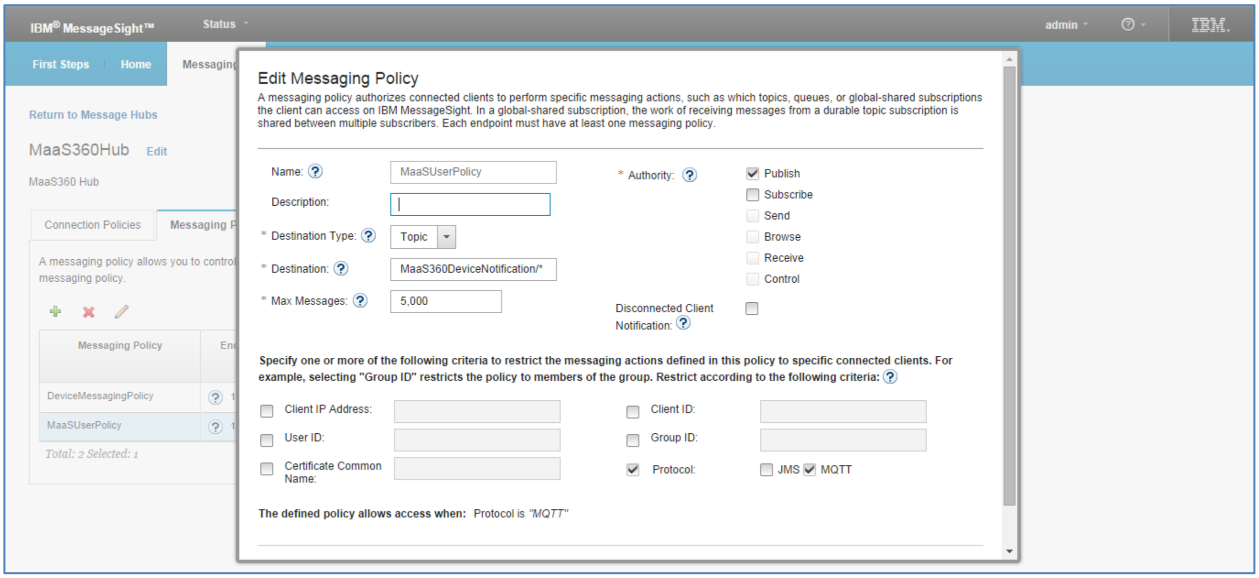
        i. **Authority**: *Publish*

ii. **Destination Type**: *Topic*

iii. **Destination**: *MaaS360DeviceNotification/**

iv. **Max Messages**: *5000*

v. **Protocol**: *MQTT*



Edit Messaging Policy

A messaging policy authorizes connected clients to perform specific messaging actions, such as which topics, queues, or global-shared subscriptions the client can access on IBM MessageSight. In a global-shared subscription, the work of receiving messages from a durable topic subscription is shared between multiple subscribers. Each endpoint must have at least one messaging policy.

Name: MaaSUserPolicy

Description:

* Destination Type: Topic

* Destination: MaaS360DeviceNotification/*

* Max Messages: 5,000

* Authority: ☑ Publish ☐ Subscribe ☐ Send ☐ Browse ☐ Receive ☐ Control

Disconnected Client Notification: ☐

Specify one or more of the following criteria to restrict the messaging actions defined in this policy to specific connected clients. For example, selecting "Group ID" restricts the policy to members of the group. Restrict according to the following criteria:

☐ Client IP Address:

☐ User ID:

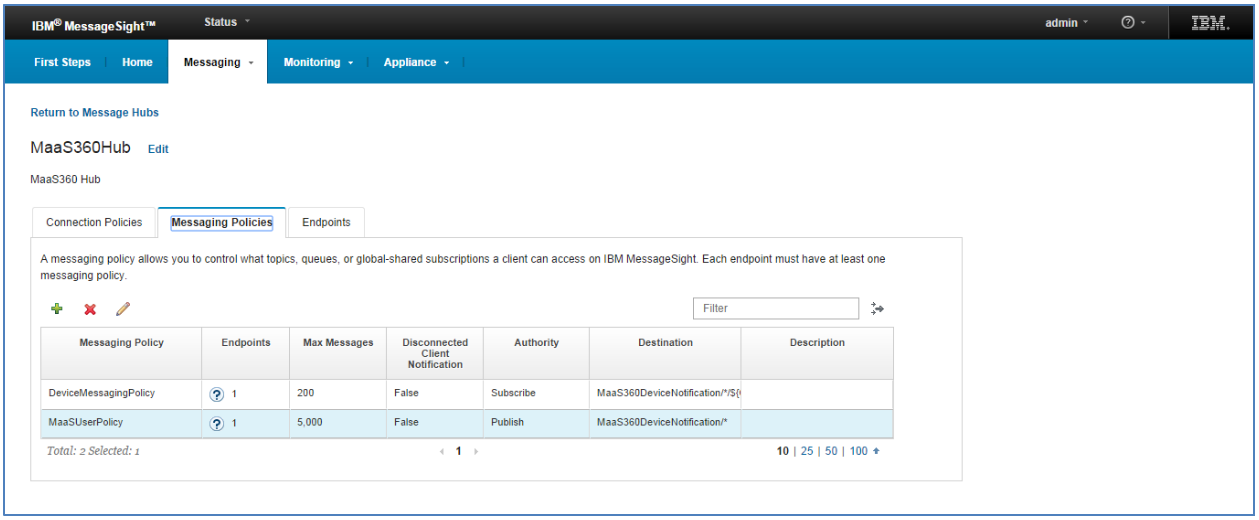
☐ Certificate Common Name:

☐ Client ID:

☐ Group ID:

☑ Protocol: ☐ JMS ☑ MQTT

The defined policy allows access when: Protocol is *"MQTT"*



MaaS360Hub

MaaS360 Hub

A messaging policy allows you to control what topics, queues, or global-shared subscriptions a client can access on IBM MessageSight. Each endpoint must have at least one messaging policy.

Messaging Policy	Endpoints	Max Messages	Disconnected Client Notification	Authority	Destination	Description
DeviceMessagingPolicy	1	200	False	Subscribe	MaaS360DeviceNotification/*/${	
MaaSUserPolicy	1	5,000	False	Publish	MaaS360DeviceNotification/*	

Total: 2 Selected: 1

11. On the next tab, **Connection Endpoints**, add one endpoint policy for Devices and another endpoint policy for MaaS App User (MaaS Server):

   a. For **DeviceMessagingEndpoint**:

      i. **Enabled**: Checked (selected)

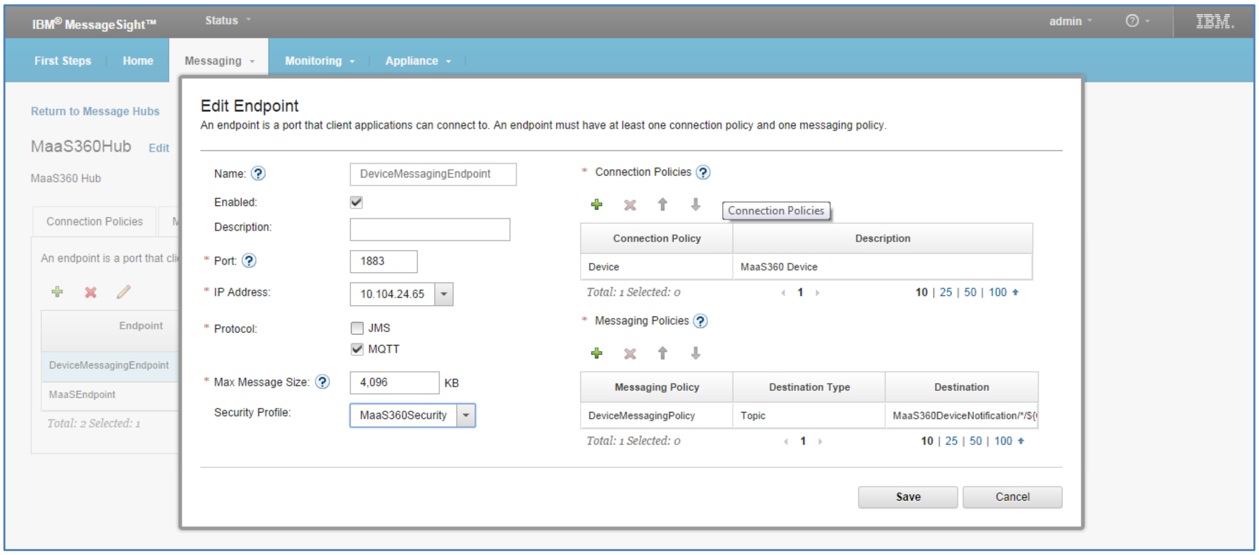
      ii. **Port**: *1883*

      iii. **IP Address**: Enter the IP address of the MessageSight server

      iv. **Protocol**: *MQTT*

v. **Max Message Size**: *4096*

vi. **Security Profile**: *MaaS360Security*



Edit Endpoint

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy.

Name:	DeviceMessagingEndpoint
Enabled:	☑
Description:	
* Port:	1883
* IP Address:	10.104.24.65
* Protocol:	☐ JMS ☑ MQTT
* Max Message Size:	4,096 KB
Security Profile:	MaaS360Security

* Connection Policies

Connection Policy	Description
Device	MaaS360 Device

Total: 1 Selected: 0 1 10 | 25 | 50 | 100

* Messaging Policies

Messaging Policy	Destination Type	Destination
DeviceMessagingPolicy	Topic	MaaS360DeviceNotification/*/${

Total: 1 Selected: 0 1 10 | 25 | 50 | 100

b. For **MaaSEndpoint**:

i. **Enabled**: Checked (selected)

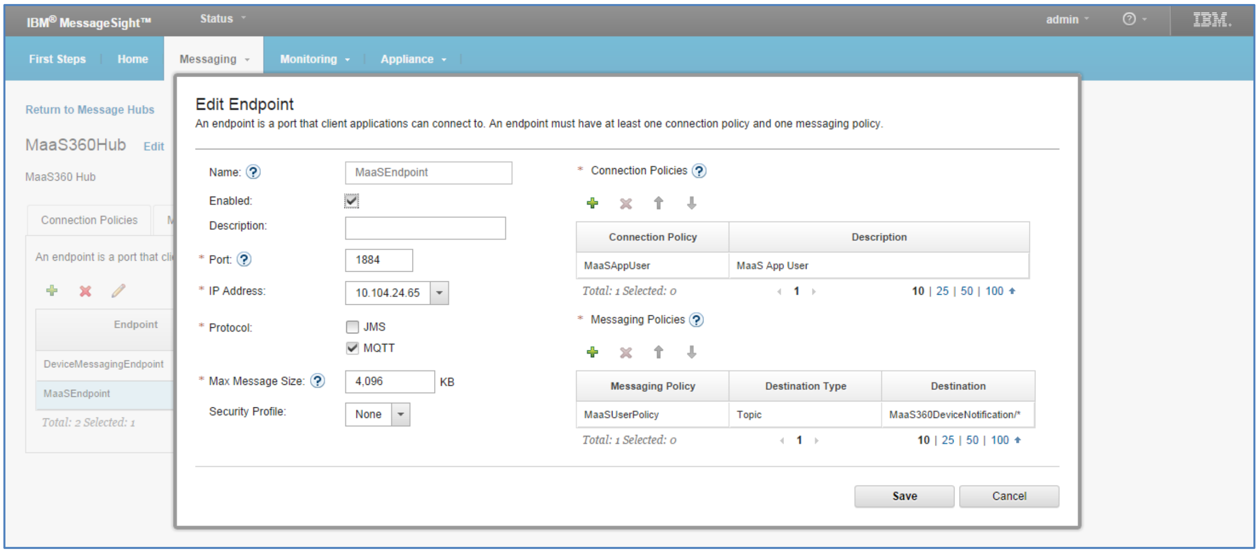
ii. **Port**: *1884*

iii. **IP Address**: Enter the IP address of the MessageSight server

iv. **Protocol**: *MQTT*

v. **Max Message Size**: *4096*

vi. **Security Profile**: *MaaS360Security*



Edit Endpoint

An endpoint is a port that client applications can connect to. An endpoint must have at least one connection policy and one messaging policy.

Name:	MaaSEndpoint
Enabled:	☑
Description:	
* Port:	1884
* IP Address:	10.104.24.65
* Protocol:	☐ JMS ☑ MQTT
* Max Message Size:	4,096 KB
Security Profile:	None

* Connection Policies

Connection Policy	Description
MaaSAppUser	MaaS App User

Total: 1 Selected: 0 1 10 | 25 | 50 | 100

* Messaging Policies

Messaging Policy	Destination Type	Destination
MaaSUserPolicy	Topic	MaaS360DeviceNotification/*

Total: 1 Selected: 0 1 10 | 25 | 50 | 100

Copyright © 2015 Fiberlink, an IBM Company. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Fiberlink Communications Corporation.

All brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Fiberlink Communications Corporation
1787 Sentry Parkway West
Blue Bell, PA 19422

February 2015