

# Inbound SCEP from MobileIron VSP Configuration Guide

## Introduction

Use this guide to configure Inbound Simple Certificate Enrollment Protocol (SCEP) from MobileIron VSP settings in a SecureAuth IdP realm.

The **Network Device Enrollment Service** (NDES) allows software on network and other devices that run without domain credentials to obtain certificates based on SCEP.

SecureAuth IdP supports both Outbound and Inbound from MobileIron SCEP calls.

**Inbound SCEP Calls from MobileIron** are made when the MobileIron server requests a certificate from SecureAuth IdP via SCEP. SecureAuth IdP can then retrieve a certificate from the Cloud Services, or from an on-premises CA, and MobileIron will provide the certificate to the user.

For **Outbound SCEP** configuration, refer to this [guide](#).

## Prerequisites

1. Have MobileIron VSP and access to the server settings
2. Access to the SecureAuth IdP Web Admin and all **Realms** requiring Inbound MobileIron SCEP configuration

## SecureAuth IdP Configuration Steps

These configuration steps are required in each SecureAuth IdP realm that will be utilizing the Inbound MobileIron SCEP calls

### System Info

The screenshot shows the 'SCEP Configuration' section of the SecureAuth IdP System Info page. It contains the following fields:

- Use SCEP: False
- SCEP Web Service URL: Default
- SCEP / NDES URL: SCEP / NDES Listener URL
- Inbound SCEP Request: True (highlighted with a red box)

1. Select **True** from the **Inbound SCEP Request**

No other configuration is required for specifically inbound SCEP calls from MobileIron

If using MobileIron VSP Inbound SCEP calls in addition to Outbound SCEP calls (using existing on-premises CA instead of SecureAuth IdP Cloud Services), distinct configuration is required

### ▼ SCEP Configuration

Use SCEP:	True
SCEP Web Service URL:	Default
SCEP / NDES URL:	SCEP / NDES Listener URL
Inbound SCEP Request:	True

1. Select **True** from the **Use SCEP** dropdown
2. Leave the **SCEP Web Service URL** as the default unless the web service is being hosted in a different location
3. Set the **SCEP / NDES URL** as the **SCEP / NDES Listener URL**
4. Select **True** from the **Inbound SCEP Request**

Click **Save** once the configurations have been completed and before leaving the **System Info** page to avoid losing changes

### License Info

#### ▼ License Info

Company Name:	Company Name
Company GUID:	

5. This information is required for the **MobileIron VSP Configuration Steps** (below)

### SecureAuth IdP IIS Manager Configuration Steps

It is recommended to lock down access of this realm by restricting it to the SCEP Client's IP Address

**Edit IP and Domain Restrictions Settings** ? x

Access for unspecified clients:  
Deny

Enable domain name restrictions

Enable Proxy Mode

Deny Action Type:  
Forbidden

OK Cancel

**Add Allow Restriction Rule** ? x

Allow access for the following IP address or domain name:

Specific IP address:  
[Text Input Field]

IP address range:  
[Text Input Field]  
Mask or Prefix:  
[Text Input Field]

OK Cancel

6. In the **IP Address and Domain Settings** for the realm being configured in the **IIS Manager**, select **Edit Feature Settings** under the **Actions** menu

7. Select **Deny** from the **Access for unspecified clients** dropdown

8. Click **Add Allow Entry**, and supply either the **Specific IP Address** or the **Range of IP** of the MobileIron VSP

## MobileIron VSP Configuration Steps

If using MobileIron Inbound SCEP calls to multiple SecureAuth IdP realms, a new **Profile** will need to be created and configured for each realm

**Modify SCEP Setting** ✕

|

Any changes will impact all devices in the labels to which this setting is applied.

Name:

Description:

Enable Proxy:   Cache locally generated keys on the VSP

User Certificate     Device Certificate

Setting Type:  ▾

URL:

Subject:

Subject Common Name Type:  ▾

Subject Alternative Name Type:  ▾

▾

▾

▾

Key Size:  ▾

Key Usage:  Signing     Encryption

Finger Print:

Challenge Type:  ▾

Issue test certificate:

|

1. In the **Policies & Configs** section, click **Add New - SCEP**
2. Set the **Name** to what will be displayed on the device for this profile, e.g. **SA Certificate**
3. Select **SCEP** from the **Setting Type** dropdown
4. Set the **URL** to the Fully Qualified Domain Name (FQDN) of the SecureAuth IdP appliance, followed by the realm number configured for Inbound SCEP calls, then **/webservice/sceprequest.svc/Request**  
  
 For example, **https://secureauth.company.com/secureauth2/webservice/sceprequest.svc/Request**
5. Set the **Subject** to the **Company GUID** and **Company Name** from the SecureAuth IdP Web Admin in the following format:  
  
**ou=XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX,o=Company Name**
6. Click **Issue Test Certificate** to issue a test certificate in real time, before clicking **Save**
7. Click **Save**

## Troubleshooting / Common Issues

Plug these URLs into a rest client to check connectivity

<https://secureauth.company.com/secureauth#/webservice/sceprequest.svc/Request?operation=Echo&message=test>

<https://secureauth.company.com/secureauth#/webservice/sceprequest.svc/Request?operation=GetCACert&message=test>