TippingPoint
Best Practice Guide

RADIUS PEAP Configuration for IPS Devices and Cisco ACS

Version: 16.1.1

TABLE OF CONTENTS

1. Introduction

This document describes how to configure a Remote Authentication Dial-In User Service (RADIUS) server (for this deployment, a Cisco Secure ACS RADIUS server) and the HP TippingPoint Intrusion Protection System (IPS) device (via SMS or LSM) using PEAP/EAP-MSCHAPv2 authentication for the X.509 certificate chains.

2. Description

The IPS device supports three types of RADIUS authentication:

- PAP
- EAP-MD5-Challenge
- PEAP/EAP-MSCHAPv2

For successful authentication to take place using the PEAP/EAP-MSCHAPv2 protocol, the IPS device must verify (during the RADIUS-PEAP handshake) that the RADIUS server's certificate matches a root certificate on its local certificate store.

To enable authentication, you must configure the entire certificate chain (Root, Intermediate, and Leaf-level) on the RADIUS server, but configure only the Root certificate on the IPS device. The IPS device can then look in its certificate store for the corresponding root CA used by the RADIUS server during the handshake. When the IPS device recognizes the root CA, the RADIUS server sends the remainder of the certificate chain to the IPS and the authentication process is completed.

3. Configure the RADIUS server

A RADIUS server can receive its certificate from either the certificate authority (CA) of your organization or from a public CA.

This sample deployment uses the following certificate chain on a Cisco Secure ACS RADIUS server:

- Root CA – hp-tpt-ca.pem(DaRoot)
- Intermediate CA – hp-tpt-ca-int.pem(Zintermediate)
- Leaf-level Server – hp-tpt-server1.pem(server1.hp-tpt.com)

Note: Certificate files have different extensions (.pem, .crt, .cer) to show different formats used to store them. You can convert them from one format to another using free online tools.

3.1. Install the certificates on the RADIUS server

Note: Three certificates need to be installed on the RADIUS server; **Root, Intermediate** and **Leaf-Level**

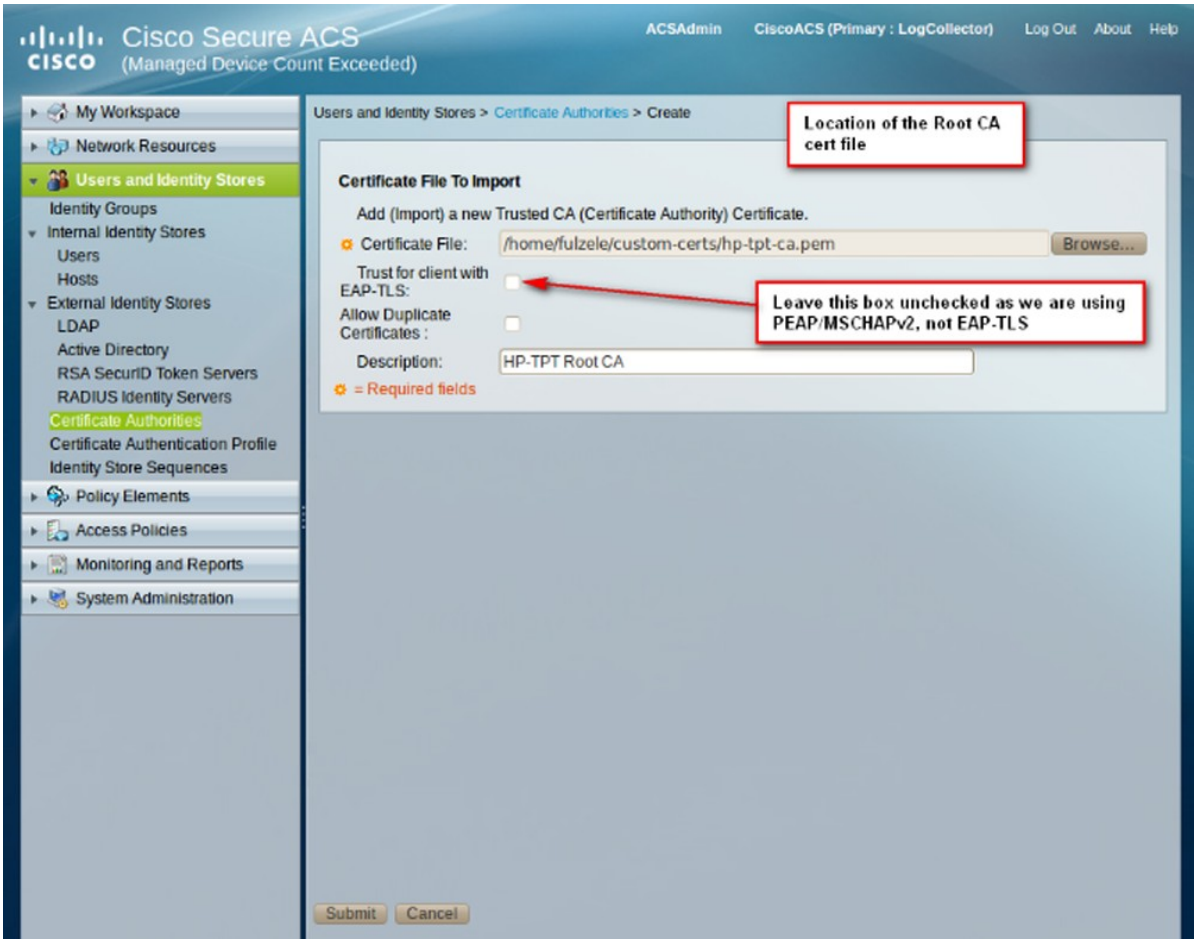
3.1.1. Installing Root and Intermediate certificates

1. On the left menu pane, select **Users and Identify Stores** and then click on **Certificate Authorities**. The right pane shows the list of current certificate authority's configured on the server.

2. Click **Add**. The **"Certificate File to Import"** screen is displayed

3. Click **Browse** and locate the Trusted CA certificate file

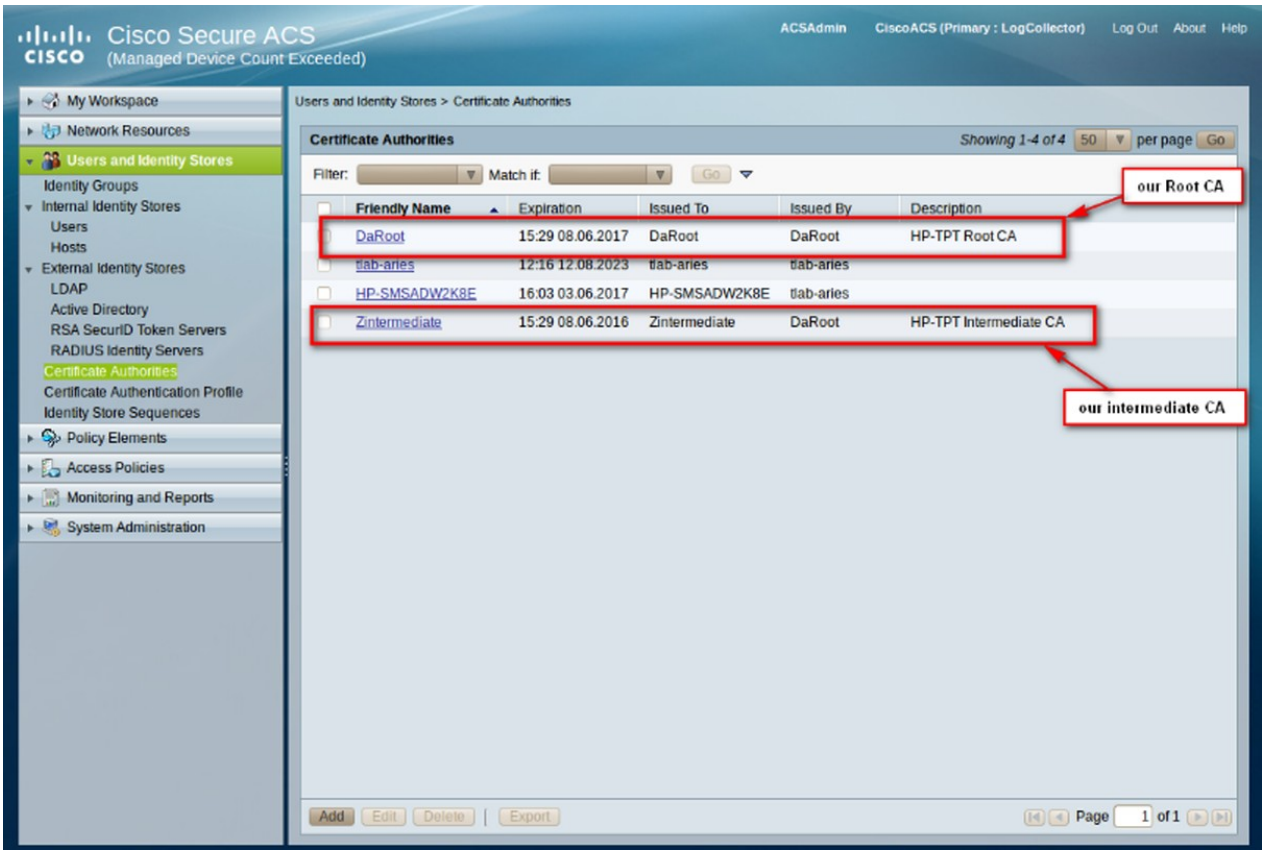
4. Click **Submit**.



You are returned **Certificates Authorities** screen.

5. Repeat the steps 1 thru 4 above for the other certificate.

   Once completed, the **Certificates Authorities** screen will list both the **Root CA** and the **Intermediate CA** certificates you added.



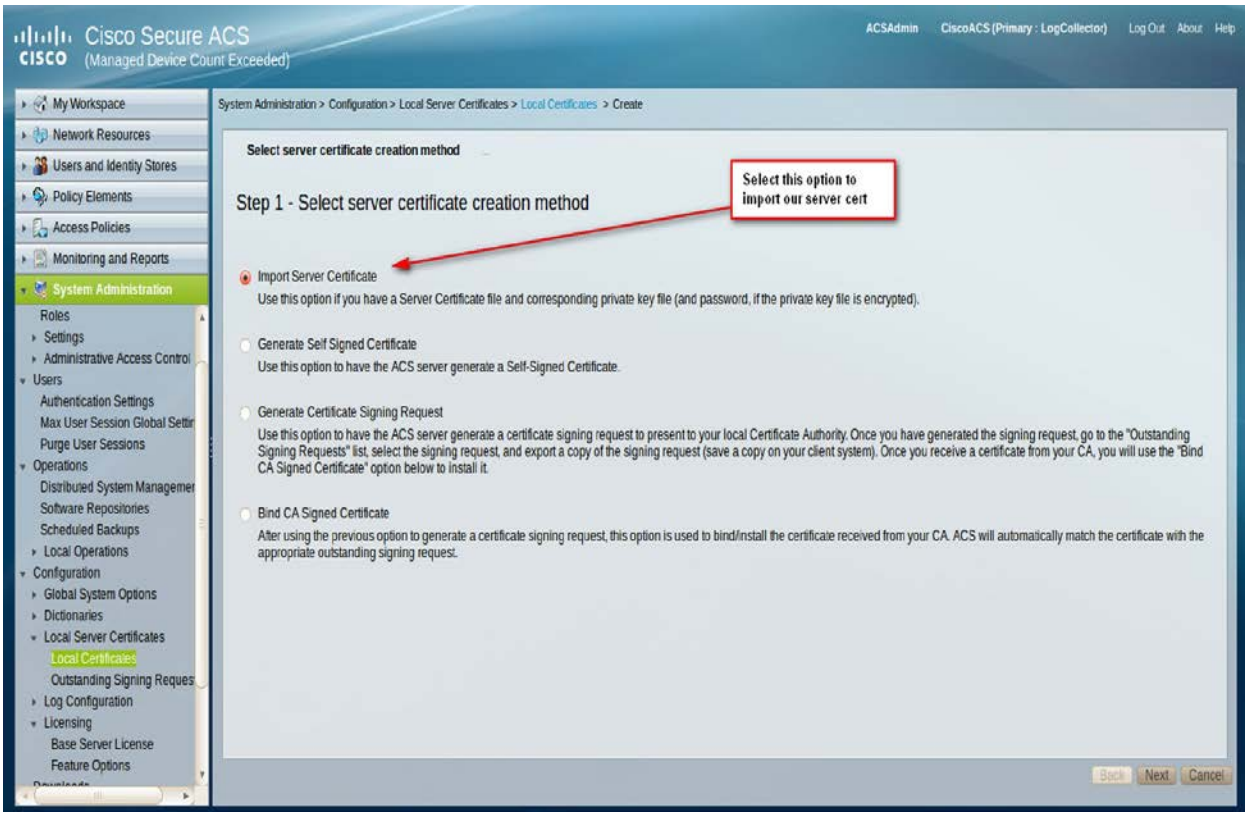
3.1.2. Installing Leaf-level certificates

1. To add the Leaf-level certificate, select **System Administration > Configuration > Local Server Certificates** and click **Local Certificates**.

2. The right pane lists all the local certificates available on the device.

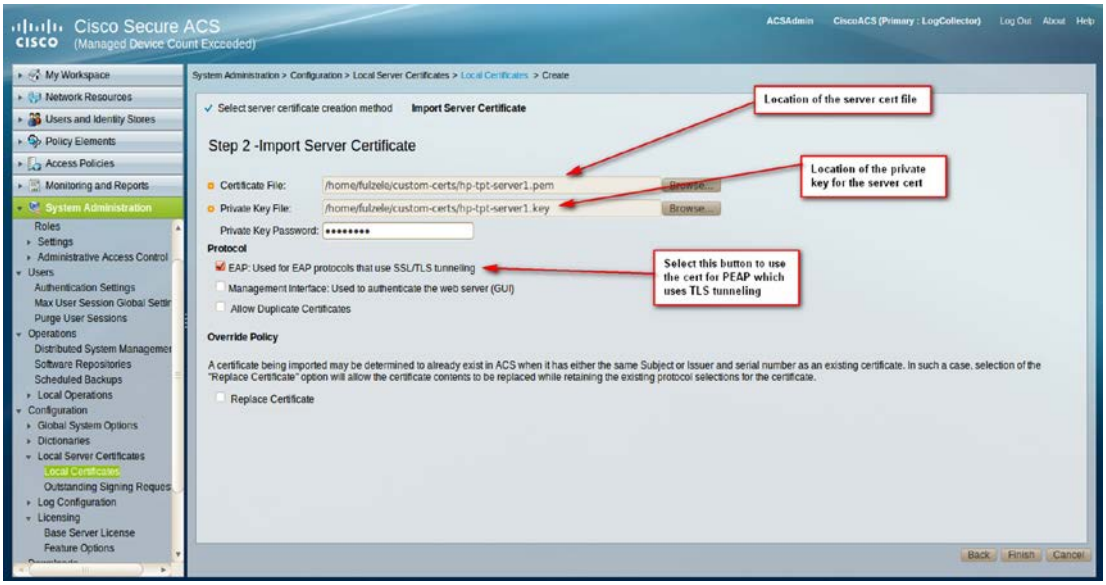
3. Click **Add**.

4. In the **"Step 1: Import Server Certificate"** page, select the **"Import Server Certificate"** option and click **Next**.

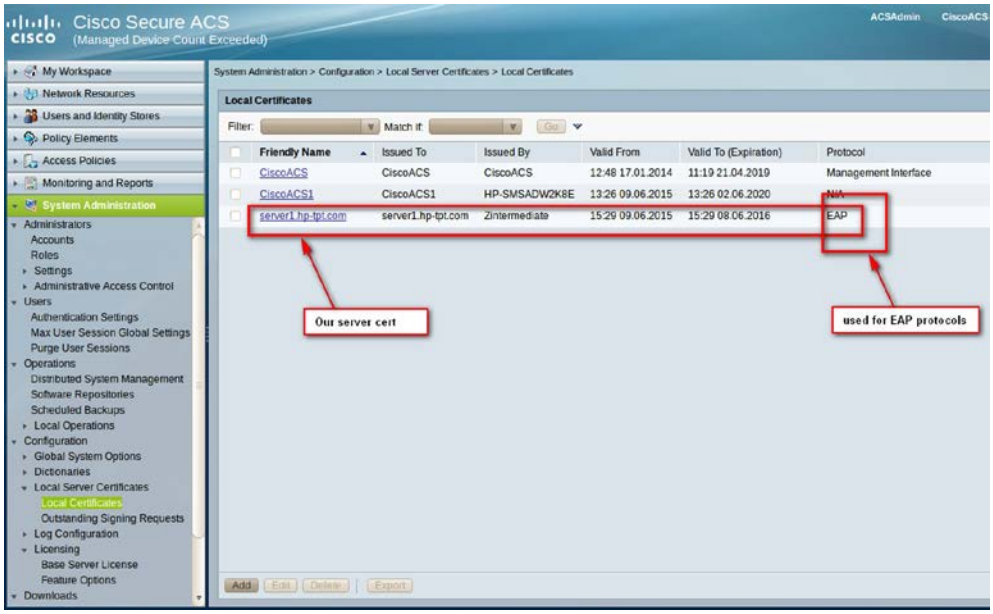


5. In the **"Step 2: Import Server Certificate"** page, specify the following information to identify the certificate to import:

   - Location of the server Certificate file
   - Location of the server Private Key file
   - Private Key Password of the certificate



6. Select **EAP** as the protocol.
7. Click **Finish**. The **Local Certificates** screen lists the entire certificate chain that you have configured on the RADIUS server.



4. RADIUS server configuration using the SMS

1. Use your SMS appliance to manage the HP TippingPoint security device that you want connected to the RADIUS server.

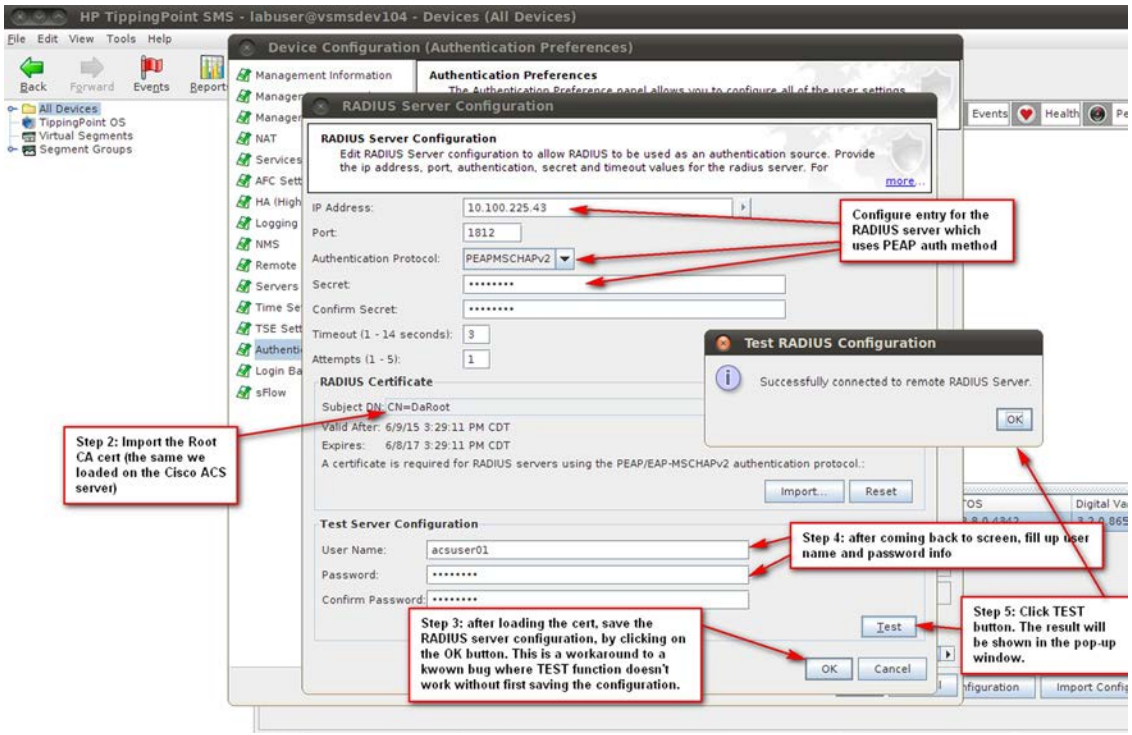
2. Right-click on the device and select **Edit > Device Configuration**. The Device Configuration dialog is displayed.

3. Click **Authentication Preferences**.

4. Select **RADIUS as Authentication Source** for the remote authentication.

5. Click **Edit** for the entry you want to configure. The RADIUS Server Configuration dialog is displayed.

6. Use the remaining steps and the following figure to configure the RADIUS server.



- Specify the RADIUS server's IP address, port, authentication protocol, and secret.

b. Click **Import** to import the Root CA certificate only.

c. Click **OK** to save the configuration before testing it.

d. Return to the RADIUS Server Configuration dialog and specify the user name and password for the server.

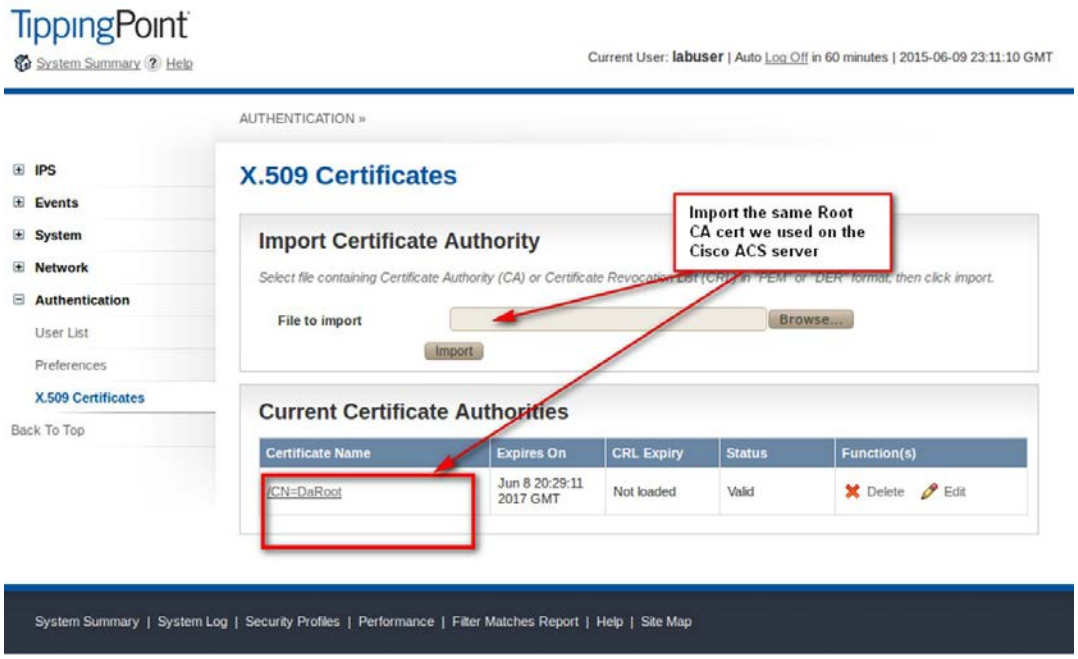
e. Click **Test**.

A popup message will confirm whether a successful connection to the server was established.

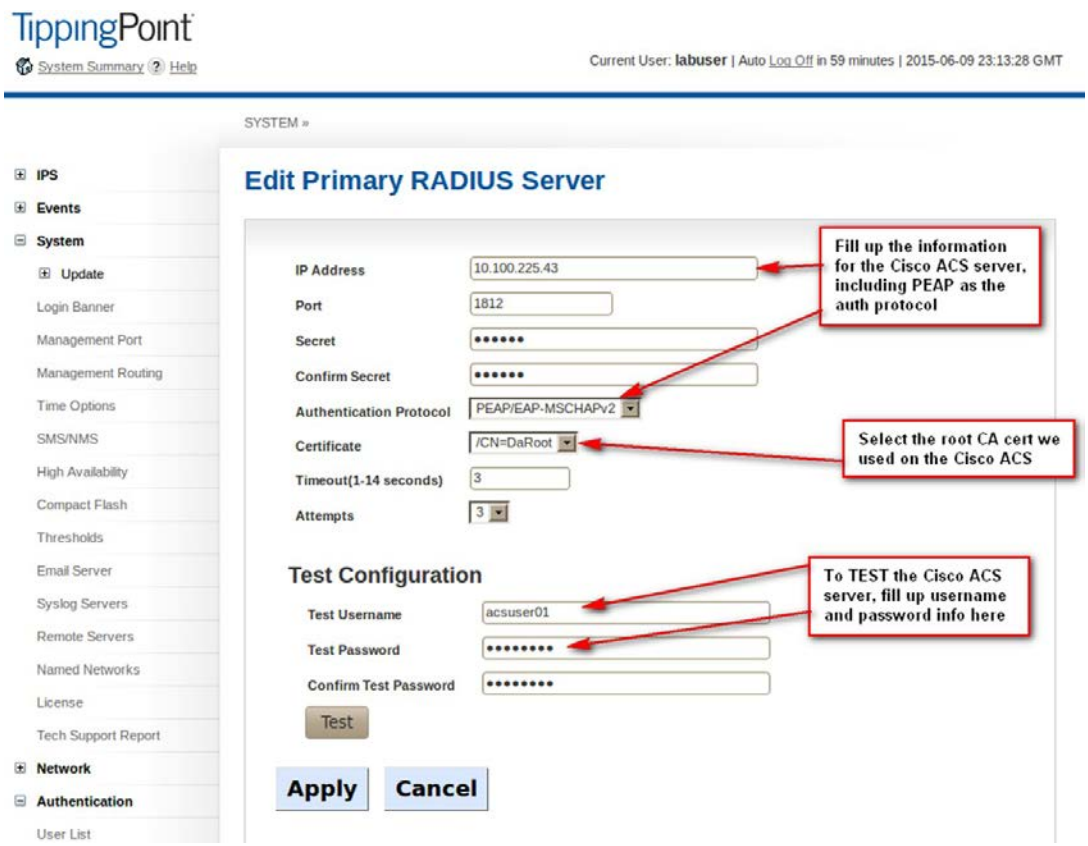
5. RADIUS server configuration using the LSM

1. Log in to the LSM as a user with device administrator privileges.
2. In the left pane, expand the **Authentication** menu and click **X.509 Certificates**.
3. On the X.509 Certificates page, browse to the location of the Root CA certificate (hp-tpt-ca.pem) that was configured on the Cisco ACS server and click **Import**.

The certificate is displayed in the Current Certificate Authorities panel.



4. From the left pane, select **System > Remote Servers**.
5. On the Remote server's page, select **RADIUS Remote Authentication** and click **Edit** for the RADIUS server entry you want to configure. The **Edit Primary RADIUS Server** dialog box is displayed.
6. Specify the RADIUS server by supplying the same identifying information you configured previously.



7. When using the LSM to configure the RADIUS server, you do not need to apply your changes before testing the connection.
8. Click **Test**. A message is generated indicating whether a connection was successful or not.
9. If the connection was successful, click **Apply** to save your configuration.