



TREND
M I C R O™

TippingPoint
Best Practice Guide

RADIUS PEAP Configuration for
IPS Devices and Cisco ACS



Version: 16.1.1

© Copyright 2016 Trend Micro.

Trend Micro Incorporated (“Trend Micro”) makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro shall not be liable for technical or editorial errors or omissions contained herein.

TABLE OF CONTENTS

1. Introduction	4
2. Description	4
3. Configure the RADIUS server	5
3.1. Install the certificates on the RADIUS server	6
3.1.1. Installing Root and Intermediate certificates	6
3.1.2. Installing Leaf-level certificates.....	8
4. RADIUS server configuration using the SMS	10
5. RADIUS server configuration using the LSM.....	11

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**.

Cisco Secure ACS
(Managed Device Count Exceeded)

ACSAdmin CiscoACS (Primary : LogCollector) Log Out About Help

My Workspace
Network Resources
Users and Identity Stores
Identity Groups
Internal Identity Stores
Users
Hosts
External Identity Stores
LDAP
Active Directory
RSA SecurID Token Servers
RADIUS Identity Servers
Certificate Authorities
Certificate Authentication Profile
Identity Store Sequences
Policy Elements
Access Policies
Monitoring and Reports
System Administration

Users and Identity Stores > Certificate Authorities > Create

Location of the Root CA cert file

Certificate File To Import
Add (Import) a new Trusted CA (Certificate Authority) Certificate.

Certificate File: /home/fulzele/custom-certs/hp-tpt-ca.pem

Trust for client with EAP-TLS:

Allow Duplicate Certificates:

Description: HP-TPT Root CA

Leave this box unchecked as we are using PEAP/MSCHAPv2, not EAP-TLS

You are returned **Certificates Authorities** screen.

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

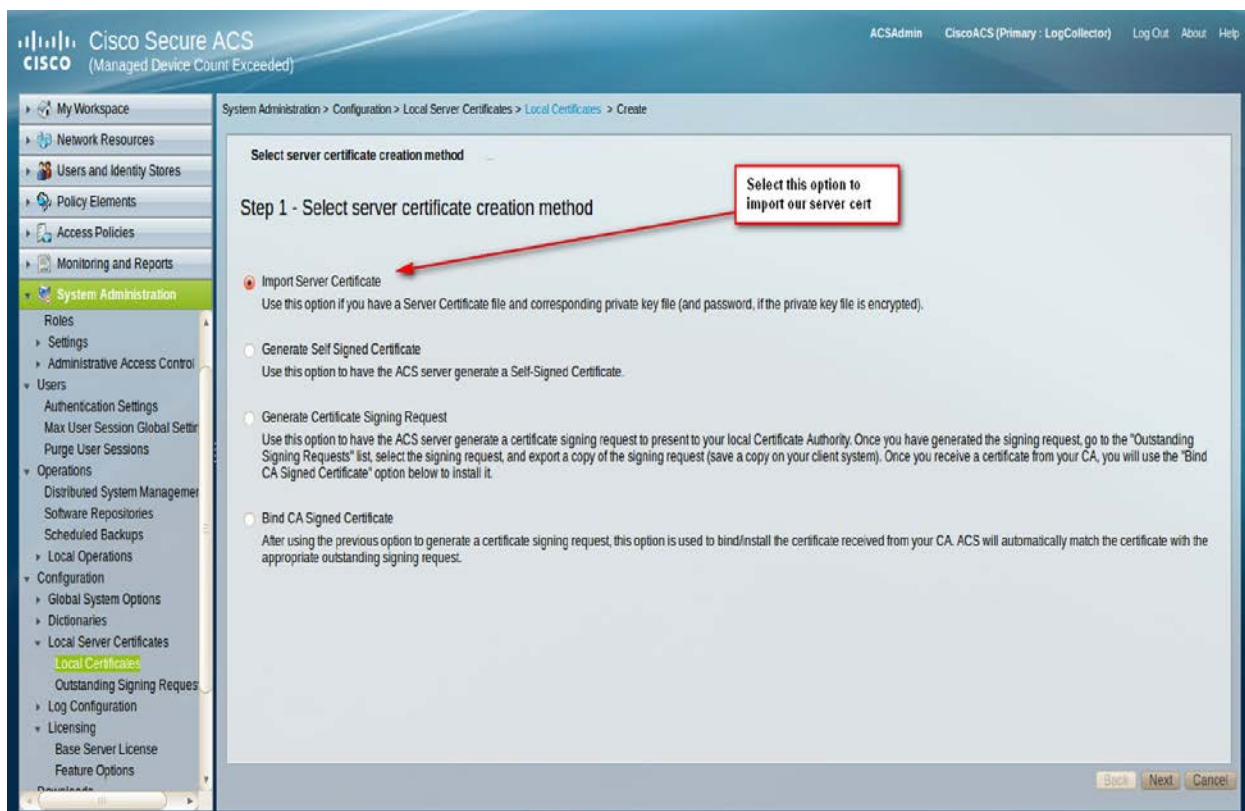
Once completed, the **Certificates Authorities** screen will list both the **Root CA** and the **Intermediate CA** certificates you added.

The screenshot shows the Cisco Secure ACS interface. The main content area displays a table of Certificate Authorities. The table has the following columns: Friendly Name, Expiration, Issued To, Issued By, and Description. Two rows are highlighted with red boxes and labeled with callouts: 'our Root CA' pointing to the 'DaRoot' row, and 'our intermediate CA' pointing to the 'Zintermediate' row.

Friendly Name	Expiration	Issued To	Issued By	Description
DaRoot	15:29 08.06.2017	DaRoot	DaRoot	HP-TPT Root CA
tiab-aries	12:16 12.08.2023	tiab-aries	tiab-aries	
HP-SMSADW2K8E	16:03 03.06.2017	HP-SMSADW2K8E	tiab-aries	
Zintermediate	15:29 08.06.2016	Zintermediate	DaRoot	HP-TPT Intermediate CA

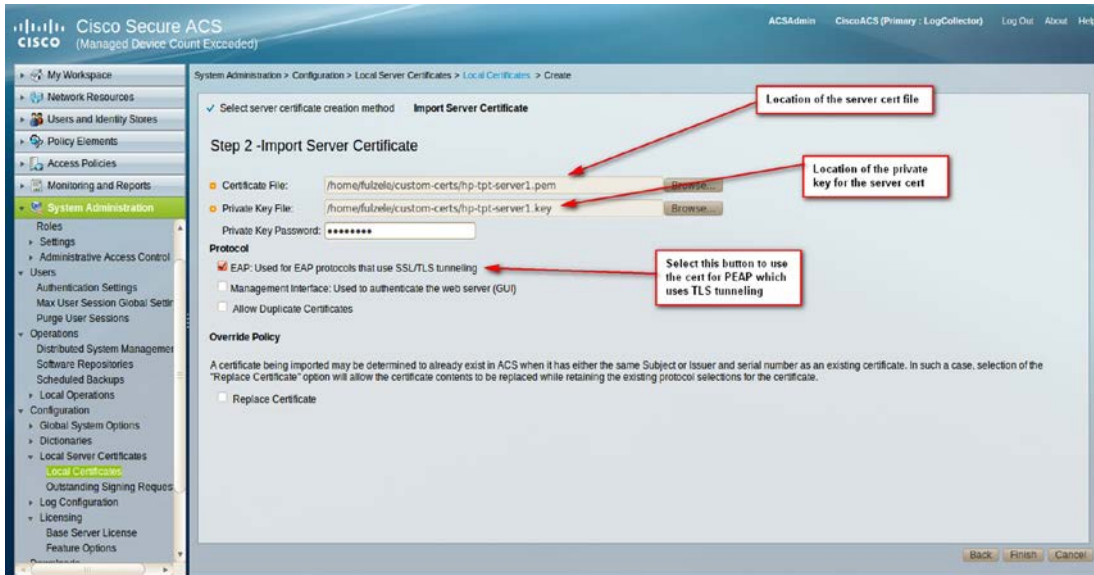
3.1.2. Installing Leaf-level certificates

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**.



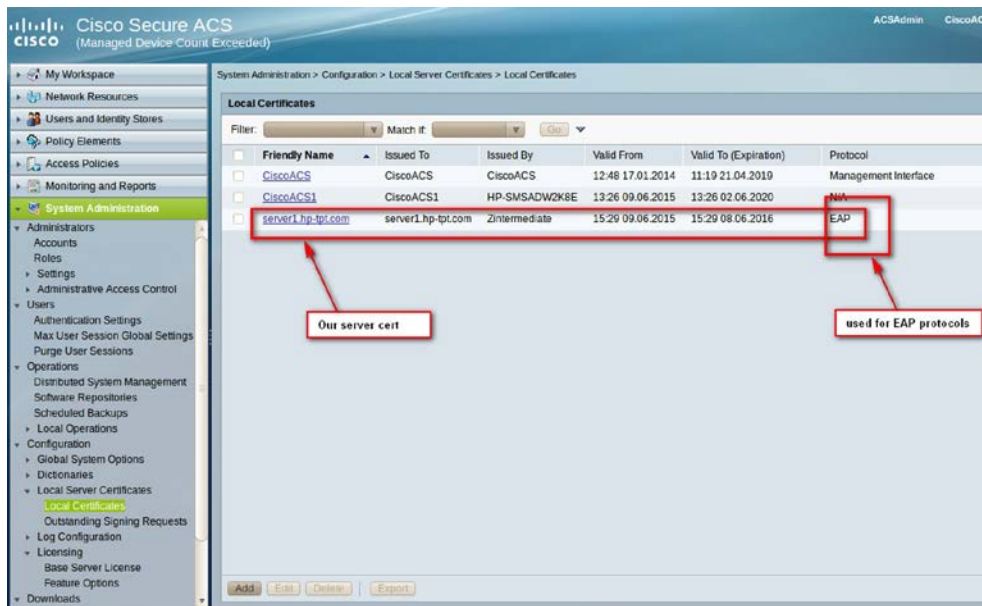
5. In the “**Step 2: Import Server Certificate**” page, specify the following information to identify the certificate to import:

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



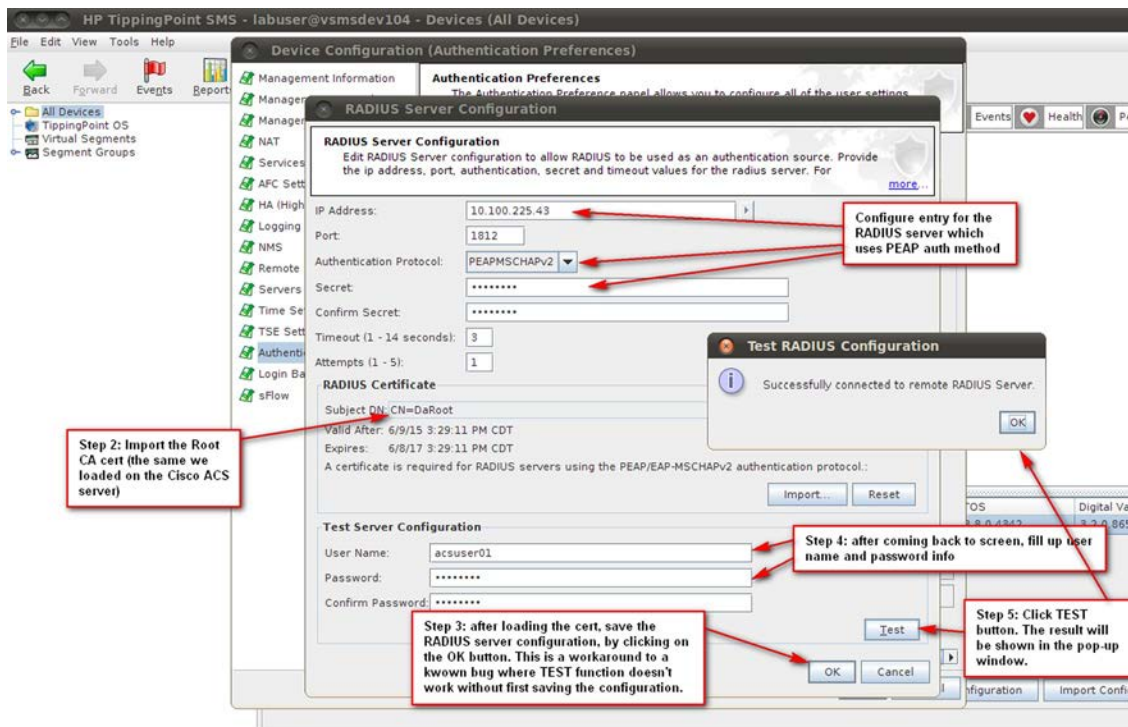
6. Select **EAP** as the protocol.

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.
- a. Click **Import** to import the Root CA certificate only.
 - b. Click **OK** to save the configuration before testing it.
 - c. 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.

System Summary ? Help

Current User: labuser | Auto Log Off in 60 minutes | 2015-06-09 23:11:10 GMT

AUTHENTICATION »

X.509 Certificates

Import Certificate Authority

Select file containing Certificate Authority (CA) or Certificate Revocation List (CRL) in "PEM" or "DER" format, then click import.

File to import

Current Certificate Authorities

Certificate Name	Expires On	CRL Expiry	Status	Function(s)
./CN=DaRoot	Jun 8 20:29:11 2017 GMT	Not loaded	Valid	<input type="button" value="Delete"/> <input type="button" value="Edit"/>

System Summary | System Log | Security Profiles | Performance | Filter Matches Report | Help | Site Map

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.

SYSTEM »

- IPS
- Events
- System
 - Update
 - Login Banner
 - Management Port
 - Management Routing
 - Time Options
 - SMS/NMS
 - High Availability
 - Compact Flash
 - Thresholds
 - Email Server
 - Syslog Servers
 - Remote Servers
 - Named Networks
 - License
 - Tech Support Report
- Network
- Authentication
 - User List

Edit Primary RADIUS Server

IP Address	<input type="text" value="10.100.225.43"/>	Fill up the information for the Cisco ACS server, including PEAP as the auth protocol
Port	<input type="text" value="1812"/>	
Secret	<input type="password" value="*****"/>	
Confirm Secret	<input type="password" value="*****"/>	
Authentication Protocol	<input type="text" value="PEAP/EAP-MSCHAPv2"/>	Select the root CA cert we used on the Cisco ACS
Certificate	<input type="text" value="/CN=DaRoot"/>	
Timeout(1-14 seconds)	<input type="text" value="3"/>	
Attempts	<input type="text" value="3"/>	

Test Configuration		
Test Username	<input type="text" value="acsuser01"/>	To TEST the Cisco ACS server, fill up username and password info here
Test Password	<input type="password" value="*****"/>	
Confirm Test Password	<input type="password" value="*****"/>	
<input type="button" value="Test"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

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.