

AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Phone Certificate Types](#)

[Configure](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document provides a sample configuration that shows how to configure the Adaptive Security Appliance (ASA) and CallManager devices to provide certificate authentication for AnyConnect clients that run on Cisco IP Phones. After this configuration is complete, Cisco IP Phones can establish VPN connections to the ASA that make use of certificates in order to secure the communication.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- AnyConnect Premium SSL License
- AnyConnect for Cisco VPN Phone License

Dependent upon the ASA version, you will see either "AnyConnect for Linksys phone" for ASA Release 8.0.x or "AnyConnect for Cisco VPN Phone" for ASA Release 8.2.x or later.

Components Used

The information in this document is based on these software and hardware versions:

- ASA - Release 8.0(4) or later
- IP Phone Models - 7942 / 7962 / 7945 / 7965 / 7975
- Phones - 8961 / 9951 / 9971 with Release 9.1(1) firmware
- Phone - Release 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) or later
- Cisco Unified Communications Manager (CUCM) - Release 8.0.1.100000-4 or later

The releases used in this configuration example include:

- ASA - Release 9.1(1)
- CallManager - Release 8.5.1.10000-26

For a complete list of supported phones in your CUCM version, complete these steps:

1. Open this URL: <https://<CUCM Server IP Address>:8443/cucreports/systemReports.do>
2. Choose **Unified CM Phone Feature List > Generate a new report > Feature: Virtual Private Network**.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

Phone Certificate Types

Cisco uses these certificate types in phones:

- **Manufacturer Installed Certificate (MIC)** - MICs are included on all 7941, 7961, and newer model Cisco IP phones. MICs are 2048-bit key certificates that are signed by the Cisco Certificate Authority (CA). When a MIC is present, it is not necessary to install a Locally Significant Certificate (LSC). In order for the CUCM to trust the MIC certificate, it utilizes the pre-installed CA certificates CAP-RTP-001, CAP-RTP-002, and Cisco_Manufacturing_CA in its certificate trust store.
- **LSC** - The LSC secures the connection between CUCM and the phone after you configure the device security mode for authentication or encryption. The LSC possesses the public key for the Cisco IP phone, which is signed by the CUCM Certificate Authority Proxy Function (CAPF) private key. This is the preferred method (as opposed to the use of MICs) because only Cisco IP phones that are manually provisioned by an administrator are allowed to download and verify the CTL file. **Note:** Due to the increased security risk, Cisco recommends the use of MICs solely for LSC installation and not for continued use. Customers who configure Cisco IP phones to use MICs for Transport Layer Security (TLS) authentication or for any other purpose do so at their own risk.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) to obtain more information on the commands used in this section.

Configurations

This document describes these configurations:

- ASA Configuration
- CallManager Configuration
- VPN Configuration on CallManager
- Certificate Installation on IP Phones

ASA Configuration

The configuration of the ASA is almost the same as when you connect an AnyConnect client computer to the ASA. However, these restrictions apply:

- The tunnel-group must have a group-url. This URL will be configured in CM under the VPN Gateway URL.
- The group policy must not contain a split tunnel.

This configuration uses a previously configured and installed ASA (self-signed or third party) certificate in the Secure Socket Layer (SSL) trustpoint of the ASA device. For more information, refer to these documents:

- [Configuring Digital Certificates](#)
- [ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example](#)
- [ASA 8.x : VPN Access with the AnyConnect VPN Client Using Self-Signed Certificate Configuration Example](#)

The relevant configuration of the ASA is:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

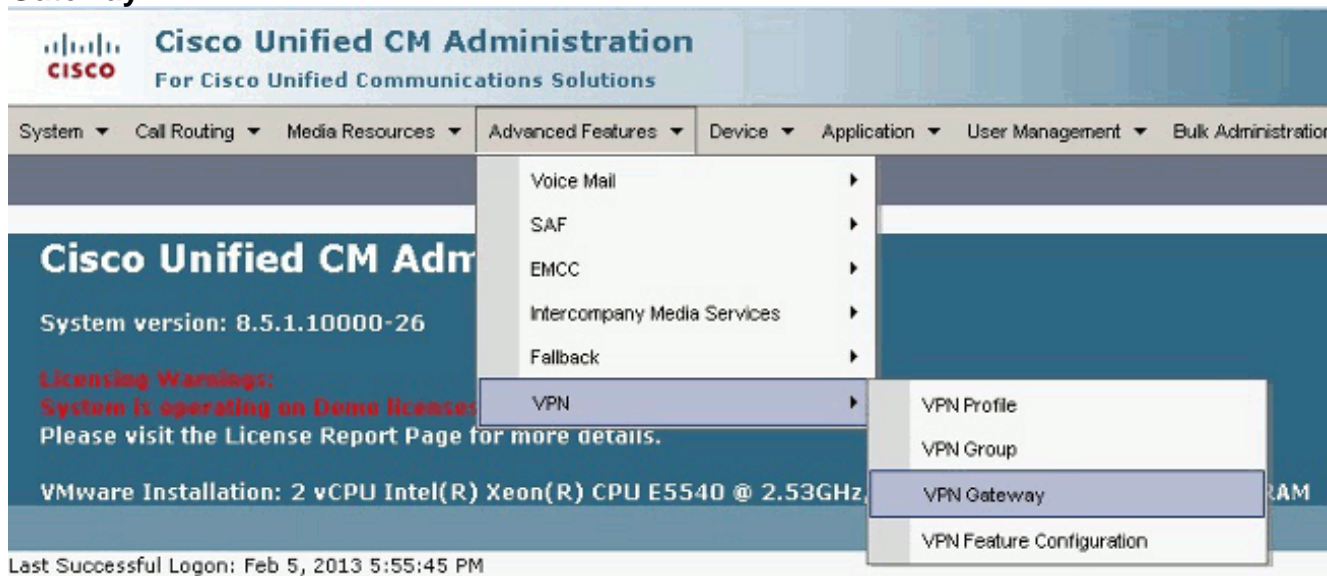
CallManager Configuration

In order to export the certificate from the ASA and import the certificate into CallManager as a Phone-VPN-Trust certificate, complete these steps:

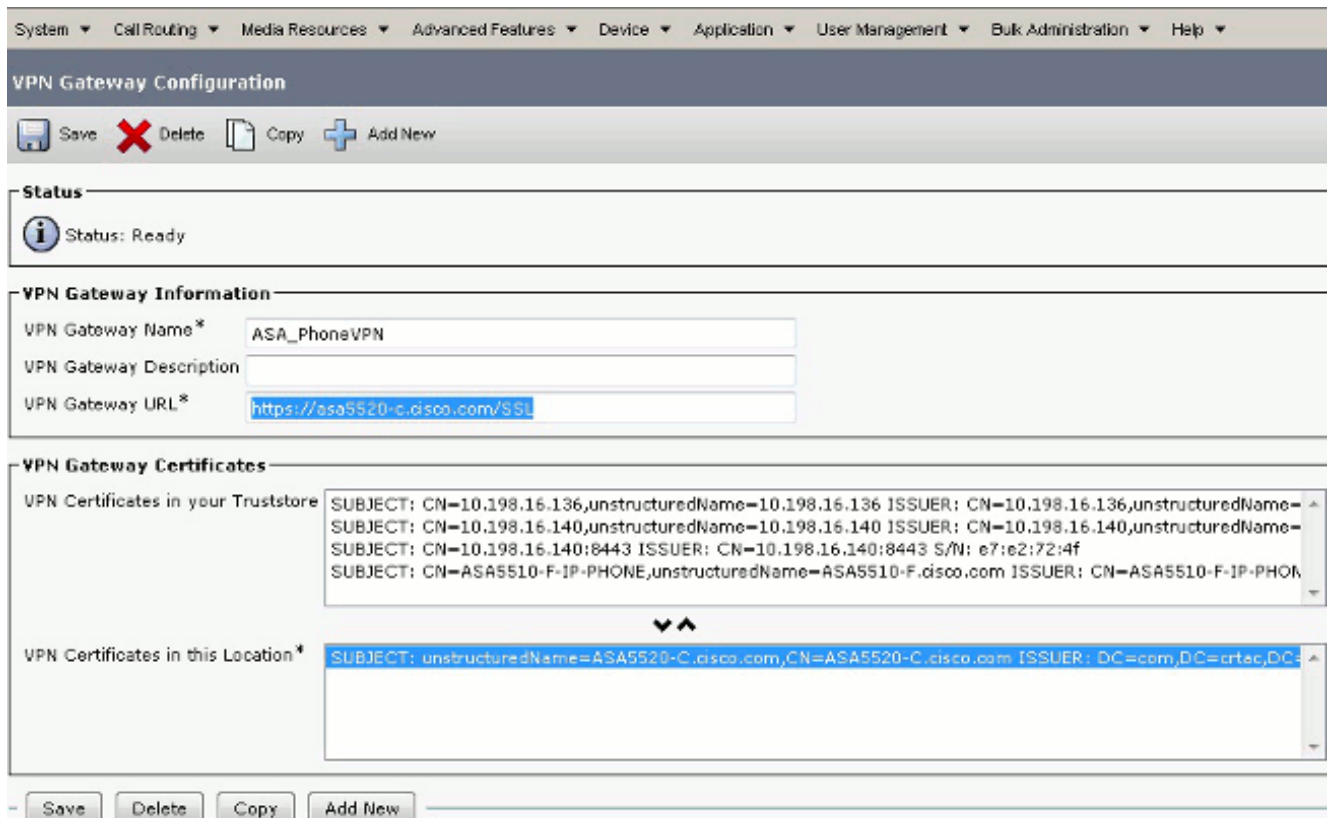
1. Register the generated certificate with CUCM.
2. Check the certificate used for SSL.ASA(config)#**show run ssl**
ssl trust-point SSL outside
3. Export the certificate.ASA(config)#**crypto ca export SSL identity-certificate**The Privacy Enhanced Mail (PEM) encoded identity certificate follows:-----BEGIN CERTIFICATE-----
ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9xOpR7BFpZd1yFyzwAPkoB11
-----END CERTIFICATE-----
4. Copy the text from the terminal and save it as a .pem file.
5. Log in to CallManager and choose **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust** in order to upload the certificate file saved in the previous step.

VPN Configuration on CallManager

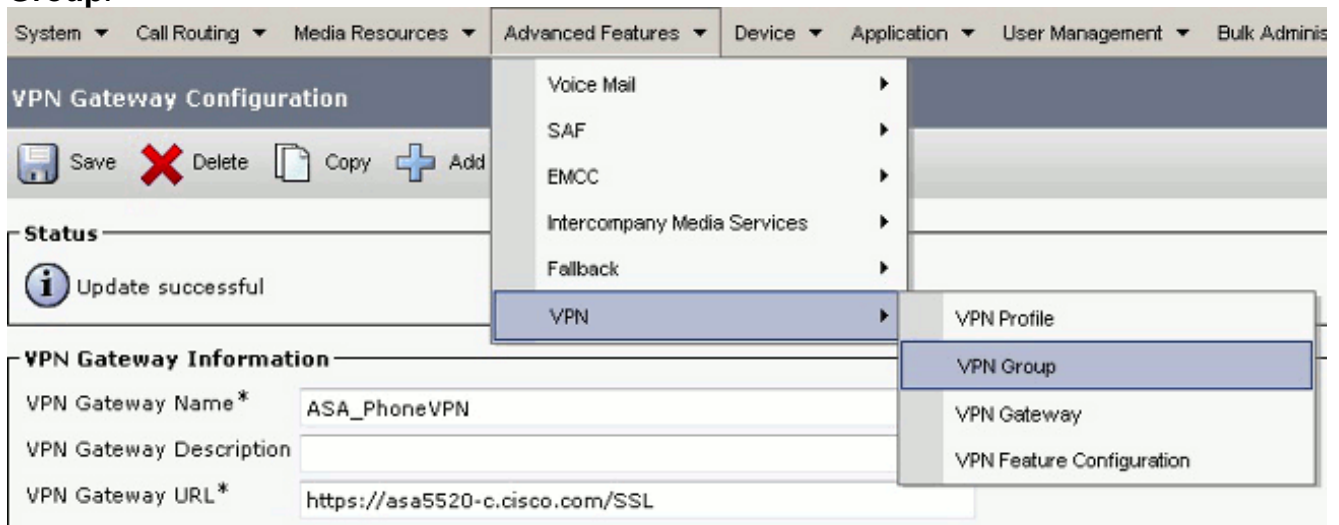
1. Navigate to Cisco Unified CM Administration.
2. From the menu bar, choose **Advanced Features > VPN > VPN Gateway**.



3. In the VPN Gateway Configuration window, complete these steps:
In the VPN Gateway Name field, enter a name. This can be any name.
In the VPN Gateway Description field, enter a description (optional).
In the VPN Gateway URL field, enter the group-url defined on the ASA.
In the VPN Certificates in this Location field, select the certificate that was uploaded to CallManager previously to move it from the truststore to this location.



- From the menu bar, choose **Advanced Features > VPN > VPN Group**.



- In the All Available VPN Gateways field, select the VPN Gateway previously defined. Click the down arrow in order to move the selected gateway to the Selected VPN Gateways in this VPN Group field.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manag

VPN Group Configuration

Save Delete Copy Add New

Status

Status: Ready

VPN Group Information

VPN Group Name* ASA_PhoneVPN

VPN Group Description

VPN Gateway Information

All Available VPN Gateways

Selected VPN Gateways in this VPN Group*

ASA_PhoneVPN

Move the Gateway down

6. From the menu bar, choose **Advanced Features > VPN > VPN**

Profile.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administ

VPN Group Configuration

Save Delete Copy Add

Status

Status: Ready

VPN Group Information

VPN Group Name* ASA_PhoneVPN





VPN Group Description

- Voice Mail ▸
- SAF ▸
- EMCC ▸
- Intercompany Media Services ▸
- Fallback ▸
- VPN ▸**
 - VPN Profile**
 - VPN Group
 - VPN Gateway
 - VPN Feature Configuration


7. In order to configure the VPN Profile, complete all fields that are marked with an asterisk (*).

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*

Enable Host ID Check

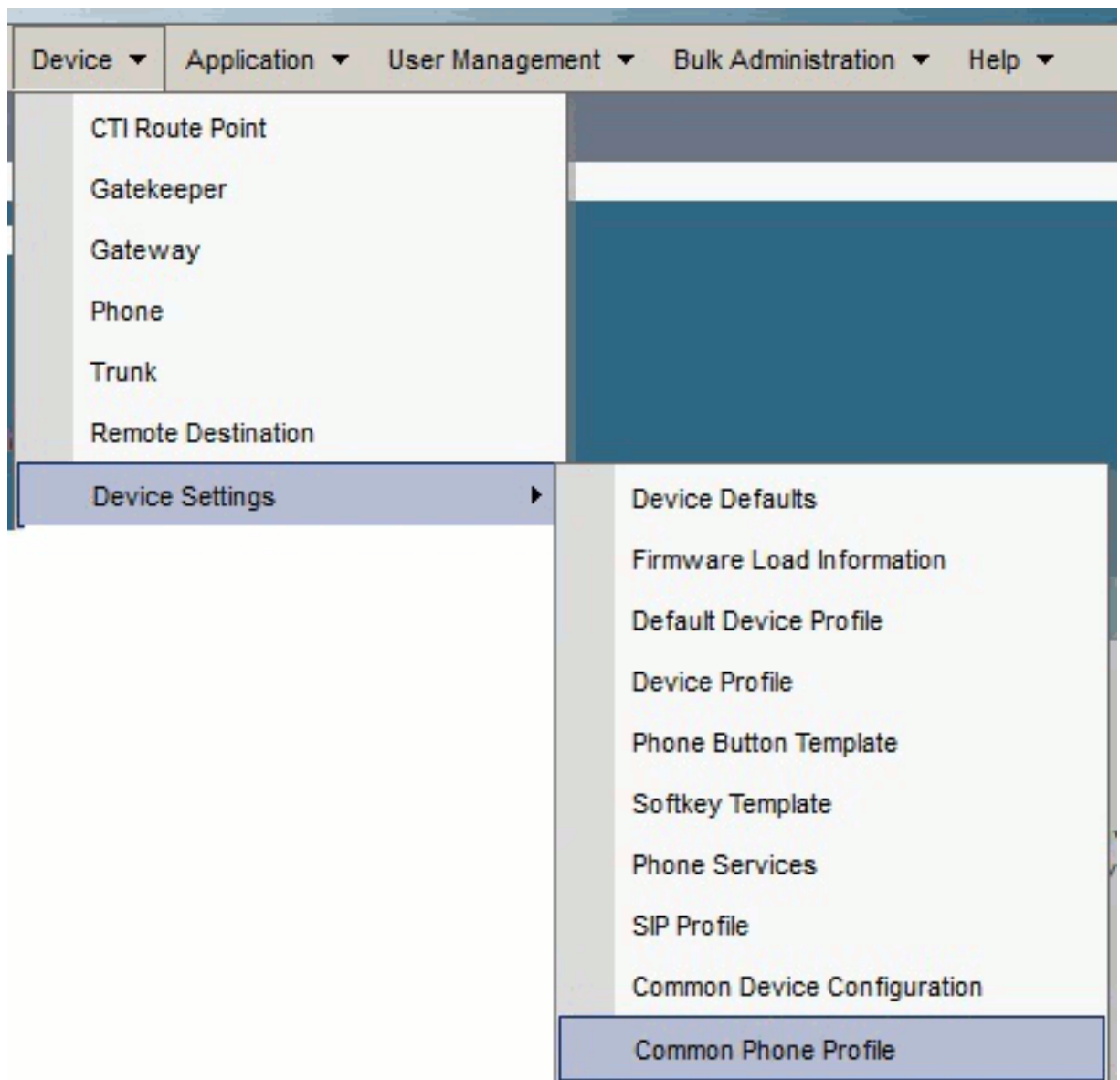
Client Authentication

Client Authentication Method*

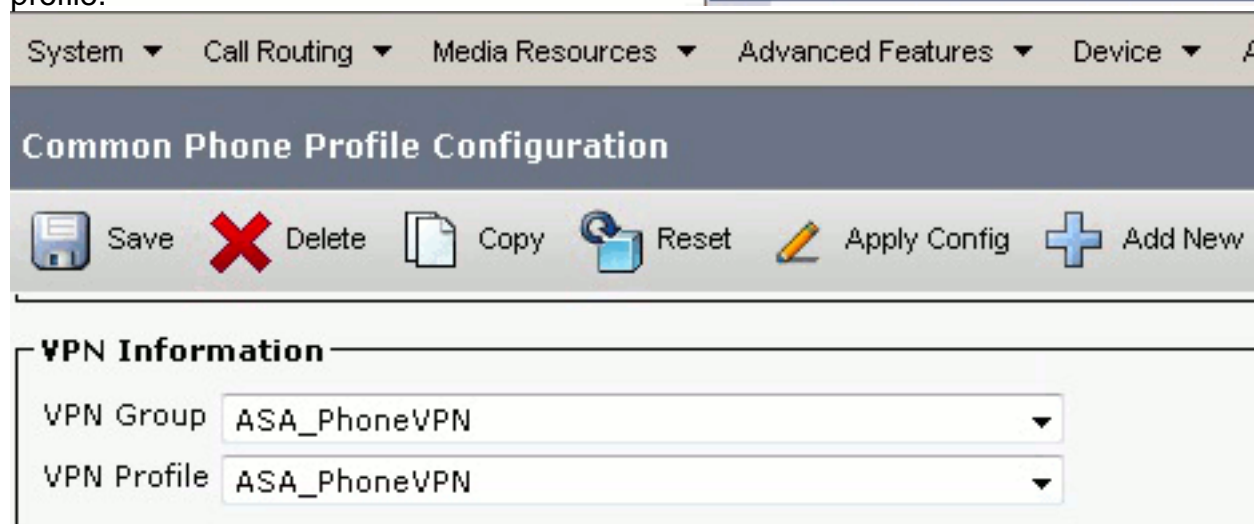
Enable Password Persistence

Enable Auto Network Detect: If enabled, the VPN phone pings the TFTP server and if no response is received, it auto-initiates a VPN connection. **Enable Host ID Check:** If enabled, the VPN phone compares the FQDN of the VPN Gateway URL against the CN/SAN of the certificate. The client fails to connect if they do not match or if a wildcard certificate with an asterisk (*) is used. **Enable Password Persistence:** This allows the VPN phone to cache the username and password for the next VPN attempt.

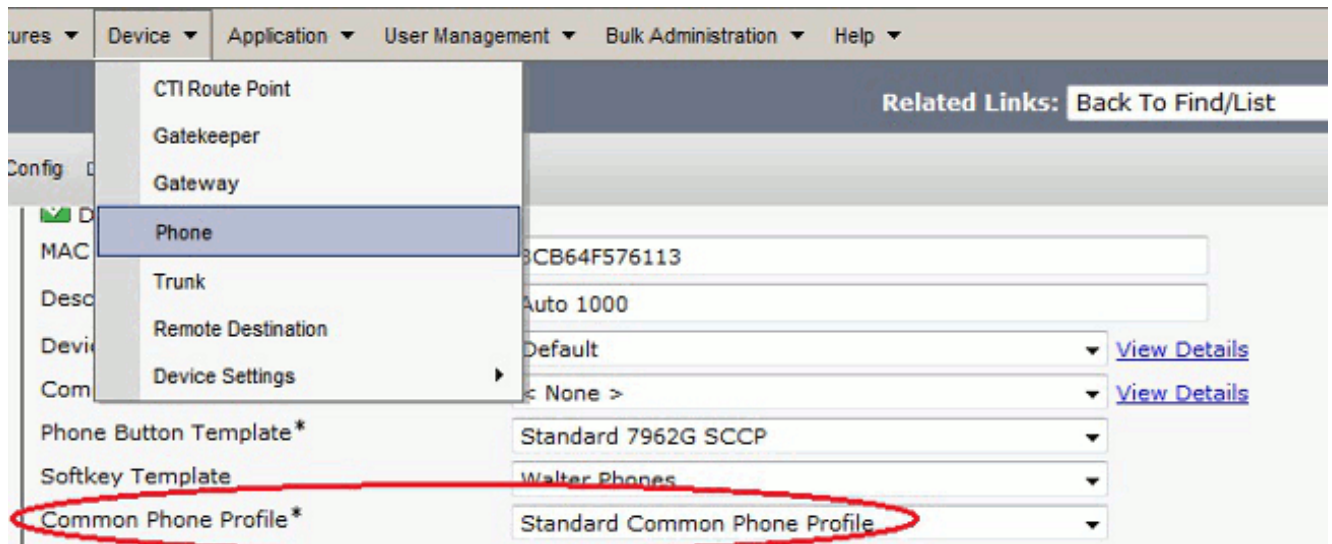
- In the Common Phone Profile Configuration window, click **Apply Config** in order to apply the new VPN configuration. You can use the "Standard Common Phone Profile" or create a new



profile.



9. If you created a new profile for specific phones/users, go to the Phone Configuration window. In the Common Phone Profile field, choose **Standard Common Phone Profile**.



10. Register the phone to CallManager again in order to download the new configuration.





Certificate Authentication Configuration

In order to configure certificate authentication, complete these steps in CallManager and the ASA:


1. From the menu bar, choose **Advanced Features > VPN > VPN Profile**.
2. Confirm the Client Authentication Method field is set to **Certificate**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*



Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

- Log in to CallManager. From the menu bar, choose **Unified OS Administration > Security > Certificate Management > Find**.
- Export the correct certificate(s) for the selected certificate authentication method: MICs: Cisco_Manufacturing_CA - Authenticate IP Phones with a MIC

Find Certificate List where ▾ begins with ▾  

Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

LSCs: Cisco Certificate Authority Proxy Function (CAPF) - Authenticate IP Phones with an LSC

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	tomcat.pem	tomcat.der
psec	certs	ipsec.pem	ipsec.der
tomcat-trust	trust-certs	CUCM85.pem	CUCM85.der
psec-trust	trust-certs	CUCM85.pem	CUCM85.der
CallManager	certs	CallManager.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TVS.pem	TVS.der
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem	

- Find the certificate, either Cisco_Manufacturing_CA or CAPF. Download the .pem file and save as a .txt file
- Create a new trustpoint on the ASA and authenticate the trustpoint with the previous saved certificate. When you are prompted for base-64 encoded CA certificate, select and paste the text in the downloaded .pem file along with the BEGIN and END lines. An example is shown:

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

- Confirm the authentication on the tunnel-group is set to certificate authentication.

```
tunnel-group
SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

Certificate Installation on IP Phones

The IP Phones can work with either MICs or LSCs, but the configuration process is different for each certificate.

MIC Installation

By default, all the phones that support VPN are pre-loaded with MICs. The 7960 and 7940 phones do not come with a MIC, and require a special installation procedure for the LSC to register securely.

Note: Cisco recommends that you use MICs for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with CUCM. Because MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.

LSC Installation

- Enable CAPF service on CUCM.
- After the CAPF service is activated, assign the phone instructions to generate a LSC in CUCM. Log in to Cisco Unified CM Administration and choose **Device > Phone**. Select the phone you configured.
- In the Certificate Authority Proxy Function (CAPF) Information section, ensure all settings are correct and the operation is set to a future date.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* Install/Upgrade ▼

Authentication Mode* By Authentication String ▼

Authentication String 123456

Key Size (Bits)* 2048 ▼

Operation Completes By 2013 3 10 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

4. If Authentication Mode is set to Null String or Existing Certificate, no further action is required.
5. If Authentication Mode is set to a string, manually select **Settings > Security Configuration > **# > LSC > Update** in the phone console.

Verify

Use this section in order to confirm that your configuration works properly.

ASA Verification

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
```

Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0

CUCM Verification

The screenshot shows the CUCM Phone Management interface. At the top, there are navigation tabs: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below the navigation is a search bar and a list of actions: Add New, Select All, Clear All, Delete Selected, Reset Selected, and Apply Config to Selected. The status bar indicates "4 records found". The main table is titled "Phone (1 - 4 of 4)". The table has the following columns: Device Name, Description, Device Pool, Device Protocol, Status, and IP Address. The first two rows show phones with status "Unknown". The third row is highlighted with a red circle around the status "Registered with: 192.168.100.1" and the IP address "10.10.10.2". A red arrow points from the text "IP Phone registered with the CUCM using VPN address" to the IP address column.

Device Name	Description	Device Pool	Device Protocol	Status	IP Address
SEPXXXXXXXXXXXX	Auto 1001	Default	SCCP	Unknown	Unknown
SEPXXXXXXXXXXXX	Auto 1000	Default	SCCP	Registered with: 192.168.100.1	10.10.10.2

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Bugs

- Cisco bug ID [CSCtf09529](#), Add support for VPN feature in CUCM for 8961, 9951, 9971 phones
- Cisco bug ID [CSCuc71462](#), IP phone VPN failover takes 8 minutes

- Cisco bug ID [CSCtz42052](#), IP Phone SSL VPN Support For Non Default Port Numbers
- Cisco bug ID [CSCth96551](#), Not all ASCII characters are supported during phone VPN user + password login.
- Cisco bug ID [CSCuj71475](#), Manual TFTP entry needed for IP Phone VPN
- Cisco bug ID [CSCum10683](#), IP phones not logging missed, placed, or received calls

Related Information

- [Technical Support & Documentation - Cisco Systems](#)