AnyConnect VPN Phone Connection to a Cisco IOS Router Configuration Example

Contents

Introduction

This document describes how to configure the Cisco IOS® Router and Call Manager devices so that Cisco IP Phones can establish VPN connections to the Cisco IOS Router. These VPN connections are needed in order to secure the communication with either of these two client authentication methods:

- Authentication, Authorization, and Accounting (AAA) server or local database
- Phone certificate

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco IOS 15.1(2)T or Later
- Feature Set/License: Universal (Data & Security & UC) for Cisco IOS Integrated Service Router (ISR)-G2
- Feature Set/License: Advanced Security for Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM) Release 8.0.1.100000-4 or Later
- IP Phone Release 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) or Later

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 releases used in this configuration example include:

- Cisco IOS Router Release 15.1(4)M4
- Call Manager Release 8.5.1.10000-26
- IP Phone Release 9.1(1)SR1S

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.

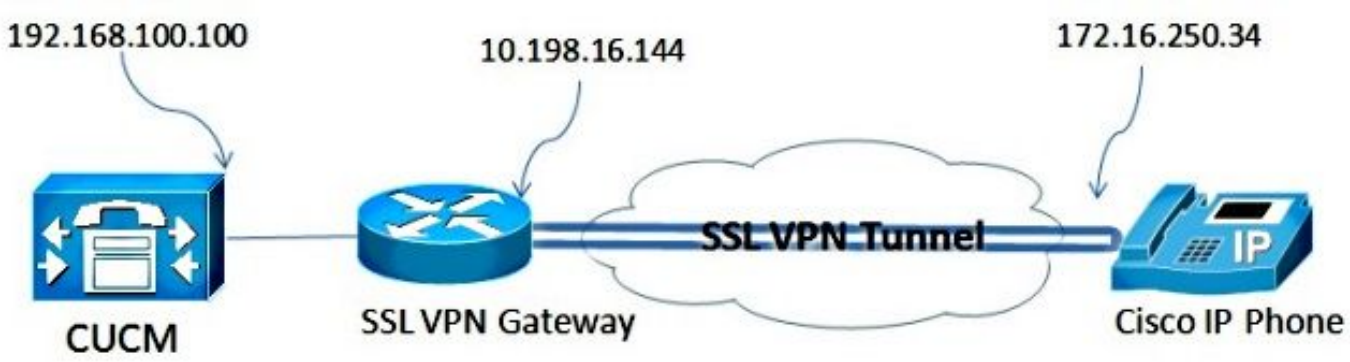
Configure

This section covers the information needed in order to configure the features described in this document.

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Topology

The topology used in this document includes one Cisco IP Phone, the Cisco IOS Router as the Secure Sockets Layer (SSL) VPN Gateway, and CUCM as the voice gateway.



SSL VPN Server Configuration

This section describes how to configure the Cisco IOS head-end in order to allow inbound SSL VPN connections.

Common Configuration Steps

1. Generate the Rivest-Shamir-Adleman (RSA) Key with a length of 1024 bytes:

   ```
   Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
   ```

2. Create the trustpoint for the self-signed certificate, and attach the **SSL RSA Key**:

   ```
   Router(config)#crypto pki trustpoint server-certificate
   enrollment selfsigned
   usage ssl-server
   serial-number
   subject-name CN=10.198.16.144
   revocation-check none
   rsakeypair SSL
   ```

3. Once the trustpoint is configured, enroll the self-signed certificate with this command:

   ```
   Router(config)#crypto pki enroll server-certificate
   % Include an IP address in the subject name? [no]: no
   Generate Self Signed Router Certificate? [yes/no]: yes

   Router Self Signed Certificate successfully created
   ```

4. Enable the correct AnyConnect package on the head-end. The phone itself does not download this package. But, without the package, the VPN tunnel does not establish. It is recommended to use the latest client software version available on Cisco.com. This example uses Version 3.1.3103.

   In older Cisco IOS versions, this is the command in order to enable the package:
   ```
   Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
   ```
   However, in the latest Cisco IOS version, this is the command:
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```

5. Configure the VPN Gateway. The WebVPN Gateway is used in order to terminate the SSL connection from the user.
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```
   Note: Either the IP address used here needs to be on the same subnet as the interface to which the phones connect, or the gateway needs to be sourced directly from an interface on

the Router. The gateway is also used in order to define which certificate is used by the Router in order to validate itself to the client.

6. Define the local pool that is used in order to assign IP addresses to the clients when they connect:
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuration with AAA Authentication

This section describes the commands you need in order to configure the AAA server or the local database in order to authenticate your phones. If you plan to use certificate-only authentication for the phones, continue to the next section.

Configure the User Database

Either the Local Database of the Router or an external AAA Server can be used for authentication:

- In order to configure the local database, enter:
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```
- In order to configure a remote AAA RADIUS server for authentication, enter:
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configure the Virtual Context and the Group-Policy

The Virtual Context is used in order to define the attributes that govern the VPN connection, such as:

- Which URL to use when you connect
- Which pool to use in order to assign the client addresses
- Which authentication method to use

These commands are an example of a context that uses AAA authentication for the client:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuration With the IP Phone Locally Significant Certificate (LSC) for Client Authentication

This section describes the commands you need in order to configure certificate-based client authentication for the phones. However, in order to do this, knowledge of the various types of phone certificates is required:

- **Manufacturer Installed Certificate (MIC) -** MICs are included on all 7941, 7961, and newer-model Cisco IP phones. MICs are 2,048-bit key certificates that are signed by the Cisco Certificate Authority (CA). In order for the CUCM to trust the MIC certificate, it uses the pre-installed CA certificates CAP-RTP-001, CAP-RTP-002, and Cisco_Manufacturing_CA in its certificate trust store. Because this certificate is provided by the manufacturer itself, as indicated in the name, it is not recommended to use this certificate for client authentication.
- **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 more secure method (as opposed to the use of MICs).
Caution: 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 in order to use MICs for Transport Layer Security (TLS) authentication, or for any other purpose, do so at their own risk.

In this configuration example, the LSC is used in order to authenticate the phones.

> **Tip**: The most secure way to connect your phone is to use dual authentication, which combines certificate and AAA authentication. You can configure this if you combine the commands used for each under one virtual context.

Configure the Trustpoint in Order to Validate the Client Certificate

The Router must have the CAPF certificate installed in order to validate the LSC from the IP phone. In order to get that certificate and install it on the Router, complete these steps:

1. Go to the CUCM Operating System (OS) Administration web page.
2. Choose **Security > Certificate Management**.
   Note: This location might change based on the CUCM version.
3. Find the certificate labeled **CAPF**, and download the **.pem** file. Save it as a **.txt** file
4. Once the certifcate is extracted, create a new trustpoint on the Router, and authenticate the trustpoint with CAPF, as shown here. When prompted for the base-64 encoded CA certificate, select and paste the text in the downloaded .pem file along with the BEGIN and END lines.
```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#

<base-64 encoded CA certificate>

quit
```

Things to Note:

- The enrollment method is terminal because the certificate has to be manually installed on the Router.
- The **authorization username** command is required in order to tell the Router what to use as the username when the client makes the connection. In this case, it uses the Common Name (CN).
- A revocation check needs to be disabled because phone certificates do not have a Certificate Revocation List (CRL) defined. So, unless it is disabled, the connection fails and the Public Key Infrastructure (PKI) debugs show this output:
```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
```

```
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configure the Virtual Context and the Group-Policy

This part of the configuration is similar to the configuration used previously, except for two points:

- The authentication method
- The trustpoint the context uses in order to authenticate the phones

The commands are shown here:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Call Manager Configuration

This section describes the Call Manager configuration steps.

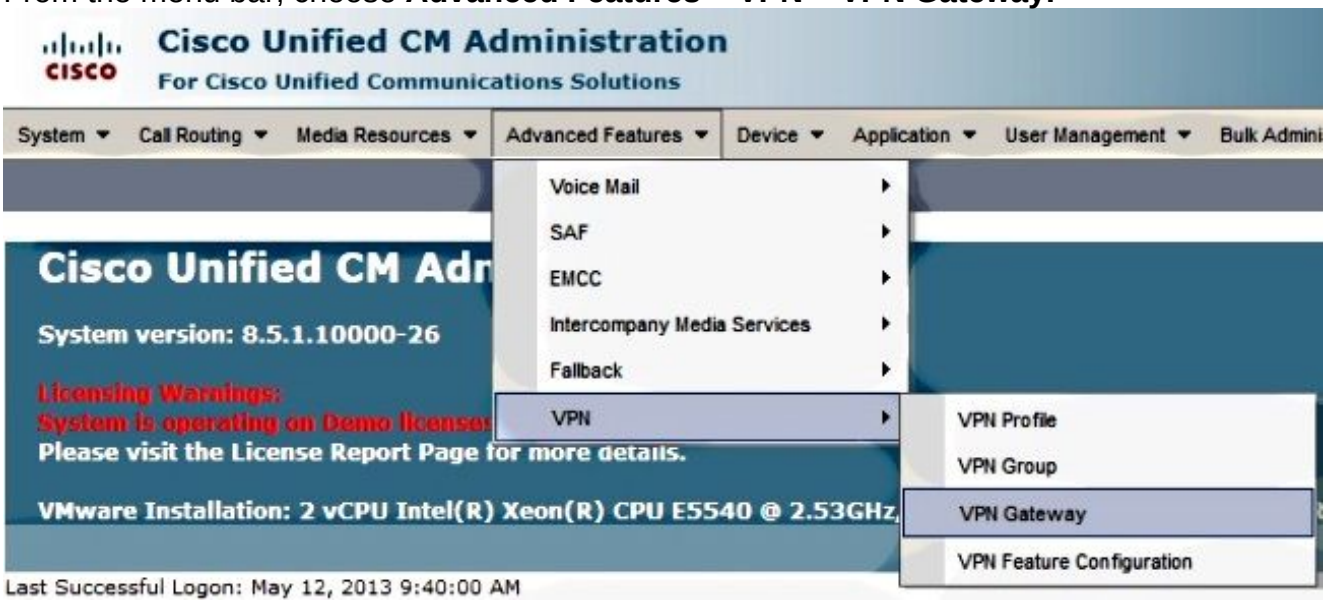
Export the Self-signed or Identity Certificate from the Router to the CUCM

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

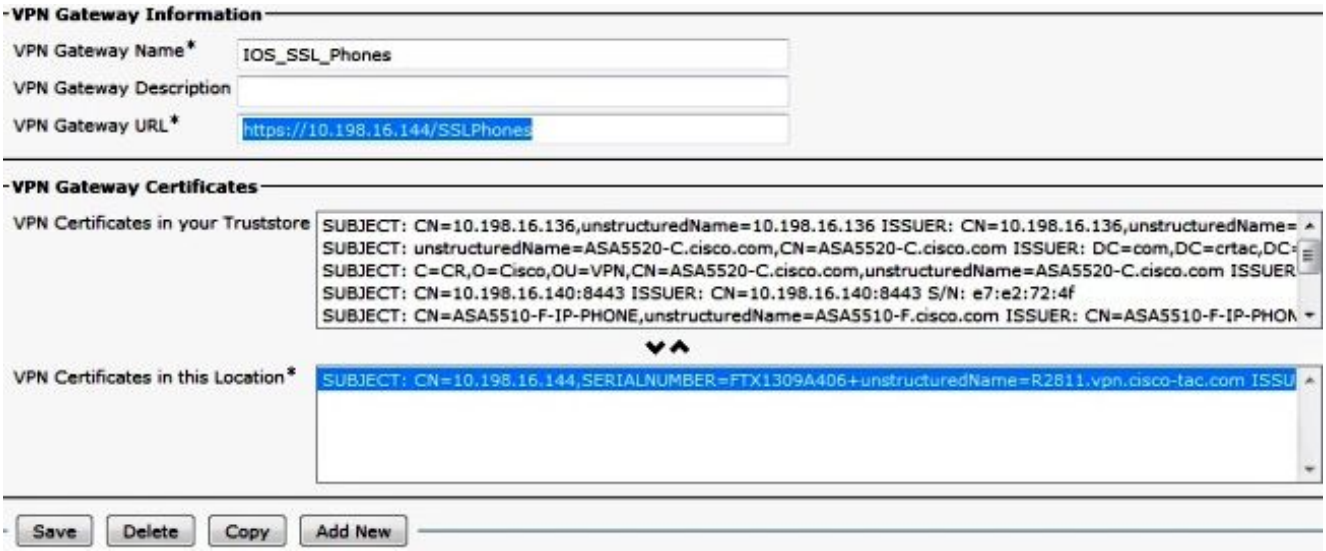
1. Check the certificate used for SSL.
   ```
   Router#show webvpn gateway SSL
   SSL Trustpoint: server-certificate
   ```
2. Export the certificate.
   ```
   Router(config)#crypto pki export server-certificate pem terminal
   The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
   -----BEGIN CERTIFICATE-----

   <output removed>

   -----END CERTIFICATE-----
   ```
3. Copy the text from the terminal and save it as a **.pem** file.
4. Log in to Call Manager, 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.

Configure the VPN Gateway, Group, and Profile in the CUCM

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

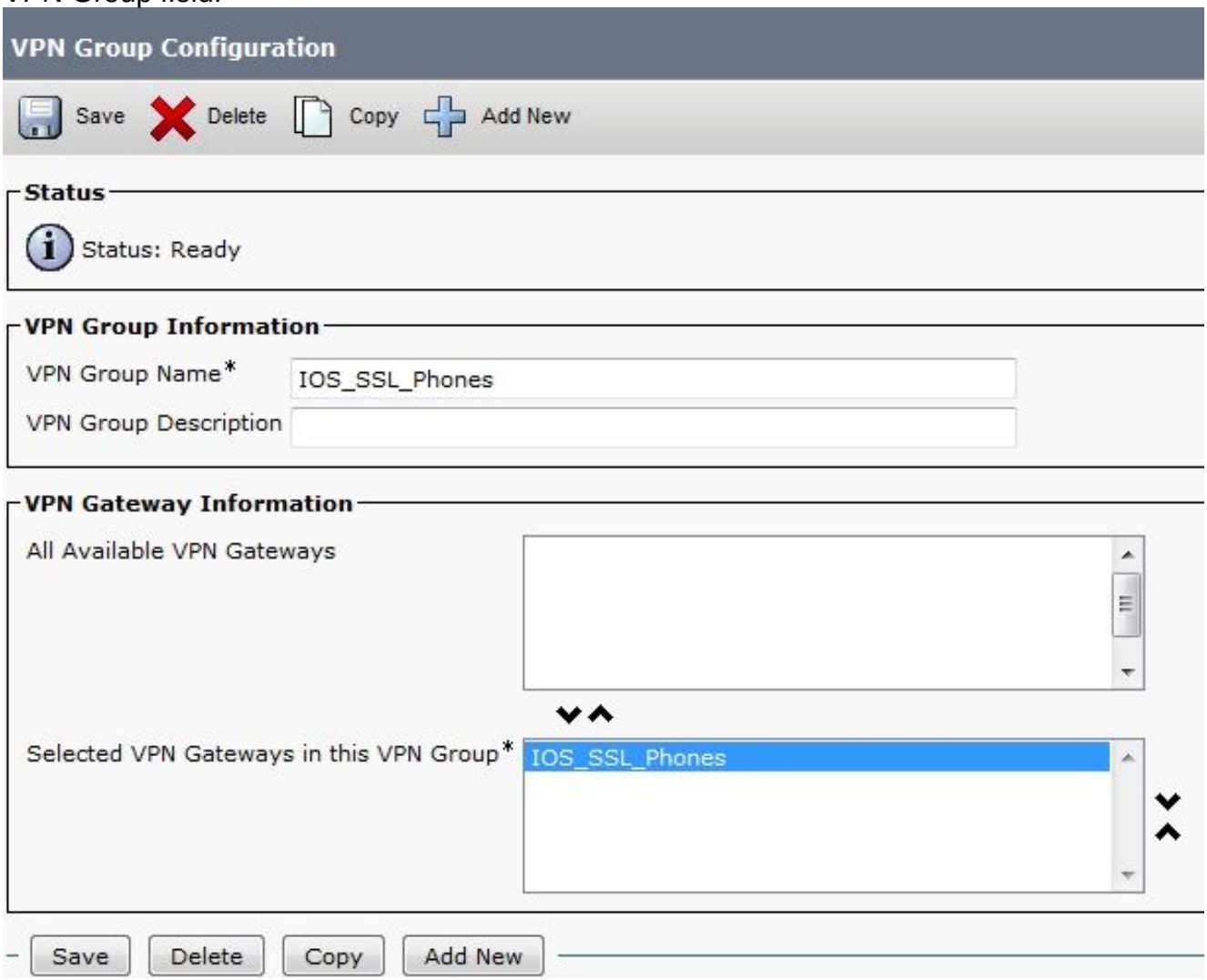


3. In the VPN Gateway Configuration window, complete these steps:
   In the VPN Gateway Name field, enter a name. This can be any name.In the VPN Gateway Description field, enter a description (optional).In the VPN Gateway URL field, enter the group-URL defined on the Router.In the VPN Certificates in this Location field, choose the certificate that was uploaded to Call Manager previously in order to move it from the trust store to this
   location.

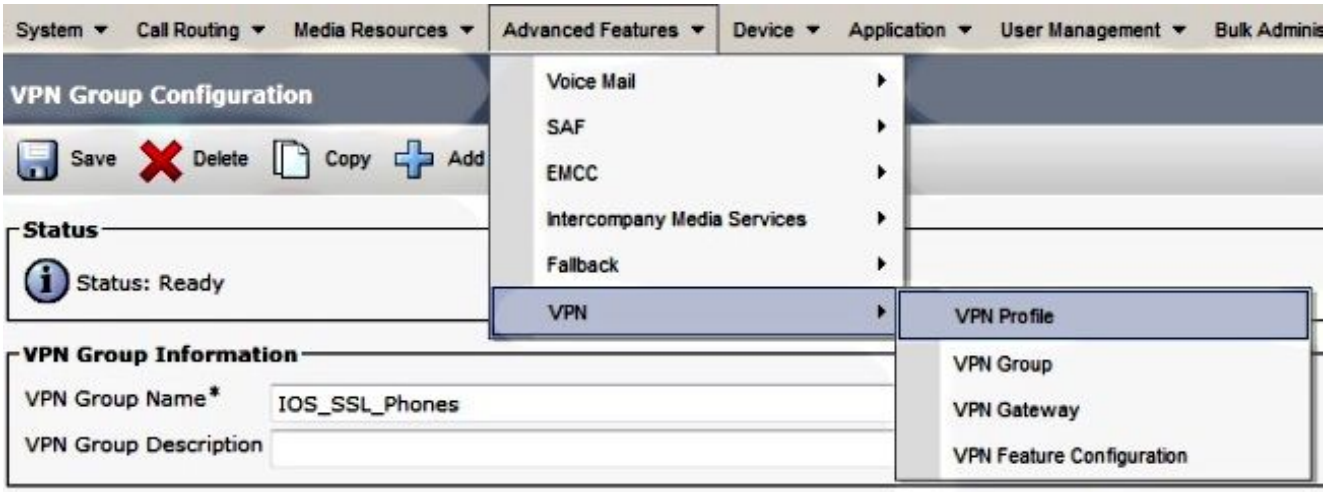


4. From the menu bar, choose **Advanced Features > VPN > VPN Group.**

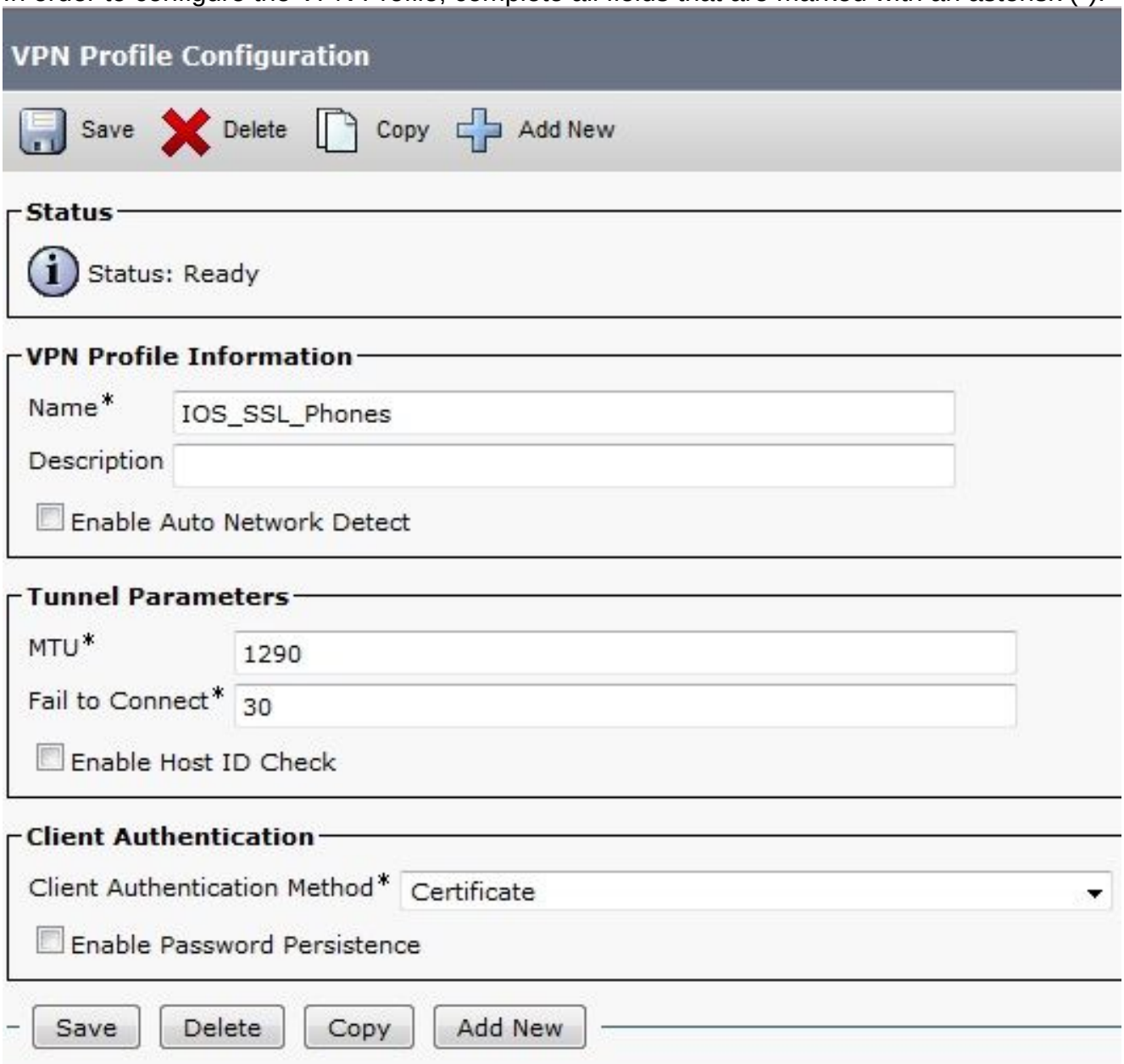
5. In the All Available VPN Gateways field, choose the **VPN Gateway** previously defined. Click the down arrow in order to move the selected gateway to the Selected VPN Gateways in this VPN Group field.



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



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

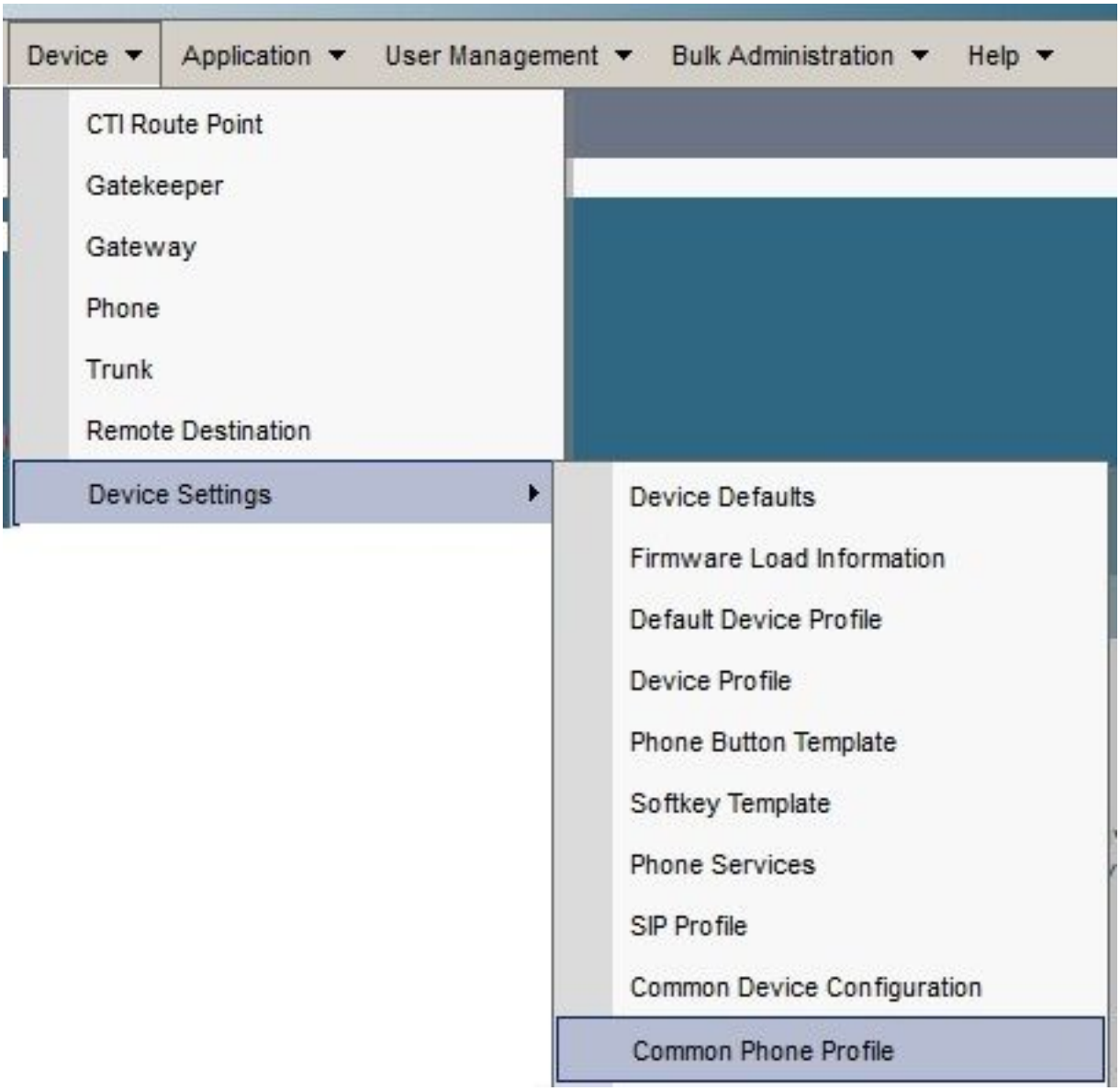


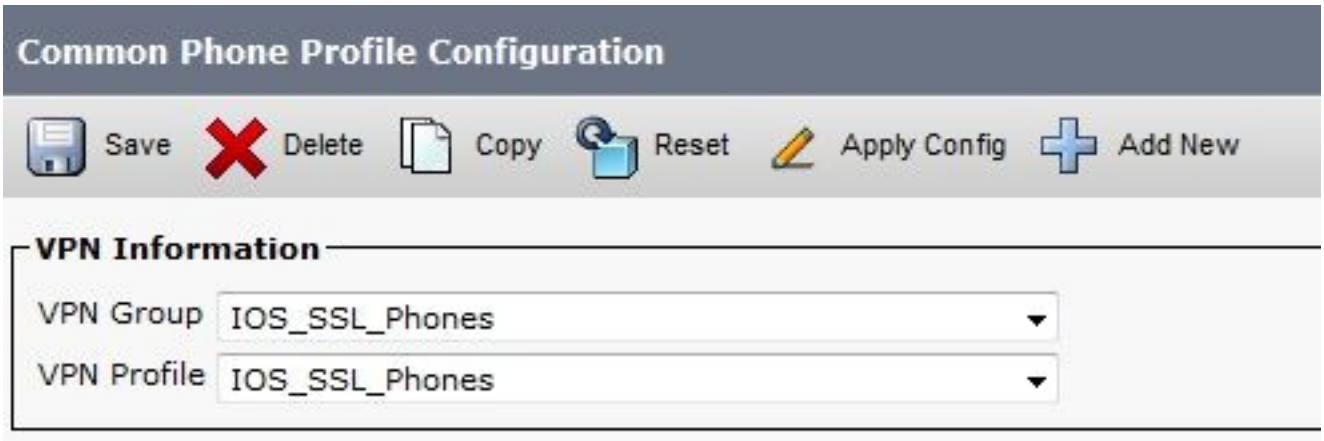
Enable Auto Network Detect: If enabled, the VPN phone pings the TFTP server. If no response is received, it auto-initiates a VPN connection.**Enable Host ID Check:** If enabled, the VPN phone compares the Fully Qualified Domain Name (FQDN) of the VPN Gateway URL against the CN/Storage Area Network (SAN) of the certificate. The client fails to connect if these items 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**.**

Apply the Group and Profile to the IP Phone With the Common Phone Profile

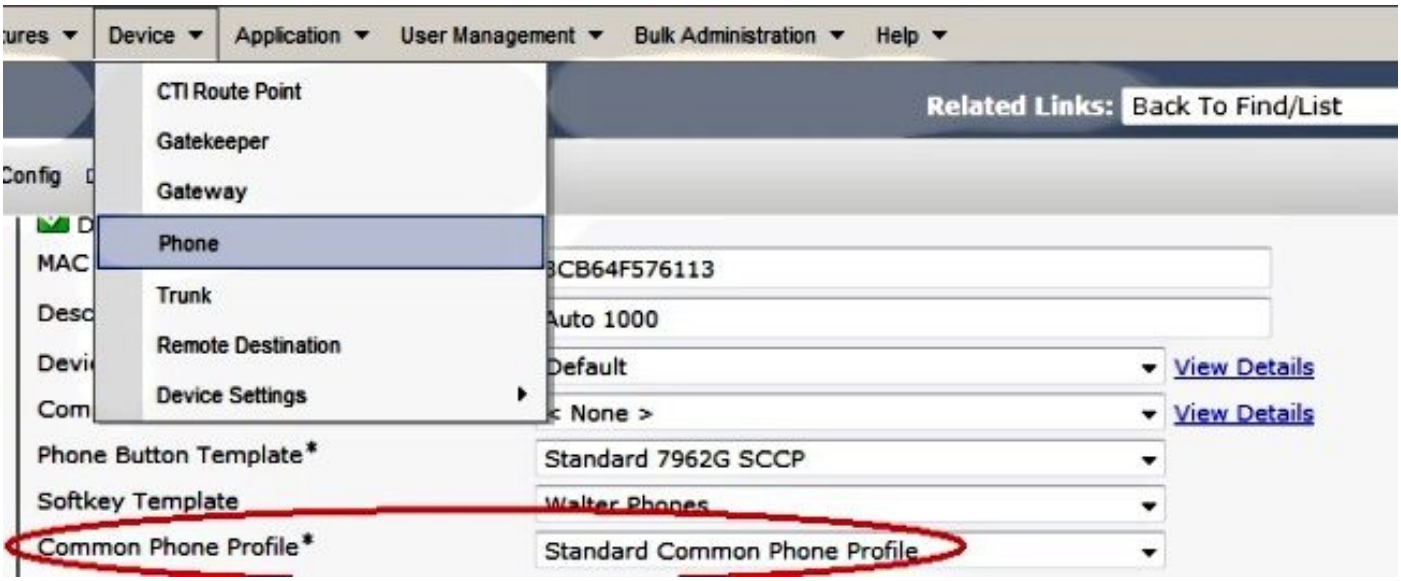
In the Common Phone Profile Configuration window, click **Apply Config** in order to apply the new VPN configuration. You can use the standard **Common Phone Profile** or create a new profile.





Apply the Common Phone Profile to the IP Phone

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



Install Locally Significant Certificates (LSC) on Cisco IP phones

The following guide can be used to install Locally Significant Certificates on Cisco IP phones. This step is only needed if authentication using the LSC is used. Authentication using the Manufacterer Installed Certificate (MIC) or username and password does not require an LSC to be installed.

Install an LSC on a Phone with CUCM Cluster Security Mode set to Non-Secure.

Register the Phone to Call Manager Again in Order to Download the New Configuration

This is the final step in the configuration process.

Verify

Router Verification

In order to check the statistics of the VPN session in the Router, you can use these commands, and check the differences between the outputs (highlighted) for username and certificate authentication:

For username/password authentication:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones                Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
```

```
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones             172.16.250.34              1         00:30:38  00:00:20
```

For certificate authentication:

```
Router#show webvpn session user SEP8CB64F578B2C context all
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint  : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932


Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C    172.16.250.34              1         3d04h     00:00:16
```

CUCM Verification

Confirm that the IP Phone is registered with the Call Manager with the assigned address the Router provided to the SSL connection.

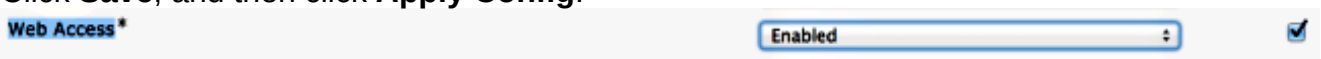
Troubleshoot

Debugs on the SSL VPN Server

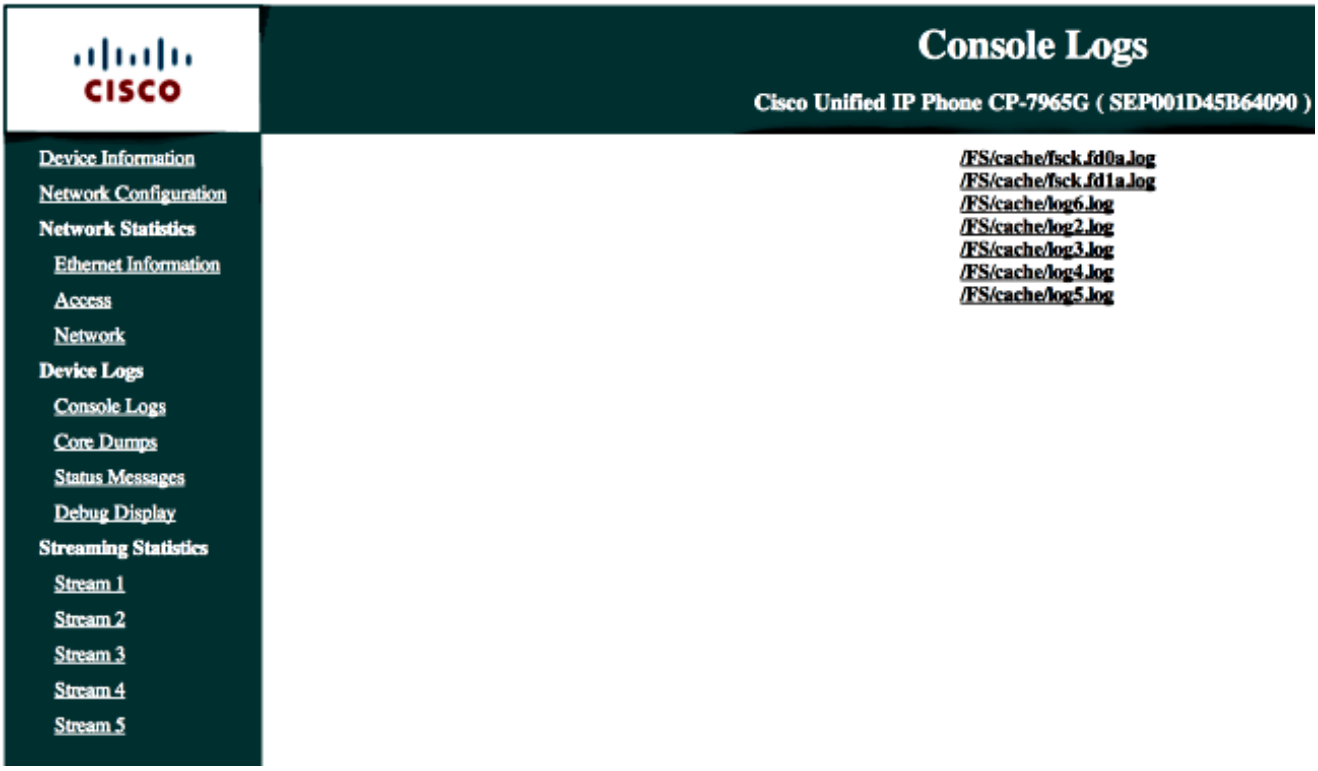
```
Router#show debug

WebVPN Subsystem:
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on


PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

Debugs From the Phone

1. Navigate to **Device > Phone** from CUCM.
2. On the device configuration page, set Web Access to **Enabled**.
3. Click **Save**, and then click **Apply Config**.



4. From a browser, enter the IP address of the phone, and choose **Console Logs** from the menu on the left.



5. Download all of the **/FS/cache/log*.log** files. The console log files contain information about why the phone fails to connect to the VPN.

Related Bugs

Cisco bug ID CSCty46387 , IOS SSLVPN: Enhancement to have a context be a default
Cisco bug ID CSCty46436 , IOS SSLVPN: Enhancement to client certificate validation behavior