VPN Client

- VPN Client Overview, on page 1
- VPN Client Prerequisites, on page 1
- VPN Client Configuration Task Flow, on page 1

VPN Client Overview

The Cisco VPN Client for Cisco Unified IP Phone creates a secure VPN connection for employees who telecommute. All settings of the Cisco VPN Client are configured through Cisco Unified Communications Manager Administration. After the phone is configured within the Enterprise, the users can plug it into their broadband router for instant connectivity.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Unified Communications Manager.

VPN Client Prerequisites

Pre-provision the phone and establish the initial connection inside the corporate network to retrieve the phone configuration. You can make subsequent connections using VPN, as the configuration is already retrieved on the phone.

VPN Client Configuration Task Flow

Pre-provision the phone and establish the initial connection inside the corporate network to retrieve the phone configuration. You can make subsequent connections using VPN, as the configuration is already retrieved on the phone.

Procedure

	Command or Action	Purpose
Step 1	Complete Cisco IOS Prerequisites, on page 3	Complete Cisco IOS prerequisites. Perform this action if you want to configure Cisco IOS VPN.
Step 2	Configure Cisco IOS SSL VPN to Support IP Phones , on page 3	Configure Cisco IOS for VPN client on an IP Phone. Perform this action if you want to configure Cisco IOS VPN.
Step 3	Complete ASA Prerequisites for AnyConnect, on page 5	Complete ASA prerequisites for AnyConnect. Perform this action if you want to configure ASA VPN.
Step 4	Configure ASA for VPN Client on IP Phone, on page 5	Configure ASA for VPN client on an IP Phone. Perform this action if you want to configure ASA VPN.
Step 5	Configure the VPN concentrators for each VPN Gateway.	To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, set up the VPN concentrator close in the network to the TFTP or Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TFTP or load server that is next to the VPN concentrator.
Step 6	Upload VPN Concentrator Certificates, on page 7	Upload the VPN concentrator certificates.
Step 7	Configure VPN Gateway, on page 8	Configure the VPN gateways.
Step 8	Configure VPN Group, on page 9	After you create a VPN group, you can add one of the VPN gateways that you just configured to it.
Step 9	Perform one of the following: • Configure VPN Profile, on page 10 • Configure VPN Feature Parameters, on page 11	You must configure a VPN profile only if you have multiple VPN groups. The VPN Profile fields take precedence over the VPN Feature Configuration fields.
Step 10	Add VPN Details to Common Phone Profile, on page 13	Add the VPN Group and VPN Profile to a Common Phone Profile.
Step 11	Upgrade the firmware for Cisco Unified IP Phone to a version that supports VPN.	To run the Cisco VPN client, a supported Cisco Unified IP Phone must be running firmware release 9.0(2) or higher. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for Unified Communications Manager for yourCisco Unified IP Phone model.
Step 12	Using a supported Cisco Unified IP Phone, establish the VPN connection.	Connect your Cisco Unified IP Phone to a VPN.

Complete Cisco IOS Prerequisites

Use this procedure to complete Cisco IOS Prerequisites.

Procedure

Step 1 Install Cisco IOS Software version 15.1(2)T or later.

Feature Set/License: Universal (Data & Security & UC) for IOS ISR-G2 and ISR-G3

Feature Set/License: Advanced Security for IOS ISR

Step 2 Activate the SSL VPN License.

Configure Cisco IOS SSL VPN to Support IP Phones

Use this procedure to complete Cisco IOS SSL VPN to Support IP Phones.

Procedure

Step 1 Configure Cisco IOS locally.

a) Configure the Network Interface.

Example:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) Configure static and default routes by using this command:

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

Example:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

Step 2 Generate and register the CAPF certificate to authenticate the IP phones with an LSC.

Step 3 Import the CAPF certificate from Unified Communications Manager.

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Note This location changes based on the Unified Communications Manager version.

b) Find the Cisco_Manufacturing_CA and CAPF certificates. Download the .pem file and save as .txt file.

c) Create trustpoint on the Cisco IOS software.

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

When prompted for the base 64-encoded CA certificate, copy and paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following Cisco IOS self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

```
Router(config)# crypto pki export <name> pem terminal
```

  Copy the text from the terminal and save it as a .pem file and upload it to the Unified Communications Manager using the Cisco Unified OS Administration.

Step 4 Install AnyConnect on Cisco IOS.

Download the Anyconnect package from cisco.com and install to flash.

Example:

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

Step 5 Configure the VPN feature.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

Complete ASA Prerequisites for AnyConnect

Use this procedure to complete ASA Prerequisites for AnyConnect.

Procedure

Step 1 Install ASA software (version 8.0.4 or later) and a compatible ASDM.

Step 2 Install a compatible AnyConnect package.

Step 3 Activate License.

a) Check features of the current license using the following command:

show activation-key detail

b) If necessary, obtain a new license with additional SSL VPN sessions and enable the Linksys phone.

Step 4 Make sure that you configure a tunnel-group with a non-default URL as follows:

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

Consider the following when configuring non-default URL:

- If the IP address of the ASA has a public DNS entry, you can replace it with a Fully Qualified Domain Name (FQDN).
- You can only use a single URL (FQDN or IP address) on the VPN gateway in Unified Communications Manager.
- It is preferred to have the certificate CN or subject alternate name match the FQDN or IP address in the group-url.
- If the ASA certificate CN or SAN does not match with the FQDN or IP address, uncheck the host ID check box in the Unified Communications Manager.

Configure ASA for VPN Client on IP Phone

Use this procedure to configure ASA for VPN Client on IP Phone.

Note Replacing ASA certificates results in non-availability of Unified Communications Manager.

Procedure

Step 1 Local configuration

a) Configure network interface.

Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) Configure static routes and default routes.

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.

Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

Step 2 Generate and register the necessary certificates for Unified Communications Manager and ASA.

Import the following certificates from the Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the `.pem` file and save as a `.txt` file.
c) Create trustpoint on the ASA.

Example:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded `.pem` file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
```

```
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

  Copy the text from the terminal and save it as a .pem file and upload it to Unified Communications Manager.

Step 3 Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA Certificate Configuration

For more information on *ASA certificate configuration*, see Configure AnyConnect VPN Phone with Certificate Authentication on an ASA

Upload VPN Concentrator Certificates

Generate a certificate on the ASA when you set it up to support the VPN feature. Download the generated certificate to your PC or workstation and then upload it to Unified Communications Manager using the procedure in this section. Unified Communications Manager saves the certificate in the Phone-VPN-trust list.

The ASA sends this certificate during the SSL handshake, and the Cisco Unified IP Phone compares it against the values stored in the Phone-VPN-trust list.

If a Locally Significant Certificate (LSC) is installed on the Cisco Unified IP Phone, it will send its LSC by default.

To use device level certificate authentication, install the root MIC or CAPF certificate in the ASA, so that the Cisco Unified IP Phone are trusted.

To upload certificates to Unified Communications Manager, use the Cisco Unified OS Administration.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 From the **Certificate Purpose** drop-down list, choose **Phone-VPN-trust**.

Step 4 Click **Browse** to choose the file that you want to upload.

Step 5 Click **Upload File**.

Step 6 Choose another file to upload or click **Close**.

For more information, see *Certificate Management* chapter.

Configure VPN Gateway

Ensure that you have configured VPN concentrators for each VPN gateway. After configuring the VPN concentrators, upload the VPN concentrator certificates. For more information, see Upload VPN Concentrator Certificates, on page 7.

Use this procedure to configure the VPN Gateway.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Gateway**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.
b) Click the **Copy** next to the VPN gateway that you want to copy.
c) Locate the appropriate VPN gateway and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Gateway Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 8.

Step 4 Click **Save**.

VPN Gateway Fields for VPN Client

The table describes the VPN Gateway fields for VPN Client.

Table 1: VPN Gateway Fields for VPN Client

Field	Description
VPN Gateway Name	Enter the name of the VPN gateway.
VPN Gateway Description	Enter a description of the VPN gateway.
VPN Gateway URL	Enter the URL for the main VPN concentrator in the gateway. **Note** You must configure the VPN concentrator with a group URL and use this URL as the gateway URL. For configuration information, refer to the documentation for the VPN concentrator, such as the following: • *SSL VPN Client (SVC) on ASA with ASDM Configuration Example*
VPN Certificates in this Gateway	Use the up and down arrow keys to assign certificates to the gateway. If you do not assign a certificate for the gateway, the VPN client fails to connect to that concentrator. **Note** You can assign up to 10 certificates to a VPN gateway, and you must assign at least one certificate to each gateway. Only certificates that are associated with the Phone-VPN-trust role appear in the available VPN certificates list.

Configure VPN Group

Use this procedure to configure VPN Group.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Group**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.
b) Click **Copy** next to the VPN group that you want to copy an existing VPN group.
c) Locate the appropriate VPN group and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Group Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 8 for the field description details.

Step 4 Click **Save**.

VPN Group Fields for VPN Client

The table describes the VPN Group Fields for VPN Client.

Table 2: VPN Group Fields for VPN Client

Field	Definition
VPN Group Name	Enter the name of the VPN group.
VPN Group Description	Enter a description of the VPN group.
All Available VPN Gateways	Scroll to see all available VPN gateways.
Selected VPN Gateways in this VPN Group	Use the up and down arrow buttons to move available VPN gateways into and out of this VPN group. If the VPN client encounters critical error and cannot connect to a particular VPN gateway, it will attempt to move to the next VPN gateway in the list. **Note** You can add up to a maximum of three VPN gateways to a VPN group. Also, the total number of certificates in the VPN group cannot exceed 10.

Configure VPN Profile

Use this procedure to configure the VPN Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Profile**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profle.
b) Click **Copy** next to the VPN profile that you want to copy an existing profile.
c) To update an existing profile, specify the appropriate filters in the **Find VPN Profile Where**, click **Find**, and modify the settings.

Step 3 Configure the fields in the **VPN Profile Configuration** window. For more information, see VPN Profile Fields for VPN Client, on page 10 for the field description details.

Step 4 Click **Save**.

VPN Profile Fields for VPN Client

The table describes the VPN profile field details.

Table 3: VPN Profile Field Details

Field	Definition
Name	Enter a name for the VPN profile.

Field	Definition
Description	Enter a description for the VPN profile.
Enable Auto Network Detect	When you check this check box, the VPN client can only run when it detects that it is out of the corporate network. Default: Disabled.
MTU	Enter the size, in bytes, for the Maximum Transmission Unit (MTU). Default: 1290 bytes.
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds
Enable Host ID Check	When you check this check box, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: Enabled
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC)
Enable Password Persistence	When you check this check box, a user password gets saved in the phone until either a failed log in attempt occurs, a user manually clears the password, or the phone resets or loses power.

Configure VPN Feature Parameters

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 2 Configure the fields in the **VPN Feature Configuration** window. For more information, see VPN Feature Parameters, on page 12.

Step 3 Click **Save**.

Perform the following tasks:

- Upgrade the firmware for Cisco Unified IP Phones to a version that supports VPN. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for your Cisco Unified IP Phone model.
- Using a supported Cisco Unified IP Phone, establish the VPN connection.

VPN Feature Parameters

The table describes the VPN feature parameters.

Table 4: VPN Feature Parameters

Field	Default
Enable Auto Network Detect	When True, the VPN client can only run when it detects that it is out of the corporate network. Default: False
MTU	This field specifies the maximum transmission unit: Default: 1290 bytes Minimum: 256 bytes Maximum: 1406 bytes
Keep Alive	This field specifies the rate at which the system sends the keep alive message. **Note** If it is non zero and less than the value specified in Unified Communications Manager, the keep alive setting in the VPN concentrator overwrites this setting. Default: 60 seconds Minimum: 0 Maximum: 120 seconds
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds Minimum: 0 Maximum: 600 seconds
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC) Default: User And Password
Enable Password Persistence	When True, a user password gets saved in the phone, if Reset button or "**#**" is used for reset. The password does not get saved and the phone prompts for credentials if the phone loses power or you initiate a factory reset. Default: False

Field	Default
Enable Host ID Check	When True, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: True

Add VPN Details to Common Phone Profile

Use this procedure to add VPN details to common phone profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Click **Find** and choose common phone profile to which you want to add the VPN details.

Step 3 In the **VPN Information** section, choose the appropriate **VPN Group** and **VPN Profile**.

Step 4 Click **Save** and then **Apply Config**.

Step 5 Click **OK** in apply configuration window.