# VPN Feature Setup

This chapter provides information about the VPN feature configuration parameters.

✎

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

## About VPN Feature Setup

The **VPN Feature Configuration** window contains the common configuration settings for the VPN feature that the system uses when you do not associate a VPN Profile with a Common Phone Profile. If you define a VPN Profile as part of configuring a Common Phone Profile, the VPN Profile settings take precedence over the VPN Feature Configuration settings.

## 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 2.

**Step 3**    Click **Save**.

**What to do next**

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 model.

- Using a supported , establish the VPN connection.

# VPN Feature Parameters

**Table 1: 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.<br><br>Default: False |
| MTU | This field specifies the maximum transmission unit:<br><br>Default: 1290 bytes<br><br>Minimum: 256 bytes<br><br>Maximum: 1406 bytes |
| Keep Alive | This field specifies the rate at which the system sends the keep alive message.<br><br>**Note** If it is non zero and less than the value specified in , the keep alive setting in the VPN concentrator overwrites this setting.<br><br>Default: 60 seconds<br><br>Minimum: 0<br><br>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.<br><br>Default: 30 seconds<br><br>Minimum: 0<br><br>Maximum: 600 seconds |
| Client Authentication Method | From the drop-down list, choose the client authentication method:<br><br>• User and password<br><br>• Password only<br><br>• Certificate (LSC or MIC)<br><br>Default: User And Password |

| Field | Default |
|---|---|
| Enable Password Persistence | When True, a user password gets saved in the phone until either a failed login attempt occurs, a user manually clears the password, or the phone resets or loses power.<br><br>Default: False |
| Enable Host ID Check | When True, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected.<br><br>Default: True |