



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, page 1](#)
- [Edit VPN feature parameters, page 1](#)
- [VPN feature parameters, page 2](#)

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.

Edit VPN feature parameters

To edit the VPN feature configuration parameters, follow this procedure:

Procedure

- Step 1** In Cisco Unified Communications Manager Administration, choose **Advanced Features > VPN > VPN Feature Configuration**.
 - Step 2** Accept the suggested values or enter a new value.
 - Step 3** Click **Save**.
-

Related Topics

[VPN feature setup, on page 1](#)

VPN feature parameters

The following table provides descriptions of the VPN feature configuration parameters.

Table 1: VPN Feature Configuration 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 Cisco 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 log-in or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds Minimum: 0 Maximum: 600 seconds

Field	Default
Client Authentication Method	<p>From the drop-down list, choose the client authentication method:</p> <ul style="list-style-type: none">• User and password• Password only• Certificate (LSC or MIC) <p>Default: User And Password</p>
Enable Password Persistence	<p>When True, 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.</p> <p>Default: False</p>
Enable Host ID Check	<p>When True, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected.</p> <p>Default: True</p>

