# Cisco AnyConnect Secure Mobility Client


- Cisco AnyConnect Feature Support, page 1
- AnyConnect Profiles and the Cisco ASA, page 3


# Cisco AnyConnect Feature Support

Cisco Virtualization Experience Media Engine supports Cisco AnyConnect Secure Mobility Client, Release 3.1. The Cisco AnyConnect Secure Mobility client provides remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). Cisco AnyConnect Secure Mobility client supports Cisco ASA version 8.0(4) or later and the Adaptive Security Device Manager (ASDM) 6.4(1) or later.

Cisco AnyConnect is available as a separate add-on that you can push to your devices using the standard add-on procedure.

**Note** Application upgrades of Cisco AnyConnect 3.1 from the ASA are not supported.

The following table shows the AnyConnect features supported on the thin clients.

***Table 1: AnyConnect Feature Support***

| Feature | Supported on SUSE Linux-based Thin Clients |
|---|---|
| Datagram Transport Layer Security (DTLS) with SSL access to VPN | Yes |
| IPSec/IKEv2 support | No |
| Compression -Increases the communications performance between the security appliance and the client | Yes |
| Fallback from DTLS to TLS if DTLS fails | Yes |
| Certificate-only authentication | No |
| Machine certificate authentication for standalone mode | No |

| Feature | Supported on SUSE Linux-based Thin Clients |
|---|---|
| RSA SecurID integration | No |
| Smartcard support | No |
| Download certificate from ASA with Get Certificate | No |
| Simple Certificate Enrollment Protocol (SCEP) to set up and renew a certificate used for client authentication | No |
| GUI interface | Yes, Legacy |
| Minimize on connect | Yes |
| IPv6 VPN access-Allows access to IPv6 resources over a public IPv4 connection | No |
| Local LAN access | No |
| Local printer access through client firewall rules | No |
| Trusted network detection (TND) | No |
| Captive portal (hotspot) detection | No |
| Start Before Logon (SBL) | No |
| Autoconnect on start | Yes |
| Resume session after loss of connectivity | Yes |
| Auto update AnyConnect | N/A (update using Dell Wyse Device Manager) |
| Auto update AnyConnect profile | Yes |
| Diagnostic AnyConnect Reporting Tool (DART) | N/A |
| Federal Information Processing Standard (FIPS) security | Yes |
| Browser-based (clientless) VPN access | No |
| Endpoint assessment (Posture) | No |
| Endpoint remediation | No |
| Web security-Enforces acceptable use policies to protect endpoints from websites found to be unsafe | No |
| Network Access Manager (NAM) - L2 | No |

# AnyConnect Profiles and the Cisco ASA

To enable Cisco AnyConnect connections, set up Cisco AnyConnect profiles on the Cisco Adaptive Security Appliance (ASA). Next, specify the required VPN INI connection parameters on the thin client. After you set up the required profiles and push the INI parameters to the client, users can then establish secure connections.

Before you provide the devices to your remote employees, push the required configuration to the devices on your local network first. You can then provide the preconfigured devices to remote users to operate behind the Cisco AnyConnect VPN.

## Profile Setup on Cisco ASA

On the Cisco Adaptive Security Appliance (ASA), AnyConnect profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (Cisco ASA) hosts that you want to make accessible. In addition, the profile specifies extra connection attributes and constraints for a user. Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and extra settings as needed.

By creating and assigning different profiles to group policies configured on the Cisco ASA, you can differentiate access to Cisco ASA features. The Cisco ASA automatically pushes the profile assigned to the user upon connection setup.

You can configure a profile using the AnyConnect profile editor, a GUI-based configuration tool launched from the Adaptive Security Device Manager (ASDM). The AnyConnect software package, version 3.0 and later, includes the editor. The editor starts when you load the AnyConnect package on the Cisco ASA as an SSL VPN client image.

For detailed configuration information, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

## Cisco AnyConnect Setup Using INI Parameters

To set up Cisco AnyConnect on the device, configure the Custom Connect INI parameter to create Cisco AnyConnect connections. Use the INI parameters to specify the Cisco Adaptive Security Appliance (ASA) address and settings.

### Custom Connect Configuration

To create the Cisco AnyConnect connection, configure the Custom Connect parameter in your INI file. The Custom Connect parameter includes a Command option to enable Cisco AnyConnect at startup and to include a Cisco AnyConnect icon on the desktop.

```
CONNECT=Custom \
Description="ASA Connection" \
AutoConnect=Yes \
Reconnect=Yes \
ReconnectSeconds=100 \
Command=/opt/cisco/anyconnect/bin/vpnui
```

**Note** In the INI file, include the `INIFileSource=cache` parameter. This parameter ensures that devices use the local cached version of the INI file if they cannot access the INI files from Cisco VXC Manager. This parameter is important for devices running the Cisco AnyConnect VPN. These devices require a configuration to reference at bootup before connecting to the network over VPN.

***Table 2: Custom Connect Options***

| Parameter | Description |
|---|---|
| AutoConnect={no, yes} | **Default is no.**<br>Yes or no option to start a connection automatically at sign-on. |
| Command=<command or application to be executed from the client> | **Mandatory Option**<br>Specifies a command or application to be executed from the client. For Cisco AnyConnect: Command=/opt/cisco/anyconnect/bin/vpnui |
| Description=<string description> | **Mandatory Option**<br>Connection description. Provides a connection name for the Desktop icon and the Connection Manager.<br>**Caution** The text must be enclosed in quotation marks if it contains spaces or punctuation characters. These characters are not allowed: & ‘ “ $ ? ! \| ; ( ) [ ] { } \ |
| Reconnect={no, yes} | **Default is no.**<br>Yes or no option to automatically reconnect to an application server after a disconnection. |
| ReconnectSeconds=<value in seconds> | **Default is 30.**<br>Specifies the amount of time in seconds (default is 30) to wait before automatic reconnection to an application server after a disconnection. Requires Reconnect=yes or 1. |

**Caution** Do not insert any additional spaces at the end of lines in the INI file. Extra spaces may cause the device to parse the INI file incorrectly.

## INI Parameters for Cisco ASA Settings

To complete the Cisco AnyConnect setup, specify the Cisco ASA address and settings using the following INI parameters. After you configure these settings and the Custom Connect parameter, push the updated INI file to your devices to enable VPN connections.

*Table 3: Cisco AnyConnect INI Parameters*

| Parameter | Description |
|---|---|
| VPNGroup=<Group name>,... (optional) | Use this parameter if you configure groups on the Cisco ASA. This parameter specifies the name or names (separated by commas) that the Cisco AnyConnect Client can use for the VPN connection. |
| VPNHeadendAddress= <FQDN or IP address> (required) | Specifies the VPN headend FQDN or IP Address to autoconfigure the Cisco AnyConnect Client. For example, VPN.Cisco.com or 192.168.0.1. |

The following shows an example configuration:

```
VPNGroup= profilename
VPNHeadendAddress=192.168.0.1
```

# Upgrades Over VPN

If you upgrade devices over a VPN connection, be aware of the following considerations:

- If the configured address discovery method for Dell Wyse Device Manager is DHCP, ensure that AnyConnect propagates these tags across the VPN.
- An image upgrade over a VPN can take a few hours (depending on the speed of the link). If the user disconnects from the VPN before the upgrade process is complete, the download starts from scratch at the next log in.