



## About This Guide

---

This guide explains how to use ASDM to configure selected VPN features on the Adaptive Security Appliance.

## Audience

This guide is for system engineers (SEs) and network administrators who use the Adaptive Security Device Manager to set up and configure ASAs for virtual private networking. You should be familiar with networking equipment, basic networking concepts and virtual private networking.

## Organization

The following table describes each chapter in this guide:

Chapter	Description
<a href="#">Chapter 1, “Enrolling for Digital Certificates”</a>	Provides information on enrolling for digital certificates, generating key pairs, creating a trustpoint, and using SCEP to obtain certificates.
<a href="#">Chapter 2, “Configuring Group Policies”</a>	Provides information on configuring group policies. Describes how group policies relate to tunnel groups and users.
<a href="#">Chapter 3, “Configuring the SSL VPN Client”</a>	Provides information on configuring SVC, which is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers.
<a href="#">Chapter 4, “Configuring Client Update for Windows and VPN 3002 Clients”</a>	Describes how to configure client update, which lets administrators at a central location automatically notify VPN client users that it is time to update VPN client software and the VPN 3002 hardware client image.
<a href="#">Chapter 5, “Configuring DDNS Updates”</a>	Describes how to configure the DHCP server to update dynamic DNS resource records.

Chapter	Description
<a href="#">Chapter 6, “Configuring an LDAP AAA Server”</a>	Presents an example configuration procedure for configuring security appliance user authentication and authorization using a Microsoft Active Directory Server (LDAP) that sits on the same internal network as the security appliance.
<a href="#">Chapter 7, “Configuring Citrix MetaFrame Services”</a>	Provides information about configuring the security appliance to support Citrix MetaFrame services. Includes instructions on configuring certificates for this purpose.
<a href="#">Chapter 8, “Configuring Single Sign-on for WebVPN”</a>	Provides information about SSO, which lets WebVPN users enter a username and password only once to access multiple protected services and web servers. Includes instructions for configuring Siteminder SSO and HTTP Form protocol.
<a href="#">Chapter 9, “Configuring Network Admission Control”</a>	Provides information on configuring Network Admission Control, which protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network.
<a href="#">Chapter 10, “Configuring L2TP over IPSec”</a>	Describes how to configure the security appliance to let remote Windows clients use Layer 2 Tunneling Protocol (L2TP) to access the public IP network to securely communicate with private corporate network servers.
<a href="#">Chapter 11, “Configuring Load Balancing”</a>	Describes the concept of load balancing and how to configure load balancing on an ASA model 5520 or higher.
<a href="#">Chapter 12, “Configuring Easy VPN Services on the ASA 5505”</a>	Describes how to configure an VPN services on an ASA 5505, which can run as a hardware client or as a headend, but not both at the same time.

## Related Documentation

This guide is a companion to the following user guides:

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA 7.1(1) from the VPN 3000 Series Concentrator*

- *Release Notes for Cisco Secure Desktop*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	User actions and commands are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
screen font	Terminal sessions and information the system displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> in the command-line interface (for example, <b>vpnclient stat</b> ).

Notes use the following conventions:



### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:



### Caution

Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, 0001.03cF.0238).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, VPN01). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.

Type of Data	Format
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.