



## Managing Remote Access VPNs: The Basics

---

Cisco Security Manager lets you configure both remote access IPSec VPNs and remote access SSL VPNs. Security Manager provides flexible configuration and management of remote access VPNs:

- You can discover existing remote access VPN configuration policies from existing live devices or from configuration files. Then, you can change and deploy new or updated policies, as necessary.
- You can use the configuration wizard to help you quickly and easily set up these two types of remote access VPNs with basic functionality.
- If you know the functions and feature your network requires, you can configure remote access VPNs independently. You can also use the wizard to create a basic remote access VPN and then configure additional features that are not included in the wizard separately.

In addition, Cisco Security Manager provides flexibility in how remote access VPN configuration policies are assigned: Device view or Policy view.

For some policies, you can also assign either the factory default policy (a private policy), or a shared policy that you created using Security Manager.

This chapter contains the following topics:

- [Understanding Remote Access VPNs, page 30-1](#)
- [Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8](#)
- [Overview of Remote Access VPN Policies, page 30-9](#)
- [Discovering Remote Access VPN Policies, page 30-12](#)
- [Using the Remote Access VPN Configuration Wizard, page 30-13](#)

## Understanding Remote Access VPNs

Security Manager supports two types of remote access VPNs: IPSec and SSL.

This section contains the following topics:

- [Understanding Remote Access IPSec VPNs, page 30-2](#)
- [Understanding Remote Access SSL VPNs, page 30-2](#)

## Understanding Remote Access IPsec VPNs

Remote access IPsec VPNs permit secure, encrypted connections between a company's private network and remote users, by establishing an encrypted IPsec tunnel across the Internet using broadband cable, DSL, dial-up, or other connections.

A remote access IPsec VPN consists of a VPN client and a VPN headend device, or VPN gateway. The VPN client software resides on a user's workstation and initiates the VPN tunnel access to the corporate network. At the other end of the VPN tunnel is the VPN gateway at the edge of the corporate site.

When a VPN client initiates a connection to the VPN gateway device, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). Next the group profile is pushed to the VPN client using mode configuration, and an IPsec security association (SA) is created to complete the VPN connection.

**Tip**

---

For a remote access IPsec VPN hosted on an ASA 8.4(x) device, you have the option of configuring IKE version 2 (IKEv2). If you decide to use IKEv2, you must configure several SSL VPN policies in addition to the regular IPsec policies. The user also must use the AnyConnect 3.0+ VPN client to make an IKEv2 connection. For more information, see [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\)](#), page 30-25.

---

For remote access IPsec VPNs, AAA (authentication, authorization, and accounting) is used for secure access. With user authentication, a valid user name and password must be entered before the connection is completed. User names and passwords can be stored on the VPN device itself, or on an external AAA server that can provide authentication to numerous other databases. For more information on using AAA servers, see [Understanding AAA Server and Server Group Objects](#), page 6-27.

**Note**

---

Site-to-site Easy VPN topologies use some of the same policies and policy objects that are used in remote access IPsec VPNs, but the policies are kept distinct from the remote access policies. In Easy VPN, the remote clients are hardware clients, such as routers, whereas in remote access IPsec VPNs, remote clients are workstations or other devices that use VPN client software. For more information, see [Understanding Easy VPN](#), page 28-1.

---

**Related Topics**

- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\)](#), page 30-25
- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(IOS and PIX 6.3 Devices\)](#), page 30-36
- [Overview of Remote Access VPN Policies](#), page 30-9
- [Discovering Remote Access VPN Policies](#), page 30-12

## Understanding Remote Access SSL VPNs

An SSL VPN lets users access enterprise networks from any Internet-enabled location. Users can make clientless connections, which use only a Web browser that natively supports Secure Socket Layer (SSL) encryption, or they can make connections using a full client (such as AnyConnect) or a thin client.

**Note**

---

SSL VPN is supported on ASA 5500 devices running software version 8.0 and later, running in single-context and router modes, on Cisco 870, 880, 890, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running software version 12.4(6)T and later, and on Cisco 1900, 2900, and 3900 Series routers running software version 15.0(1)M and later. For the 880 Series routers, the minimum software version is 12.4(15)XZ, which is mapped to 12.4(20)T in Security Manager.

---

On IOS devices, remote access is provided through an SSL-enabled VPN gateway. Using an SSL-enabled Web browser, the remote user establishes a connection to the SSL VPN gateway. After the remote user is authenticated to the secure gateway via the Web browser, an SSL VPN session is established and the user can access the internal corporate network. A portal page lets users access all the resources available on the SSL VPN networks.

On ASA devices, remote users establish a secure, remote access VPN tunnel to the security appliance using the Web browser. The SSL protocol provides the secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

User authentication can be done using usernames and passwords, certificates, or both.

**Note**

---

Network administrators provide user access to SSL VPN resources on a group basis instead of on an individual user basis.

---

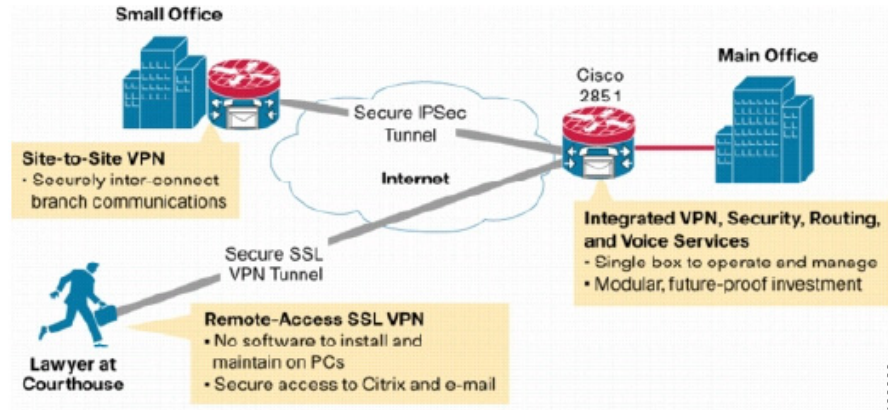
This section contains the following topics:

- [Remote Access SSL VPN Example, page 30-3](#)
- [SSL VPN Access Modes, page 30-4](#)
- [Understanding and Managing SSL VPN Support Files, page 30-5](#)
- [Prerequisites for Configuring SSL VPNs, page 30-7](#)
- [SSL VPN Limitations, page 30-8](#)

## Remote Access SSL VPN Example

The following illustration shows how a mobile worker can access protected resources from the main office and branch offices. Site-to-site IPsec connectivity between the main and remote sites is unaltered. The mobile worker needs only Internet access and supported software (Web browser and operating system) to securely access the corporate network.

Figure 30-1 Secure SSL VPN Access Example



## SSL VPN Access Modes

SSL VPN provides three modes of remote access on IOS routers: Clientless, Thin Client and Full Client. On ASA devices, there are two modes: Clientless (which includes Clientless and Thin Client port forwarding) and AnyConnect Client (a full client).

### Clientless Access Mode

In Clientless mode, the remote user accesses the internal or corporate network using a Web browser on the client machine. No applet downloading is required.

Clientless mode is useful for accessing most content that you would expect in a Web browser, such as Internet access, databases, and online tools that employ a Web interface. It supports Web browsing (using HTTP and HTTPS), file sharing using Common Internet File System (CIFS), and Outlook Web Access (OWA) email. For Clientless mode to work successfully, the remote user's PC must be running Windows 2000, Windows XP, or Linux operating systems.

Browser-based SSL VPN users connecting from Windows operating systems can browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a Web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.

### Thin Client Access Mode

Thin Client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port. In this mode, the remote user downloads a Java applet by clicking the link provided on the portal page. The Java applet acts as a TCP proxy on the client machine for the services configured on the SSL VPN gateway. The Java applet starts a new SSL connection for every client connection.

The Java applet initiates an HTTP request from the remote user client to the SSL VPN gateway. The name and port number of the internal email server is included in the HTTP request. The SSL VPN gateway creates a TCP connection to that internal email server and port.

Thin Client mode extends the capability of the cryptographic functions of the Web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).

**Note**

The TCP port-forwarding proxy works only with Sun's Java Runtime Environment (JRE) version 1.4 or later. A Java applet is loaded through the browser that verifies the JRE version. The Java applet refuses to run if a compatible JRE version is not detected.

When using Thin Client mode, you should be aware of the following:

- The remote user must allow the Java applet to download and install.
- For TCP port-forwarding applications to work seamlessly, administrative privileges must be enabled for remote users.
- You cannot use Thin Client mode for applications such as FTP, where the ports are negotiated dynamically. That is, you can use TCP port forwarding only with static ports.

**Full Tunnel Client Access Mode**

Full Tunnel Client mode enables access to the corporate network completely over an SSL VPN tunnel, which is used to move data at the network (IP) layer. This mode supports most IP-based applications, such as Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet. Being part of the SSL VPN is completely transparent to the applications run on the client. A Java applet is downloaded to handle the tunneling between the client host and the SSL VPN gateway. The user can use any application as if the client host was in the internal network.

The tunnel connection is determined by the group policy configuration. The SSL VPN client (SVC) or AnyConnect client is downloaded and installed to the remote client, and the tunnel connection is established when the remote user logs in to the SSL VPN gateway. By default, the client software is removed from the remote client after the connection is closed, but you can keep it installed, if required.

**Note**

Full Tunnel SSL VPN access requires administrative privileges on the remote client.

## Understanding and Managing SSL VPN Support Files

SSL VPNs sometimes require supporting files that reside in the device's flash storage. This is especially true of SSL VPNs configured on ASA devices. Supporting files include Cisco Secure Desktop (CSD) packages, AnyConnect client images, and plug-in files. Security Manager includes many of these files for your use. However, some supporting files, such as graphic files used for portal pages, or client profiles used for AnyConnect clients are not provided by Security Manager.

Typically, you need to create a File Object to specify a supporting file, and you then select the File Object when you create a policy that refers to it. You can create the File Objects that you need when you create the policies, or you can create them before you start defining policies. For more information, see [Add and Edit File Object Dialog Boxes](#), page 34-36.

When you deploy policies to the devices, any supporting files referenced in your policies are copied to the device and placed in flash memory in the `\csm` folder. For the most part, you do not have to do any manual work to make this happen. The following are some situations where you might need to do some manual work:

- If you are trying to discover existing SSL VPN policies, or rediscover them, file references from the SSL VPN policies must be correct. For detailed information on how supporting files are handled during policy discovery, see [Discovering Remote Access VPN Policies](#), page 30-12.
- If you have configured the ASA device in an Active/Failover configuration, you must get the supporting files onto the failover device. The supporting files are not copied over to the failover device during a failover. You have these choices for getting the files onto the failover device:

- Manually copy the files from the \csm folder on the active unit to the failover unit.
- After deploying the policies to the active unit, force a failover and redeploy the policies to the now-active unit.
- If you are using a VPN cluster for load balancing, the same supporting files must be deployed to all devices in the cluster.

### Cisco Secure Desktop (CSD) Packages

These packages are for ASA SSL VPNs. You select a package in the Dynamic Access policy. The package you select must be compatible with the ASA operating system version running on the device. When you create a Dynamic Access policy for an ASA device, the version number that is compatible with the device's operating system is displayed in the Version field.

You can find the CSD packages in Program Files\CSCOpX\files\vm\repository\. The file names are in the form securedesktop-asa\_k9-version.pkg or csd\_version.pkg, where *version* is the CSD version number such as 3.5.1077.

Following is the CSD compatibility with ASA versions for the CSD packages shipped with Security Manager:

- csd\_3\_6\_181-3.6.181.pkg—ASA 8.4 or later.
- csd\_3\_5\_2008-3.5.2008.pkg—ASA 8.0(4) or later.
- csd\_3\_5\_2001-3.5.2001.pkg—ASA 8.0(4) or later.
- csd\_3\_5\_1077-3.5.1077.pkg—ASA 8.0(4) or later.
- csd\_3\_5\_841-3.5.841.pkg—ASA 8.0(4) or later.
- csd\_3\_4\_2048-3.4.2048.pkg—ASA 8.0(4) or later.
- csd\_3\_4\_1108-3.4.1108.pkg—ASA 8.0(4) or later.
- securedesktop\_asa\_k9-3.3.0.151.pkg—ASA 8.0(3.1) or later.
- securedesktop\_asa-k9-3.3.0.118.pkg—ASA 8.0(3.1) or later.
- securedesktop-asa-k9-3.2.1.126.pkg—ASA 8.0(3) or later.
- securedesktop-asa\_k9-3.2.0.136.pkg—ASA 8.0(2) or later.

For more information on CSD version compatibility with ASA versions, see the CSD release notes at [http://www.cisco.com/en/US/products/ps6742/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6742/prod_release_notes_list.html) and [Supported VPN Platforms](#) on Cisco.com.

For more information on creating Dynamic Access policies to specify the CSD, see [Configuring Cisco Secure Desktop Policies on ASA Devices](#), page 32-9.

### AnyConnect Client Images

These images are for remote access SSL and IKEv2 IPsec VPNs hosted on an ASA. The AnyConnect client is downloaded to the user's PC and manages the client's VPN connection. Security Manager includes several AnyConnect images, which you can find in Program Files\CSCOpX\files\vm\repository\. The package names indicate the workstation operating system and the anyconnect release number in this general pattern:

anyconnect-client\_OS\_information-anyconnect\_release.pkg. For example, anyconnect-win-3.0.0610-k9-3.0.0610.pkg is the AnyConnect 3.0(0610) client for Windows workstations. The k9 indicates that the package includes encryption. In this example, the AnyConnect release number is repeated; in some file names, the release number appears once.

Packages are available for the following workstation operating systems (OS). For specific information on which OS versions that each client supports, see the documentation for the AnyConnect client on Cisco.com.

- Linux—Packages start with anyconnect-linux, or anyconnect-linux-64 for 64-bit versions.
- Mac OS—Packages start with anyconnect-macosx for Mac OS X on i386 workstations, and anyconnect-macosx-powerpc for Mac OS X on Power PC workstations.
- Windows—Packages start with anyconnect-win.

You can also download other AnyConnect client packages to the Security Manager server or your local Security Manager client and use them in remote access policies. However, Security Manager might not be able to configure newer parameters for those clients, although it might be possible to use FlexConfigs to configure newer parameters.

For more information on the AnyConnect client, its profiles, and how to configure policies to load the client onto the device, see the following topics:

- [Understanding SSL VPN AnyConnect Client Settings, page 31-61](#)
- [Configuring SSL VPN AnyConnect Client Settings \(ASA\), page 31-63](#)
- [Cisco AnyConnect Profile Editor, page 31-62](#)

#### Plug-in Files

These files are used as browser plug-ins. You can find plug-in files in Program Files\CSCOPx\files\vm\repository\. For complete information on the available files, see [Configuring SSL VPN Browser Plug-ins \(ASA\), page 31-59](#).

## Prerequisites for Configuring SSL VPNs

For a remote user to securely access resources on a private network behind an SSL VPN gateway, the following prerequisites must be met:

- A user account (login name and password).
- An SSL-enabled browser (such as Internet Explorer, Netscape, Mozilla, or Firefox).
- An email client (such as Eudora, Microsoft Outlook, or Netscape Mail).
- One of the following operating systems:
  - Microsoft Windows 2000 or Windows XP, with either JRE for Windows version 1.4 or later, or a browser that supports ActiveX controls.
  - Linux with JRE for Linux version 1.4 or later. To access Microsoft shared files from Linux in clientless remote access mode, Samba must also be installed.

#### Related Topics

- [SSL VPN Access Modes, page 30-4](#)
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\), page 30-14](#)
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\), page 30-32](#)

## SSL VPN Limitations

SSL VPN configurations in Security Manager are subject to the following limitations:

- SSL VPN license information cannot be imported into Security Manager. As a result, certain command parameters, such as **vpn sessiondb** and **max-webvpn-session-limit**, cannot be validated.
- You must configure DNS on each device in the topology in order to use clientless SSL VPN. Without DNS, the device cannot retrieve named URLs, but only URLs with IP addresses.
- If you share your Connection Profiles policy among multiple ASA devices, bear in mind that all devices share the same address pool unless you use device-level object overrides to replace the global definition with a unique address pool for each device. Unique address pools are required to avoid overlapping addresses in cases where the devices are not using NAT.
- If the device configuration contains an address pool for SSL VPN with a name that begins CSM\_ (the naming convention used by Cisco Security Manager), Cisco Security Manager cannot detect whether the addresses in that pool overlap with the pool configured in your SSL VPN policy. (This can occur, for example, when the pool was configured by a user on a different installation of Security Manager.) This can lead to errors during deployment. Therefore, we recommend that you configure the same IP address pool as a network/host object in Security Manager and define it as part of the SSL VPN policy. This enables the proper validation to take place.
- The same IP address and port number cannot be shared by multiple SSL VPN gateways on the same IOS device. As a result, deployment errors can occur if a duplicate gateway exists in the device configuration but was not redefined using the Security Manager interface. If such an error occurs, you must choose a different IP address and port number and redeploy.
- If you define AAA authentication or accounting as part of an SSL VPN policy, the **aaa new-model** command is deployed to enable AAA services. Bear in mind that this command is not removed if you later delete the SSL VPN policy, as there might be other parts of the device configuration that require the **aaa new-model** command for AAA services.



### Note

In addition, we recommend that you define at least one local user on the device with a privilege level of 15. This ensures that you will not be locked out of the device if the **aaa new-model** command is configured without an associated AAA server.

### Related Topics

- [SSL VPN Access Modes, page 30-4](#)
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\), page 30-14](#)
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\), page 30-32](#)

## Understanding Devices Supported by Each Remote Access VPN Technology

There are three types of remote access VPN: IKE version 1 (IKEv1) IPsec, IKE version 2 (IKEv2) IPsec, and SSL. The devices on which you can configure these technologies differs, and broadly speaking, the configuration for each type of VPN differs for ASA/PIX 7.0+ compared to IOS/PIX 6.3 devices.



The following table describes the basic device support. When you select a device, the device type will determine which remote access policies are visible or configurable.



**Tip**

Some device models have NO-VPN versions, which do not support VPN configuration. Thus, although the 3845 model might be supported for a type of VPN, the 3845 NOVPN model is not supported. In addition, the Cisco Catalyst 6500 series ASA Services Module (running software release 8.5(x)) does not support any type of VPN.

**Table 30-1** *Devices Supported by Each Remote Access Technology*

Technology	Supported Platforms
IKE version 1 IPsec	<ul style="list-style-type: none"> <li>ASA/PIX 7.0+—ASA 5500 series and PIX 515, 515E, 525, or 535 with PIX Software 7.0+ (including 8.0+), running in single context and router modes.</li> <li>IOS/PIX 6.3—Cisco IOS security routers (including Aggregation Service Routers, or ASRs), Catalyst 6500/7600, and PIX Firewalls running PIX Software 6.3 only.</li> </ul>
IKE version 2 IPsec	ASA 5500 series only, running ASA Software 8.4(x) only.
SSL	<ul style="list-style-type: none"> <li>ASA—ASA 5500 series devices running software version 8.0 and later, running in single-context and router modes.</li> <li>IOS—Cisco 870, 880, 890, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running software version 12.4(6)T and later, and on Cisco 1900, 2900, and 3900 Series routers running software version 15.0(1)M and later. For the 880 Series routers, the minimum software version is 12.4(15)XZ, which is mapped to 12.4(20)T in Security Manager.</li> </ul> <p><b>Tip</b> No version of PIX is supported for SSL VPN configuration.</p>

#### Related Topics

- [Understanding Remote Access IPSec VPNs, page 30-2](#)
- [Understanding Remote Access SSL VPNs, page 30-2](#)
- [Using the Remote Access VPN Configuration Wizard, page 30-13](#)
- [Overview of Remote Access VPN Policies for ASA and PIX 7.0+ Devices, page 31-2](#)
- [Overview of Remote Access VPN Policies for IOS and PIX 6.3 Devices, page 33-2](#)

## Overview of Remote Access VPN Policies

The following list summarizes the various policies used in remote access VPN configuration based on the technology used in the VPN. Possible remote access VPN types are: IKE version 1 (IKEv1) IPsec, IKE version 2 (IKEv2) IPsec, and SSL. Where indicated, many of these policies apply to specific device types only. To see an edited version of this list per device type, see the following topics:

- [Overview of Remote Access VPN Policies for ASA and PIX 7.0+ Devices, page 31-2](#)
- [Overview of Remote Access VPN Policies for IOS and PIX 6.3 Devices, page 33-2](#)

**Note**

You cannot configure SSL VPNs on PIX devices; PIX devices support remote access IKEv1 IPsec VPNs only.

**Note**

You can create Unified ACL object on-the-fly in certain Remote Access VPN policies, such as Dynamic Access Policy. However, when you create Unified ACL object on-the-fly, Cisco Security Manager displays an error message. To overcome this issue, you must select the created ACL in the Selector window and save the policy.

- **Policies used with remote access IKEv1 and IKEv2 IPsec and SSL VPNs:**
  - **ASA Cluster Load Balancing (ASA/PIX 7.0+)**—In a remote client configuration in which you are using two or more devices connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. Load balancing is effective only on remote sessions initiated with an ASA device. For more information, see [Understanding Cluster Load Balancing \(ASA\), page 31-5](#).
  - **Connection Profiles (ASA/PIX 7.0+)**—A connection profile is a set of records that contain VPN tunnel connection policies, including the attributes that pertain to creating the tunnel itself. Connection profiles identify the group policies for a specific connection, which includes user-oriented attributes. For more information, see [Configuring Connection Profiles \(ASA, PIX 7.0+\), page 31-7](#).
  - **Dynamic Access (ASA 8.0+)**—Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles that each user might inhabit within an organization, and logins from remote access sites with different configurations and levels of security. Dynamic access policies (DAP) let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. For more information, see [Chapter 32, “Managing Dynamic Access Policies for Remote Access VPNs \(ASA 8.0+ Devices\)”](#).
  - **Global Settings**—You can define global settings that apply to all devices in your remote access VPNs. These settings include Internet Key Exchange (IKE), IKEv2, IPsec, NAT, and fragmentation definitions. The global settings typically have defaults that work in most situations, so configuring the Global Settings policy is optional in most cases; configure it only if you need non-default behavior or if you are supporting IKEv2 negotiations. For more information, see [Configuring VPN Global Settings, page 26-29](#).
  - **Group Policies (ASA/PIX 7.0+)**—You can view the user group policies defined for your remote access VPN connection profiles. From this page, you can specify new ASA user groups and edit existing ones. When you create a connection profile, if you specify a group policy that has not been used on the device, the group policy is automatically added to the Group Policies page; you do not need to add it to this policy before you create the connection profile. For more information, see [Configuring Group Policies for Remote Access VPNs, page 31-26](#).
  - **Public Key Infrastructure**—You can create a Public Key Infrastructure (PKI) policy to generate enrollment requests for CA certificates and RSA keys, and to manage keys and certificates. Certification Authority (CA) servers are used to manage these certificate requests and issue certificates to users who connect to your IPsec or SSL remote access VPN. For more information, see [Understanding Public Key Infrastructure Policies, page 26-50](#) and [Configuring Public Key Infrastructure Policies for Remote Access VPNs, page 26-55](#).

- **Policies used in remote access IPsec VPNs only:**
  - **Certificate To Connection Profile Maps, Policy and Rules** (IKEv1 IPsec only, ASA/PIX 7.0+ only.)—Certificate to connection profile map policies let you define rules to match a user's certificate to a permission group based on specified fields. To establish authentication, you can use any field of the certificate, or you can have all certificate users share a permission group. You can match the group from the DN rules, the Organization Unit (OU) field, the IKE identity, or the peer IP address. You can use any or all of these methods. For more information, see [Configuring Certificate to Connection Profile Map Policies \(ASA\)](#), page 31-36.
  - **IKE Proposal**—Internet Key Exchange (IKE), also called ISAKMP, is the negotiation protocol that enables two hosts to agree on how to build an IPsec security association. IKE is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs). Use the IKE Proposal policy to define the requirements for phase 1 of the IKE negotiation. For more information, see [Configuring an IKE Proposal](#), page 26-9.
  - **IPsec Proposal (ASA/PIX 7.x)**—An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA. The policy is used for IKE phase 2 negotiations. For more information, see [Configuring an IPsec Proposal on a Remote Access VPN Server \(ASA, PIX 7.0+ Devices\)](#), page 31-40.
  - **IPsec Proposal (IOS/PIX 6.x)**—An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA. The policy is used for IKE phase 2 negotiations. For more information, see [Configuring an IPsec Proposal on a Remote Access VPN Server \(IOS, PIX 6.3 Devices\)](#), page 33-3.
  - **High Availability** (IOS/PIX 6.3)—High Availability (HA) is supported by the creation of an HA group made up of two or more hub devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. For more information, see [Configuring High Availability in Remote Access VPNs \(IOS\)](#), page 33-11.
  - **User Groups (IOS/PIX 6.x)**—A user group policy specifies the attributes that determine user access to and use of the VPN. For more information, see [Configuring User Group Policies](#), page 33-13.
- **Policies used in remote access IKEv2 IPsec and SSL VPNs only:**
  - **Access** (ASA only.)—An Access policy specifies the security appliance interfaces on which a remote access SSL or IKEv2 IPsec VPN connection profile can be enabled, the port to be used for the connection profile, Datagram Transport Layer Security (DTLS) settings, the SSL VPN session timeout and maximum number of sessions. You can also specify whether to use the AnyConnect VPN Client or AnyConnect Essentials Client. For more information, see [Understanding SSL VPN Access Policies \(ASA\)](#), page 31-43.
  - **Other Settings** (ASA only.)—The SSL VPN Other Settings policy defines settings that include caching, content rewriting, character encoding, proxy and proxy bypass definitions, browser plug-ins, AnyConnect client images and profiles, Kerberos Constrained Delegation, and some other advanced settings. For more information, see [Configuring Other SSL VPN Settings \(ASA\)](#), page 31-50.
  - **Shared License** (ASA only.)—Use the SSL VPN Shared License page to configure your SSL VPN Shared License. For more information, see [Configuring SSL VPN Shared Licenses \(ASA 8.2+\)](#), page 31-74.

- **SSL VPN (IOS devices only.)**—The SSL VPN policy table lists all of the contexts that define the virtual configurations of the SSL VPN. Each context has a gateway, domain or virtual hostname, and user group policies. For more information, see [Configuring an SSL VPN Policy \(IOS\)](#), page 33-14.

## Discovering Remote Access VPN Policies

Security Manager allows you to import the configurations of remote access IPsec VPN policies during policy discovery. You can also discover SSL VPN policies on ASA devices, but not on IOS devices. To discover remote access VPN policies, select the **RA VPN Policies** option in the Discover Device settings when adding the device to the inventory or when discovering policies on a device already in the inventory. For more information on adding devices or discovering policies, see the following topics:

- [Adding Devices to the Device Inventory](#), page 3-6
- [Discovering Policies on Devices Already in Security Manager](#), page 5-15

You can discover configurations on devices that are already deployed in your remote access VPN network, so that Security Manager can manage them. These configurations are imported into Security Manager as remote access VPN policies. Remote access VPN policy discovery can be performed by importing the configuration of a live device or by importing a configuration file. However, SSL VPN policies that refer to files in flash storage cannot be discovered from configuration files, therefore, we recommend that you do not discover SSL VPNs from configuration files.

When you initiate policy discovery on a device in a remote access VPN, the system analyzes the configuration on the device and then translates this configuration into Security Manager policies so that the device can be managed. Warnings are displayed if the imported configuration completes only a partial policy definition. If additional settings are required, you must go to the relevant page in the Security Manager interface to complete the policy definition. You can also rediscover the configurations of devices that are already managed with Security Manager.

When discovering SSL VPN policies, files residing in flash storage that are referenced in SSL VPN policies are copied to the Security Manager server to be stored in the /csm directory on the target device when policies are deployed from Security Manager. If the flash storage contains files that you want to use, but they are not referenced by an SSL VPN policy, either configure commands that refer to them or manually copy them to the Security Manager server. Policy discovery fails if an SSL VPN policy on the device refers to a file that has been deleted from flash; in this case, either fix the configuration directly before discovering the device, or deselect the **RA VPN Policies** option when adding the device and create the desired SSL VPN configuration in Security Manager.

### Tips

- You should perform deployment immediately after you discover the policies on a device before you make any changes to policies or unassign policies from the device; otherwise, the changes that you configure in Security Manager might not be deployed to the device.
- For ASA and PIX 7.0+ devices, the default connection profiles and group policy are discovered and added to the Connection Profiles and Group Policies policy. You can modify these default profiles and group, but you cannot delete them:
  - **DefaultRAGroup**—The default connection profile for remote access IPsec VPNs.
  - **DefaultWEBVPNGroup**—The default connection profile for SSL VPNs. This connection profile is discovered only for ASA 8.0+ devices.

- DfltGrpPolicy—The default group policy, which is used by the default connection profiles. When discovered, Security Manager uses the name *<device\_display\_name>*DfltGrpPolicy. However, when you deploy configurations, the device display name is stripped off and DfltGrpPolicy is used.

This naming convention is necessary because group policies are modeled as shared policy objects, and you might have modified the default group policy differently on your devices. However, the naming convention does not prevent you from using shared policies that incorporate the default group policy; the device display name is stripped from the object name regardless of the device to which it is assigned. For example, if you use the object 10.100.10.1DfltGrpPolicy with device 10.200.11.1, Security Manager still uses “DfltGrpPolicy” in the configuration.



**Note** Although these default connection profiles use the DfltCustomization object for SSL VPN portal customization, Security Manager does not discover it. To modify DfltCustomization, you must do so directly on the device. However, you can simply create your own customization object and specify it in the default connection profile to use non-default settings.

#### Related Topics

- [Discovering Policies, page 5-12](#)
- [Site-To-Site VPN Discovery, page 25-19](#)
- [VPN Discovery Rules, page 25-21](#)

## Using the Remote Access VPN Configuration Wizard

You can use the Remote Access VPN Configuration wizard to create the policies required to configure a basic IPsec or SSL VPN. The wizard provides simplified options to configure the basic settings. Thus, after using the wizard, you might need to configure additional settings in the individual remote access VPN policies.



#### Tip

The wizard never creates a valid IKEv2 IPsec VPN. You must always configure additional policies to complete an IKEv2 configuration.



#### Note

For Remote Access VPN Multi-Context Mode, only Remote Access SSL VPN is supported for ASA devices running the software version 9.5(2) or later.

Depending on the device type and VPN type (IPsec or SSL), the wizard takes you through the steps to configure a basic remote access VPN.

To access the Remote Access Configuration wizard:

1. In Device view, select the device to configure as your remote access server from the Device selector.
2. Select **Remote Access VPN > Configuration Wizard** from the Policy selector.
3. Select the radio button corresponding to the type of remote access VPN you want to create: **Remote Access SSL VPN** or **Remote Access IPsec VPN**.
4. Click **Remote Access Configuration Wizard** to open the appropriate wizard.

For detailed information on how to use each version of the wizard, see the following topics:

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\)](#), page 30-14
- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\)](#), page 30-25
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\)](#), page 30-32
- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(IOS and PIX 6.3 Devices\)](#), page 30-36

## Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices)

This procedure describes how to create or edit SSL VPNs on ASA devices using the Remote Access SSL VPN Configuration Wizard.

### Related Topics

- [Understanding Remote Access SSL VPNs](#), page 30-2
- [Understanding Devices Supported by Each Remote Access VPN Technology](#), page 30-8

- 
- Step 1** In Device view, select the desired ASA device.
- Step 2** From the Policy selector, select **Remote Access VPN > Configuration Wizard**.
- Step 3** Select the **Remote Access SSL VPN** radio button.
- Step 4** Click **Remote Access Configuration Wizard**. The Access page opens. For a description of the elements on this page, see [SSL VPN Configuration Wizard—Access Page \(ASA\)](#), page 30-16.
- Step 5** Specify the interfaces on which you want to enable the SSL VPN connections. Click **Select** to select an interface or an interface role object that identifies the interfaces.
- Step 6** Specify the port number you want to use for the SSL VPN sessions. Enter the port number or the name of a port list object that defines the number, or click **Select** to select the object or to create a new object.

The default port is 443, for HTTPS traffic. The port number can be 443, or within the range of 1024-65535. If you change the port number, all current SSL VPN connections terminate, and current users must reconnect.




---

**Note** If HTTP port redirection is enabled, the default HTTP port number is 80.

---

- Step 7** To allow users to select a tunnel group from a list of tunnel group connection profiles configured on the device at login, select the **Allow Users to Select Connection Profile in Portal Page** option.
- Step 8** To allow users to use the AnyConnect VPN client to connect to the SSL VPN, select the **Enable AnyConnect Access** check box.
- Step 9** Click **Next**. The Connection Profile page opens. For a description of the elements on this page, see [SSL VPN Configuration Wizard—Connection Profile Page \(ASA\)](#), page 30-17.

**Step 10** In **Connection Profile Name**, enter the name of the connection profile. This is the name of the tunnel group, and will appear in the Remote Access VPN > Connection Profiles policy. For more information about the connection profile policy, see [Configuring Connection Profiles \(ASA, PIX 7.0+\)](#), page 31-7.

**Step 11** On the Connection Profile page, configure these options that will later appear in the General tab of the connection profile (see [General Tab \(Connection Profiles\)](#), page 31-10):

- **Group Policy**—Enter the name of the ASA Group Policy policy object that will be the default group for the connection profile, or click **Select** to select the object. If the required object does not yet exist, click **Select**, then click the **Create (+)** button in the ASA User Groups Selector dialog box, which opens a wizard to guide you through the creation process as described in [Creating User Groups with the Create Group Policy Wizard](#), page 30-20.

For more information about ASA Group Policies objects, see [ASA Group Policies Dialog Box](#), page 34-1.

- **Group Policies**—This table lists all group policies currently used on the device, whether for SSL or IPsec VPNs. You can click **Edit** to add other group policies.
- **Global IP Address Pool**—Enter the address pools from which IP addresses are assigned. The server uses these address pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.

Specify the pools as address ranges or network/host objects that contain address ranges, in the format *Start\_Address-End\_Address*, for example, 10.100.10.2-10.100.10.254. Click **Select** to select network/host objects or to create new objects.

**Step 12** On the Connection Profile page, configure these options that will later appear in the SSL VPN tab of the connection profile (see [SSL Tab \(Connection Profiles\)](#), page 31-22):

- **Portal Page Customization**—The name of the SSL VPN Customization policy object that defines the default portal page for the VPN. Click **Select** to select the object or to create a new object.



**Note**

You can set up different login windows for different groups by using a combination of customization profiles and tunnel groups. For example, assuming that you had created a customization profile called salesgui, you can create an SSL VPN tunnel group called sales that uses that customization profile.

- **Connection URL**—The URL of the connection profile. This URL provides users with direct access to the customized portal page. Select a protocol (**http** or **https**) from the list, and specify the URL including the name of the connection profile, in the field provided.

The URL is made up of the host name or IP address of the ASA device and port number, and the alias used to identify the SSL VPN connection profile.



**Note**

If you do not specify a URL, you can access the portal page by entering the portal page URL, and then selecting the connection profile alias from a list of configured connection profile aliases configured on the device. See [SSL VPN Configuration Wizard—Access Page \(ASA\)](#), page 30-16.

**Step 13** On the Connection Profile page, configure the AAA options for authentication, authorization, and accounting, and secondary authentication, which will later appear on the AAA and Secondary AAA tab of the connection profile (see [AAA Tab \(Connection Profiles\)](#), page 31-13 and [Secondary AAA Tab \(Connection Profiles\)](#), page 31-17).

**Step 14** Click **Finish** to save your changes.

## SSL VPN Configuration Wizard—Access Page (ASA)

Use the Access page of the SSL VPN Configuration Wizard to configure the security appliance interfaces for SSL VPN sessions. After you complete the wizard, you can later edit these settings in the SSL VPN Access policy; see [SSL VPN Access Policy Page, page 31-44](#).

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access SSL VPN on an ASA device (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)). The Access page is the first page that appears.

### Related Topics

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\), page 30-14](#)
- [Understanding Interface Role Objects, page 6-73](#)

### Field Reference

**Table 30-2** *SSL VPN Wizard—Access Page (ASA)*

Element	Description
Interfaces to Enable SSL VPN Service	The interfaces or interface roles that identify the interfaces on which you want to enable SSL VPN connections. Click <b>Select</b> to select interfaces or interface roles, or to create new interface roles.
Port Number	The port number to use for the SSL VPN sessions. Enter a port number or port list object name, or click <b>Select</b> to select an object that defines the port, or to create a new object.  The default port is 443, for HTTPS traffic. The port number can be 443, or within the range of 1024-65535. If you change the port number, all current SSL VPN connections terminate, and current users must reconnect.  <b>Note</b> If HTTP port redirection is enabled, the default HTTP port number is 80.
Portal Page URLs	The URLs that users would use to connect to the VPN. The URLs are displayed after you specify the interfaces and port number.
Allow Users to Select Connection Profile in Portal Page	Whether to present a list of configured connection profiles (tunnel groups) from which the user can select the appropriate profile when the user logs in (for example, in the SSL VPN portal page). If you do not select this option, the user cannot select a profile and must use the default profile for the connection.



**Table 30-2** *SSL VPN Wizard—Access Page (ASA) (continued)*

Element	Description
Enable AnyConnect Access	<p>Whether to allow the user to use the AnyConnect VPN client to make an SSL or IKEv2 IPsec VPN connection. The option is selected by default. For details about AnyConnect VPN clients, see <a href="#">Understanding SSL VPN AnyConnect Client Settings, page 31-61</a>.</p> <p><b>Note</b> To enable AnyConnect Essentials, go to Remote Access VPN &gt; SSL VPN &gt; Access. For details, see <a href="#">Configuring an Access Policy, page 31-49</a>.</p>

## SSL VPN Configuration Wizard—Connection Profile Page (ASA)

Use the Connection Profile page in the SSL VPN Configuration wizard to configure the tunnel group policies on your security appliance. You can specify a name for the tunnel connection profile policy that you are adding, select the user group policy, specify address pools for this policy, and specify authentication server group settings.

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access SSL VPN on an ASA device (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)); then click **Next** until you reach this page.

### Related Topics

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\), page 30-14](#)
- [ASA Group Policies Dialog Box, page 34-1](#)
- [Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 31-77](#)
- [Understanding Networks/Hosts Objects, page 6-80](#)
- [Understanding AAA Server and Server Group Objects, page 6-27](#)

### Field Reference

**Table 30-3** *SSL VPN Configuration Wizard, Connection Profile Page (ASA)*

Element	Description
Connection Profile Name	The name of the connection profile (tunnel group).

**Table 30-3** *SSL VPN Configuration Wizard, Connection Profile Page (ASA) (continued)*

Element	Description
Group Policy	<p>Default ASA user group associated with the device. Enter an ASA user group policy or click <b>Select</b> to select one from a list or to create a new one.</p> <p>If required, the name of the ASA group policy object that defines the default user group associated with the connection profile. A group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS/LDAP server.</p> <p>Click <b>Select</b> to select an existing object or to create a new one. If you click the <b>Create (+)</b> button in the group policy selection dialog box, you are guided through the group creation process using a wizard, as explained in <a href="#">Creating User Groups with the Create Group Policy Wizard, page 30-20</a>.</p>
Full Tunnel	A read-only field that indicates whether full tunnel access mode is configured for the object selected in the Group Policy field.
Group Policies	<p>The names of all ASA user group policies that are configured for the device, even those that are configured for IPsec VPN connections only. The contents of this table is identical to the contents of the Remote Access VPN &gt; Group Policies policy. The table shows whether full tunnel access mode is enabled or disabled for each group policy.</p> <p>You can change the list by clicking <b>Edit</b>. This opens a dialog box where you can select additional group policies, or deselect currently selected policies (do not deselect policies that are used by other connection profiles). You can also create new group policies (click the <b>Create (+)</b> button below the available group policies list) or edit the group policy object by selecting it and clicking the <b>Edit (pencil)</b> button below either list.</p> <p>If you create a new group policy, the Create Group Policy wizard is used to guide you through the process. See <a href="#">Creating User Groups with the Create Group Policy Wizard, page 30-20</a>.</p>
Portal Page Customization	The name of the SSL VPN Customization policy object that defines the default portal page for the VPN. This profile defines the appearance of the portal page that allows the remote user access to all resources available on the SSL VPN. Click <b>Select</b> to select the object or to create a new object.
Connection URL	<p>The URL of the connection profile. This URL provides users with direct access to the customized portal page.</p> <p>Select a protocol (<b>http</b> or <b>https</b>) from the list and specify the URL, including host name or IP address of the ASA device and port number and the alias used to identify the SSL VPN connection profile.</p> <p><b>Note</b> If you do not specify a URL, you can access the portal page by entering the portal page URL, and then selecting the connection profile alias from a list of configured connection profile aliases configured on the device. See <a href="#">SSL VPN Configuration Wizard—Access Page (ASA), page 30-16</a>.</p>

**Table 30-3** *SSL VPN Configuration Wizard, Connection Profile Page (ASA) (continued)*

Element	Description
Global IPv4 Address Pool	<p>The address pools from which IPv4 addresses will be assigned to clients if no pool is specified for the interface to which the client connects. Address pools are entered as a range of addresses, such as 10.100.12.2-10.100.12.254. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.</p> <p>Enter the address pool ranges or the names of network/host objects that define these pools. Click <b>Select</b> to select existing network/host objects or to create new ones. Separate multiple entries with commas.</p>
Global IPv6 Address Pool	<p>The address pools from which IPv6 addresses will be assigned to clients if no pool is specified for the interface to which the client connects. Address pools are entered as a range of addresses, such as 2001:db8::1-2001:db8::2:1. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools. .</p> <p>Enter the address pool ranges or the names of network/host objects that define these pools. Click <b>Select</b> to select existing network/host objects or to create new ones. Separate multiple entries with commas.</p>
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the tunnel group is configured on the local device). Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>
Use LOCAL if Server Group Fails	<p>Whether to fall back to the local database for authentication if the selected authentication server group fails.</p>
Authorization Server Group	<p>The name of the authorization server group (LOCAL if the tunnel group is configured on the local device). Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>
Accounting Server Group	<p>The name of the accounting server group. Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>
Secondary Authentication	<p>Whether to enable double authentication, which prompts the user for two sets of credentials (username and password) before completing the remote access VPN connection.</p> <ul style="list-style-type: none"> <li>• <b>Enable Secondary Authentication</b>—Select this option to require double authentication.</li> <li>• <b>Authentication Server Group</b>—The name of the authentication server group (LOCAL if the tunnel group is configured on the local device) to be used with the second set of credentials. Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</li> <li>• <b>Use LOCAL if Server Group Fails</b>—Whether to fall back to the local database for authentication if the selected authentication server group fails.</li> </ul>

## Creating User Groups with the Create Group Policy Wizard

When you are using the Remote Access SSL VPN Configuration wizard to create an SSL VPN on ASA or IOS devices, you can create new ASA group policy or IOS user group objects using a wizard. The wizard lets you configure select elements of the group, so you might need to edit the object after creating it to configure additional settings.

The Create Group Policy wizard is available only through the Remote Access SSL VPN Configuration wizard. For an explanation of how to start and use the wizard, see the following topics:


The following procedure assumes that you are already in the Remote Access SSL VPN Configuration wizard, as described in the following topics:

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(ASA Devices\)](#), page 30-14
- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\)](#), page 30-32

### Related Topics

- [SSL VPN Access Modes](#), page 30-4

- 
- Step 1** When using the Remote Access VPN Configuration wizard for SSL VPNs, proceed to the page where you select group policies. On this page, you can open the selection page for user groups by doing the following:
- ASA devices—On the Connection Profile page of the wizard, click **Select** next to the Group Policy field, or click **Edit** next to the Group Policies table.
  - IOS devices—On the Gateway and Context page of the wizard, click **Edit** next to the Group Policies table.
- Step 2** In the Group Policy Selector dialog box, click the **Create (+)** button below the list of available group policies to start the Create Group Policy wizard. The wizard starts at the Group Policy page.
- You can also do the following on the Group Policy Selector:
- Select existing groups and click >> to use them in the SSL VPN. When selecting a group for the default group on an ASA (the Group Policy field), you select the object simply by clicking it in the list.
  - Select an existing group and click **Edit (pencil)** to change its properties.
- Step 3** On the Group Policy page, configure the following options:
- **Name**—The name of the user group. Enter up to 128 characters, including uppercase and lowercase characters and most alphanumeric or symbol characters.
  - **Access Method**—Select the required remote access method options, as follows:
    - **Full Tunnel**—To access to the corporate network completely over an SSL VPN tunnel. This is the recommended option.
    - **Clientless**—To access the internal or corporate network using a web browser on the client machine.
    - **Thin Client**—To download a Java applet that acts as a TCP proxy on the client machine.
- Step 4** Click **Next**. The page that opens next depends on which access methods you selected. This procedure assumes that you selected all methods, in which case the Full Client page opens.

- Step 5** On the Full Client page, select whether to restrict access to full tunnel only or to allow other methods of access if the full client download fails. Also, specify DNS and WINS server information, and configure split tunneling if you want to allow it. For an explanation of the options, see [Create Group Policy Wizard—Full Tunnel Page, page 30-21](#).
- Step 6** Click **Next**. The Clientless and Thin Client page opens.
- Step 7** On the Clientless and Thin Client page, configure these access modes. For an explanation of the options, see [Create Group Policy Wizard—Clientless and Thin Client Access Modes Page, page 30-24](#).
- Step 8** Click **Finish** to create the group policy object.
- Step 9** When you complete the wizard, the group policy is added to the available groups list, but it is not selected (unless you are configuring the default group for an ASA). To select it, highlight it in the available groups list and click >> to move it to the selected groups list.
-  **Note** To specify a user group as the default user group, select it and click **Set As Default**. This option is only available for IOS routers.
- Step 10** Click **OK** in the Group Policy Selector page to save your changes and return to the Remote Access SSL VPN Configuration wizard.
- 

## Create Group Policy Wizard—Full Tunnel Page



**Note** This page is available only if you selected the **Full Client** option in the Group Policy of the Create Group Policy wizard.

---

In this page, you can configure the mode used to access the corporate network.

### Navigation Path

For information on starting the Create Group Policy wizard, see [Creating User Groups with the Create Group Policy Wizard, page 30-20](#).

## Field Reference

Table 30-4 Create User Group Wizard—Full Tunnel Page

Element	Description
Mode	<p>The access modes to allow in the SSL VPN. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Use Other Access Modes if SSL VPN Client Download Fails</b>—To allow the remote client to use clientless or thin client access modes if the download of the VPN client fails.</li> <li>• <b>Full Tunnel Only</b>—Prohibit clientless or thin client access. The user must have the full client installed and functional to connect to the VPN.</li> </ul> <p>Ensure that you configure the full client images on the device. For ASA devices, use the Client Settings tab of the SSL VPN &gt; Other Settings policy; see <a href="#">Configuring SSL VPN AnyConnect Client Settings (ASA), page 31-63</a>. For IOS devices, the client is managed using a FlexConfig policy; see <a href="#">Predefined FlexConfig Policy Objects, page 7-19</a>.</p>
Client IP Address Pools (IOS device only.)	<p>The IP address ranges of the address pool that full tunnel clients will draw from when they log on. The address pool must be in the same subnet as one of the device's interface IP addresses.</p> <p>Enter the address range separating the first and last IP address with a hyphen, for example, 10.100.10.2-10.100.10.255. If you enter a single address, the pool has just one address. Do not enter subnet designations.</p> <p>You can also enter the name of a network/host policy object that defines the range, or click <b>Select</b> to select the object from a list or to create a new object. Separate multiple ranges with commas.</p>
Primary IPv4 DNS Server	The IPv4 address of the primary DNS server for the group. Enter the IPv4 address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.
Secondary IPv4 DNS Server	The IPv4 address of the secondary DNS server for the group. Enter the IPv4 address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.
Primary IPv6 DNS Server	The IPv6 address of the primary DNS server for the group. Enter the IPv6 address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.
Secondary IPv6 DNS Server	The IPv6 address of the secondary DNS server for the group. Enter the IPv6 address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.
Default DNS Domain	The domain name of the DNS server to be used for Full Client SSL VPN connections.
Primary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.
Secondary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click <b>Select</b> to select an object from a list or to create a new object.

Table 30-4 Create User Group Wizard—Full Tunnel Page (continued)

Element	Description
Split Tunnel Option	<p>Whether to allow split tunneling for IPv4 traffic and if so, which traffic should be secured or transmitted unencrypted across the public network:</p> <ul style="list-style-type: none"> <li>• <b>Disabled—(Default)</b> No IPv4 traffic goes in the clear or to any other destination than the gateway. Remote users reach networks through the corporate network and do not have access to local networks.</li> <li>• <b>Tunnel Specified Traffic—</b>Tunnel all IPv4 traffic from or to the addresses listed in the <b>Networks</b> or <b>Destinations</b> field. Traffic to all other addresses travels in the clear and is routed by the remote user's Internet service provider.</li> <li>• <b>Exclude Specified Traffic—</b>IPv4 traffic goes in the clear from and to the addresses listed in the <b>Networks</b> or <b>Destinations</b> field. This is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.</li> </ul>
IPv6 Split Tunnel Option	<p>Whether to allow split tunneling for IPv6 traffic and if so, which traffic should be secured or transmitted unencrypted across the public network:</p> <ul style="list-style-type: none"> <li>• <b>Disabled—(Default)</b> No IPv6 traffic goes in the clear or to any other destination than the gateway. Remote users reach networks through the corporate network and do not have access to local networks.</li> <li>• <b>Tunnel Specified Traffic—</b>Tunnel all traffic from or to the addresses listed in the <b>Networks</b> or <b>Destinations</b> field. Traffic to all other addresses travels in the clear and is routed by the remote user's Internet service provider.</li> <li>• <b>Exclude Specified Traffic—</b>Traffic goes in the clear from and to the addresses listed in the <b>Networks</b> or <b>Destinations</b> field. This is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.</li> </ul>
Networks (ASA device only.)	<p>If you select Tunnel Specified Traffic or Exclude Specified traffic in the Split Tunnel Option, enter the name of the ACL object that defines the traffic to be tunneled or excluded. Click <b>Select</b> to select the object or to create a new object.</p>
Destinations (IOS device only.)	<p>If you select Tunnel Specified Traffic or Exclude Specified traffic in the Split Tunnel Option, specify the IP addresses that define the traffic to be tunneled or excluded.</p> <p>Enter network addresses such as 10.100.10.0/24 or host addresses such as 10.100.10.12. You can also enter the name of a network/host policy object, or click <b>Select</b> to select the object from a list or to create a new object. Separate multiple addresses with commas.</p>

**Table 30-4** Create User Group Wizard—Full Tunnel Page (continued)

Element	Description
Exclude Local LANs (IOS device only.)	Whether to exclude local LANs from the encrypted tunnel. This option is available only if you selected the <b>Exclude Specified Traffic</b> split tunnel option. By selecting this option, you do not have to enter local LAN addresses into the destinations field to allow users to communicate with systems (such as printers) that are attached to their LAN.  When selected, this attribute disallows a non split-tunneling connection to access the local subnetwork at the same time as the client.
Split DNS Names	A list of domain names to be resolved through the split tunnel to the private network. All other names are resolved using the public DNS server.  Enter up to 10 entries in the list of domains, separated by commas. The entire string can be no longer than 255 characters.

## Create Group Policy Wizard—Clientless and Thin Client Access Modes Page

In the Clientless and Thin Client page of the Create Group Policy wizard, you can configure the Clientless and Thin Client modes to be used for accessing the corporate network in your SSL VPN.



### Note

This page is only available if you selected the **Clientless** or **Thin Client** options in step 1 of the Create Group Policy wizard.

### Navigation Path

For information on starting the Create Group Policy wizard, see [Creating User Groups with the Create Group Policy Wizard, page 30-20](#).

### Related Topics

- [SSL VPN Access Modes, page 30-4](#)
- [Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 31-82](#)
- [Add or Edit Port Forwarding List Dialog Boxes, page 34-39](#)

### Field Reference

**Table 30-5** Create User Group Wizard—Clientless and Thin Client Page

Element	Description
<b>Clientless</b>	Appears only if you selected <b>Clientless</b> in step 1 of the wizard.
Portal Page Websites	The name of the SSL VPN bookmarks policy object that includes the web site URLs to display on the portal page. These web sites help users access desired resources. Enter the name of the object or click <b>Select</b> to select it from a list or to create a new object.
Allow Users to Enter Websites	Whether to allow the remote user to enter web site URLs directly into the browser. If you do not select this option, the user can access only those URLs included on the portal.



**Table 30-5 Create User Group Wizard—Clientless and Thin Client Page (continued)**

Element	Description
<b>Thin Client</b>	Appears only if you selected <b>Thin Client</b> in step 1 of the wizard.
Port Forwarding List	The name of the port forwarding list policy object assigned to this group. Port forwarding lists contain the set of applications that users of clientless SSL VPN sessions can access over forwarded TCP ports. Enter the name of the object or click <b>Select</b> to select it from a list or to create a new object.
Port Forwarding Applet Name (ASA device only.)	The application name or short description to display on the Port Forwarding Java applet screen on the portal, up to 64 characters. This is the name of the applet users will download to act as a TCP proxy on the client machine for the services configured on the SSL VPN gateway.
Download Port Forwarding Applet on Client Login	Whether the port forwarding Java applet should be automatically downloaded to the client when a user logs into the SSL VPN. If you do not automatically download the applet, users must download it manually after login.

## Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard (ASA and PIX 7.0+ Devices)

This procedure describes how to create IPsec VPNs on ASA or PIX 7.0+ devices using the Remote Access VPN Configuration Wizard.



### Tip

The wizard allows you to select shared policies to use in the VPN on the Defaults page (the final step of the wizard). If you want to use this feature, you must first ensure that all required shared policies are configured and submitted to the database. For information on configuring shared policies and VPN policy defaults, see [Understanding and Configuring VPN Default Policies, page 25-12](#).

### Related Topics

- [Understanding Remote Access IPsec VPNs, page 30-2](#)
- [Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8](#)

- 
- Step 1** In Device view, select the desired ASA or PIX 7.0+ device.
- Step 2** From the Policy selector, select **Remote Access VPN > Configuration Wizard**.
- Step 3** Select the **Remote Access IPsec VPN** radio button.
- Step 4** Click **Remote Access Configuration Wizard**. The Connection Profile page opens. For a description of the options that appear on this page, see [Remote Access VPN Configuration Wizard—IPsec VPN Connection Profile Page \(ASA\), page 30-28](#).
- Step 5** On the Connection Profile page, configure these basic options:
- **Connection Profile name**—Enter the name of the connection profile. This is the name of the tunnel group, and will appear in the Remote Access VPN > Connection Profiles policy. For more information about the connection profile policy, see [Configuring Connection Profiles \(ASA, PIX 7.0+\), page 31-7](#).

- **IKE Versions**—Select the IKE versions to use during IKE negotiations between the VPN server and the remote users, version 1, 2 or both. IKEv2 is supported on ASA Software release 8.4(1)+ only.
- Step 6** On the Connection Profile page, configure these options that will later appear in the General tab of the connection profile (see [General Tab \(Connection Profiles\)](#), page 31-10):
- **Group Policy**—Enter the name of the ASA Group Policy policy object that will be the default group for the connection profile, or click **Select** to select the object. If the required object does not yet exist, click **Select**, then click the **Create (+)** button in the ASA User Groups Selector dialog box to open the dialog boxes that are used to create these objects.
- When creating a new group policy object, you must select the same IKE versions that you select in the Connection Profile page of the wizard. These options are on the Technology page of the Add ASA Group Policies dialog box: Easy VPN/IPSec IKEv1 and Easy VPN/IPSec IKEv2.
- For more information about ASA Group Policies objects, see [ASA Group Policies Dialog Box](#), page 34-1.
- **Global IP Address Pool**—Enter the address pools from which IP addresses are assigned. The server uses these address pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.
- Specify the pools as address ranges or network/host objects that contain address ranges, in the format *Start\_Address-End\_Address*, for example, 10.100.10.2-10.100.10.254. Click **Select** to select network/host objects or to create new objects.
- Step 7** On the Connection Profile page, configure the AAA options for authentication, authorization, and accounting, which will later appear on the AAA tab of the connection profile (see [AAA Tab \(Connection Profiles\)](#), page 31-13).
- Step 8** Click **Next** to move to the IPsec Settings page.
- Step 9** On the IPsec Settings page, configure the options for IPsec, which will later appear on the IPsec tab of the connection profile (see [IPsec Tab \(Connection Profiles\)](#), page 31-19). Note that some of these settings apply to IKEv1 only.
- **Preshared Key, Confirm**—Enter the IKEv1 preshared key for the tunnel group in each field. The maximum length of a preshared key is 127 characters.
- You cannot configure a preshared key for remote access IKEv2 IPsec VPNs.
- **Trustpoint Name**—Enter the name of the PKI enrollment policy object that defines the trustpoint name, if any trustpoints are configured, for an IKEv1 connection. A trustpoint represents a Certificate Authority (CA)/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. Click **Select** to select the object from a list or to create a new object.
- For IKEv2, the trustpoint name is not configured here, but on the IKEv2 Settings tab of the Global Settings policy. The configuration is explained later in this procedure.
- The other options (other than the client table) apply to both IKEv1 and IKEv2. Change the settings if you need non-default behavior. For an explanation of the options, including the client software update table, see [Remote Access VPN Configuration Wizard—IPsec Settings Page \(ASA\)](#), page 30-29.
- Step 10** Click **Next** to move to the VPN Defaults page.
- Step 11** On the Defaults page, select the additional shared policies that you want to assign to the VPN. Initially, the policies listed are those chosen on the Security Manager Administration VPN Defaults page.
- For more information about selecting these policies, see [Remote Access VPN Configuration Wizard—Defaults Page](#), page 30-31.

**Step 12** Click **Finish** to save your changes.

Because the wizard does not configure all possible options, inspect the policies created and configure any additional options that you want to implement.

The remaining steps are required if you selected IKE version 2 as a supported IKE version, or if you specified an IPsec trustpoint.

**Step 13** (IKEv2 Optional.) Configure group aliases and double authentication if required:

- a. Select the Connection Profiles policy.
- b. Select the connection profile you configured in the wizard, and click the **Edit Row (pencil)** button to open the Connection Profiles dialog box.
  - If you want to configure double authentication, select the Secondary AAA tab and configure the required settings. For more information, see [Secondary AAA Tab \(Connection Profiles\)](#), page 31-17.
  - If you want to configure aliases for the profile, which helps users select the correct profile during login, select the SSL tab and configure the alias table. For more information, see [SSL Tab \(Connection Profiles\)](#), page 31-22.
  - There are several additional connection profile settings that are not configured in the wizard. Examine the tabs in the Connection Profile dialog box to determine if additional changes are required.
- c. Click **OK** in the Connection Profiles dialog box to save your changes.

**Step 14** (IKEv2 Requirement.) Select the **Remote Access VPN > SSL VPN > Access** policy and configure at least the following. For detailed information about configuring an Access policy, see [Understanding SSL VPN Access Policies \(ASA\)](#), page 31-43.

- Add the remote access VPN interface to the access interfaces table.
- Select **Allow Users to Select Connection Profile in Portal Page**.
- Select **Enable AnyConnect Access**.

**Step 15** (IKEv2 Requirement.) Select the **Remote Access VPN > SSL VPN > Other Settings** policy, and click the **Client Settings** tab.

In the AnyConnect Client Image table, add an AnyConnect 3.0 or higher client image, one that supports IKEv2 negotiations.

For more information on configuring client images, see [Configuring SSL VPN AnyConnect Client Settings \(ASA\)](#), page 31-63.

**Step 16** (IKEv2 Requirement.) Select the **Remote Access VPN > Global Settings** policy, and click the IKEv2 Settings tab.

At minimum, configure the **RA Trustpoint** for remote access IKEv2 authentication. Enter the name of the PKI enrollment object that identifies the certificate authority (CA) server or click **Select** to select the object or to create a new one.

For more information on configuring IKEv2 global settings, see [Configuring VPN Global IKEv2 Settings](#), page 26-36.

**Step 17** (IKEv1, IKEv2 Requirement.) Select the **Remote Access VPN > Public Key Infrastructure** policy and ensure that the following PKI enrollment objects are selected:

- (IKEv1) The object specified on the IPsec tab of the connection profile, if a trustpoint is configured.
- (IKEv2) The object specified on the IKEv2 Settings tab of the Global Settings policy.



**Note** In the wizard, you might have applied a shared Public Key Infrastructure policy that already specifies these objects.

**Step 18** (IKEv2 Optional.) IKEv2 connections require the use of the AnyConnect 3.0+ client. The AnyConnect client might need to download files, such as software upgrades, profiles, localization and customization files, CSD, SCEP, and so forth. The wizard does not enable these types of download.

To enable AnyConnect file downloads:

- a. Select **Remote Access VPN > IPsec VPN > IPsec Proposal**.
- b. Select the IPsec proposal created by the wizard, and click **Edit Row (pencil)** to open the IPsec Proposal Editor. For information about the various options, see [IPsec Proposal Editor \(ASA, PIX 7.0+ Devices\)](#), page 31-41.
- c. Select the **Enable Client Services** option, and enter a port number if you do not want to use the default port 443. (You can use the same port number used for SSL VPN or other SSL uses.)
- d. Click **OK** to save your changes.

## Remote Access VPN Configuration Wizard—IPsec VPN Connection Profile Page (ASA)

Use the Connection Profile page of the Remote Access VPN Configuration wizard to configure the connection profile policies on your security appliance for a remote access IPsec VPN. You can specify a name for the connection profile policy that you are adding, select the IKE versions to allow during IKE negotiations, select the user group policy, specify address pools for this policy, and specify authentication, authorization, and accounting server group settings.

For more information about using the wizard to configure remote access IPsec VPNs on ASA, see [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\)](#), page 30-25.

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access IPsec VPN on an ASA or PIX 7.0+ device (see [Using the Remote Access VPN Configuration Wizard](#), page 30-13). The IPsec Connection Profile page is the first page that appears.

### Field Reference

**Table 30-6 Remote Access VPN Configuration Wizard, IPsec Connection Profile Page (ASA)**

Element	Description
Connection Profile Name	The name of the connection profile (tunnel group).
IKE Versions	The IKE versions to use during IKE negotiations between the VPN server and the remote users. IKEv2 is supported on ASA Software release 8.4(1)+ only; you cannot change the option selection on other types of device.  Select <b>IKE Version 1</b> , <b>IKE Version 2</b> , or <b>Both</b> (to allow either version). IKEv2 connections are allowed using Anyconnect clients only.

**Table 30-6 Remote Access VPN Configuration Wizard, IPsec Connection Profile Page (ASA)**

Element	Description
Group Policy	<p>If required, the name of the ASA group policy object that defines the default user group associated with the connection profile. A group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS/LDAP server.</p> <p>Click <b>Select</b> to select an existing object or to create a new one.</p> <p><b>Tip</b> If you enable IKEv2 for this VPN, there are special considerations for the group policy you choose. For detailed information, see <a href="#">Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard (ASA and PIX 7.0+ Devices)</a>, page 30-25.</p>
Global IP Address Pool	<p>The address pools from which IP addresses will be assigned to clients if no pool is specified for the interface to which the client connects. Address pools are entered as a range of addresses, such as 10.100.12.2-10.100.12.254. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.</p> <p>Enter the address pool ranges or the names of network/host objects that define these pools. Click <b>Select</b> to select existing network/host objects or to create new ones. Separate multiple entries with commas.</p>
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the tunnel group is configured on the local device). Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>
Use LOCAL if Server Group Fails	<p>Whether to fall back to the local database for authentication if the selected authentication server group fails.</p>
Authorization Server Group	<p>The name of the authorization server group (LOCAL if the tunnel group is configured on the local device). Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>
Accounting Server Group	<p>The name of the accounting server group. Enter the name of a AAA server group object or click <b>Select</b> to select it from a list or to create a new object.</p>

## Remote Access VPN Configuration Wizard—IPsec Settings Page (ASA)

Use the IPsec Settings page of the Remote Access VPN Configuration wizard to configure the IPsec settings on your security appliance for a remote access IPsec VPN. Some of these settings apply to IKE version 1 (IKEv1) only; if you are configuring an IKEv2-only VPN, these fields are greyed and unconfigurable.

For more information about using the wizard to configure remote access IPsec VPNs on ASA, see [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\)](#), page 30-25.

**Navigation Path**

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access IPsec VPN on an ASA or PIX 7.0+ device (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)); then click **Next** until you reach this page.

**Field Reference****Table 30-7 Remote Access VPN Configuration Wizard, IPsec VPN Wizard—IPsec Settings (ASA)**

Element	Description
Preshared Key (IKEv1 only.)	<p>The preshared key for the connection profile. The maximum length of a preshared key is 127 characters. Enter the key again in the Confirm field.</p> <p><b>Tip</b> You cannot configure preshared keys for IKEv2 remote access VPNs.</p>
Trustpoint Name (IKEv1 only.)	<p>The name of the PKI enrollment policy object that defines the trustpoint name if any trustpoints are configured for IKEv1 connections. A trustpoint represents a Certificate Authority (CA)/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.</p> <p>Click <b>Select</b> to select the object from a list or to create a new object.</p> <p><b>Tip</b> This trustpoint is used for IKEv1 negotiations only. To configure the global trustpoint for IKEv2 negotiations, use the IKEv2 Settings tab of the Global Settings policy; see <a href="#">Configuring VPN Global IKEv2 Settings, page 26-36</a>.</p>
IKE Peer ID Validation	<p>Select whether IKE peer ID validation is ignored (Do not check), required, or checked only if supported by a certificate. During IKE negotiations, peers must identify themselves to one another.</p>
Enable Sending Certificate Chain	<p>Whether to enable the sending of the certificate chain for authorization. A certificate chain includes the root CA certificate, identity certificate, and key pair.</p>
Enable Password Update with RADIUS Authentication	<p>When selected, enables passwords to be updated with the RADIUS authentication protocol.</p> <p>Whether to enable passwords to be updated with the RADIUS authentication protocol. For more information, see <a href="#">Supported AAA Server Types, page 6-28</a>.</p>
ISAKMP Keepalive	<p>Whether to monitor ISAKMP keepalive. If you select the <b>Monitor Keepalive</b> option, you can configure IKE keepalive as the default failover and routing mechanism. Enter the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>Confidence Interval</b>—The number of seconds that a device waits between sending IKE keepalive packets.</li> <li>• <b>Retry Interval</b>—The number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.</li> </ul> <p>For more information, see <a href="#">Configuring VPN Global ISAKMP/IPsec Settings, page 26-32</a>.</p>

**Table 30-7 Remote Access VPN Configuration Wizard, IPsec VPN Wizard—IPsec Settings (ASA)**

Element	Description
Client Software Update table (IKEv1 only.)	<p>The VPN client revision level and URLs for client platforms. You can configure different revision levels for All Windows Platforms, Windows 95/98/ME, Windows NT4.0/2000/XP, or the VPN3002 Hardware Client.</p> <p>To configure the client for a platform, select it, click the <b>Edit Row</b> button, and fill in the <a href="#">IPsec Client Software Update Dialog Box, page 31-21</a>.</p>

## Remote Access VPN Configuration Wizard—Defaults Page

Use the Defaults page of the Remote Access VPN Configuration wizard to select the shared policies to assign to the remote access IPsec VPN. Initially, the policies selected are those configured in the Security Manager Administration VPN Defaults for remote access VPNs. For information on how to configure these defaults, see [Understanding and Configuring VPN Default Policies, page 25-12](#).

Required policies must always have a policy selected. If “Factory Default” is shown, then the policy applied is not a shared policy but default policy settings supplied by Security Manager. If you can select the empty option, the policy is optional and you need to configure it only if you want the associated features.

When evaluating which policies to assign (if any), keep the following in mind:

- The drop-down lists for each policy type list the existing shared policies that you can select. You can select only shared policies that have been committed to the Security Manager database (and approved, if you are using Workflow mode with an approver). You cannot create a shared policy and use it before you submit it.
- To view the content of a policy, select it and click the **View Content** button. You are presented with a read-only view of the policy. Use this to help verify that you are selecting the desired policy.



### Note

If you try to select a default policy that is currently locked by another user, a message is displayed warning you of a lock problem. To bypass the lock, select a different policy or cancel the VPN creation until the lock is removed. For more information, see [Understanding Policy Locking, page 5-8](#).

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access IPsec VPN (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)) and click **Next** until you reach this page.

### Related Topics

- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(ASA and PIX 7.0+ Devices\), page 30-25](#)
- [Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard \(IOS and PIX 6.3 Devices\), page 30-36](#)
- [Overview of Remote Access VPN Policies, page 30-9](#)

**Field Reference****Table 30-8 Remote Access VPN Configuration Wizard, Defaults Page**

Element	Description
ASA Cluster Load Balance	Defines load balancing for an ASA device in your remote access VPN.
High Availability	Defines a High Availability (HA) policy on a Cisco IOS router in a remote access VPN.
Certificate to Connection Profile Map Policy	(IKEv1 only.) Defines the certificate to connection profile map options for an ASA device in your remote access VPN.
IKE Proposal	Defines the set of algorithms that two peers use to secure the IKE negotiation between them.
IPSec Proposal	Defines the crypto maps required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA.
Public Key Infrastructure	Defines the Public Key Infrastructure (PKI) policy used to generate PKI enrollment requests for PKI certificates and RSA keys.
VPN Global Settings	Defines global settings for IKE, IPsec, IKEv2, NAT, and fragmentation that apply to devices in your remote access VPN.

## Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices)

This procedure describes how to create or edit SSL VPNs on IOS devices using the Remote Access SSL VPN Configuration Wizard.

**Related Topics**

- [Understanding Remote Access SSL VPNs, page 30-2](#)
- [Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8](#)

- 
- Step 1** In Device view, select the desired IOS device.
- Step 2** From the Policy selector, select **Remote Access VPN > Configuration Wizard**.
- Step 3** Select the **Remote Access SSL VPN** radio button.
- Step 4** Click **Remote Access Configuration Wizard**. The Gateway and Context page opens. For a description of the elements on this page, see [SSL VPN Configuration Wizard—Gateway and Context Page \(IOS\), page 30-33](#).
- Step 5** Select the gateway to be used as a proxy for connections to the protected resources in your SSL VPN. Options are:
- **Use Existing Gateway**—Lets you use an existing gateway object. If you select this option, specify the name of the SSL VPN Gateway policy object that defines the gateway. Click **Select** to select the object or to create a new object.
  - **Create Using IP Address**—Lets you configure a new gateway object using a reachable (public, static) IP address on the router. Enter the IP address.
  - **Create Using Interface**—Lets you configure a new gateway using the public, static IP address of a router interface. Select the interface or interface role object.



If you elected to create a new gateway using an IP address or an interface:

- Specify a gateway name.
- Specify the number of the port that will carry the HTTPS traffic. The default is 443, unless HTTP port redirection is enabled, in which case the default HTTP port number is 80. If you want to use a different port, it must be between 1024 and 65535.

- Step 6** Enter the name of the name of the context that defines the virtual configuration of the SSL VPN.
- Step 7** Select the user groups that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway. The table shows whether full client access is enabled for the group. Click **Edit** to select the desired groups, or to create new groups.
- Step 8** Configure the AAA options for authentication, authentication domain, and accounting. For detailed information, see [SSL VPN Configuration Wizard—Gateway and Context Page \(IOS\), page 30-33](#).
- Step 9** Click **Next**. The Portal Page Customization page opens. For a description of the elements on this page, see [SSL VPN Configuration Wizard—Portal Page Customization Page \(IOS\), page 30-35](#).
- Step 10** On the Portal Customization page, configure the following options. The bottom of the page is a preview of what the portal page will look like based on your selections; use the preview to fine-tune your selections.
- **Title**—The name of the portal page, which appears at the top of the page.
  - **Logo**—The graphic to show in the title area of the page: None, Default (the Cisco logo graphic), or Custom. If you select custom, click **Select** to select the graphic on the Security Manager server. You must copy the custom graphic to the server before you can use it in the portal customization.  
The source image file for the logo can be a GIF, JPG, or PNG file, with a file name of up to 255 characters, and up to 100 kilobytes in size.
  - **Login Message**—The text that should appear above the login prompt.
  - **Title and Text Colors**—The colors to use for the title and login area and the fonts.
- Step 11** Click **Finish** to save your changes.
- 

## SSL VPN Configuration Wizard—Gateway and Context Page (IOS)

A gateway and context must be configured on a device before a remote user can access resources on a private network behind the SSL VPN. Use this step of the SSL VPN Configuration wizard to specify a gateway and context configuration, including information that will allow users to access a portal page.

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access SSL VPN on an IOS device (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)). The Gateway and Context page is the first page that appears.

### Related Topics

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\), page 30-32](#)
- [Add or Edit SSL VPN Gateway Dialog Box, page 34-63](#)
- [Understanding AAA Server and Server Group Objects, page 6-27](#)

## Field Reference

Table 30-9 SSL VPN Configuration Wizard, Gateway and Context Page

Element	Description
Gateway	<p>The gateway to be used as a proxy for connections to the protected resources in your SSL VPN. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Use Existing Gateway</b>—When selected, enables you to use an existing gateway for your SSL VPN.</li> <li>• <b>Create Using IP Address</b>—When selected, enables you to configure a new gateway using a reachable (public static) IP address on the router.</li> <li>• <b>Create Using Interface</b>—When selected, enables you to configure a new gateway using the public static IP address of the router interface.</li> </ul>
Gateway Name	<p>The name of the SSL VPN gateway policy object that defines the gateway:</p> <ul style="list-style-type: none"> <li>• If you selected Use Existing Gateway, click <b>Select</b> to select the object from a list or to create a new object.</li> </ul> <p><b>Note</b> After selecting the gateway, the port number and digital certificate required to establish a secure connection are displayed in the relevant fields.</p> <ul style="list-style-type: none"> <li>• If you selected Create Using IP Address or Interface, enter the name of the object that you want to create (up to 128 characters).</li> </ul>
IP Address	<p>Available if you selected to create a gateway using an IP address.</p> <p>The IP address on the router that should be used as the gateway address.</p>
Interface	<p>Available if you selected to create a gateway using an interface.</p> <p>The name of the interface, or the interface role object that defines the interface, that should be used as the SSL VPN gateway. Click <b>Select</b> to select the interface or interface role, or to create a new interface role.</p>
Port	<p>The port number used for SSL VPN connections. The default is 443, unless HTTP port redirection is enabled, in which case the default HTTP port number is 80. If you enter a different number, it must be between 1024 and 65535.</p> <ul style="list-style-type: none"> <li>• If you selected Use Existing Gateway, this is a read-only field that shows the port number configured in the selected object.</li> <li>• If you selected Create Using IP Address or Interface, enter the port number or the name of a port list object that specifies the number, or click <b>Select</b> to select the port list object.</li> </ul>
Trustpoint	<p>The digital certificate required to establish the secure connection. A self-signed certificate is generated when an SSL VPN gateway is activated.</p>

**Table 30-9** *SSL VPN Configuration Wizard, Gateway and Context Page (continued)*

Element	Description
Context Name	The name of the context that defines the virtual configuration of the SSL VPN.  <b>Note</b> To simplify the management of multiple context configurations, make the context name the same as the domain or virtual hostname.
Portal Page URL	The URL for the SSL VPN, which is filled in when you select (or define) a gateway object. Users connect to this URL to enter the VPN.
Group Policies	The user groups that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway. The table shows whether full client access is enabled for the group. Click <b>Edit</b> to select the desired groups, or to create new groups.
Authentication Server Group	The authentication server groups. The list is in prioritized order. Authentication is attempted using the first group and proceeds through the list until the user is successfully authenticated or denied. Use the LOCAL group if the users are defined on the gateway itself.  Enter the names of the AAA server groups; separate multiple entries with commas. You can click <b>Select</b> to select the groups or to create new ones.
Authentication Domain	A list or method for SSL VPN remote user authentication. If you do not specify a list or method, the gateway uses global AAA parameters for remote-user authentication.
Accounting Server Group	The accounting server group. Enter the name of the AAA server group policy object, or click <b>Select</b> to select it from a list or to create a new object.

## SSL VPN Configuration Wizard—Portal Page Customization Page (IOS)

Use this step of the SSL VPN Configuration wizard to define the appearance of the portal page that remote users see when connecting to the SSL VPN. The portal page allows remote users access to all websites available on the SSL VPN networks.

### Navigation Path

(Device view) Open the Remote Access VPN Configuration Wizard for configuring a remote access SSL VPN on an ASA device (see [Using the Remote Access VPN Configuration Wizard, page 30-13](#)); then click **Next** until you reach this page.

### Related Topics

- [Creating SSL VPNs Using the Remote Access VPN Configuration Wizard \(IOS Devices\), page 30-32](#)

## Field Reference

Table 30-10 SSL VPN Configuration Wizard, Portal Page Customization Page

Element	Description
Title	The text displayed at the top of the page. Control the color using the Primary settings in the Title Color and Text Color fields.
Logo	The graphic displayed next to the title. Select None, Default, or Custom. To configure a custom graphic, you must copy the desired graphic to the Security Manager server, then click <b>Browse</b> to select the file. Supported graphic types are GIF, JPG, and PNG, with a maximum size of 100 KB.
Login Message	The text displayed immediately above the login prompt. Control the color using the Secondary settings in the Title Color and Text Color fields.
Title Color	The colors used for the title and login area and the text: <ul style="list-style-type: none"> <li>Primary—The Title, Login Box title, and the text in those areas.</li> <li>Secondary—The Login Box username/password background and the text in that area.</li> </ul> Click <b>Select</b> to choose background colors. For text, select either Black or White from the text list.
Text Color	
Preview	A preview of how the portal page will appear based on your selections.

## Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (IOS and PIX 6.3 Devices)

This procedure describes how to create or edit IPSec VPNs on IOS and PIX 6.3 devices using the Remote Access VPN Configuration Wizard.

**Tip**

The wizard allows you to select shared policies to use in the VPN on the Defaults page (the final step of the wizard). If you want to use this feature, you must first ensure that all required shared policies are configured and submitted to the database. For information on configuring shared policies and VPN policy defaults, see [Understanding and Configuring VPN Default Policies, page 25-12](#).

**Related Topics**

- [Understanding Remote Access IPSec VPNs, page 30-2](#)
- [Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8](#)

- 
- Step 1** In Device view, select the desired IOS or PIX 6.3 device.
- Step 2** From the Policy selector, select **Remote Access VPN > Configuration Wizard**.
- Step 3** Select the **Remote Access IPSec VPN** radio button.
- Step 4** Click **Remote Access Configuration Wizard**. The User Group Policy page opens.
- Step 5** Select the required user groups from the Available User Groups list and click >>.

- If the required user group is not in the list, click **Create (+)** to open the Add User Groups dialog box, which enables you to create or edit a user group object. See [Add or Edit User Group Dialog Box, page 34-72](#).
- You can edit an existing user group by selecting it in either list and clicking **Edit (pencil)**.
- To deselect a user group, select it and click <<.

**Step 6** Click **Next**. The Defaults page opens.

**Step 7** Select the shared policies to assign to the VPN. Initially, the selected policies are those configured on the Security Manager Administration VPN Defaults page. You can use the defaults or select different policies, if any are available. For more information about these policy defaults, see [Remote Access VPN Configuration Wizard—Defaults Page, page 30-31](#).

**Step 8** Click **Finish** to save your changes.

Inspect the policies created and configure any additional options that you want to implement.

---

