

VPN Concentrator for WebVPN using the SSL VPN Client Configuration Example

Document ID: 67917

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configuration
- Configure to Disable Certificate Warning

Verify

Troubleshoot

- Managing the Concentrator from the Public Network
- WebVPN Authentication Fails

Related Information

Introduction

This document provides a sample configuration on how to configure a WebVPN tunnel between a Cisco SSL VPN Client tunnel (SVC) and the Cisco VPN 3000 Concentrator that uses an internal database for authentication. The Cisco SSL VPN Client supports applications and functions unavailable to a standard WebVPN connection.

WebVPN provides Secure Socket Layer (SSL) VPN remote-access connectivity from almost any Internet-enabled location that uses only a Web browser and its native SSL encryption. This enables companies to extend their secure enterprise networks to any authorized user by providing remote access connectivity to corporate resources from any Internet-enabled location.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- In order to use SSL VPN Client release 1.0.2, you must upgrade the VPN Concentrator to release 4.7.2 or later. SSL VPN Client release 1.0.2 does not operate with the VPN Concentrator that runs releases earlier than 4.7.2.
- SSL VPN Client works only with Microsoft Windows XP or Windows 2000.
- Refer to Using the Command-Line Interface for Quick Configuration for a basic idea on how to use the VPN Concentrator Command Line Interface (CLI).

Components Used

The information in this document is based on these software and hardware versions:

- VPN 3015 release 4.7.2.B, and SVC release 1.0.2.127

- Windows 2000 PC using Internet Explorer 6.0 SP1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

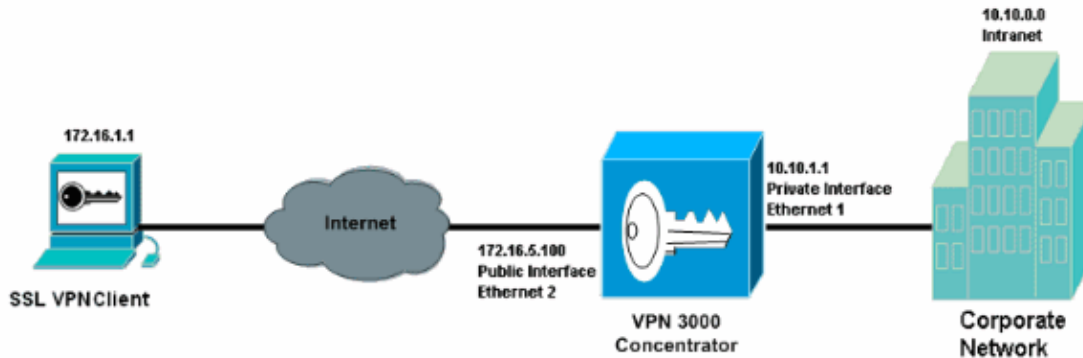
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configuration

VPN Concentrators are not pre-programmed with IP addresses in their factory settings. You have to use the console port to configure the initial configurations which are a menu-based CLI. Refer to *Configuring VPN Concentrators through the Console* for information on how to configure through the console.

After you configure the IP address on the Ethernet 1 (private) interface, the rest can be configured either using the CLI or via the browser interface. The browser interface supports both HTTP and HTTP over Secure Socket Layer (SSL).

Complete these steps:

1. Type the IP address of the private interface from the web browser in order to enable the GUI interface.

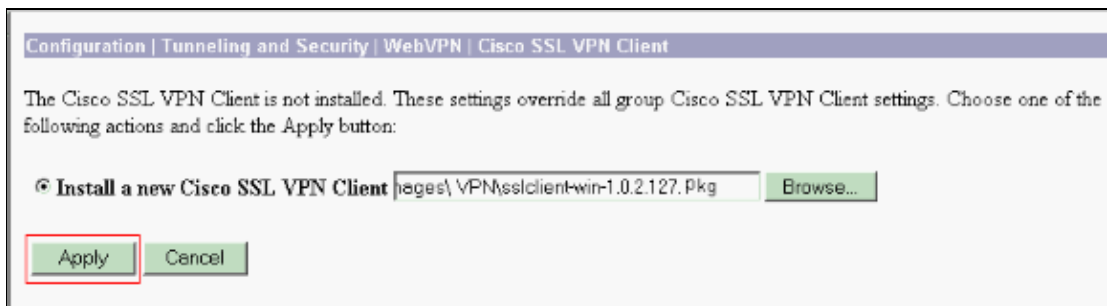
The factory default username and password are **admin** which is case sensitive.

2. Once you are logged in as an Administrator, begin to install the SSL VPN Client software to the VPN Concentrator.

This step is required only when you upgrade a VPN Concentrator from an older release to 4.7. Choose **Configuration > Tunneling and Security > WebVPN > Cisco SSL VPN Client** in order to install the SSL VPN Client.

Note: New VPN Concentrators that run release 4.7 or later come pre-loaded with the SSL VPN Client. By default, the SSL VPN Client is disabled and you need to enable it. This is explained in step 4.

Note: The SSL VPN Client and VPN Concentrator software can be obtained from the Cisco software download (registered customers only) page.

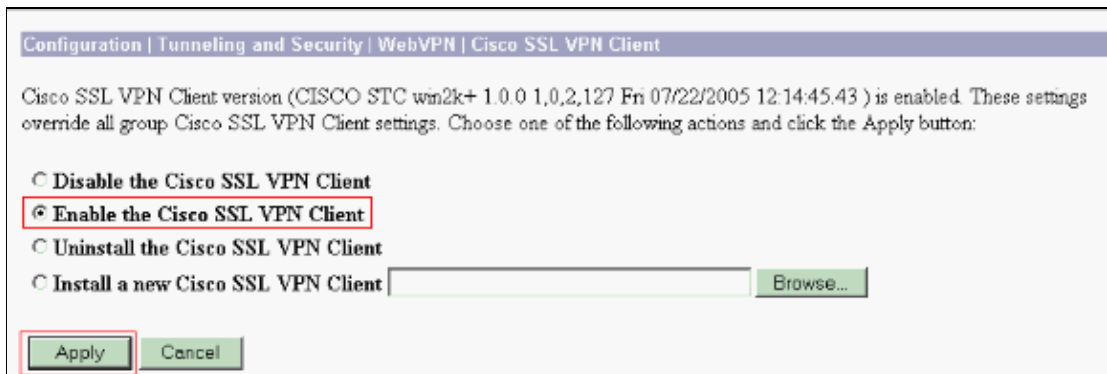


3. Click on the link provided in the confirmation window to continue to enable the SSL VPN Client on the VPN Concentrator.



4. Select **Enable the Cisco SSL VPN Client** and click **Apply**.

This enables the SSL VPN Client on the VPN Concentrator. If your VPN Concentrator was pre-loaded with the SSL VPN Client, go directly to **Configuration > Tunneling and Security > WebVPN > Cisco SSL VPN Client** and enable the SSL VPN Client.



5. Choose **Configuration > User Management > Groups > Add** in order to configure a group for the SSL VPN Client.

If you use an external authentication such as the Cisco ACS server, select **External** in the Type field. Enter a group name and an associated password in this window.

This example uses the name 'sslgroup' for the group. The internal database (on the VPN Concentrator) is also used to authenticate the SSL VPN Client users.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters		
Attribute	Value	Description
Group Name	sslgroup	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Add Cancel

Note: In order to configure the Cisco VPN 3000 Concentrator for RADIUS authentication, refer to Configuring the Cisco VPN 3000 Concentrator with MS RADIUS.

6. Select the WebVPN Tab in the same window in order to enable the SSL VPN Client for group name sslgroup. Select the necessary options.

The **Cisco SSL VPN Client Keepalive Frequency** option is needed only to ensure that an SSL VPN Client connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

The **Keep Cisco SSL VPN Client** option ensures that the SSL VPN Client is always installed in the client PC. If this option is not selected, the SSL VPN Client needs to be installed every time you want a WebVPN tunnel from the client PC.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

WebVPN Parameters			
Attribute	Value	Inherit?	Description
Enable URL Entry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to place the URL entry box onto the home page.
Enable File Access	<input type="checkbox"/>	<input type="checkbox"/>	Check to enable Windows file access through HTTPS. When enabling File Access, a NetBIOS Name Server needs to be configured under System Servers .
Enable File Server Entry	<input type="checkbox"/>	<input type="checkbox"/>	Check to place the file server entry box onto the home page. File Access must be enabled.
Enable File Server Browsing	<input type="checkbox"/>	<input type="checkbox"/>	Check to enable browsing the Windows network for domains/workgroups, servers and shares. File Access must be enabled.
Enable Port Forwarding	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to enable port forwarding
Enable Outlook/Exchange Proxy	<input type="checkbox"/>	<input type="checkbox"/>	Check to enable the Outlook/Exchange proxy.
Apply ACL	<input type="checkbox"/>	<input type="checkbox"/>	Check to apply the WebVPN ACL defined for the users of this group.
Enable Auto Applet Download	<input type="checkbox"/>	<input type="checkbox"/>	Check to enable auto applet download on login.
Enable Citrix MetaFrame	<input type="checkbox"/>	<input type="checkbox"/>	Check to allow access using Citrix MetaFrame terminal services.
Enable Cisco SSL VPN Client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to enable use of the Cisco SSL VPN Client.
Require Cisco SSL VPN Client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to require use of the Cisco SSL VPN Client.
Keep Cisco SSL VPN Client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to keep the Cisco SSL VPN Client installed on the client workstation.
Cisco SSL VPN Client Keepalive Frequency	30	<input checked="" type="checkbox"/>	(seconds) Enter the Cisco SSL VPN Client Keepalive Frequency. Enter 0 to disable.
Port Forwarding Name	Application Access	<input checked="" type="checkbox"/>	Enter the display name the users see when using TCP Port forwarding
Homepage		<input checked="" type="checkbox"/>	Enter the URL of the web page to be displayed to the user upon login.

Content Filter Parameters			
Filter Java/ActiveX	<input type="checkbox"/>	<input type="checkbox"/>	Check to remove <applet>, <embed> and <object> tags from HTML.
Filter Scripts	<input type="checkbox"/>		Check to remove <script> tags from HTML.
Filter Images	<input type="checkbox"/>		Check to remove tags from HTML.
Filter Cookies from Images	<input type="checkbox"/>		Check to remove cookies that are delivered with images. Advertisers use cookies to track visitors.
WebVPN ACLs			
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>		<input checked="" type="checkbox"/>	The WebVPN Access Control List to apply to user sessions. <ul style="list-style-type: none"> • If you do not define any filters, all connections are permitted. • If you configure a permit filter, the default action is to deny connections other than what the filter defines. • A WebVPN ACL can have a total of 255 characters. • Source and destination IDs are IP addresses and wildcard masks or hostnames. • WebVPN ACLs are not applied to SSL VPN Client connections. Only IP ACLs are applied to the SSL VPN Client.
Syntax for protocol filters: [permit deny] [ip smtp imap4 pop3 cifs http https] Src-ID Dst-ID Example: permit ip any host 10.86.9.22 Example: permit ip any 192.168.1.0 0.0.0.255			
Syntax for URL filters: [permit deny] URL URL-definition Example: deny url http://www.example.com			

Apply Cancel

7. Choose **Configuration > User Management > Users > Add** in order to configure an SSL VPN Client user credentials.

You can also assign a static IP address to the users through this window.

In this example, the user name is test. This user is added to the group sslgroup. IP addresses are also assigned with the configuration of a pool of IP addresses.

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	test	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	sslgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

8. Choose **Configuration > System > Address Management > Assignment** and check the necessary option as shown and click **Apply** in order to configure the IP address assignment method.

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client.

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply Cancel

9. Choose **Configuration > System > Address Management > Pools > Add** in order to configure an associated IP address pool.

In this example, you configure an IP address range that is a part of the same subnet of the corporate network.

Configuration | System | Address Management | Pools | Add

Add an address pool.

Range Start	<input type="text" value="10.10.1.2"/>	Enter the start of the IP pool address range.
Range End	<input type="text" value="10.10.1.10"/>	Enter the end of the IP pool address range.
Subnet Mask	<input type="text" value="255.255.0.0"/>	Enter the subnet mask of the IP pool address range. Enter 0.0.0.0 to use default behavior.

10. Choose **Configuration > System > IP Routing > Default Gateway** in order to ensure that you have all necessary routes and default gateways configured properly.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway	<input type="text" value="172.16.1.1"/>	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	<input type="text" value="1"/>	Enter the metric, from 1 to 16.
Tunnel Default Gateway	<input type="text" value="0.0.0.0"/>	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	<input checked="" type="checkbox"/>	Check to allow learned default gateways to override the configured default gateway.

- The interface that terminates the SSL VPN Client needs to have an SSL certificate associated with it.
11. Choose **Administration > Certificate Management** in order to confirm that SSL certificates are generated for the interfaces.

If the certificates are not generated you can generate them when you choose **Generate**. This is an option available under **Actions** in the SSL Certificates box for the respective interface.

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.10.1.1 at Cisco Systems, Inc.	10.10.1.1 at Cisco Systems, Inc.	10/15/2008	View Renew Delete Export Generate Enroll Import
Public	172.16.5.100 at Cisco Systems, Inc.	172.16.5.100 at Cisco Systems, Inc.	10/15/2008	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
512 bits	RSA	02/12/2005	Generate


Enrollment Status [[Remove All](#): [Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

12. Choose **Configuration > Interfaces** and select the respective interface to specifically allow the **HTTPS** session on the interface that terminates the SSL VPN Client.
13. Go to the WebVPN tab and check **Allow WebVPN HTTPS sessions**.

In this example, you are terminating the SSL VPN Client on the public Interface of the VPN Concentrator.

Configuration | Interfaces | Ethernet 2

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth | **WebVPN**

WebVPN Parameters		
Attribute	Value	Description
Allow Management HTTPS sessions	<input type="checkbox"/>	Check to enable management HTTP and HTTPS sessions on this interface. Disabling will prevent managing the device through a web browser on this interface.
Allow WebVPN HTTPS sessions	<input checked="" type="checkbox"/>	Check to enable WebVPN HTTPS sessions on this interface.
Redirect HTTP to HTTPS	<input checked="" type="checkbox"/>	Check to force any connections coming in as HTTP to be redirected to HTTPS. This provides additional security. Unencrypted HTTP sessions will no longer be allowed on this interface.
Allow POP3S sessions	<input type="checkbox"/>	Check to enable POP3S e-mail sessions on this interface using an e-mail program.
Allow IMAP4S sessions	<input type="checkbox"/>	Check to enable IMAP4S e-mail sessions on this interface using an e-mail program.
Allow SMTPS sessions	<input type="checkbox"/>	Check to enable SMTPS e-mail sessions on this interface using an e-mail program.

Configure to Disable Certificate Warning

When you generate the SSL certificate on the VPN Concentrator, always use an IP address or DNS name of the interface. But, if you type something else which does not match your inputs when you open the browser in order to connect the SSL, you receive security warnings messages such as `hostname mismatch errors`. You should type what you previously used when the certificate was generated.

You can choose **Administration > Certificate Management**, and delete and generate the SSL certificate in order to fix this issue.

When you choose **Generate**, you get the **Administration > Certificate Management > Generate SSL Certificate**. At this window, you can generate the SSL certificate for the interface to where you connect. At the **Common Name (CN)** field, you need to fill this space with either an IP address or the DNS name of the interface, which must be similar to what you typed in the browser in order to make the SSL client connection avoid the mismatch error message.

But, even though you do this, a window appears to let you know these messages:

- The security certificate date is valid.
- The security certificate has a valid name that matches the name of the page you attempt to view.

These messages have the green mark, but the yellow mark indicates that the certificate is not yet stored under the trusted certificates of the IE certificate store.

Click the third button of the **View Certificate** box in order to save the certificate and no longer receive this error message. Choose **Install Certificate** at the wizard and click **Next**. Then, choose **Place all the certificates in the following store** and click **Browse**.

Finally, choose the **Trusted Root Certification Authorities** folder and click **Next**. Choose **Finish** and **Yes** at the final warning window. You should receive another message that says that the import was successful.

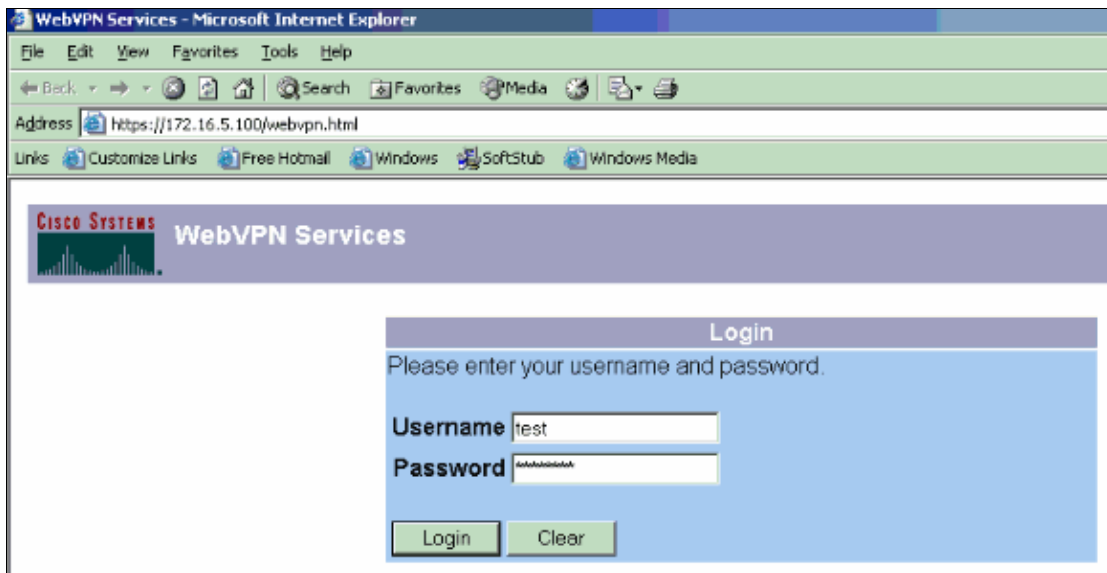
Note: This is a process that you need to make in every computer that uses the SSL client connection, because every computer needs to store the certificate under its own certificate storage.

Verify

Complete these steps in order to confirm that your configuration works properly.

1. Open the Web browser on the Client PC that is going to connect to the VPN Concentrator and enter **https://concentrator_ip_address**.
2. At the login prompt, enter the user credentials that you created earlier and select **Login**.

In this example, type **https://172.16.5.100**, enter the username **test**, and its associated password that you created earlier.

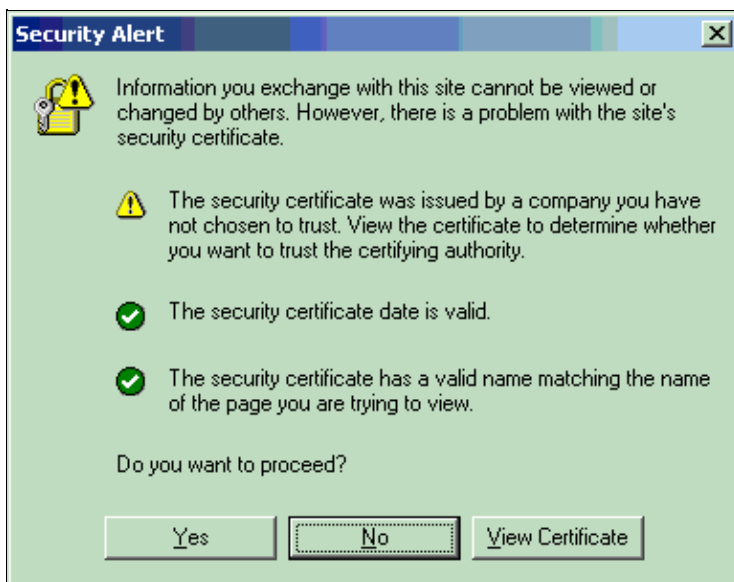


This starts the download of the SSL VPN Client on to the client PC.

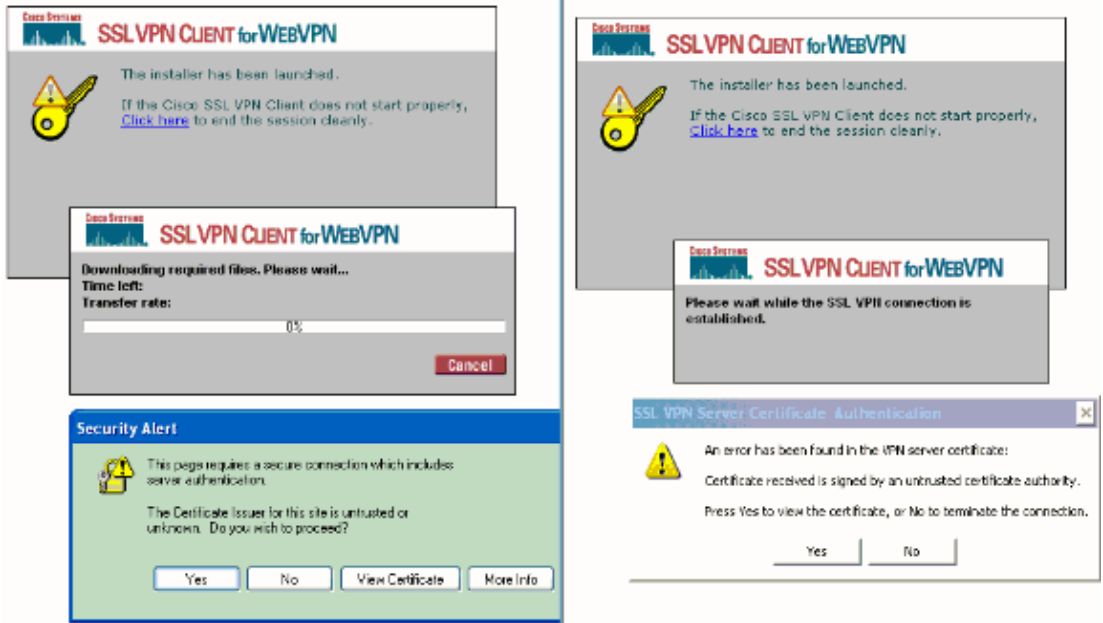
3. When you receive the certificate warning, you can either select **Yes** or **View Certificate**.

Refer to View Certificate on how to proceed with this option.

In this example, **Yes** is selected on the certificate warnings.

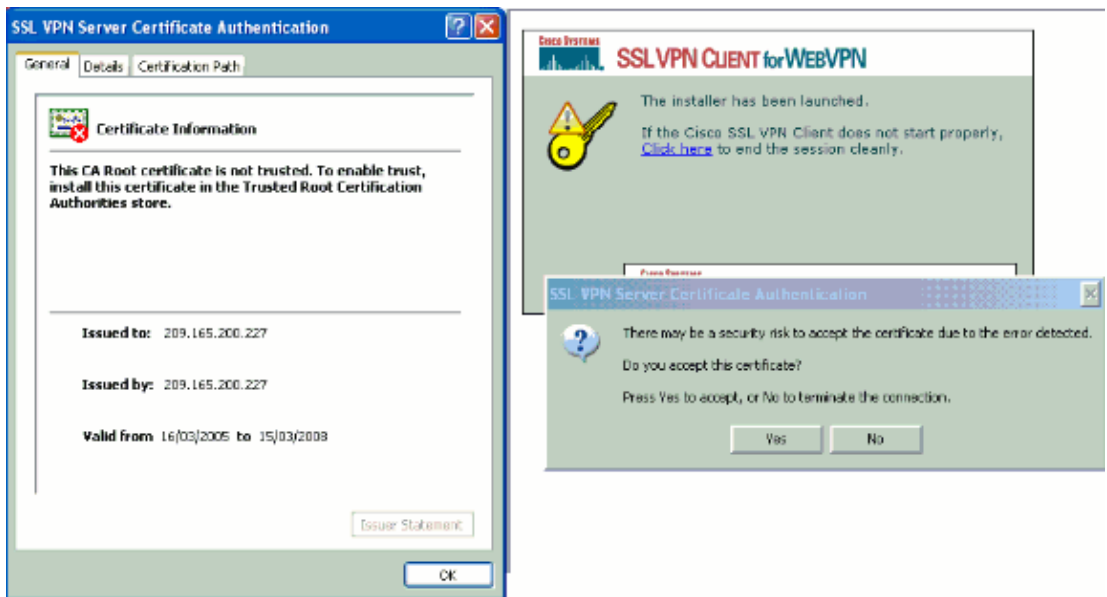


4. Click **Yes** when you are prompted with an alert which states that the certificate issuer is unknown or untrusted.
5. Click **Yes** in order to display the certificate information.



6. Click **OK** on the certification authentication window to install the certificate as a trusted certificate.

Click **Yes** when you are prompted with a certificate warning in the next window.

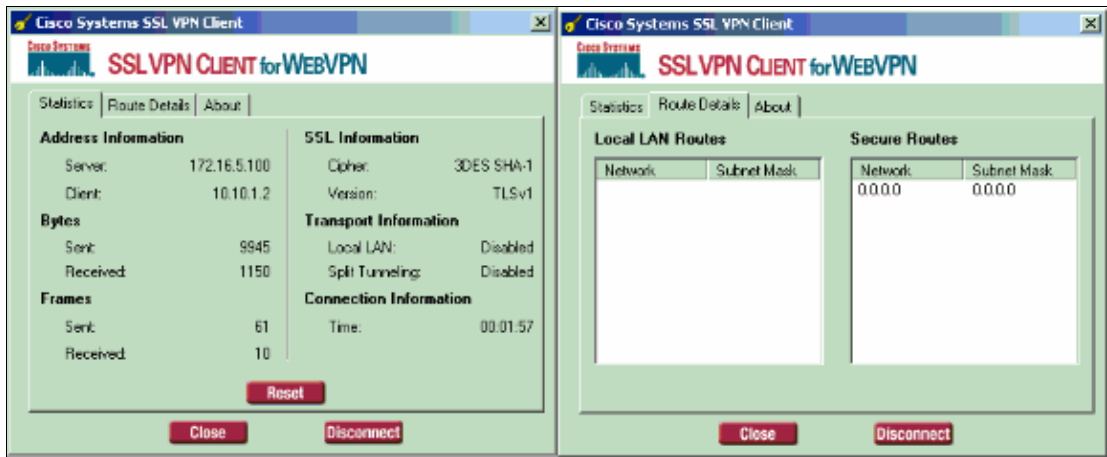


Once you click Yes, the SSL VPN Client is installed on the client PC. The WebVPN connection is automated as well. Once the tunnel is established, you can see the Key icon on the Windows taskbar.



7. Right-click the **Key** icon and select **Status** in order to view the WebVPN connection properties in the SSL VPN Client.

In this example the SSL VPN Client is assigned an IP address of 10.10.1.2 which is part of the IP address pool you defined.



Troubleshoot

Complete these steps in order to troubleshoot your configuration. On the VPN Concentrator you can enable **Event Classes** to log events. This helps you to troubleshoot if your SSL VPN tunnel does not come up.

1. Choose **Configuration > System > Events > Classes > Add** in order to enable all relevant Event Classes.

In this example you need to enable the classes **Auth, SSL, STC, and WebVPN**.

Note: When you enable Event Classes and set Severity levels, this impacts the performance of the VPN Concentrator. Make it a point to disable once you have finished troubleshooting your problem.

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name Select the event class to configure.

Enable Check to enable special handling of this class.

If one of the following values has been set to *Use Event List*, the Event List can be seen by viewing **Configuration | System | Events | General**.

Changing a value set to *Use Event List* will override the sections of the Event List referring to this event class.

Events to Log Select the events to enter in the log.

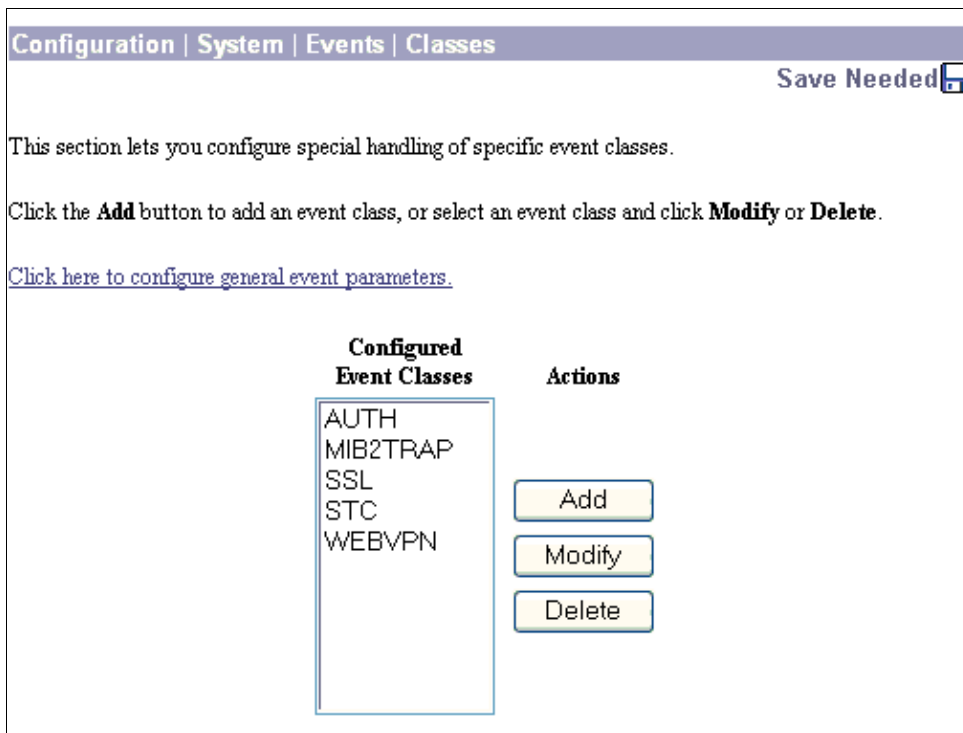
Events to Console Select the events to display on the console.

Events to Syslog Select the events to send to a Syslog Server.

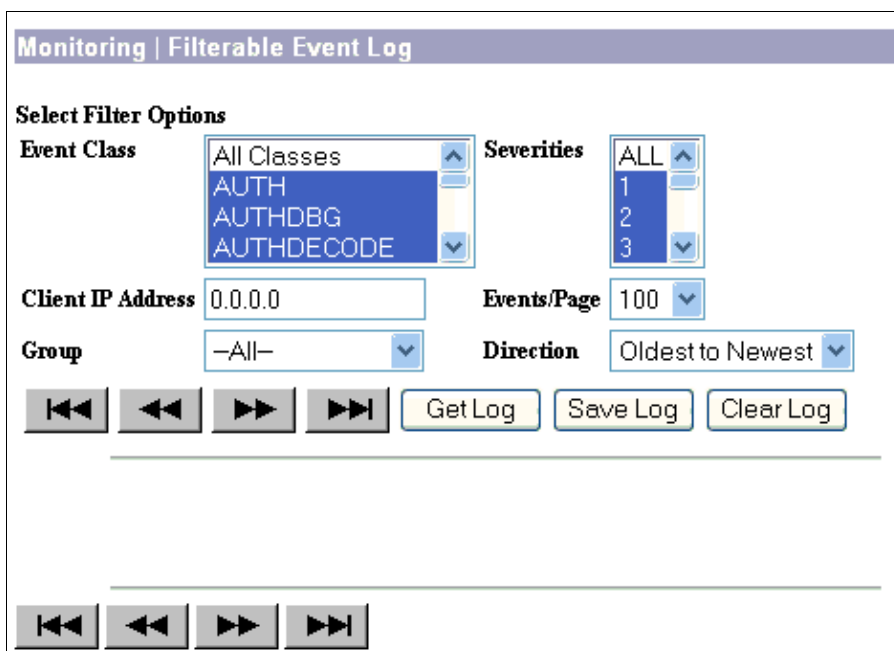
Events to E-mail Select the events to send to an E-mail Recipient.

Events to Trap Select the events to send to an SNMP Trap Destination.

2. Similarly enable all the other Event Classes.



3. Choose **Monitoring > Filterable Event Log** in order to monitor the enabled alarms and click **Get Log** to view the event logs.



The log is displayed in a text file format. You can save the log with the **Save Log** option.

Log of SSL VPN Client when connecting

```
1 10/18/2005 13:27:32.270 SEV=4 AUTH/22 RPT=3 172.16.1.1
User [test] Group [sslgroup] connected, Session Type: WebVPN
```

```
2 10/18/2005 13:27:32.270 SEV=5 WEBVPN/1 RPT=13 172.16.1.1
Group [sslgroup] User [test]
WebVPN session started.
```

Log of a SSL VPN Client issuing a disconnect

```

3 10/18/2005 13:28:26.240 SEV=4 AUTH/28 RPT=3 172.16.1.1
User [test] Group [sslgroup] disconnected:
  Session Type: SSL VPN Client
  Duration: 0:00:53
  Bytes xmt: 244
  Bytes rcv: 7083
  Reason: User Requested

4 10/18/2005 13:28:26.240 SEV=5 WEBVPN/2 RPT=13 172.16.1.1
Group [sslgroup] User [test]
WebVPN session terminated; User Requested.

```

If you encounter the Reason: bad handshake type error, it could be due to a problem with the expired SSL certificate on one or more interfaces of the VPN Concentrator. The workaround is to delete the expired certificate and regenerate a new one for the particular interface. Choose **Administration > Certificate Management** and click **Generate** in order to renew the certificate. Refer to Obtaining SSL Certificates for more information on how to generate a new certificate.

Managing the Concentrator from the Public Network

With the introduction of SSL VPN functionality, HTTP/HTTPS access to the Public interface became a necessity. The default configuration however, is to allow SSL VPN access while disallowing management access to the same Public interface.

Use this procedure in order to configure the VPN Concentrator so that you can manage it from the public network for releases 4.1 and later.

1. Select **Configuration > Interfaces > Ethernet 2 (Public)**, then choose the WebVPN tab.
2. Check the **Allow Management HTTPS sessions** check box.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager interface. The 'WebVPN' tab is selected, displaying the 'WebVPN Parameters' table. The table has three columns: Attribute, Value, and Description. The 'Allow Management HTTPS sessions' checkbox is checked. The 'Redirect HTTP to HTTPS' checkbox is also checked. The other checkboxes are unchecked.

Attribute	Value	Description
Allow Management HTTPS sessions	<input checked="" type="checkbox"/>	Check to enable management HTTP and HTTPS sessions on this interface. Disabling will prevent managing the device through a web browser on this interface.
Allow WebVPN HTTPS sessions	<input checked="" type="checkbox"/>	Check to enable WebVPN HTTPS sessions on this interface.
Redirect HTTP to HTTPS	<input checked="" type="checkbox"/>	Check to force any connections coming in as HTTP to be redirected to HTTPS. This provides additional security. Unencrypted HTTP sessions will no longer be allowed on this interface.
Allow POP3S sessions	<input type="checkbox"/>	Check to enable POP3S e-mail sessions on this interface using an e-mail program.
Allow IMAP4S sessions	<input type="checkbox"/>	Check to enable IMAP4S e-mail sessions on this interface using an e-mail program.
Allow SMTPS sessions	<input type="checkbox"/>	Check to enable SMTPS e-mail sessions on this interface using an e-mail program.

3. Check the **Redirect HTTP to HTTPS** checkbox for enhanced security.
4. Click the **Apply** button and save the configuration.

Note: This checkbox setting overrides the rules that the Public filter defines (or whatever filter is applied to the Public interface). You do not need to add rules to filters in WebVPN supported code.

In order to access the management screen from the Public interface, the URL now becomes **http[s]://<concentrator public IP address>/admin.html**.

WebVPN Authentication Fails

- **Problem:** The WebVPN users are not able to authenticate against the RADIUS server, but can authenticate successfully with the local database of the VPN Concentrator. Errors such as `Login failed` and the message in this example screen shot are seen.



Cause: These kinds of problems happen very often when you use any database other than the internal database of the VPN Concentrator. WebVPN users hit the Base Group when they first connect to the VPN Concentrator and therefore must use the default authentication method. Often this method is set to the internal database of the VPN Concentrator and not a configured RADIUS or other server.

Solution: When a WebVPN user authenticates, the VPN Concentrator checks the list of servers defined at **Configuration >System > Servers > Authentication** and uses the top one. Make sure to move the server that you want WebVPN users to authenticate with to the top of this list. For example, if RADIUS should be the authentication method, you need to move the RADIUS server to the top of the list to push the authentication to it.

Note: Just because WebVPN users initially hit the Base Group does not mean that they are confined to the Base Group. Additional WebVPN groups can be configured on the VPN Concentrator and users can be assigned to them by the RADIUS server by populating attribute 25 with **OU=groupname** . Refer to [Locking Users into a VPN 3000 Concentrator Group Using a RADIUS Server](#) for a more detailed explanation.

Related Information

- [Release Notes for Cisco SSL VPN Client, Release 1.0.2](#)
- [Cisco SSL VPN Client Support Page](#)
- [Cisco VPN 3000 Concentrator FAQ](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation – Cisco Systems](#)

