

SSL VPN Client FAQ

Document ID: 67909

Questions

Introduction

Products Support

Installation

Licensing

Services

Error Messages

Miscellaneous

Related Information

Introduction

This document provides information on the most frequently asked questions (FAQ) related to the SSL VPN Client (SVC). Cisco SVC provides end users who run Microsoft Windows XP or Windows 2000 with the benefits of a Cisco IPsec VPN Client without the administrative overhead required to install and configure an IPsec client. Cisco SVC supports applications and functions unavailable to a standard WebVPN connection.

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

Products Support

Q. Is the SSL VPN Client supported on the Cisco ASA 5500 Adaptive Security Appliance?

A. The SSL VPN Client is supported in Software Version 7.1 of the Cisco ASA 5500 Adaptive Security Appliance.

Q. Is the SSL VPN Client supported on the IOS Routers or Cisco 6500/7600?

A. The SSL VPN Client is supported on the Cisco 870, 1800, 2800, 3700, 3800, 7200, and 7301 routers that run advanced security images of Cisco IOS Software Release 12.4(6)T. For more information on IOS WebVPN, refer to Cisco IOS WebVPN resources. The Cisco WebVPN services module supports SSL VPN Client on the Cisco 6500/7600.

Q. What software release do I need on the Cisco VPN 3000 Concentrator in order to support the Cisco SSL VPN Client?

A. Cisco VPN 3000 Concentrators run Software Release 4.7 or later for the support of SSL VPN Client Software Release 1.0.1 or later.

Note: For Cisco SSL VPN Client Release 1.0.2, Cisco VPN 3000 Concentrators run Software Release 4.7.2 or later. Cisco SSL VPN Client Release 1.0.2 does not operate with a VPN 3000 Concentrator that runs a Software Release earlier than 4.7.2.

If you need to upgrade the VPN 3000 Concentrator to Software Release 4.7.2, refer to the Upgrading to Release 4.7.2 section of Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7.2.

Q. Is Two-Factor Authentication supported in SSL VPN Client?

A. SSL VPN Client supports Two-Factor Authentication in ASA version 8.2(x) and later. It is not supported in versions earlier than 8.2.(x).

Installation

Q. How do I install a Cisco SSL VPN Client on the Cisco VPN 3000 Concentrator?

A. Complete these steps to install a Cisco SSL VPN Client on the VPN 3000 Concentrator:

Note: Before you start the download, make sure that your desktop can access the Cisco VPN 3000 Concentrator.

1. Download the SSL Client file **sslclient-win*.pkg** on your desktop. Proceed to step 2 if the VPN 3000 Concentrator does not run Software Release 4.7.2. Proceed directly to step 3 if the the VPN 3000 Concentrator runs Software Release 4.7.2 .
2. Upgrade the VPN 3000 Concentrator to Software Release 4.7.2. Refer to the Upgrading to Release 4.7.2 section of Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7.2.
3. On the VPN Concentrator, choose **Configuration > Tunneling and Security > WebVPN > Cisco SSL VPN Client** and click **Install a new SVC**.
4. Click **Browse** and go to the directory where you downloaded the SSL VPN Client software.
5. Click **Apply** to download the SSL VPN Client on the VPN 3000 Concentrator.

Note: The SSL VPN Client is already loaded on Cisco VPN 3000 Concentrator Release 4.7.

Q. Do SVC and CSD support Chinese language Windows 2000 and XP?

A. No.

Q. Does Installation of the SVC work with MSJVM?

A. Yes, although note that Microsoft does not support this past December 31, 2007. In fact, this can no longer be downloaded from the Microsoft web site; it directs you to alternative (Sun JVM) Java clients.

Q. Does the SVC Client support Windows 98?

A. There are no plans to support Windows 98 with this SVC. Windows 98 is over 7 years old and is almost at the EOS point by Microsoft. Only Windows 2000 and XP are supported because only those Windows operating systems permit the installation of a network driver without a reboot.

Q. How do I stop the SSL VPN Client from attempting to install on the PC every time I connect to the WebVPN?

A. Check the **KEEP THE CISCO SSL VPN CLIENT** option on the SSL VPN Client workstation. The next time you try to login with the SSL VPN Client, it verifies with the VPN Concentrator to make sure that the version it has is the same as that of the VPN Concentrator and that it is the latest.

Choose **Configuration > User Management > Base Group, Group and/or User parameters** and **WebVPN Tab: Keep Cisco SSL VPN Client** in order to accomplish this.

Q. How do I install SVC silently and uninstall SVC from the client system?

A. In order to install SVC without any prompts, use the `stcie /nodlgnoerr` switch (/? for help). In order to uninstall it, use the `uninstall invisible`.

Q. Can Install Enabler be uninstalled by non-privileged users?

A. No, administrator privileges are required for install and uninstall.

Q. The pre-installer STCIE.EXE only seems to install the STCAgent service. Can it also install the LSP Cisco Systems SSL VPN Adapter ?

A. The goal is to install the bare minimum needed for the rest of the installation to continue and keep the size of the file download to a minimum, not to install the entire package.

Q. What is the process of installation of the SVC, and can this be packaged with Microsoft's SMS?

A. The STCIE is an install enabler. It does not install the driver. It just installs enough code to provide the privilege boost needed to complete the install. In the discussion below, the problem cannot be solved with the install enabler since the issue is that the temporary file download and execute are blocked by the CSA policy that they run.

In addition, the `svcxxx.zip` can be unzipped at any path and that puts `STCIE.EXE` at any path that the user chooses. The `STCIE.EXE` does not install the entire SVC package. It only installs enough components to download and install the entire SVC when the user connects to SG the next time (with admin privileges). The `STCIE.EXE` is also known as "installation enabler." The SVC install path is in the code and is not configurable. Possibly a configurable installation path is not a good SVC feature. Also, the "`C:\Documents and Settings\normlee\Local Settings\Temp\Temp8-Fg2e8`" is a SVC temporary store which is acquired from OS and is not visible for the user. If there is an issue for this temporary store, it is the OS configuration issue. Retrieved from "http://vpnpedia/index.php/SSL_VPN_FAQ."

Q. Are RADIUS with Expiry and MS IAS supported with the SSL VPN Client?

A. No. RADIUS with Expiry is not supported for SSL VPN; support for this feature is only available in ASA, and there are no plans for this feature to be available for current 3K systems.

Q. Can SVC coexist with the Nortel Client?

A. Tested with Version 4.65 Nortel Client with SVC, it works fine.

Licensing

Q. I have a 10–user license for SSL VPN on ASA. How do I upgrade to a 100 SSL VPN user license?

A. You cannot directly upgrade to a 100–user license from a 10–user license. You need to purchase a 10–25 SSL VPN, then 25–50 SSL VPN, and then 50–100 SSL VPN. If you try to directly upgrade, this can hamper usage of other licenses as well. Refer to Licensing information (registered customers only) for more information.

Services

Q. What kind of access control lists (ACLs) does the SSL VPN Client support?

A. The SSL VPN Client supports IP type ACLs and not WebVPN ACLs. You can filter SSL VPN Client traffic when you choose **Filters** under the General Group tab. This is similar to the VPN Client software.

Q. Can I assign IP addresses through DHCP to devices when I use the SSL VPN Client?

A. Yes, when you use the SSL VPN Client you can obtain IP addresses from a DHCP server or from a local pool of addresses created on the VPN 3000 Concentrator.

Q. The SSL VPN Client works fine but does not resolve DNS names, why?

A. If you have configured the VPN Client or PPTP client to use the same group as that of the SSL VPN Client, ensure that you have enabled IPsec on the group where the client connects. This resolves the DNS issue.

Q. Can remote machine control be done through SVC, even if split tunneling is enabled?

A. RDP drops the connection by design. No other *remote control* applications have been tested.

Q. Can the SSL VPN Client (SVC) have support for the password expiry feature?

A. No.

Q. Login fails in SSL VPN when non-ASCII characters (ä,ü) are present in the username or password. Why does this happen?

A. This issue is due to Cisco Bug ID CSCso04556 (registered customers only) .

In order to workaroud this issue, avoid special (non-ASCII) characters in the username and password.

Error Messages

Q. The SSL VPN Client fails to launch on Windows Vista with Internet Explorer 7, and the user gets the Installer is downloading Active x....Installer was not able to start SSL VPN client.... error message, why?

A. Cause:

The error appears because the SSL VPN Client (SVC) fails to initiate a connection.

This happens because of ActiveX install/download problems on Windows Vista with Microsoft Internet Explorer 7. Windows Vista is shipped with Internet Explorer 7, which has an entirely new model that deals with ActiveX. Aside from the differences in ActiveX, the networking stack has been rewritten, and the routing table is different. There are a few other quirks that can affect the client, as well.

Resolution:

SVC is not compatible with or supported on Windows Vista with the Internet Explorer 7 browser as of now.

The workaround is to use supported platforms, such as Windows XP, with Internet Explorer 7.

Note: SVC is supported on Windows Vista with the Internet Explorer 7 browser in ASA version 8.x and later.

Q. Users behind a Microsoft Proxy receive the "None of the authentication protocols offered by the proxy server are supported." error when they connect to the VPN Concentrator through the SSL VPN Client, why?

A. This error message usually means that the proxy server is configured to use an authentication mechanism that is not supported by the SSL VPN Client. At this point, NT LAN Manager (NTLM) and Basic are the only protocols supported by the SSL VPN Client. Always use NTLM when you use the Proxy server.

Q. I receive the The SSL VPN Client was unable to modify the IP forwarding table. An SSL VPN connection will not be established error message, and the VPN fails to connect. Why does this happen?

A. This issue is due to Cisco bug ID CSCeh52036 (registered customers only) . Refer to the bug for more information.

Q. How do you resolve these errors when trying to modify a customization object for SSL VPN in the ASDM? "[ERROR] import webvpn customization name1 disk0:/tmpAsdmImportFile1943056207 " "%ERROR: attempt to index field `auth-page' (a nil value)"

A. This error behavior has been observed and filed as Cisco bug ID CSCti42085 (registered customers only) . In order to resolve this error, fix the DfltCustomization XML and then retry.

1. Export the DfltCustomization.
2. Look for the <form-order> tag and then for this list:

```
<form-order>
  <username><![testuser[200]]></username>
  <secondary-password><![testuser[500]]></secondary-password>
  <secondary-username><![testuser[500]]></secondary-username>
  <internal-password><![testuser[400]]></internal-password>
  <group><![testuser[100]]></group>
  <password><![testuser[300]]></password>
</form-order>
```

Notice that the secondary-username and secondary-password have the same order identifier.

3. Correct this by changing the secondary-password entry to 600.

```
<form-order>
  <username><![testuser[200]]></username>
  <secondary-password><![testuser[500]]></secondary-password>
  <secondary-username><![testuser[600]]></secondary-username>
  <internal-password><![testuser[400]]></internal-password>
  <group><![testuser[100]]></group>
  <password><![testuser[300]]></password>
</form-order>
```

4. Import the corrected XML file over the existing DfltCustomization. ASDM should now be able to re-order the Logon Form Fields Order.

Miscellaneous

Q. Can a Windows login script get executed when connected through the SSL VPN Client?

A. This is not possible through the SSL VPN Client because there is no START BEFORE LOGIN equivalent at this time.

Q. Can I have a list of authentication servers when I use the SSL VPN Client?

A. Yes, if the first server in the list is unreachable, the next server in the list is contacted.

Q. How can I avoid certificate warnings for SVC in the Concentrator?

A. Distribute the trusted root of the concentrator and import the Concentrator certificate from a well-known, trusted root.

Q. Is the SSL rekey lighter weight than IPsec?

A. The SSL rekey does not require an RSA crypto or DH operation. The master secret that was used in the initial handshake is combined with new random data from the server and client to generate new keys. Note that in the SSL rekey, all the handshakes are encrypted with SSL.

Q. If ActiveX and Java are disabled, I cannot execute SVC installation through the browser. Should I get STCIE.EXE?

A. If both ActiveX and Java fail to detect on the client PC, the user is directed to the WebVPN portal page, but only if the "Require Cisco SSL VPN Client" option under the WebVPN parameters for the group of interest is not checked. If this option is checked, the redirect to the WebVPN portal page does not occur. There is no option to download an install package for the SSL VPN Client.

Note: There is a sslclient-win-1.0.0.x.zip file that contains a pre-install package to install the SVC Agent service (with admin privileges) onto a client PC. This install procedure is detailed in the release notes. Once installed, this allows for the full SSL VPN Client package to be downloaded and installed while in non-admin mode with the ActiveX/Java download mechanism, which does need to be enabled on the client PC.

Q. What privileges are required to be present within IE to allow for ActiveX to function?

A. When a "Guest" account is created on a client PC, it is important to determine with which group that "Guest" account is associated. In order to do this, right-click **My Computer** and choose **Manage > Local users and Groups > Users**. Choose a user, double-click, and determine of which group that user is a member. The list includes Administrators, Power Users, and Users. The Users group does not allow for ActiveX to function, whereas the others do.

Q. If you want users to establish an SSL VPN tunnel on a Corporate Machine, is there anything that can be done to check the platform before the VPN is established or even before authentication?

A. Yes, use Cisco Secure Desktop with the registry, file/hash, or digital certificate to make this determination.

Q. How does the SSLv3/TLSv1 negotiation work?

A. The SSLv3/TLSv1 negotiation and certificate acceptance policies are the "standard" Microsoft implementation. In other words, the SSLv3/TLSv1 uses the embedded Microsoft SChannel.dll file, and the certificate handling is the "standard" browser implementation as part of the IE certificate store, that is, the method of SSL negotiation and certificate handling does not change from the "MS default" behavior.

Q. When was the configurable heartbeat implemented in both SVC and the 3K?

A. These DDTSS cover the changes needed in the SSL VPN Client when you operate behind a Netcache Proxy Server and are implemented in SVC Release 1.0.1.116 released on June 30, 2005. The CSCsb08657 SVC fails to pass data when it is behind a NAT device, through a Proxy Server CSCsb01423 SVC Intermittent Terminations, or when behind a Netcache Proxy Server CSCsa97704. A configurable heartbeat is needed to keep a proxy connection open. The correspondent changes required for the head–end VPN3000 were released as part of the 4.7.2. release on June 21, 2005. If the 4.7.2. release (or later) is used, it is necessary to upgrade the version of SVC to 1.0.1.116 or later. CSCei01721 – a configurable heartbeat is needed to keep the SVC proxy connection up.

Q. When was auto proxy support added to SVC?

A. This was added as part of the DDTSS CSCsd05126 in the 1.1.0.x release.

Related Information

- **[Release Notes for Cisco SSL VPN Client, Release 1.0.2](#)**
- **[Release Notes for Cisco SSL VPN Client, Release 1.0.1](#)**
- **[Cisco SSL VPN Client Product Support Pages](#)**
- **[Cisco VPN 3000 Series Concentrators](#)**
- **[Cisco VPN 3002 Hardware Clients](#)**
- **[IPsec Negotiation/IKE Protocols](#)**
- **[Technical Support & Documentation – Cisco Systems](#)**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 22, 2008

Document ID: 67909
