Cisco Secure Desktop (CSD) on IOS Configuration Example using SDM

Document ID: 70791

Introduction **Prerequisites** Requirements Components Used Network Diagram **Related Products** Conventions Configure Phase I: Prepare your router for CSD configuration with SDM. Phase I: Step 1: Configure a WebVPN gateway, WebVPN context, and group policy. Phase I: Step 2: Enable CSD in a WebVPN context. Phase II: Configure CSD using a web browser. Phase II: Step 1: Define Windows locations. Phase II: Step 2: Identify Location criteria Phase II: Step 3: Configure Windows location modules and features. Phase II: Step 4: Configure Windows CE, Macintosh, and Linux features. Verify Test the CSD Operation Commands Troubleshoot Commands **NetPro Discussion Forums – Featured Conversations Related Information**

Introduction

Although Secure Sockets Layer (SSL) VPN (Cisco WebVPN) sessions are secure, the client may still have cookies, browser files, and email attachments remaining after a session is complete. Cisco Secure Desktop (CSD) extends the inherent security of SSL VPN sessions by writing session data in an encrypted format to a special *vault* area of the client's disk. In addition, this data is removed from the disk at the end of the SSL VPN session. This document presents a sample configuration for CSD on a Cisco IOS[®] router.

CSD is supported on the following Cisco device platforms:

- Cisco IOS Routers Version 12.4(6)T and later
- Cisco 870,1811,1841,2801,2821,2841,3725,3745,3825,3845,7200 and 7301 routers
- Cisco VPN 3000 Series Concentrators Version 4.7 and later
- Cisco ASA 5500 Series Security Appliances Version 7.1 and later
- Cisco WebVPN Services Module for Cisco Catalyst and Cisco 7600 Series Version 1.2 and later

Prerequisites

Requirements

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

Requirements for the Cisco IOS router

- Cisco IOS router with Advanced Image 12.4(6T) or later
- Cisco Router Secure Device Manager (SDM) 2.3 or higher

If your router is not already loaded with SDM, you can obtain a free copy from SDM Download. A valid CCO account and service contract is required. Refer to Configure Your Router with Security Device Manager for more details.

• A copy of the CSD for IOS package on your management station

You can obtain a copy of CSD from Software Download: Cisco Secure Desktop The software is free if you have a CCO account with a service contract.

• A router self-signed digital certificate or authentication with a Certificate Authority (CA)

Note: Anytime you use digital certificates, make sure that you set the router's hostname, domain name, and date/time/timezone correctly.

- An enable secret password on the router
- DNS enabled on your router. Several WebVPN services require DNS to work properly.

Requirements for Client computers

- Remote clients should have local administrative privileges; it is not required, but it is highly suggested.
- Remote clients must have Java Runtime Environment (JRE) Version 1.4 or higher.
- Remote client browsers: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2, or Firefox 1.0
- Cookies enabled and Popups allowed on remote clients

Components Used

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

- Cisco IOS router 3825 with Version 12.9(T)
- SDM Version 2.3.1

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

Network Diagram

This document uses this network setup:

This example uses a Cisco 3825 Series router to allow secure access to the company's intranet. The Cisco 3825 Series router enhances the security of SSL VPN connections with configurable CSD features and characteristics. Clients can connect to the CSD–enabled router via one of these three SSL VPN methods:

Clientless SSL VPN (WebVPN), Thin–Client SSL VPN (Port–Forwarding), or SSL VPN Client (Full Tunneling SVC).



Related Products

This configuration can also be used with these hardware and software versions:

- Cisco router platforms 870,1811,1841,2801,2811,2821 2851,3725,3745.3825,3845, 7200 and 7301
- Cisco IOS Advanced Security Image Version 12.4(6)T and later

Conventions

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

Configure

A WebVPN gateway allows a user to connect to the router via one of the SSL VPN technologies. Only one WebVPN gateway per IP address is allowed on the device, although more than one WebVPN context can be attached to a WebVPN gateway. Each context is identified by a unique name. Group Policies identify the configured resources available to a particular WebVPN context.

Configuration of CSD on an IOS router is accomplished in two phases:

Phase I: Prepare your router for CSD configuration with SDM

1. Configure a WebVPN gateway, WebVPN context, and group policy .

Note: This step is optional and is not covered in great detail in this document. If you have already configured your router for one of the SSL VPN technologies, omit this step.

2. Enable CSD in a WebVPN context .

Phase II: Configure CSD using a web browser.

- 1. Define Windows Locations .
- 2. Identify Location criteria .
- 3. Configure Windows location modules and features .

Phase I: Prepare your router for CSD configuration with SDM.

CSD can be configured with SDM or from the command-line interface (CLI). This configuration uses SDM and a web browser.

These steps are used to complete the configuration of CSD on your IOS router.

Phase I: Step 1: Configure a WebVPN gateway, WebVPN context, and group policy.

You can use the WebVPN Wizard to accomplish this task.

1. Open SDM and go to **Configure > VPN > WebVPN**. Click the **Create WebVPN** tab and check the **Create a new WebVPN** radio button. Click **Launch the selected task**.



2. The WebVPN Wizard screen lists the parameters that you can configure. Click Next.



3. Enter the IP address for the WebVPN gateway, a unique name for the service, and Digital Certificate information. Click **Next**.

WebVPN Wizard IP Address and Name This is the IP address users will enter to access the WebVPN portal page. If multiple is services are configured in this router, the unique name is used to distinguish the services IP Address: 192.168.0.37 Name: cisco	VebVPN ice.
Enable secure SDM access through 192.168.0.37 Digital Certificate When users connect, this digital certificate will be sent to their web browser to authent router. Certificate: TP-self-signed-577183110	icate the
Information URL to login to this WebVPN service: https://192.168.0.37/cisco	

4. User accounts can be created for authentication to this WebVPN gateway. You can use either local

accounts or accounts created on an external Authentication, Authorization, and Accounting (AAA) server. This example uses local accounts on the router. Check the radio button **Locally on this router** and click **Add**.

WebVPN Wizard	
WebVPN Wizard	User Authentication You can configure user accounts locally on this router. You can configure user accounts on a AAA server so that the router can contact this server to authenticate users when they try to log on. Specify how WebVPN should authenticate the users when they login. © External AAA server © Locally on this router! © First on an external AAA server and then locally on this router © Use the AAA authentication method list: Sdm_vpn_xauth_ml_9 © Create user accounts locally on this router. Add Edit Add Edit
	< Back Next > Finish Cancel Help

5. Enter the account information for the new user on the Add an Account screen and click **OK**.

Add an Account	
Enter the username and password	
Username:	user_1
Password	
Password	<none></none>
New Password:	*****
Confirm New Password:	*****
Encrypt password using MD5 ha	sh algorithm
Privilege Level:	1 💌
OK R Cance	l Help

6. After you have created your users, click **Next** on the User Authentication page.

WebVPN Wizard		
WebVPN Wizard	User Authentication You can configure user accounts locally on this router. You can configure user acco AAA server so that the router can contact this server to authenticate users when they login. C External AAA server Locally on this router First on an external AAA server and then locally on this router Use the AAA authentication method list: sdm_vpn_xauth_ml_9 Verate user accounts locally on this router. Username wishaw ausnml sales newcisco User_1	unts on a / try to log Add Edit
	< Back Next & Finish Cancel	Help

7. The Configure Intranet Websites screen allows you to configure the website available to users of the WebVPN gateway. Since this document's focus is the configuration of CSD, disregard this page. Click **Next**.

WebVPN Wizard			
WebVPN Wizard	Configure Intranet Websites You can configure groups of intranet websites here. Each group can be given a heading and can contain one or more websites. Each of these groups will appear in the portal page as links that users can click to navigate to these sites. Add or select the group of websites you want to display in the portal page.		
	Action	URL List	Add Edit Delete
		< Back Next Finish Ca	ncel Help

8. Although the next WebVPN Wizard screen allows you the choice to enable the Full Tunnel SSL VPN Client, the focus of this document is how to enable CSD. Uncheck **Enable Full Tunnel** and click **Next**.

WebVPN Wizard	
WebVPN Wizard	Enable Full Tunnel Enabling full tunnel downloads the WebVPN full tunnel client software to the client.
	IP Address Pool Create a new or select an existing address pool from which clients will be given an IP address when they connect. IP Address Pool:
	 Install Full Tunnel Client The full tunnel client software should be installed on your router, so that it can be downloaded by clients when they connect to WebVPN service on this router. Specify the location of the full tunnel software install bundle. Location:
	Download latest Full Tunnel client install bundle. Keep the Full Tunnel Client software installed on client's PC. Click Advanced Tunnel Options to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.
	< Back Next * Finish Cancel Help

9. You can customize the appearance of the WebVPN Portal Page to users. In this case, the default appearance is accepted. Click **Next**.

WebVPN Wizard	
WebVPN Wizard	Customize WebVPN Portal Page You can customize the WebVPN portal page that is displayed to users. You can select a predefined theme for the portal page. A theme defines colors for texts and background and a logo. You can create new themes, and customize colors, text and logo in Edit WebVPN mode. Theme: Open Highway
	CISCO SYSTEMS Web VPN Server It the Floating Toolbar does not open, click here to open it
	Websites Internet Enter Web address (URL): Go
	< Back Next * Finish Cancel Help

10. The Wizard displays the last screen in this series. It shows a summary of the configuration for the WebVPN gateway. Click **Finish** and, when prompted, click **OK**.

WebVPN Wizard		
WebVPN Wizard	Summary of the Configuration	
	WebVPN Service Name : cisco WebVPN Policy Name : policy_1 WebVPN Gateway Name : gateway_1 User Authentication Method List : Local	4
	Intranet websites: Disabled Full Tunnel Configuration SVC Status : No IP Address Pool : <none> Split Tunneling : Disabled Split DNS : Disabled Install Full Tunnel Client : Disabled</none>	
A		2
	DNS is not enabled on your router. As some WebVPN services require DNS to recommended that you enable DNS.	o work, it is
	< Back Next > Finish Cancel	Help

Phase I: Step 2: Enable CSD in a WebVPN context.

Use WebVPN Wizard to enable CSD in a WebVPN context.

- 1. Use the advanced features of the WebVPN Wizard to enable CSD for the newly created context. The Wizard gives you the opportunity to install the CSD package if it is not already installed.
 - a. In SDM, click the **Configure** tab.
 - b. In the navigation pane, click **VPN** > **WebVPN**.
 - c. Click the **Create WebVPN** tab.
 - d. Check the **Configure advance features for an existing WebVPN** radio button.
 - e. Click the Launch the selected task button.

🛤 Cisco Router and Security Device M	anager (SDM): 172.22.1.	151		
File Edit View Tools Help				
Home De Configure	Monitor Reliesh	Save Search	ମ୍ମୁ Help	CISCO SYSTEMS
Tasks 🛃 VPN				
Presentation Security Pudit Security Pudit NBT Consistence Security Pudit Security Pudit Security Pudit Security Prevention Security Prevention Security Prevention Security Prevention NBT NBT NBC	PN emote ever tipoint VPN Galeways nents Recom DNS is no require D Create Use ti You c Config Desit	APN Edit WebVPN guide you through Web he selected task buttor Use Case Scenario Use Case Scenario Control Cont	VPN configuration tasks. Select VPN configuration tasks. Select s some Web/PN services sed that you enable DNS. Web/PN. g Web/PN. g Web/PN for a new group of for an existing Web/PN for a for an existing Web/PN	ct a task; then click Finable DHS. f users a new group of users. For example company. , full tunnel, and Cisco Secure cted task
Additional Tasks	How do I	: How Do I Confirm n	w WebVPN Is working?	■ 60
Configuration delivered to router.	/ `			21:09:34 UTC Sun Aug 06 2006 📑

2. The welcome page for the Advanced WebVPN Wizard displays. Click Next.



3. Choose the WebVPN and user group from the fields' drop–down boxes. The Advanced WebVPN Wizard features will be applied to your choices. Click **Next**.

WebVPN Wizard	
WebVPN Wizard	Select the WebVPN user group Select the WebVPN and the user group within that WebVPN for whom you want to configure additional advanced features. First select the WebVPN where the user group is defined and then select the user group. WebVPN: User Group: policy_1 Default Group: policy_1
	< Back Next + Finish Cancel Help

4. The Select Advanced Features screen allows you to choose from the listed technologies.

- a. Check Cisco Secure Desktop.
- b. In this example, the choice is **Clientless Mode**.
- c. If you choose any of the other listed technologies, additional windows open to allow input of related information.
- d. Click the **Next** button.



5. The Configure Intranet Websites screen allows you to configure the website resources you want available to the users. You can add the company's internal websites such as Outlook Web Access (OWA).

WebVPN Wizard			X
WebVPN Wizard	Configure Intranet Websites You can configure groups of intranet websites here. Each group can be given a heading and can contain one or more websites. Each of these groups will appear in the portal page as links that users can click to navigate to these sites. Add or select the group of websites you want to display in the portal page.		
	Action	URL List	Add Edit Delete
		< Back Next > Finish Ca	ncel Help

6. In the Enable Cisco Secure Desktop (CSD) screen, you have the opportunity to enable the CSD for this context. Check the box beside **Install Cisco Secure Desktop** (CSD) and click **Browse**.

WebVPN Wizard	
WebVPN Wizard	Enable Cisco Secure Desktop (CSD) Installs Cisco Secure Desktop (CSD) Software on client's PC when they connect to WebVPN server. WebVPN sessions may leave cookies, browser history files, temporary files, and e-mail attachments on the client PC even after the session is over. Cisco Secure Desktop creates a secure partition and encrypts all information stored on client PC. At session close, it removes all data using the US Department of Defence sanitation algorithm and deletes the partition. Implement Cisco Secure Desktop (CSD). Specify the location of Cisco Secure Desktop (CSD) install bundle (.pkg) file. Location: Download latest Cisco Secure Desktop Install bundle.
	< Back Next > Finish Cancel Help

7. From the Select CSD Location area, check My Computer.

- a. Click the **Browse** button.
- b. Choose the CSD IOS package file on your management workstation.
- c. Click the **OK** button.
- d. Click the Next button.

8. A Summary of the Configuration screen displays. Click the **Finish** button.

WebVPN Wizard		×
WebVPN Wizard	Summary of the Configuration	
	WebVPN Service Name : cisco WebVPN Policy Name : policy_1 Intranet websites: Disabled Install Cisco Secure Desktop (CSD). : Enabled Location: C:\CISCO\downloads\securedesktop-ios-3.1.1.32-k9.pkg	
(IN)	5	>
	DNS is not enabled on your router. As some WebVPN services require DNS to w recommended that you enable DNS.	ork, it is
	< Back Next > Finish Cancel H	Help

9. Click **OK** when you see that the CSD package file has been successfully installed.

WebVPN Wizard		×
WebVPN Wizard	Summary of the Configuration	
	WebVPN Service Name : cisco WebVPN Policy Name : policy_1 Intranet websites: Disabled Install Cisco Secure Desktop (CSD). : Enabled Location: C:\CISCO\downloads\securedesktop-ios-3.1.1.32-k9.pkg	
	Information 🔀	
		ırk, it is
	<back cancel="" finish="" h<="" next≻="" th=""><th>lelp</th></back>	lelp

Phase II: Configure CSD using a web browser.

These steps are used to complete the configuration of CSD on your web browser.

Phase II: Step 1: Define Windows locations.

Define the Windows locations.

- 1. Open your web browser at https://WebVPNgateway_IP Address/csd_admin.html, for example, https:/192.168.0.37/csd_admin.html.
- 2. Enter the username **admin**.
 - a. Enter the password, which is the enable secret of the router.

b. Click Login .	
WebVPN CSD Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
File Edit View Favorites Tools Help	#
🔇 Back • 💿 - 💌 😰 🏠 🔎 Search 👷 Favorites 🤣 😒 - چ 🔟 • 🦲 🎉 🦓	
Address 🕘 https://192.168.0.37/csd_admin.html	🔁 Go Links 🎾
Coogle - 💽 Search - 🧭 🥩 🖓 18 Mocked 🤟 Check - 🖄 Autolink - 🗐 AutoFi 💆 Options 🖉	
WebVPN CSD Manager	
Cisco Secure Desktop Admin Login	
Please enter the admin username and password.	
Username: admin	
Password:	
Login Clear	
4	
	<u>×</u>
😫 Done 🛗 🕥 Extern	et 🤃

3. Accept the certificate offered by the router, choose the context from the drop–down box, and click **Go**.

https://192.168.0.37/csd_admin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
File Edit View Favorites Tools Help	
🔇 Back • 🐑 - 💌 😰 🏠 🔎 Search 🧙 Favorites 🤣 😂 - چ 🔟 • 🕞 🏭 🥸	
Address 🕘 https://192.168.0.37/csd_admin.html	Links ³⁹
Google - 💽 G. Search 🔹 🧭 🕼 18 blockad 🥙 Check 🔹 🎘 Autolick 👻 🖓 Autolick 🐇 🖓 Options 🖉	
WebVPN CSD Manager	X
Virtual Context: Geo Go	
🖉 Done 🔮 Internet	

4. The Secure Desktop Manager for WebVPN opens.

https://192.168.0.37/csd_ar	imin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.					
File Edit View Favorites Tools	File Edit View Favorites Tools Help 🥂					
🔇 Back • 🐑 · 💌 😰 (😋 Back • 😥 · 🖹 🖻 🏠 🔎 Search 👷 Favorites 🤣 🍰 - 🌺 🔟 • 🔜 🏭 🦓					
Address 🚵 https://192.168.0.37/csd_	admin.html	💌 🛃 Go Links 🎾				
Google -	💌 💽 Search 🔹 🧭 🥵 🤮 18 blocked 🛛 🌱 Check 🔹 🌂 Autolink 🕤 🗐 AutoFil 🔤 Option	15 <i>D</i>				
WebVP	N CSD Manager	\boxtimes				
	Virtual Context: cisco 🛩 Go					
SECURE DESKTOP	MANAGER for WEBVPN	Release Notes Help				
Settings Saved	Secure Desktop Manager					
Secure Desitor Manager Windows Location Settings Windows CE Windows CE Mac & Unux Cache Cleaner TU Upload/Download Settings	This interface lets you set up all the settings of the Secure Desktop Anager sub-tree at near left. If you make chan appears above the sub-tree. To begin configuration cluck on "Windows Location Settings" and define the different locations that users will co settings for each of the locations using the locations sub-tree items. Click on the "Nac & Linux Cache Cleaner" I Mac & Linux users. You can also use "Upload / Download Settings" to upload any saved configurations or down configuration.	ges, dick "Save" when it meet from. Then define the to configure the settings for load the current				
2 Done		S Internet				

5. From the left pane, choose Windows Location Settings.

- a. Place the cursor in the box next to Location name, and enter a location name.
- b. Click Add.
- c. In this example, three location names are shown: Office, Home, and Insecure. Each time a new location is added, the left pane expands with the configurable parameters for that location.

🔄 https://192.168.0.37/csd_admin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.					
File Edit View Favorites Tools Help					
🌀 Back 🔹 🕥 🕐 💌 😰 🗆	🏠 🔎 Search 👷	Favorites 🚱 🍰 🦉	· 🔜 🛍 🦓		
Address 🚵 https://192.168.0.37/csd_	admin.html				💌 🛃 Go 🛛 Links 🍟
Google -	🖌 🖸 Search 🔹 🧭	🤣 🐴 18 blocked 🗳 Check 🔹	🌂 Autolink 👻 👹 Auto	El 🛃 Options	I
WebVP	N CSD Man	ager			\boxtimes
		Virtual Context: cisco 💌	Go		
SECURE DESKTOP	MANAGER for WEB	VPN			Release Notes Help
A Settings Modified Save	Windows Location	Settings			
Secure Desktop Manager Control Vindows Location Settings Coffice Control Logger Control L	Locations in priority order:	Coffice Home Insecure Add Delete Cose all opened browser windows upon in	Move Up Move Down		
VPN Feature Policy during Windows Installation Failure:					
	Web Browsing:	OFF 💌	File Access:	OFF 💌	
	Port Forwarding:	OFF V	Full Tunneling:	OFF 💌	
8					 Internet

6. After you create the Windows locations, click **Save** at the top of the left pane.

Note: Save your configurations often because your settings will be lost if you become disconnected from the web browser.

9 https://192.168.0.37/csd_ar	amin. Intml - Microsoff	Internet explorer provided by Ce	co Systems, Inc.		
File Edit View Favorites Tools	Help				At
🔾 Back • 🐑 · 💌 🛃	🏠 🔎 Search 🤸	Favorites 🕢 🍰 🦉	· 🔜 🛍 🦓		
Address 🗿 https://192.168.0.37/csd_	admin.html				💌 🛃 Go Links 🏁
Google -	🖌 🖸 Search 🔹 🥥	🥩 🐴 18 blocked 👋 Check 🔹	🔍 AutoLink 🕝 🗐 Auto	Fil 🛃 Options	Ð
Cisco Systems WebVP	N CSD Man	ager			X
		Virtual Context: cisco 👻	Go		
SECURE DESKTOP	MANAGER for WEB	/PN			Release Notes Help
A Settings Modified Save	Windows Location	Settings			
Secure Desktop Manager Secure Desktop Manager Secure Desktop Sectors Settings Secure Desktop General Secure Desktop Secure Desktop General Secure Desktop S	Locations in priority order: Location nerve:	Cffice Home Trisecure	Move Up Move Down		
Image: Secure Desktop Browser ACCI Delete Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desktop General Image: Secure Desk					
🧃 javascript: ;					Internet

Phase II: Step 2: Identify Location criteria

In order to distinguish Windows locations from each other, assign specific criteria to each location. This allows CSD to determine which of its features to apply to a particular Windows location.

- 1. In the left pane, click **Office**.
 - a. You can identify a Windows location with certificate criteria, IP criteria, a file, or registry criteria. You can also choose the Secure Desktop or Cache Cleaner for these clients. Since these users are internal office workers, identify them with IP criteria.
 - b. Enter the IP address ranges in the **From** and **To** boxes.
 - c. Click Add. Uncheck Use Module: Secure Desktop.
 - d. When prompted, click Save, and click OK.

🗈 https://192.16B.O.37/csd_admin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc. 📃 💷 🔀						
File Edit View Favorites Tools	File Edit View Favorites Tools Help					
🌀 Back 🔹 🕥 · 💌 🛃	🏠 🔎 Search 🤺	* Favorites 🚱 🔗 - چ 😥 - 🧾 鑬 🦓				
Address 🙋 https://192.168.0.37/csd_	admin.html		So Links **			
Google -	🔽 🖸 Search 🔹 🧭	🕼 🤣 🛂 18 blocked 🛛 🌱 Check 🔹 🍕 AutoLink 🔹 🗐 AutoFil	Notions 🖉			
Cisce States WebVP	WebVPN CSD Manager					
		Virtual Context: cisco 🛩 Go				
SECURE DESKTOP	MANAGER for WEB	VPN	Release Notes Help			
A Settings Modified Save	Identification for O	ffice				
A Secure Desktop Manager		Enable identification using certificate oritoria:				
- 🚰 Windows Location Settings	Name/Issuer:					
Section 2017 Policy Section 2017 Policy	(Issued To/By)					
- 🔄 Keystroke Logger						
- Ed Secure Desktop General		Enable identification using IP oritoria:				
Secure Desktop Settings	172.22.1.70 - 172.22	1.90				
E- C Home						
- Keystroke Looper	From:					
- Cache Geaner	Ter	Add Delete				
-Eg Secure Desktop General -Eg Secure Desktop Settings	101					
Secure Desktop Browser		Enable identification using File or Registry orkeria:				
- Keystroke Logger						
Cache Cleaner	1					
- Eg Secure Desktop General	Add Delete					
- Go Secure Desktop Browser						
- @ Mac & Linux Cache Cleaner	Use Module:	Secure Desktop or Cache Cleaner				
└──↑↓ Upload/Download Settings		5d				
			Internet			

2. In the left pane, click the second Windows Location Setting **Home**.

- a. Make sure Use Module: Secure Desktop is checked.
- b. A file will be distributed that identifies these clients. You could choose to distribute certificates and/or registry criteria for these users.
- c. Check Enable identification using File or Registry criteria.
- d. Click Add.

E https://192.168.0.37/csd_a	dmin.html - Microsol	I Internet Explorer provided by Lisco Systems, Inc.	🖃 🖵 🔽
File Edit View Favorites Tools	Help		At 1
Ġ Back • 🜍 · 💌 🛃	🏠 🔎 Search 🤺	- Favorites 🤣 🍰 - 🌺 🔟 - 🛄 鑬 🦓	
Address 🚵 https://192.168.0.37/csd_	admin.html		👻 🛃 Go 🛛 Links 🏁
Google -	🖌 🖸 Search 🔹 🥝	🛛 🤣 🚰 18 blocked 🥙 Check 🔹 🎘 AutoLink 🕤 💮 AutoFil 🛃 Opti	ons 🖉
WebVP	N CSD Mar	nager	\mathbf{X}
		Virtual Context: cisco 💌 Go	
SECURE DESKTOP	MANAGER for WEB	VPN	Release Notes Help
A Settings Modified Save	Identification for H	ome	
A Secure Desiton Manager		Enable identification using certificate oriteria:	
- 🚰 Windows Location Settings	Name/Issuer:		
E-102 Office	(Issued To/By)		
- E Keystroke Logger			
-Eg Secure Desktop General		Enable identification using IP oriteria:	
- Secure Desktop Settings			
E- C Home	1		
- To VPW Feature Policy - E Keystroke Logger	From:	· · · · · · · · · · · · · · · · · · ·	
- Cache Cleaner	To:	Add Delete	
Secure Desktop Settings			
Secure Desktop Browser		Enable identification using File or Registry oritoria:	
- 75 VPN Feature Policy			
- Cache Cleaner			
- Ed Secure Desktop General	Add Delete		
Secure Desktop Browser	12		
- Cathe Cleaner	Use Module:	🗹 Secure Desktop or 🔲 Cache Cleaner	
—↑↓ Upload/Download Settings			
2			
12 C			Unternet .:

3. In the dialog box, choose **File**, and enter the path to the file.

- a. This file must be distributed to all your home clients.
- b. Check the radio button **Exists**.
- c. When prompted, click **OK** , and click **Save**.

101 https://192.166.0.3//csd_a	dmin, html - Mic	rosoft Internet Explorer provided by Cisco Systems, Inc.	
File Edit View Favorites Tools	Help		A
🔇 Back + 🕥 - 💌 🖻	🏠 🔎 Search	🗙 Favorites 🥝 🍰 🌺 📝 🛛 🗾 🏭 🦓	
Address 🗿 https://192.168.0.37/csd	admin.html		So Links **
Google -	G Search	- 🌀 🥩 🖓 18 blocked 🥙 Check - 🔍 AutoLink - 🧐	AutoFil R Options
Cisco Statian automatilian	N CSD N	lanager	\boxtimes
		Virtual Context: cisco 💌 Go	
SECURE DESKTOP	MANAGER for	WebVPN	Release Notes Help
A Settings Modified Save	Identification	for Home	
A Secure Desiton Manager		Enable identification using certificate criteria:	
- 🖓 Windows Location Settings	Nane/Isr		7
D-@ Office	(Issued		
- Keystroke Logger	10(04)		
- 😭 Cache Geaner		ype: 🔘 Registry 💿 File	
-Eg Secure Desktop General	P	ath: c:i,donotdelete.t:xt	
Secure Desktop Browser		Exists	
E-10 Home -17. VPM Feature Policy	Lances and		
- 🚔 Keystroke Logger	From:	Does not exist	
- Gathe Cleaner	To:	Version less than	n
- Secure Desktop Settings		Checksum (in hex) (ex. 0x52a8b391)	Ĩ
Secure Desktop Browser			
- W Insecure			
- 🔄 Keystroke Logger			
- Cache Cleaner		· u	
- 🐻 Secure Desktop Settings	Add Dele	ite .	
- Go Secure Desktop Browser		_	
- C Mac & Linux Cache Cleaner	Use Module:	Secure Desktop or Cache Cleaner	
□-↑↓ Upload/Download Settings			
8			😗 Internet

- 4. To configure the identification of **Insecure** locations, simply do not apply any identifying criteria.
 - a. Click **Insecure** in the left pane.
 - b. Leave all the criteria unchecked.
 - c. Check Use Module: Secure Desktop.
 - d. When prompted, click **Save**, and click **OK**.

*2_https://192.166.0.37/csd_a	dmin.html - Microsof	Internet Explorer provided by Cisco Systems, Inc.				
File Edit View Favorites Tools	s Help		*			
😋 Back + 🐑 · 💌 😰	🔇 Back • 🜍 • 💌 😰 🏠 🔎 Search 👷 Favorites 🤣 🎯 • 🌄 🕅 • 🛄 🏭 🚳					
Address 🗃 https://192.168.0.37/csd	admin.html		💌 🛃 Go Links 🏁			
Google -	🖌 🖸 Search 🔹 🥥	🛛 🥩 🚰 18 blocked 🛛 🌴 Check 🔹 🎘 AutoLink 🕤 💮 AutoFil 💽 Options	B			
WebVP	WebVPN CSD Manager					
		Virtual Context: cisco 🛩 Go				
SECURE DESKTOP	MANAGER for WEB	VPN	Release Notes Help			
A Settings Modified Save	Identification for In	secure				
🙆 Secure Desktop Manager		Enable identification using certificate oriteria:				
Windows Location Settings Gfice Gfice Kensterie Leases	Name/Issuer: (Issued To/By)					
- Cache Geaner - Egi Secure Desktop General		Enable identification using IP oritoria:				
Secure Desktop Settings						
- Keystroke Logger	From:	FINITE - FINITE - FINITE - FINITE				
- Cache Geaner - Cache Desktop General - Cache Desktop Settings	То:	Add Delete				
Secure Desktop Browser		Enable identification using File or Registry oritoria:				
-26 VPN Feature Policy -6 Keystroke Logger -6 Cache Cleaner						
- 🐻 Secure Desktop General - 🐻 Secure Desktop Settings - 🚱 Secure Desktop Browser	Add Delete					
— III Windows CE — III Windows CE — III Mac & Linux Cache Cleaner — III Upload/Download Settings	Use Module:	🗹 Secure Desktop or 🔲 Cache Cleaner by				
<u>ا</u>			Internet			

Phase II: Step 3: Configure Windows location modules and features.

Configure the CSD features for each Windows location.

1. Under **Office**, click **VPN Feature Policy**. Since these are trusted internal clients, neither CSD nor Cache Cleaner was enabled. None of the other parameters is available.

https://192.168.0.37/csd_a	dmin.html - Micr	osoft Internet Explorer provided by Cisco Systems, Inc.			
File Edit View Favorites Tools	Help				
G Back • 🕑 · 💌 🖻	🚱 Back • 🙄 · 🖹 🖻 🏠 🔎 Search 👷 Favorites 🤣 🙆 • 🍃 🔟 • 📴 🏭 🦓				
Address 🚵 https://192.168.0.37/csd_	admin.html		💌 🛃 Go 🛛 Links 🎬		
Google +	🖌 🖸 Search 🔹	🌀 🥩 🚰 18 blocked 🧳 Check 🔹 🎘 AutoLink 🕣 🗐 AutoFil	Notions 🥖		
WebVP	WebVPN CSD Manager				
		Virtual Context: cisco 🛩 Go			
SECURE DESKTOP	MANAGER for V	VebVPN	Release Notes Help		
A Settings Modified Save	VPN Feature P	olicy under Windows Installations			
A Secure Desktop Manager	Web Browsing:	ON M			
Windows Location Settings		1			
- Groce - Chice - Conce - Conc	File Access:	0N V			
- 🖾 Secure Desktop General - 🐻 Secure Desktop Settings					
는 6월 Secure Desktop Browser 요. 생 Home	Port Forwarding:	ON 💌			
- 🎼 VPN Feature Policy - 🚔 Keystroke Logger					
- 😭 Cache Cleaner - 🔯 Secure Desktop General	Full Tunneling:	ON V			
- 10 Secure Desktop Settings					
Solution					
Keystroke Logger					
- Secure Desktop General					
- Secure Desktop Settings					
- Windows CE					
14 Upload/Download Settings					
🛃 Done			Internet		

2. Turn on the features as shown.

- a. In the left pane, choose VPN Feature Policy under Home.
- b. Home users will be allowed access to the corporate LAN if the clients meet certain criteria.
- c. Under each method of access, choose **ON if criteria are matched**.

🔹 https://192.168.0.37/csd_admin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.					
File Edit View Favorites Tools Help					
🔇 Back 🔹 🐑 · 💌 😰 🏠 🔎 Search 👷 Favorites 🤣 😥 - 😓 🔟 🔹 🛄 🍇					
Address 🕘 https://192.168.0.37/csd_	admin.html		💌 🛃 Go Links 🎾		
Google -	🖌 🖸 Search 🔹	🥝 😻 🚰 18 blocked 🤎 Check 🔹 🛝 AutoLink 🕘 🗐 AutoFil 🔤 Option	s Ø		
WebVP	N CSD M	anager	\boxtimes		
		Virtual Context: cisco 🗸 Go			
SECURE DESKTOP	MANAGER for W	VEBVPN	Release Notes Help		
A Settings Modified Save	VPN Feature P	olicy under Windows Installations			
A Secure Desiton Manager	Web Browsing:	ON if orkeria are matched			
Windows Location Settings					
- S VPN Feature Policy					
- 🚍 Keystroke Logger	File Access:	ON if orkeria are matched			
Secure Desktop General					
Secure Desktop Browser	Port Forwarding:	ON if oriteria are matched 💙			
- C VPN Feature Policy					
Keystroke Logger					
-Eg Secure Desktop General	Ful Tunneling:	ON if orkeria are matched			
- B Secure Desktop Settings					
E 💮 Insecure		R			
Keystroke Logger		*			
- Cache Cleaner - Eg Secure Desktop General					
- B Secure Desktop Settings					
- 🗐 Windows CE					
Turner & Unice Cache Obaner Turner & Upload/Download Settings					
🛃 Done			S Internet		

3. For Web Browsing, click the ellipsis button and choose the criteria that must match. Click **OK** in the dialog box.



4. You can configure the other access methods in a similar fashion.

- a. Under Home, choose Keystroke Logger.
- b. Place a check mark next to Check for keystroke loggers.
- c. When prompted, click Save, and click OK.

https://192.168.0.37/csd_a	dmin.html - Microsof	t Internet Explorer provided by Cisco Systems, Inc.	_ D
File Edit View Favorites Tools	i Help		A.
🔇 Back • 🕥 · 💌 🖉	🏠 🔎 Search 🤺	Favorites 🤣 🔗 🍓 🗹 • 🧾 🎇 🦓	
Address 💩 https://192.168.0.37/csd	admin.html		💌 🛃 Go Links 🎽
Google -	💌 🖸 Search 🔹 🧭) 💋 🚰 18 blocked 🤎 Check • 🌂 AutoLink 🔹 🗐 AutoFil 🛃 Options	8
Cisce Staties WebVP	N CSD Mar	nager	\boxtimes
		Virtual Context: cisco 🗸 Go	
SECURE DESKTOP	MANAGER for WEE	VPN	Release Notes Help
A Settings Modified Save	Keystroke Logger		
A Secure Decision Manager		Check for keystrake loggers	
- A Windows Location Settings		Force admin control on list of safe modules:	
E-S Office	Path of safe		
- Keystroke Logger	modules:		
-Eg Secure Desktop General			
Secure Desktop Settings			
E- Home			
VPN Feature Policy			
- Cache Cleaner			
- Ed Secure Desktop General			
- Go Secure Desktop Browser	Module path:		
- K VPN Feature Policy			
- Cache Cleaner		Add Delete	
- Secure Desktop General			
- Secure Desktop Settings			
- 📴 Windows CE			
T↓ Upload/Download Settings			
8			🙂 Internet

5. Under the Home windows location, choose **Cache Cleaner**. Leave the default settings as shown in the screen shot.



6. Under Home, choose Secure Desktop General. Check Suggest application uninstall upon Secure Desktop closing. Leave all other parameters at their default settings as shown in the screen shot.



7. For Secure Desktop Settings under Home, choose Allow e-mail applications to work transparently. When prompted, click Save, and click OK.

https://192.168.0.37/csd_a	dmin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.	_ 🗆 🔀		
File Edit View Favorites Tools Help 🧗				
🚱 Back • 🐑 · 💌 🖻 🏠 🔎 Search 👷 Favorites 🤣 🔗 - چ 🔟 • 🧫 🏭 🍇				
Address 🕘 https://192.168.0.37/csd_	admin.html	👻 🛃 Go Links 🎾		
Google +	💌 💽 Search 🔹 🥝 🥩 🚰 18 blocked 🛛 🌴 Check 🔹 🎘 AutoLink 🕤 💮 AutoFil 🌆 Options	Ø		
WebVPN CSD Manager				
	Virtual Context: cisco 👻 Go			
SECURE DESKTOP	MANAGER for WEBVPN	Release Notes Help		
A Settings Modified Save	Secure Desktop Settings			
A Secure Desiton Manager	Put Secure Desktop in restricted mode (only browser can be launched)			
- 🚮 Windows Location Settings	Restrict network folder and drive access on Secure Desktop			
□-③ Office 爲 VPN Feature Policy	Restrict removable drive access on Secure Desktop			
Keystroke Logger	Restrict registry tools on Secure Desitop			
-Eg Secure Desktop General	Restrict DOS-CMD tools on Secure Desktop			
- Secure Desktop Settings	Restrict Printing on Secure Desktop			
E- Home	Do not encrypt files on network drives			
- Keystroke Logger	Do not encrypt files on removable drives			
- Cache Cleaner	Allow e-mail applications to work transparently			
Secure Desktop Settings	hê l			
니 Gg Secure Desktop Browser				
- 17 VPN Feature Policy				
Carbo Caster				
- Secure Desktop General				
- Secure Desktop Settings				
- Windows CE				
- C Mac & Linux Cache Cleaner				
- IA chosticovinger serings				
8		😨 Internet		

- 8. The configuration of **Secure Desktop Browser** is dependent upon whether or not you want these users to access a company website with preconfigured favorites.
 - a. Under Insecure, choose VPN Feature Policy.
 - b. Because these are not trusted users, allow only web browsing.
 - c. Choose **ON** from the drop–down menu for **Web Browsing**.
 - d. All other access is set to **OFF**.

https://192.168.0.37/csd_a	dmin.html - Micro	soft Internet Explorer provided by C	isco Systems, Inc.		
File Edit View Favorites Tools Help				A.	
🌀 Back 🔹 🐑 🕐 💌 😰	🚱 Back • 💬 · 💌 🖻 🏠 🔎 Search 👷 Favorites 🤣 😥 • 🥁 💹 • 🔜 🏭 🦓				
Address 🕘 https://192.168.0.37/csd	admin.html			👻 🛃 Go 🛛 Links 🎽	
Google -	🗹 🖸 Search 🔹	Ø Ø № 18 blocked * Check •	🎋 AutoLink 🕜 🗐 AutoFil 🛃 Opt	ions 🥒	
WebVP	N CSD M	anager		X	
		Virtual Context: cisco 🛩	Go		
SECURE DESKTOP	MANAGER for W	/ebVPN		Release Notes Help	
A Settings Modified Save	VPN Feature P	licy under Windows Installations			
🙆 Secure Desktop Manager	Web Browsing:	ON M			
一册 Windows Location Settings	1				
- 15 VPN Feature Policy	File Arress:	ARE V			
- Cache Geaner	THE ALLESS.				
-Eg Secure Desktop General					
- 🔂 Secure Desktop Browser	Port Forwarding:	OFF 💌			
- Keystroke Looper					
- Cache Cleaner	Ful Tunneling:	OFF ¥			
Secure Desktop Settings					
E- Secure Desitop Browser		,			
- Keystroke Logger					
- 😭 Cache Cleaner - 🖾 Secure Desitop General					
- Secure Desktop Settings					
- B Windows CE					
Mac & Linux Cache Cleaner Tupload/Download Settings					
8				Internet	

9. Check the **Check for keystroke loggers** check box.

https://192.168.0.37/csd_a	dmin.html - Microsof	t Internet Explorer provided by Cisco Systems, Inc.	
File Edit View Favorites Tools	i Help		
🕝 Back • 🐑 · 💌 🖻 🏠 🔎 Search 👷 Favorites 🤣 😥 • 🥃 🕅 • 🥃 🎎 🦓			
Address 🚵 https://192.168.0.37/csd	admin.html		💌 🛃 Go Links 🌺
Google -	🞽 🖸 Search 🔹 🥝	🕼 🥵 🎦 18 blocked 🧳 Check • 🌂 AutoLink - 🗐 AutoFil	🛃 Options 🥒
WebVP	N CSD Mar	nager	\boxtimes
		Virtual Context: cisco 🛩 Go	
SECURE DESKTOP	MANAGER for WEB	VPN	Release Notes Help
A Settings Modified Save	Keystroke Logger		
Secure Desktop Manager Content of the secure Desktop Secure Desk	Path of safe modules:	Check for keystroke loggers Force admin control on list of safe modules: Add Delete	
Done .	1		 Internet

10. Configure the Cache Cleaner for Insecure.

- a. Check the **Clean the whole cache in addition to the current session cache (IE only)** check box.
- b. Leave the other settings at their defaults.



- 11. Under Insecure, choose Secure Desktop General.
 - a. Reduce the time-out inactivity to 2 minutes.
 - b. Check the Force application uninstall upon Secure Desktop closing check box.



12. Choose Secure Desktop Settings under Insecure, and configure very restrictive settings as shown.

https://192.168.0.37/csd_ar	Imin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.		
File Edit View Favorites Tools Help 🦧			
🔇 Back • 🐑 · 😠 😰 🏠 🔎 Search 👷 Favorites 🤣 🔗 - 😓 🔟 • 🔜 🏭 🖓			
Address 截 https://192.168.0.37/csd_	adminhtml	👻 🛃 Go Links 🎾	
Google -	💌 💽 Search 🔹 🧭 🥵 18 blocked 🤎 Check 🔹 🎘 Autolink 🕤 💮 AutoFil 🛃 Options	9	
WebVP	N CSD Manager	\boxtimes	
	Virtual Context: cisco 🛩 Go		
SECURE DESKTOP	MANAGER for WEBVPN	Release Notes Help	
A Settings Modified Save	Secure Desktop Settings		
Secure Desktop Manager Secure Desktop Manager Secure Desktop General Mindows CE Mindows CE	Image: Construction of the second of the		
a		🔮 Internet 🔡	

13. Choose **Secure Desktop Browser**. In the Home Page field, enter the website to which these clients will be guided for their home page.

a https://192.168.0.37/csd_a	Imin.html - Microsoft Internet Explorer provided by Cisco Systems, Inc.			
File Edit View Favorites Tools	Help	A*		
🕝 Back • 🕑 • 💌 🖻 🏠 🔎 Search 👷 Favorites 🤣 🔗 - چ 🔟 • 🧫 🎉 🦓				
Address () https://192.168.0.37/csd	admin.html	🕑 🛃 Go Links 🎬		
Google -	🝸 💽 Search 🔹 🧭 🥵 🥵 18 blocked 🛛 🌴 Check 🔹 🎘 Autolink 👘 💮 AutoFil 🌆 Options	8		
WebVP	N CSD Manager	\boxtimes		
	Virtual Context: cisco 🖌 Go			
SECURE DESKTOP	MANAGER for WEBVPN	Release Notes Help		
A Settings Modified Save	Secure Desktop Browser			
A Secure Decitor Manager	Home Page: www.clsco.com			
- All Windows Location Settings	Customize bookmarks:			
E-G2 Office	avorites			
- E Keystroke Logger				
- Eg Secure Desktop General				
- Secure Desktop Settings				
E- A Home				
- K VPN Feature Policy				
- Cache Cleaner				
- E Secure Desktop General				
Secure Desktop Settings				
E 💮 Insecure				
-25 VPN Feature Policy				
- 🚱 Cache Cleaner	1			
- Kong Secure Desitop General	Add Bookmark Add Folder Delete Overwrite			
Secure Desktop Browser				
- 💮 Windows Ce. - 💮 Mac & Linux Cache Cleaner				
14 Upload/Download Settings				
E Done	energe her service and the service of the	Internet		

Phase II: Step 4: Configure Windows CE, Macintosh, and Linux features.

Configure the CSD features for Windows CE, Macintosh, and Linux.

1. Choose **Windows CE** under Secure Desktop Manager. Windows CE has limited VPN features. Turn **Web Browsing to ON**.



2. Choose Mac & Linux Cache Cleaner.

- a. The Macintosh and Linux Operating Systems have access only to the cache cleaner aspects of CSD. Configure them as shown in the graphic.
- b. When prompted, click Save, and click OK.



Verify

Test the CSD Operation

Test the operation of CSD by connecting to the WebVPN gateway with an SSL enabled browser at https://WebVPN_Gateway_IP Address.

Note: Remember to use the unique name of the context if you created different WebVPN contexts, for example, https://192.168.0.37/cisco.



Commands

Several **show** commands are associated with WebVPN. You can execute these commands at the command–line interface (CLI) to show statistics and other information. For detailed information about **show** commands, refer to Verifying WebVPN Configuration.

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Commands

Several **debug** commands are associated with WebVPN. For detailed information about these commands, refer to Using WebVPN Debug Commands.

Note: The use of **debug** commands can adversely impact your Cisco device. Before you use **debug** commands, refer to Important Information on Debug Commands.

For more information about clear commands, refer to Using WebVPN Clear commands.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN

Service Providers: VPN Service Architectures

Service Providers: Network Management

Virtual Private Networks: General

Related Information

- WebVPN and DMVPN Convergence Deployment Guide
- SSL VPN WebVPN
- Cisco IOS SSLVPN
- Technical Support & Documentation Cisco Systems

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Oct 10, 2006

Document ID: 70791