Cisco Cloud Web Security
AnyConnect Web Security Deployment Guide

September 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Cloud Deployment</td>
<td>1</td>
</tr>
<tr>
<td>Additional Redirect Methods</td>
<td>1</td>
</tr>
<tr>
<td>Prepare</td>
<td>2</td>
</tr>
<tr>
<td>Deploy</td>
<td>5</td>
</tr>
<tr>
<td>Configure AnyConnect Secure Mobile Client – Web Security Module</td>
<td>5</td>
</tr>
<tr>
<td>Create an AnyConnect Web Security Service Profile Using the stand-alone Profile Editor</td>
<td>5</td>
</tr>
<tr>
<td>Install AnyConnect Web Security using the web deploy method</td>
<td>12</td>
</tr>
<tr>
<td>Install AnyConnect Web Security using the pre-deploy method for PC</td>
<td>16</td>
</tr>
<tr>
<td>Install AnyConnect Web Security using the pre-deploy method for Mac</td>
<td>21</td>
</tr>
<tr>
<td>Test</td>
<td>23</td>
</tr>
<tr>
<td>Verify web redirection to the cloud</td>
<td>23</td>
</tr>
<tr>
<td>Manage and configure web filtering policy</td>
<td>23</td>
</tr>
<tr>
<td>Appendix</td>
<td>27</td>
</tr>
</tbody>
</table>
Introduction

Authenticate and redirect web traffic securely whenever the end user is off the corporate network. CWS leverages cached user credentials and directory information when they are away from the office or VPN, ensuring that exactly the same web-usage policies are applied.

This document provides directions to redirect network traffic to CWS through the AnyConnect Web Security Client.

*Note: we refer to our cloud proxies as towers. You will see the terms “proxy” and “tower” used interchangeably throughout the document.

Cloud Deployment

Deployment is divided into the following three sections

Prepare  Deploy  Test

Additional Redirect Methods

There are 4 additional redirection methods that have corresponding deployment guides. Deployment guides for each redirection methods can be found [here](#), under Technical Collateral.

<table>
<thead>
<tr>
<th><strong>Cisco Integrated Services Router (ISR G2 with CWS Connector)</strong></th>
<th>Save bandwidth, money and resources by intelligently redirecting Internet traffic from branch offices directly to the cloud to enforce security and control policies. Apply acceptable use policy to all users regardless of location.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Generation Firewall (ASA/ASAv with CWS Connector)</strong></td>
<td>Capitalize ASA investments by offloading content scanning to Cisco’s cloud through CWS. Apply acceptable use policy to the company, groups or individual users.</td>
</tr>
<tr>
<td><strong>Web Security Appliance (WSA/WSAv with CWS Connector)</strong></td>
<td>Integrate CWS and WSA to enable identity information to the cloud and extend other on-premises enterprise features to Cloud Web Security customers.</td>
</tr>
<tr>
<td><strong>Standalone Deployment</strong></td>
<td>Deploy a simple web security solution that does not require any additional hardware. Connect to Cisco’s Cloud Web Security service using existing browser settings and PAC/WPAD files.</td>
</tr>
</tbody>
</table>
Prepare

The AnyConnect Web Security client is primarily intended for protecting roaming machines, however it can also be used when the device is accessing the Internet from within the company’s internal network if no other deployment method is in place.

*Note: if there is another static deployment method to CWS from the company’s network, TND (Trusted Network Detection) must be configured for the AnyConnect Web Security client, following the steps outlined under Supplemental tutorial: TND (Trusted Network Detection) in this guide.

When the AnyConnect Web Security client is running on the company’s network, it may be necessary to adjust your Firewall settings to ensure that it can access the destinations listed below.

The client connects with the CWS cloud infrastructure via 80.254.145.118 and periodically checks the list of towers that are available. The full path for this list is http://80.254.145.118/websecurity-config-v2ip.xml. While it is rare that the list changes, the client should be able to reach this destination.

The Ingress IP addresses and ranges of CWS proxies that are used by the AnyConnect Web Security client are listed below.

Ensure that these Ingress IP’s are not blocked by your Firewall, or configure the Firewall to allow access only to specific destinations as necessary.

<table>
<thead>
<tr>
<th>Region</th>
<th>Site</th>
<th>Ingress IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>America</td>
<td>Chicago (CHI2)</td>
<td>108.171.131.128-159</td>
</tr>
<tr>
<td></td>
<td>Dallas (DAL1)</td>
<td>108.171.132.128-159</td>
</tr>
<tr>
<td></td>
<td>San Jose (SJL1)</td>
<td>108.171.135.128-159</td>
</tr>
<tr>
<td></td>
<td>Secaucus (SCS2)</td>
<td>108.171.130.128-159</td>
</tr>
<tr>
<td></td>
<td>Toronto (TOR1)</td>
<td>108.171.140.128-159 + 184.150.236.(42,50,58,66)</td>
</tr>
<tr>
<td></td>
<td>Washington (WDC1)</td>
<td>108.171.133.128-159</td>
</tr>
<tr>
<td></td>
<td>Sao Paulo (SAO2)</td>
<td>108.171.138.128-159</td>
</tr>
<tr>
<td></td>
<td>Vancouver (VAN1)</td>
<td>69.10.152.(42,50,58,66)</td>
</tr>
<tr>
<td></td>
<td>Sao Paulo (SAO1)</td>
<td>201.94.155.(42,50,58,66)</td>
</tr>
<tr>
<td>Region</td>
<td>Site</td>
<td>Ingress IPs</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APAC</td>
<td>Tokyo (TOK3)</td>
<td>108.171.142.128-159 + 122.50.127.(42,50,58,66)</td>
</tr>
<tr>
<td></td>
<td>Singapore (SIN4)</td>
<td>108.171.141.128-159 + 202.79.203.(42,50,58,66,74,82,90,98,104,106,108,110)</td>
</tr>
<tr>
<td></td>
<td>Sydney (SYD3)</td>
<td>108.171.134.128-159</td>
</tr>
<tr>
<td></td>
<td>New Zealand</td>
<td>210.55.211.61, 210.55.211.189</td>
</tr>
<tr>
<td></td>
<td>Bangalore (BAN1)</td>
<td>115.111.223.(42,50,58,66)</td>
</tr>
<tr>
<td></td>
<td>Chennai (CHE1)</td>
<td>108.171.159.(40,42,44,46)</td>
</tr>
<tr>
<td></td>
<td>Hong Kong (HKG2)</td>
<td>202.167.250.(42,50,58,66,74,82,90,98,104,106,108,110) + 108.171.143.128-159</td>
</tr>
<tr>
<td></td>
<td>Johannesburg (JOH1)</td>
<td>196.26.220.(42,50,58,66)</td>
</tr>
<tr>
<td>Europe</td>
<td>London (LON5)</td>
<td>108.171.128.128-159</td>
</tr>
<tr>
<td></td>
<td>Frankfurt (FRA2)</td>
<td>108.171.129.128-159</td>
</tr>
<tr>
<td></td>
<td>Copenhagen (COP2)</td>
<td>108.171.137.128-159 + 80.254.154.(42,50,58,66,74,82,90,98,104,106,108,110)</td>
</tr>
<tr>
<td></td>
<td>Paris (PAR2)</td>
<td>108.171.139.128-159 + 80.254.150.(42,50,58,66,74,76,78)</td>
</tr>
<tr>
<td></td>
<td>Zurich (ZUR1)</td>
<td>80.254.155.(42,50,58,66,74,82,90,98)</td>
</tr>
</tbody>
</table>

The **Egress IP’s** listed below are the CWS proxy IP addresses from where the requested website will see the requests originating.

*Note: Any websites that read the XFF header will be aware of the original public facing Egress IP address from where the user is breaking out.*
<table>
<thead>
<tr>
<th>Region</th>
<th>Site</th>
<th>Egress IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>America</td>
<td>Chicago (CHI2)</td>
<td>108.171.131.160-239</td>
</tr>
<tr>
<td></td>
<td>Dallas (DAL1)</td>
<td>108.171.132.160-239</td>
</tr>
<tr>
<td></td>
<td>San Jose (SJL1)</td>
<td>108.171.135.160-239</td>
</tr>
<tr>
<td></td>
<td>Secaucus (SCS2)</td>
<td>108.171.130.160-239</td>
</tr>
<tr>
<td></td>
<td>Toronto (TOR1)</td>
<td>108.171.140.160-239 + 184.150.236.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>Washington (WDC1)</td>
<td>108.171.133.224-239</td>
</tr>
<tr>
<td></td>
<td>Sao Paulo (SAO2)</td>
<td>108.171.138.160-239</td>
</tr>
<tr>
<td></td>
<td>Vancouver (VAN1)</td>
<td>69.10.152.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>Sao Paulo (SAO1)</td>
<td>201.94.155.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>Tokyo (TOK3)</td>
<td>108.171.142.160-239 + 122.50.127.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>Sydney (SYD3)</td>
<td>108.171.134.160-239</td>
</tr>
<tr>
<td></td>
<td>New Zealand</td>
<td>210.55.211.93, 210.55.211.221</td>
</tr>
<tr>
<td></td>
<td>Bangalore (BAN1)</td>
<td>115.111.223.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>Chennai (CHE1)</td>
<td>108.171.159.(41,43,45,47)</td>
</tr>
<tr>
<td></td>
<td>Johannesburg (JOH1)</td>
<td>196.26.220.(43,51,59,67)</td>
</tr>
<tr>
<td></td>
<td>London (LON5)</td>
<td>108.171.128.160-239</td>
</tr>
<tr>
<td></td>
<td>Frankfurt (FRA2)</td>
<td>108.171.129.160-239</td>
</tr>
<tr>
<td></td>
<td>Zurich (ZUR1)</td>
<td>80.254.155.(43,51,59,67,75,83,91,99)</td>
</tr>
</tbody>
</table>
Configure AnyConnect Secure Mobile Client – Web Security Module

This document is intended to provide an overview of the deployment process. For more detailed information and troubleshooting, please refer to the Admin Guide.

Create an AnyConnect Web Security Service Profile Using the stand-alone Profile Editor

A service profile is simply a file containing configuration settings for the AnyConnect Web Security client. This includes, but is not limited to, the ports AnyConnect Web Security will monitor for traffic, any conversations between the client and host that AnyConnect Web Security should not broker, how AnyConnect Web Security connects to scanning towers, client authentication to the Cisco Cloud Web Security service, the service password for disabling the AnyConnect Web Security service, and end-user identification for the purposes of web filtering policy and reporting.

The stand-alone service Profile Editor is an application that provides a GUI for creating and editing the service profile. This application saves the configuration settings in a clear text xml file which can be used to make changes to the service profile. It also encrypts configuration settings in a secondary WSO file used by the AnyConnect Web Security client to configure itself.

*Note: The stand-alone AnyConnect Web Security Profile Editor can be downloaded from Cisco.com or your ScanCenter portal → Admin → Download → Secure Mobility → AnyConnect Profile Editor

There are two conventions to bear in mind when using the pre-deploy or network push method. First, the service profile name must be exactly websecurity_serviceprofile. It is not case-sensitive. Second, the profile must be saved to a particular location. From the root of the installation point, you should have a profiles folder containing a web security folder. It is the web security folder in which the MSI installer expects to find the websecurity_serviceprofile.wso file. The xml version of the service profile can reside here too, but technically there is no need for it.

*Note: For security reasons, Cisco recommends the xml file be saved to a location where users do not have read access, as a service password can clearly be read from the .xml service profile.

Reference video: Create an AnyConnect Web Security Service Profile using the stand-alone Profile Editor

Be sure to have the following before you begin:

- Ingress IPs of VPN gateways if using a VPN client in split tunnel mode
- Authentication license key
- NetBIOS domain name

Step 1: Download the AnyConnect Profile Editor to the desktop of the server that will be hosting the AnyConnect Secure Mobility deployment installation files. The Profile Editor can be installed on any Windows-based machine. It does not need to be a server.

*Note: The AnyConnect Profile Editor is only available for Windows

Step 2: Run the installer. Select Custom Install. You will only need the Cisco Web Security Profile Editor. All others can be deselected.
**Step 3:** After installation is complete, launch the Web Security Profile Editor.

*Notice the Update Proxies button in the upper right. This button only appears if there are updates to the list of available AnyConnect Web Security scanning towers.

**Step 4:** Press the *Update* Proxies button to download the new tower information that will be embedded in the service profile. The AnyConnect Web Security client also does this check each time the service starts.

The default scanning tower is the scanning tower that the AnyConnect Web Security client will automatically attach to when the service starts.

**Step 5:** Select the scanning tower geographically closest to where the AnyConnect Web Security clients will be located when not roaming.

Traffic listing port by default is configured for port 80 for clear text web traffic and ports 8080 and 3128. Both of which are tower ports.

*Note: Adding port 443 for encrypted web traffic may also be a good idea even if your organization does not intend to filter or monitor port 443 traffic. Some websites may initiate conversations on port 80 but require client authentication and will forward the conversation to a webpage on port 443. If that happens and AnyConnect Web Security is not brokering port 443 traffic, the clients IP address will change. This often causes the remote host to drop the connection. To avoid this, simply add port 443.

**Step 6:** Select the *Exceptions* branch. Host exceptions are endpoints which should not be filtered. Click *Add*.

*Notice that the DNS host names can use wild cards. This method can also be used to exception an entire domain. For example, *.cisco.com.*
**Step 7:** Add these IP addresses so that AnyConnect Web Security will not attempt to filter traffic when conversation is already being forwarded to the Cisco Cloud Web Security service. Click Add. Failure to do so could result in irregularities when applying web filtering policy and in reporting.

Static exceptions should contain IP addresses and IP subnets in CIDR notation for endpoints and networks that should not be filtered.

Tower exceptions are trusted tower servers.

*Note: The RFT 1918 subnets have been included by default as these addresses are not routable across the internet. Additionally, you should add the ingress IP addresses of your VPN gateways if you are using a VPN client in split tunnel mode.

*Note: The subnets with the first octets of 224.0.0.0/4 and 240.0.0.0/4. At the time this tutorial was created, these subnets created a problem with rendering alert pages from the Cisco Cloud Web Security service. If you are having alert issues when receiving alert pages while only using your AnyConnect Web Security client, be sure to test offsite. Then remove these subnets.

*Note: The IP address 80.254.145.118 is the host AnyConnect Web Security will check in with to learn about new scanning towers and should remain in static exceptions.

**Step 8:** Select the Preferences branch. User *Controllable* is enabled by default. This option allows the end-user to toggle the next two options on this page. If User *Controllable* is disabled, then the next two options will be grayed out. They will be configured in the AnyConnect Web Security client the same way they are configured in the service profile.

*Automatic Scanning Proxy Selection* allows the AnyConnect Web Security client to automatically connect to the best performing AnyConnect Web Security scanning tower available. This can be a good option for an end-user who travels often or if one service profile is preferred when AnyConnect Web Security users are geographically dispersed. A caveat to using this option is if the end-user is between coverage zones of the local egress is backhauled to a coverage zone different from where the end-user is located geographically. This may cause web-based applications (which rely on locality) to behave unexpectedly. For instance, search results may be localized to an entirely different region.
When enabled, **Order scanning proxies by response time** will sort the list of scanning towers from best performing to worst performing in top to bottom fashion. This is a manual alternative to the aforementioned option but the end-user will only be able to select a scanning tower if the **User Controllable** option is enabled.

**Supplemental tutorial: Cloud-Hosted Configuration**

**Overview**
Cloud-Hosted configuration allows you to push later versions of the client’s configuration to the roaming clients via the Internet from ScanCenter. To enable the client to listen out for new configurations, the initial profile that you roll out to the client must have this setting activated.

**Configuration**
After initially enabling this feature in the profile, all further actions for hosting newer configurations are performed in ScanCenter. Refer to the [chapter in the ScanCenter Admin Guide](#) for full details.

Note the following points when working with hosted configuration:

1. Allow access to the Ingress IP's of the CWS towers/proxies for AnyConnect Web Security via TCP port 443 (and also port 8080 in case of deploying in plain mode). The full list of towers/proxies for AnyConnect Web Security can be found in the **Prepare** section of this guide. This is relevant for the Web Security client in general regardless to Hosted Config.

2. The client itself must also be able to access 80.254.145.118 on TCP port 80 where it fetches the list of proxy towers and keeps itself up to date. This is relevant for the Web Security client in general regardless to Hosted Config.

3. You also need to allow the AnyConnect Web Security module to make connections to Verisign over TCP port 80. On this range, clients check the certificate of revocation at [Tj.symcb.com](http); [T1.symcb.com](http) and [T2.symcb.com](http).
4. The AnyConnect client downloads its config files from the resource service through a hardcoded hostname in the AnyConnect binary. The request is made to hostedconfig.scansafe.net/ (IP: 46.255.41.2). The exchange is encrypted and over TCP port 443.

5. Ensure clients are using the same license key (company/group/user) which is associated with the Hosted Config that was defined and hosted in ScanCenter.

6. Client machines running the ACWS agent must have the Thawte Primary Root CA and Thawte SSL CA – G2 in the Trusted Root Certification Authority Store.

Supplemental tutorial: TND (Trusted Network Detection)

Overview
TND (Trusted Network Detection) is defined as part of the AnyConnect Web Security profile, via the Profile Editor. When used, the AnyConnect Web Security client will detect when the client is on a trusted network (assuming that it is already breaking out securely), and disengage from intercepting web traffic on the client.

A number of TND servers can be defined in the profile, and this is useful for clients that roam between different internal networks that are already secured.

Configuration
In the Profile Editor on the Preferences page, the admin defines all required trusted servers by their IP or FQDN, as well as the port (default = 443 which will be used if not specified).

The admin simply has to enter the IP address or FQDN of the internal-facing SSL server in the Profile Editor, and upon clicking Add, Profile Editor will communicate with the SSL server to get its certificate hash, and add it into the configuration page of Profile Editor.

For best results, the Profile Editor should be run within the internal network when defining this so it can access the internal-facing SSL server and get the hash. If this is not possible or if the hash is not extracted it can be manually exported from the SSL server or via an x509 openssl command, and then manually entered into Profile Editor (the certificate hash needs to be SHA256 hash, however the certificate itself can be of any encryption algorithm).
Note that if you are using a split-tunnel VPN, the internal-facing SSL server used for TND configuration should not be accessible via the VPN, but only when the client is connected to the network directly.

End of supplemental tutorials

**Step 9:** Select the `Authentication` branch.

**Step 10:** Enter your authentication license key in the `Proxy Authentication License Key` field. This is how the Cisco Cloud Web Security service will authenticate the AnyConnect Web Security client. An incorrect or invalid authentication license key will cause the scanning tower to drop the traffic.

![Authentication Profile](image)

**Figure 2.5**

Service Password is the password that is used to disable the AnyConnect Web Security client listening service, preventing the AnyConnect Web Security client from filtering web traffic. This password should be changed before rolling out AnyConnect Web Security in your environment.

*Note: The License Key can be generated from the ScanCenter portal

**Step 11:** Enter your NetBIOS domain name in the `Use Enterprise Domains` field. Alternatively, you may enter an asterisk in lieu of a NetBIOS domain name and AnyConnect Web Security will attempt to match the logged on username with any domain the local machine is joining to. This setting allows AnyConnect Web Security to properly report the group memberships of the logged on domain user to the Cisco Cloud Web Security service.

The `Group Include/Exclude List` can be used if you want specific groups sent to or omitted from the Cisco Cloud Web Security service. If left blank, then all groups of a logged member will be reported to the Cisco Cloud Web Security service.
Supplemental tutorial: Fail-Open / Fail-Close

On the Advanced page, the Connection Failure Policy dropdown list defines whether the Web Security agent will fail open or fail close in case it cannot communicate with any of the datacenter proxies on the list.

If you select Fail Close, then the next line becomes available to select, and that determines how the Web Security agent will behave if a captive portal is detected.

![Advanced page screenshot]

Figure 2.6

When Captive Portal is set to Fail Open, then the user will be able to access a captive portal (i.e. in a hotel or an airport) without the agent intercepting the web traffic, allowing the user to authenticate. Once the user has passed the captive portal, and is granted internet access, the agent will continue to work in fail close mode as set in the first dropdown window.

When the Connection Failure Policy is set to Fail Open, the Captive Portal setting will default to Fail Open also, and will become unavailable for changing.
End of supplemental tutorial

**Step 12:** To save the configuration, click **File**, and **Save**.

**Step 13:** Browse to the installation folder. Click the **Profiles folder** → **Web Security**. The file name should be exactly `websecurity_serviceprofile`. Note that case sensitivity does not matter.

**Step 14:** Click **Save** and **Continue**.

**Step 15:** Open **Windows Explorer** and drill down to the save location. We see the profile editor saved the configuration to a clear text `.xml` file and an encrypted WSO file.

*Note that the xml file does not need to reside in this folder, only the WSO file does. The xml file should be saved to a location users do not have read-access to so they cannot open the xml file and learn what the service password is.*

**Install AnyConnect Web Security using the web deploy method**

Cisco defines the web deploy method as an ASA pull. A client connects to the ASA, which will initiate the installation of AnyConnect Web Security. Web deployment specifically requires the AnyConnect Secure Mobility VPN client to be installed.
Reference video: [Install AnyConnect Web Security using the web-deploy method](#)

Be sure to have the following before you begin:

- ASA version required is an 8.4 or later or ASDM 6.4 or later.
- Working AnyConnect Secure Mobility VPN client
- Web Security service profile
- AnyConnect Secure Mobility web-deploy image (can be obtained from cisco.com)
- Lockdown transform (sample transforms on cisco.com)
- Workstation for testing

**Scenario 1: AnyConnect Secure Mobility VPN installed**

**Step 1:** Connect to an ASA using ASDM. Note the ASA version is 8.4 and ASDM version is 6.4. This is essential as earlier versions are not compatible with Cisco AnyConnect Web Security.

**Step 2:** Click on **Configuration**→**Remote Access VPN**.

**Step 3:** Expand **Network Client Access**. The AnyConnect Secure Mobility VPN client has already been configured on this ASA.

**Step 4:** Click on **AnyConnect Client Settings**.

*Note: The AnyConnect Secure Mobility image loaded is intended for the target OS in your environment and is the version you want to install.
Step 5: Click on AnyConnect Client Profile. Note there is an existing service profile for the VPN client configuration.

Step 6: Click on AnyConnect Connection Profiles. Note that AnyConnect Secure Mobility VPN client access has been enabled for the outside interface only.

Step 7: Edit the default connection profile or create a new one as necessary.

Step 8: Assign a VPN address pool and assign a default group policy

Step 9: Select AnyConnect Client Profile. Click Add.

Step 10: Supply a friendly name under the profile name field such as websecurity_serviceprofile. Change profile usage to Web Security.

Step 11: Under Group Policy, select the group policy which appeared under the connection profile. In this case it is Default Group Policy. Click OK.

Step 12: To configure the service policy, click Edit. See Create an AnyConnect Web Security service profile for reference. It is the same process as creating an AnyConnect Web Security service profile using the stand-alone Profile Editor.

Step 13: By simply clicking the OK button, the service profile configuration is saved in the web security service profile defined in the step 12.

Step 14: Once the web security service profile has been configured, click Apply. Click on Group Policies.

Step 15: Edit the Group Policy. In this case, it is the default policy. Under the General branch, expand More Options. Only enable the tunneling protocols that should be used. In this case, check SSL VPN Client.

Step 16: Expand Advanced and select Split Tunneling. Notice that a full tunnel configuration is used. This would be typical for a VPN client without web security.

Step 17: Break the full tunnel by configuring a split tunnel. Set the policy to Tunnel Network List Below. Click Manage.

Step 18: Under the Standard ACL tab, click Add ACL. Provide a friendly name for the ACL such as ‘Protected network.’ Click OK.
**Step 19:** Click *Add ACE*. Action should be bulleted on *Permit*. Address should be the inside network or the object representing the LAN VPN clients should have access to.

**Step 20:** Select the object. Click *Address*. Click *OK* through each of the three dialog boxes.

**Step 21:** Now click on the *AnyConnect Client* branch. Click on the drop down list for optional client Modules to download.

**Step 22:** Select *AnyConnect DART* and *AnyConnect Web Security*. Click *OK*. Under client profiles to download, click *Add*. Change profile name to the web security service profile and click *OK*.

**Step 23:** Expand the *AnyConnect Client* branch and select *Log-in Setting*. Ensure that *Do not prompt user* to choose and *Download AnyConnect Client* are bulleted. Click *OK*. Click *Apply*.

**Step 24:** To prevent end-users from disabling the AnyConnect Web Security service, lockdown mode should be applied. To achieve this, expand the *AnyConnect Customization/Localization* branch.

**Step 25:** Select *Customized Installer Transforms*. You have already downloaded a copy of simple transforms from [cisco.com](http://cisco.com) and uploaded it to the ASA. Click *Import*.

**Step 26:** Enter a friendly name in the name field. Make sure the leading character is an underscore. Example: _anyconnect-win-lockdown. This will tell the ASA to apply the transform to all AnyConnect modules. The platform should be win.

![Figure 2.12](image)

**Step 27:** Bullet the location where the lockdown transform is saved. In this case it is the ASA *Flash file system*.

**Step 28:** Click Browse *Flash*. Select the transform file. Click *OK*. Click *Import Now*. Click *OK*.

**Step 29:** Now that AnyConnect has been configured, log on to a Windows client that already has the AnyConnect VPN installed.

*Note: in this scenario, the log on does not require administrator privileges to update the AnyConnect Secure Mobility client with web security.*

**Step 30:** Connect to the ASA using the AnyConnect VPN client to initiate the installation of AnyConnect Web Security.

*Note: the AnyConnect UI may not reflect that the AnyConnect Web Security module is active.*
**Step 31:** Open Windows Services. Notice the Cisco AnyConnect Web Security Agent and the service status displays *Started*. Simply logging off and logging back on will update the AnyConnect Web Security UI to reflect that the web security client is active. Otherwise, it will update on the next reboot.

![Services.png](image)

Figure 2.13

**Scenario 2:** Log on to a machine that does not have the AnyConnect Web Security client installed. These actions can be facilitated through Microsoft Group Policy and Active Directory. Cisco recommends using these options to provide users with the cleanest and most trouble-free experience.

**Step 1:** Open a web browser and browse to the outside interface of the ASA using the HTTPS.

**Step 2:** Authenticate using whatever method has been configured for VPN client access and the installation will commence. By clicking on the AnyConnect tray icon, you can see that all components have been installed correctly.

**Step 3:** Browse to [whoami.scansafe.net](http://whoami.scansafe.net) to verify that the end user is being identified correctly. The user name should reflect the logged on user and the groups should reflect the groups of which the user is a member of.

*Note: Confirm traffic is redirecting to AnyConnect by looking for “connectorVersion: AP ACx.x.xxxxx”*

*Note: By opening Services, you can see that there are two services for AnyConnect. One specifically deals with the AnyConnect Web Security service and the other-AnyConnect Secure Mobility, controls the VPN client service.

However, the web security service is controlled by the secure mobility service. The lockdown transform can only be applied when installing or upgrading the client. Meaning that in scenario 1, even though the web security service has lockdown applied, the secure mobility service does not. In this scenario, the web security service can be disabled simply by disabling the Secure Mobility Agent.

To circumvent this problem, either perform a clean installation of the AnyConnect Web Security client as in Scenario 2, or only use Scenario 1 when upgrading to a newer client version.

**Install AnyConnect Web Security using the pre-deploy method for PC**

When you are deploying the AnyConnect Web Security client, you can either run the setup executable, a startup script via a Group Policy Object (Microsoft AD), or a software management solution. The installation script at the end of this document can be used in a Group Policy Object or with a software management solution.

This section of deploying the AnyConnect Web Security client using the pre-deploy method for PC will focus on using the script found at the end of this document in an Active Directory Group Policy Object. The use of this script or method is not mandatory, but is offered as a convenience for rolling out the AnyConnect Web Security client.
Log on to a Windows server that will host the AnyConnect Secure Mobility installation point.

Download the AnyConnect Secure Mobility Client installation files from cisco.com or from the ScanCenter portal: Admin → Downloads → Secure Mobility. The AnyConnect installation script used in this guide (AnyConnectInstallationScript.CMD) can be found at the end of the document in the Appendix.

Reference video: Install AnyConnect Web Security using the pre-deploy method for PC

**Review of AnyConnect Installation Script**

```
::: version 1.0
@echo off
setlocal
::: *** please configure these variables ***
set SOURCE=0
set LOCKDOWN=0
set HIDE_UNINSTALL=0
set LOG_PATH=%TEMP%
set LOG_NAME_PREFIX=%COMPUTERNAME%
set DELAY=0
set DELAY_TIMER=10
set UPGRADE_REBOOT_SUPPRESS=0
set FORCE_SERVICE_PROFILE=0
set SILENT=0
set VPN_DISABLE=1
set ENABLE_DETECT_LAPTOP=1
set TEST_MODE=0
```

**SOURCE**: location of the AnyConnect Secure Mobility Client Installation files. When source = 0, the script will auto-detect its location to find the AnyConnect Secure Mobility Client installation files. Note that this feature will only work if the AnyConnect Web Security installation script and AnyConnect Secure Mobility Client installation files reside in the same folder.

**LOCKDOWN**: when enabled, will prevent the AnyConnect Web Security service from being managed by any account other than the local system account. This ensures that if the local user has administrator privileges, they will not be able to disable the AnyConnect Web Security service, hardening the AnyConnect Web Security service. Though Cisco recommends enabling lockdown, it should only be done when rolling out the client in production. While in the proof of concept stage, you may find it easier to test without lockdown enabled.

**HIDE_UNINSTALL**: will remove the AnyConnect Web Security components from the Add or Remove Programs or the Programs And Features user interface, depending on the version of Windows. Once this is enabled, AnyConnect Secure Mobility clients can only be removed programmatically. Fortunately, a removal script (AnyConnectRemovalScript.CMD) is also included in the index later in this document.

**LOG_PATH**: where the AnyConnect Web Security installation logs will be saved.

**LOG_NAME_PREFIX**: a string that will be applied to the installation logs. The system variable %COMPUTERNAME% is a good candidate as the system variable %USERNAME% is not available.
during start-up script events. No user is logged on during this time. The purpose of the prefix is that if LOG_PATH contains a UNC path to a writable network share, then AnyConnect Web Security installation logs can be centralized rather than residing locally on the client’s machines. Therefore, each log file name must be unique to prevent overwriting.

DELAY- useful if installing the AnyConnect Secure Mobility client using a logon script (instead of a startup script) and wanting to perform the install after the user logs on.

DELAY_TIMER- in seconds and is only used when DELAY is enabled.

UPGRADE_REBOOT_SUPPRESS- only observed by the installation script if the script detects an upgrade event, which occurs when the AnyConnect Secure Mobility installation files on the network are a greater version than the files on the end-point.

When the AnyConnect Secure Mobility client is upgraded, the service will be stopped and the client cannot be restarted until the local machine is rebooted. To prevent an automatic reboot, enable this option.

*Note: Windows XP is not compatible with this option and will reboot regardless.

FORCE_SERVICE_PROFILE- only observed by the installation script if the installation script detects an upgrade event.

During an upgrade, the service profile is not copied down by default. To force the network copy of a service profile to copy down during the upgrade, enable this option.

SILENT- will remove the progress bar during the installation, making the installation or upgrade completely silent.

VPN_DISABLE- enabled by default. This will prevent the AnyConnect Secure Mobility VPN client from installing along with Web Security module. If this option is enabled and the AnyConnect Secure Mobility VPN client is already installed on the end-point, the VPN client will be removed. Disable this option to allow the AnyConnect Secure Mobility VPN client to be installed/Upgraded.

ENABLE_DETECT_LAPTOP- when enabled the installation script will ask the local machine if it is a laptop or portable computer. If the end-point is then the AnyConnect Secure Mobility client will be installed, the script will terminate without installing AnyConnect.

In order to use this option there are two additional scripts that should reside in the same folder as the AnyConnect installation script, they are getchassistype.vbs and detectlaptop.vbs. These scripts can also be found in the appendix at the end of this guide.

getchassistype.vbs is a tool that will display the kind of computer the local machine thinks it is, when run on a Windows computer. If you are having issues with the DETECT_LAPTOP option, then use this tool to determine what the chassis type is. Update the detectlaptop.vbs script to enable or disable the different chassis type that should receive the AnyConnect Web Security client.

The purpose behind DETECT_LAPTOP is to make deployment easier. When this option is enabled administrators do not need to determine which computer objects in Active Directory are laptops and which are desktops/servers.
*Note: if DETECT_LAPTOP is disabled (i.e. DETECT_LAPTOP=0) Then the getchassistype.vbs and detectlaptop.vbs scripts are not required.

TEST_MODE- when enabled and run from a command line, the installation script will print what options are enabled and what mode the script will run in. This can be a good place to start troubleshooting if the installation does not occur. Note that when this option is enabled, the installation script will not install the AnyConnect Web Security client.

For the purpose of this example and most proof of concepts, the default values of these options will suffice.

**Step 1:** Open Group Policy Manager and create a Group Policy object to deploy the AnyConnect Web Security Client. If you would like to simply get the AnyConnect Web Security client installed on a workstation to start testing the client itself, log on to the testing system as administrator and run the installation script.

**Step 2:** Right click on the Group Policy Objects folder and select View. Provide a friendly name for this Group Policy object, such as AnyConnect Web Security.

**Step 3:** Select the newly created Group Policy object. Notice that the Group Policy object is not yet linked to an OU or Domain Object, and the security filter is set to its default group Authenticated Users.

**Step 4:** Right click on the Group Policy object and select Edit. Drill down into Computer Configuration→Windows Settings→Scripts→Startup.

**Step 5:** Click Add. Click Browse.

**Step 6:** To get the UNC path, go through My Network Places→Entire Network→Microsoft Windows Network. Choose the domain and select the computer hosting the AnyConnect Web Security installation point.

**Step 7:** Continue to browse through the installation point and select the installation script. Notice that the path is in UNC format and is pointing to the installation script.
*Note that if you are using Windows 2008, go through the network or the host named in the search bar. Click Ok and Ok again.

**Step 8:** Drill down into *Administrative Templates under Computer Settings → System → Logon* and enable *Always wait for the network at computer startup and logon*. This will ensure that all Windows services that are required for AnyConnect Web Security to properly install will be started. Otherwise, the installation of AnyConnect Web Security may fail.

![Image](image1.png)

*Note that if delay is enabled in the installation script, then this group policy setting is not required, though it will still ensure that all necessary services are present for the installation. Consider giving about 5-10 minutes of delay to ensure the end-user has logged on to the computer before the installation commences if this group policy setting is not enabled.

**Step 9:** Right click the *Domain Object*. Select *Link an existing GPO*, then the AnyConnect Web Security Group Policy Object. Click Ok. If preferred, the Group Policy Object may be linked instead to an OU that contains computer objects to receive AnyConnect Web Security.

![Image](image2.png)

**Step 10:** Power-on or reboot a client laptop connected to the production network to get Group Policy and run the start-up script. Note that the event that causes a startup script to launch is power-on or reboot. A simple log off and log in will not cause the startup script to launch.

**Step 11:** Click on the AnyConnect tray icon. Make sure that you have a green check and the name of the tower that AnyConnect Web Security has attached to. If you do not, then contact Cisco Support or your Service Delivery Manager for troubleshooting assistance.
Step 12: To verify AnyConnect Web Security has correctly identified the logged on user, browse to whoami.scansafe.net. Note the user name and group memberships.

Install AnyConnect Web Security using the pre-deploy method for Mac
Cisco defines the pre-deploy method as a “network push.” However, in this tutorial, we will be installing AnyConnect Web Security locally. This will demonstrate how to configure an AnyConnect disk image before deployment. Once the disk image is configured, a software management solution may be used to push AnyConnect Web Security to an OS X client. Pre-deploy does not require the AnyConnect VPN to be installed. An administrator account is required to install AnyConnect Web Security.

Reference video: Install AnyConnect Web Security using pre-deploy for Mac

Be sure to have the following before you begin:

- AnyConnect Web Security service profile
- AnyConnect Mac pre-deploy disk image. This can be obtained from cisco.com or your Service Delivery Manager
- VPN disable service profile (VPNDisable_ServiceProfile.xml). This can be obtained from cisco.com, your Service Delivery Manager, or in the appendix at the end of this document
- MacBook

Step 1: Log on to a Mac and download the AnyConnect Web Security disk image along with the VPN disable service profile. Copy the web security service profile to the desktop.

*Note: You must configure the AnyConnect Web Security disk image before installing AnyConnect Web Security.

Step 2: Run Disk Utility. Select the disk image file. Click Convert.

Step 3: Save the name with an “rw” for re-write.
Step 4: Select a location to save the converted disk image to and change the image format to read/write. Click Save.

Step 5: Mount and open the converted disk image.

*Note: If the AnyConnect Web Security VPN client is already in use in your organization, do not disable the AnyConnect Web Security VPN client. However, if you do not use a VPN client or your VPN client of choice is something other than AnyConnect, then follow these next steps.

Step 6: Open the transforms folder, and edit the ACTransforms file in a text editor.

Step 7: Find the word false after disableVPN and change it to true. Save and close the file.

![ACTransforms.xml](image)

Step 8: Copy the VPNdisable_ServiceProfile to the VPN folder. Save and close the file.

*Note: This next step must be performed to properly install and configure AnyConnect Web Security whether you are installing the AnyConnect Web Security VPN client or not.

Step 9: Copy the Web Security service profile to the web security folder. Back out of the profiles folder to the root of the disk image.

Step 10: Run the AnyConnect Web Security meta package installer. Once installation has completed, know that AnyConnect Web Security has started, but the AnyConnect Web Security menu bar icon is not immediately present.


*Note: Make sure that the name of the tower that AnyConnect Web Security has attached to is displayed. If not, contact support or your Service Delivery Manager for troubleshooting assistance.

Step 12: To verify AnyConnect Web Security is correctly identifying the logged on user, browse to whoami.scansafe.net.

*Note that because you have logged on locally and not with the domain account, no group information shows available. However, the local login is still correctly identified.
Test

Verify web redirection to the cloud

Step 1: From a client machine, browse to whoami.scansafe.net. If a message is displayed, “User is not currently using the service,” then the traffic is not redirected to the Cisco cloud. This can be useful in determining if: the user is being resolved correctly, any groups being discovered, the internal/external IP of the user/location, and what Connector is in use.

*Note: HTTPS inspection must be enabled.

This is an example of a successful whoami.scansafe.net output:

```plaintext
authUserName: "WinNT://CISCO\user"
authenticated: true
cmpanyName: Cisco
connectorGuid: 0123456789ABCDEF0123456789ABCDEF
connectorVersion: AP_ACx.x.xxxxx
countryCode: US
externalIp: 12.34.56.78
groupNames:
  - "WinNT://CISCO\Group"
internalIp: 1.2.3.4
logicalTowerNumber: 1784
staticGroupNames:
  - "WinNT://CISCO\Group"
userName: "WinNT://CISCO\user"
```

Step 2: From a client machine, browse to policytrace.scansafe.net and enter a URL to see how the web request is processed against the current web filtering policy.

Step 3: With SearchAhead enabled in ScanCenter (the CWS admin portal), browse to Google, Bing, or Yahoo and search for something. The SearchAhead data should be prepended to each search result in the form of a green, yellow, or red dot. Mouse over the dot to see what information is contained within.

Manage and configure web filtering policy

A web filtering policy is a set of rules which define the websites users have access to. Similar to a firewall's ACL, all rules are evaluated from top to bottom and the first match wins. Therefore, only one rule will ever apply to a single web request. Rules are comprised of three criteria and an action. The three criteria are group membership, filter, and schedule. If group membership is not assigned to a rule, than it will apply to everyone by default. Only assign a group if a rule should apply to a specific set of people or computers using the Cisco Cloud Web Security service.

Reference video: Manage and configure a web filtering policy

The filter defines categories of website, content, or file types which are evaluated against the web request. The web request must match the filter for the rule to be true. The schedule defines the time of day or day of week the rule should be active. By default, the schedule is set to any time. A web request must be made within the scheduled time frame in order for the rule to be true.
To summarize:

1. All 3 criteria must be true to apply the rule’s action to the web request.
2. If any criteria are false the rule is ignored and the next rule down is evaluated.
3. The default rule, or rule of last resort, is an implicit allow.

**Step 1:** Log on to the Cisco Cloud Web Security portal at [https://scancenter.scansafe.com/](https://scancenter.scansafe.com/).

**Step 2:** From the web filtering tab, mouse over Management and select Filters.

**Step 3:** Click Create Filter sub tab. The first thing that comes up is the categories.

*Note: To gain a better understanding of each category, select the Help tab to view the online portal documentation. In the table of contents, select Web Filtering Categories→Categories. You will find a definition of each category and some examples to test.*

**Step 4:** Provide a friendly name in the filter name field.

**Step 5:** Select categories that are typically deemed inappropriate for most organizations. Once finished, click Save in the lower right corner.

![Figure 2.51](image1)

**Step 6:** Click on Domains/URLs. This page is divided into two fields- Domain URLs and Network IPs. This is where more granular configuration can be made for defining specific hosts, domains, or networks.

**Step 7:** In the domains URL field, enter a fully qualified URL such as cnn.com, host name such as online.wsj.com, and a URL such as www.bbc.co.uk/news. Click Save.

*Note: No delineation characters or wildcard characters are needed. Also, no protocol prefix is required.*

**Step 8:** If you require the ability to filter HTTP and HTTPS sites separately, check Enable HTTP/HTTPS Web Split under Web Filtering→Management→Global Settings.

![Figure 2.52](image2)

**Step 9:** Check Enable HTTP/HTTPS Split and click Save. Back at the filter, there is now two sets of categories, HTTP and HTTPS. Because of the additional management overhead, only enable this option if you absolutely require it.
**Step 10:** In the Networks/IP field, enter the address of a host such as 1.2.3.4 and click Save. Notice that a subnet mask has been applied in CIDR notation.

**Step 11:** To specify a subnet, you will have to apply a subnet mask. Click Save.

*Note that content types allow you to specify types of content on a web page. If a rule is to block content specified in its filter, it will not deny access to the web page but rather specific content will not be rendered.*

**Step 12:** Custom content can be specified in the custom filter below by entering the MIME type you wish to filter for. Each type should be on a separate line. When finished, click Save.

File types work in a similar way to content types. Filed being served on a webpage are being analyzed. Additional or custom file types can be specified in the other file extensions to block a field.

Exceptions provide a similar UI as Domains/URLs. The difference is that any web request that matches an exception will cause the rule to evaluate defaults and therefore be ignored.

For example, suppose you want to allow tobacco.org for education purposes. However, because you have selected the tobacco category, this filter will be applied to a blocked rule.

**Step 13:** Enter the fully qualified domain name of tobacco.org as a domain URL exception. Notice on the left-side margin that there are yellow exclamation marks next to file types and exceptions. These appear when changes have been made without saving.

**Step 14:** Click the Save All Settings button to save the changes made to both areas. Now you need to embed the filter in a rule. The filter will be triggered by anything in it that makes a match. If you want to achieve the AND operation, then add 2 filters to a rule (maximum of 2).

**Step 15:** Mouse over to Management and select Policy. Click the Create A Rule sub tab.

**Step 16:** Enter a friendly name in the name field. *Note: Rules and filters can share the same name, but rules cannot share the same name as other rules, just as filters cannot share the same name as other filters. This way you can match rule and filter names for easier management.*

**Step 17:** Pull down the list of rule actions. Notice that there are five possible actions that can be applied to a rule. The first two, Block and Allow, are self-explanatory. Anonymous will record the actions of a web requestor, just not their identity, while still continuing down to the next rules in order to apply policy. Warn is similar to allow, but the web requestor is presented with a customizable warning page before honoring their web request.

**Step 18:** Authenticate is used for clientless authentication based deployment models. Click on Block, because we want this to be a block rule.

**Step 19:** If you want to add a group to this rule, click Add Group. Clicking any letter of the alphabet will display what groups have been configured in the CCWS portal by their leading alpha, or simply click go to list all the groups.

**Step 20:** Pull down the add filter list and select the desired filter. In this case, we are going to select the Global Block Filter. Click Add. Notice that the schedule is set to any time.
**Step 21:** Pull down the add schedule list and see that there are two additional pre-defined schedules—*Lunch* and *Working Hours*. You may find define additional schedules or modify the times of the pre-defined schedules under *Web Filtering → Management → Schedules*. When finished, click *Create Rule*. Verify web redirection to the cloud.
Appendix

The AnyConnectInstallationScript.CMD, AnyConnectRemovalScript.CMD, GetChassisType.VBS, and DetectLaptop.VBS scripts below are examples and provided as-is. Although they are safe and known to work as intended, they are not officially supported by Cisco TAC. However, you may find support at the Cisco Support Community.

AnyConnectInstallationScript.CMD is the main script that performs the installation. AnyConnectRemovalScript.CMD is used to remove the AnyConnect client when installed with the hidden option. GetChassisType.VBS is a tool used to determine what type of form factor the endpoint is. DetectLaptop.VBS is called by the installation script when the detect laptop option is enabled. VPNDisable_ServiceProfile.XML is used on OS X machines to prevent the installation of the AnyConnect VPN client.

AnyConnectInstallationScript.CMD, GetChassisType.VBS, and DetectLaptop.VBS should be used together and reside in the same folder for proper execution.

AnyConnectInstallationScript.CMD and AnyConnectRemovalScript.CMD must reside in the same folder as the AnyConnect Security Mobility MSI files for the autodetect option to work (i.e. SOURCE=0).

Note that AnyConnectInstallationScript.CMD and AnyConnectRemovalScript.CMD are a Windows command shell scripts. GetChassisType.VBS and DetectLaptop.VBS are visual basic scripts. Please be mindful when assigning the file extensions as noted below.

To create the scripts, copy the text for each script as instructed below, paste into a simple text editor with word wrap disabled, and save the file with the proper file extension as noted in the names of each file.
AnyConnectInstallationScript.CMD

:: version 1.0
@echo off
setlocal

:: *** Please configure these variables ***
set SOURCE=0
set LOCKDOWN=0
set HIDE_UNINSTALL=0
set LOG_PATH=%TEMP%
set LOG_NAME_PREFIX=%COMPUTERNAME%
set DELAY=0
set DELAY_TIMER=10
set UPGRADE_REBOOT_SUPPRESS=0
set FORCE_SERVICE_PROFILE=0
set SILENT=0
set VPN_DISABLE=1
set ENABLE_DETECT_LAPTOP=1

set TEST_MODE=0

:: *** Do NOT change these variables! ***
set DESTINATION=%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client
set UPGRADE_TRUE=0
if %PROCESSOR_ARCHITECTURE% == x86 ( set PROGRAMDIR=%ProgramFiles% ) else ( set "PROGRAMDIR=%ProgramFiles(x86)" )
if %SOURCE% == 0 goto :setsource

:sourcelocal
for /f "delims=" %%a in ('dir /B "%SOURCE%\anyconnect-websecurity-win-*"') do @set VERSION=%%a
set VERSION=%VERSION:~27,9%
set VERSION=%VERSION:-=%
if %TEST_MODE%==1 ( echo. *** Test Mode Enabled ***
 echo. Source path=%SOURCE%
 echo. Log path=%LOG_PATH%
 echo. Log name prefix=%LOG_NAME_PREFIX%
)
echo. Source version=%VERSION%
echo. Program Files Folder=%PROGRAMDIR%
)
if %TEST_MODE%==1 (  
if %LOCKDOWN%==1 echo. Lockdown mode enabled
if %HIDE_UNINSTALL%==1 echo. Hide Uninstall mode enabled
if %VPN_DISABLE%==0 echo. VPN client enabled
if %ENABLE_DETECT_LAPTOP%==1 echo. Detect laptop enabled
)

if %ENABLE_DETECT_LAPTOP% == 1 ( "%SOURCE%/DetectLaptop.vbs"
if NOT EXIST "%temp%/GetIsLaptop.txt" goto :eof
del "%temp%/GetIsLaptop.txt"
)

if exist "%PROGRAMDIR%/Cisco\Cisco AnyConnect Secure Mobility
Client\acwebsecagent.exe" ( goto :upgrade ) else (  
if NOT exist "%DESTINATION%/Web Security" md "%DESTINATION%/Web Security"
)

:install
if %DELAY% LSS 1 goto :continue
set /A COUNTER=%DELAY_TIMER% + 1
if %TEST_MODE%==1 ( echo. Delay enabled=%DELAY_TIMER% seconds ) else ( ping 127.0.0.1 -n %COUNTER% -w 1000 > NUL
)

:continue
set DISPLAY=/passive
if %SILENT%==1 ( if %TEST_MODE%==1 echo. Silent mode enabled set DISPLAY=/quiet
)

set RESTART=/norestart
if %UPGRADE_TRUE%==1 ( if %UPGRADE_REBOOT_SUPPRESS%==0 ( set RESTART=/forcerestart
if %TEST_MODE%==1 echo. Upgrade reboot enabled
)
)

if %TEST_MODE%==0 (  

if NOT exist "%DESTINATION%\Web Security\WebSecurity_ServiceProfile.wso" copy "%SOURCE%\Profiles\websecurity\WebSecurity_ServiceProfile.wso" "%DESTINATION%\Web Security\WebSecurity_ServiceProfile.wso" /Y
)

if %TEST_MODE%==1 (echo. Installing AnyConnect...
) else (msiexec /package "%SOURCE%\anyconnect-win-%VERSION%-pre-deploy-k9.msi" /norestart
 %DISPLAY% LOCKDOWN=%LOCKDOWN% ARPSYSTEMCOMPONENT=%HIDE_UNINSTALL% PRE_DEPLOY_DISABLE_VPN=%VPN_DISABLE% /lvx*
"%LOG_PATH%\%LOG_NAME_PREFIX%_AnyConnectInstall_BASE.log"
msiexec /package "%SOURCE%\anyconnect-websecurity-win-%VERSION%-pre-deploy-k9.msi" /norestart %DISPLAY% LOCKDOWN=%LOCKDOWN% ARPSYSTEMCOMPONENT=%HIDE_UNINSTALL% /lvx*
"%LOG_PATH%\%LOG_NAME_PREFIX%_AnyConnectInstall_WS.log"
msiexec /package "%SOURCE%\anyconnect-dart-win-%VERSION%-k9.msi" %RESTART% %DISPLAY% ARPSYSTEMCOMPONENT=%HIDE_UNINSTALL% /lvx*
"%LOG_PATH%\%LOG_NAME_PREFIX%_AnyConnectInstall_DART.log"
) goto :eof

:upgrade
for /f "delims=" %%a in ('findstr "," "%DESTINATION%\update.txt"') do @set CURVER=%%a
set CURVER=%CURVER:,=.
if %TEST_MODE%==1 echo. Local version=%CURVER%

for /f "tokens=1,2,3 delims=." %%a in ("%VERSION%") do set MGRVER=%%a&set MNRVER=%%b&set BLDNUM=%%c
for /f "tokens=1,2,3 delims=." %%a in ("%CURVER%") do set LMGRVER=%%a&set LMRVER=%%b&set LBLDNUM=%%c

set TEMPBLDNUM=%BLDNUM:=0,1%
set TEMPLBDNUM=%BLDNUM:=0,1%

if %TEMPBLDNUM%==0 (set BLDNUM=%BLDNUM:=1,4%)
if %TEMPLBDNUM%==0 (set LBLDNUM=%LBLDNUM:=1,4%
else (set LBLDNUM=%LBLDNUM:=-%
)

if /i %LMGRVER% LSS %MGRVER% goto :doupgrade
if /i %LMRVER% LSS %MRVER% goto :doupgrade
if /i %LBLDNUM% LSS %BLDNUM% goto :doupgrade
goto :eof
:doupgrade
if %TEST_MODE%==1 (  
if %FORCE_SERVICE_PROFILE%==1 echo. Local service profile will be replaced with  
source version  
if %UPGRADE_REBOOT_SUPPRESS%==1 echo. Upgrade reboot suppressed  
echo. Perform upgrade  
)
set UPGRADE_TRUE=1
if %TEST_MODE%==0 (  
if %FORCE_SERVICE_PROFILE% EQU 1 copy  
"%SOURCE%\Profiles\websecurity\WebSecurity_ServiceProfile.wso" "%DESTINATION%\Web  
Security\WebSecurity_ServiceProfile.wso" /Y  
)
goto :install

:setsource
set SOURCE=%~dp0
set SOURCE=%SOURCE:~0,-1%
goto :sourcelocal

:eof
endlocal
__________________________ Stop copying above this line ________________________
AnyConnectRemovalScript.CMD

:: version 1.0
@echo off
setlocal

:: *** Please configure these variables ***
set SOURCE=0
set LOG_PATH=%TEMP%
set LOG_NAME_PREFIX=%COMPUTERNAME%
set REBOOT_DISABLE=0
set SILENT=0

:: *** Do NOT change these last two variables! ***
set DESTINATION=%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client

if %SOURCE% == 0 goto :setsourcelocal

for /f "delims=" %%a in ('dir /B "%SOURCE%\anyconnect-websecurity-win-*"') do @set

set VERSION=%%a
set VERSION=%VERSION:~27,9%
set TEMPVERSION=%VERSION:~0,1%
if %TEMPVERSION%==0 (set VERSION=%VERSION:~1,4%)
else (set VERSION=%VERSION:=-%)

if not exist "%DESTINATION%\update.txt" goto :eof

set DISPLAY=/passive
if %SILENT%==1 set DISPLAY=/quiet
set RESTART=/forcerestart
if %REBOOT_DISABLE%==1 set RESTART=/norestart

if exist "%DESTINATION%\Web Security\WebSecurity_ServiceProfile.wso" DEL /F "%DESTINATION%\Web Security\WebSecurity_ServiceProfile.wso"
msiexec /x "%SOURCE%\anyconnect-dart-win-%VERSION%-k9.msi" /norestart %DISPLAY% /lxv* ">
images/long image.png
"%LOG_PATH%\LOG_NAME_PREFIX\AnyConnectRemove_DART.log"

msiexec /x "%SOURCE%\anyconnect-websecurity-win-%VERSION%-pre-deploy-k9.msi" /norestart %DISPLAY% /lxv* "%LOG_PATH%\LOG_NAME_PREFIX\AnyConnectRemove_WS.log"

msiexec /x "%SOURCE%\anyconnect-win-%VERSION%-pre-deploy-k9.msi" %RESTART% %DISPLAY% /lxv* "%LOG_PATH%\LOG_NAME_PREFIX\AnyConnectRemove_BASE.log"
goto :eof
:setsource
set SOURCE=%~dp0
set SOURCE=%SOURCE:~0,-1%
goto :sourcelocal

:eof
Endlocal

__________________________ Stop copying above this line ___________________________
GetChassisType.VBS

Option Explicit
Dim strComputer, strChassis, objWMIService, objChassis, colChassis, objItem
strComputer = "."
Set objWMIService = GetObject(“winmgmts:" & 
"\{impersonationLevel=impersonate}!\" & 
strComputer & 
"\root\cimv2"
) 
Set colChassis = objWMIService.ExecQuery(“Select * from Win32_SystemEnclosure”,,16)
For Each objChassis in colChassis
  For Each objItem in objChassis.ChassisTypes
    Select Case objItem
      Case 1 strChassis = “Virtual Machine or Other”
      Case 2 strChassis = “Unknown”
      Case 3 strChassis = “Desktop”
      Case 4 strChassis = “Thin Desktop”
      Case 5 strChassis = “Pizza Box”
      Case 6 strChassis = “Mini Tower”
      Case 7 strChassis = “Full Tower”
      Case 8 strChassis = “Portable”
      Case 9 strChassis = “Laptop”
      Case 10 strChassis = “Notebook”
      Case 11 strChassis = “Hand Held”
      Case 12 strChassis = “Docking Station”
      Case 13 strChassis = “All in One”
      Case 14 strChassis = “Sub Notebook”
      Case 15 strChassis = “Space-Saving”
      Case 16 strChassis = “Lunch Box”
      Case 17 strChassis = “Main System Chassis”
      Case 18 strChassis = “Lunch Box”
      Case 19 strChassis = “SubChassis”
      Case 20 strChassis = “Bus Expansion Chassis”
      Case 21 strChassis = “Peripheral Chassis”
      Case 22 strChassis = “Storage Chassis”
      Case 23 strChassis = “Rack Mount Unit”
      Case 24 strChassis = “Sealed-Case PC”
    End Select
  Next
Next
WScript.Echo “Computer chassis type: “ & strChassis
WScript.Quit

_________________________________________ Stop copying above this line ___________________________________________
DetectLaptop.VBS

Option Explicit
Dim ChassisID(24)

'************************************************
'To include chassis types to receive AnyConnect,
'change the corresponding value from 0 to 1:
'************************************************

ChassisID(1) = 0 'Virtual Machine or Other
ChassisID(2) = 0 'Unknown
ChassisID(3) = 0 'Desktop
ChassisID(4) = 0 'Thin Desktop
ChassisID(5) = 0 'Pizza Box
ChassisID(6) = 0 'Mini Tower
ChassisID(7) = 0 'Full Tower
ChassisID(8) = 1 'Portable
ChassisID(9) = 1 'Laptop
ChassisID(10) = 1 'Notebook
ChassisID(11) = 0 'Hand Held
ChassisID(12) = 0 'Docking Station
ChassisID(13) = 0 'All in One
ChassisID(14) = 1 'Sub Notebook
ChassisID(15) = 0 'Space-Saving
ChassisID(16) = 0 'Lunch Box
ChassisID(17) = 0 'Main System Chassis
ChassisID(18) = 0 'Expansion Chassis
ChassisID(19) = 0 'SubChassis
ChassisID(20) = 0 'Bus Expansion Chassis
ChassisID(21) = 0 'Peripheral Chassis
ChassisID(22) = 0 'Storage Chassis
ChassisID(23) = 0 'Rack Mount Chassis
ChassisID(24) = 0 'Sealed-Case PC

'************************************************
'Do not change any code below this line!
'************************************************

Dim strComputer, strChassis, intChassisID, wshShell, objWMIService, objChassis, colChassis, objItem
strComputer = "."
Set wshShell = createobject("Wscript.Shell")
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}" & strComputer & "\" & strComputer & "\root\cimv2")
Set colChassis = objWMIService.ExecQuery("Select * from Win32_SystemEnclosure",,16)
For Each objChassis in colChassis
    For Each objItem in objChassis.ChassisTypes
        Select Case objItem
        Case 1 intChassisID = 1
        Case 2 intChassisID = 2
        Case 3 intChassisID = 3
        Case 4 intChassisID = 4
        Case 5 intChassisID = 5
        Case 6 intChassisID = 6
        Case 7 intChassisID = 7
        Case 8 intChassisID = 8
        Case 9 intChassisID = 9
        Case 10 intChassisID = 10
        Case 11 intChassisID = 11
        Case 12 intChassisID = 12
        Case 13 intChassisID = 13
        Case 14 intChassisID = 14
        Case 15 intChassisID = 15
        Case 16 intChassisID = 16
        Case 17 intChassisID = 17
        Case 18 intChassisID = 18
        Case 19 intChassisID = 19
        Case 20 intChassisID = 20
        Case 21 intChassisID = 21
        Case 22 intChassisID = 22
        Case 23 intChassisID = 23
        Case 24 intChassisID = 24
        End Select
    Next
Next

If ChassisID(intChassisID) = 1 Then
    Dim strFilePath, strText, objFile
    Set wshShell = CreateObject("WScript.Shell")
    strFilePath = wshShell.ExpandEnvironmentStrings("%TEMP%") & "\GetIsLaptop.txt"
    strText = "Laptop"
    objFile = WriteFileText(strFilePath,strText)
End If
WScript.Quit
Function WriteFileText(strFilePath, strText)
    Dim objFSO, objTextFile
    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objTextFile = objFSO.CreateTextFile(strFilePath,True)
    objTextFile.Write(strText)
    objTextFile.Close
End Function

__________________________ Stop copying above this line ______________________
VPNDisable_ServiceProfile.XML

<?xml version="1.0" encoding="utf-8"?>

<!--
Cisco AnyConnect VPN Profile -

This profile is a sample intended to allow for the disabling of VPN service for those installations that do not require VPN support.
-->

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">

<ClientInitialization>
    <ServiceDisable>true</ServiceDisable>
</ClientInitialization>

</AnyConnectProfile>