



Cisco AnyConnect Secure Mobility Client

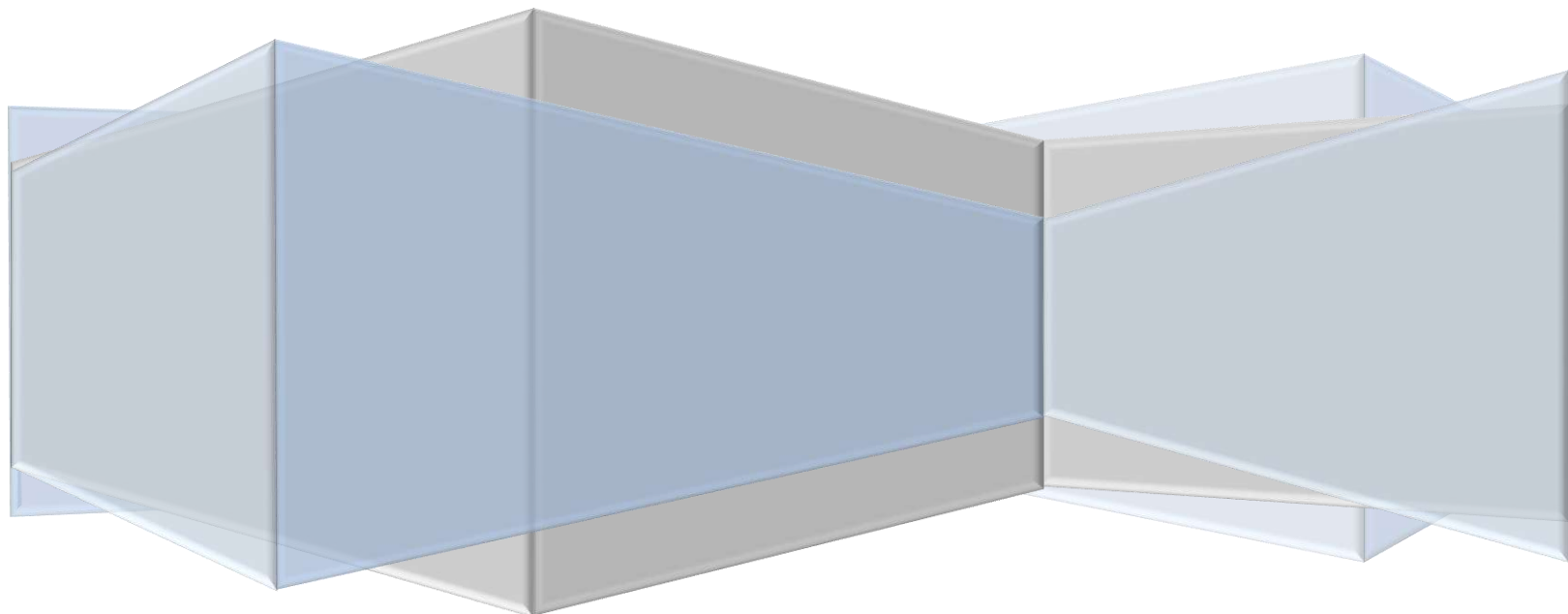


Table of Contents

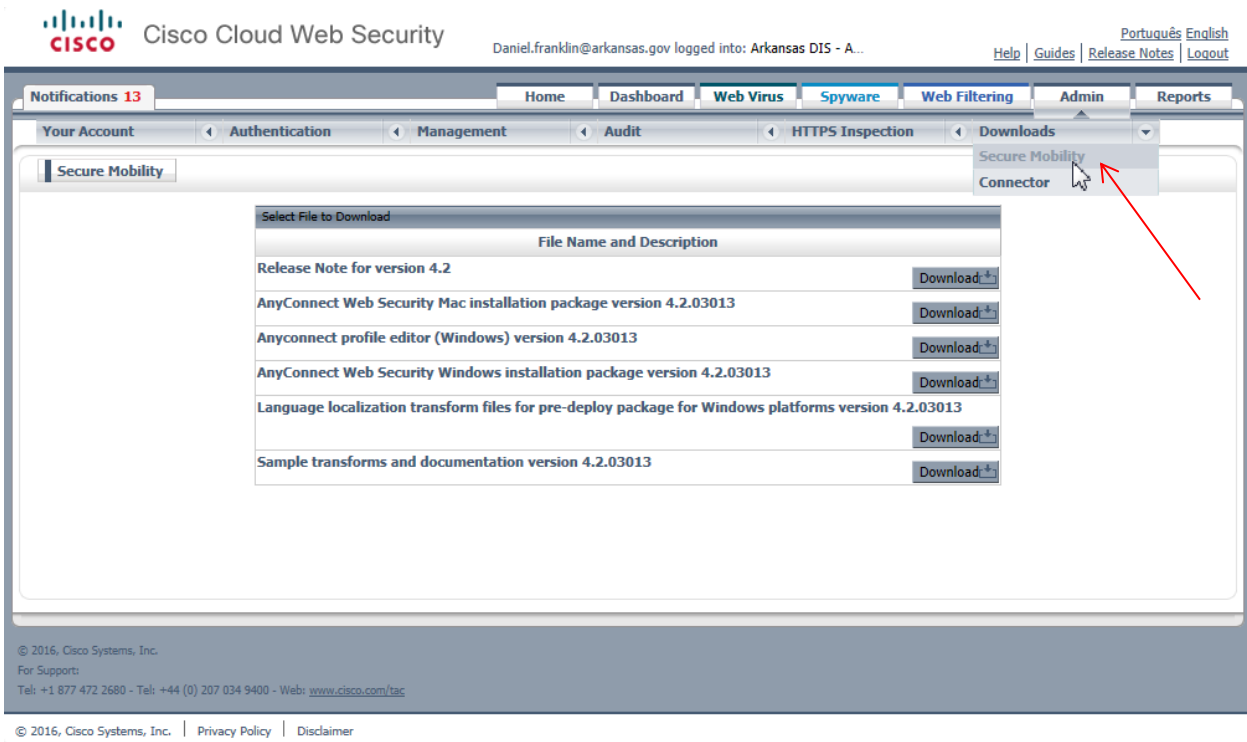
Downloading AnyConnect Secure Mobility Files	2
Creating AnyConnect Group	3
Creating Group Authentication Keys	5
Creating AnyConnect Block Filter	6
Applying AnyConnect Block filter to AnyConnect Group.....	7
Installing AnyConnect Web Security Profile Editor.....	10
Using AnyConnect Web Security Profile Editor	13
Installing AnyConnect Web Security Client.....	17

Downloading AnyConnect Secure Mobility Files

1. Login to CWS <http://scancenter.scansafe.com>



2. Click the **Admin** tab to display the administration menus.
3. Click **Downloads**, then **Secure Mobility**



4. Download Both Anyconnect profile editor (Windows) version 4.2.x AND AnyConnect Web Security Windows installation package version 4.2.x to a new Folder

The screenshot shows the Cisco Cloud Web Security interface. At the top, there is a navigation bar with tabs for Home, Dashboard, Web Virus, Spyware, Web Filtering, Admin, and Reports. Below this is a sub-navigation bar with tabs for Your Account, Authentication, Management, Audit, HTTPS Inspection, and Downloads. The main content area is titled 'Secure Mobility' and contains a 'Select File to Download' section. This section has a table with the following columns: 'File Name and Description' and 'Download'. The table lists several files, with two highlighted in blue and their download buttons pointed to by red arrows:

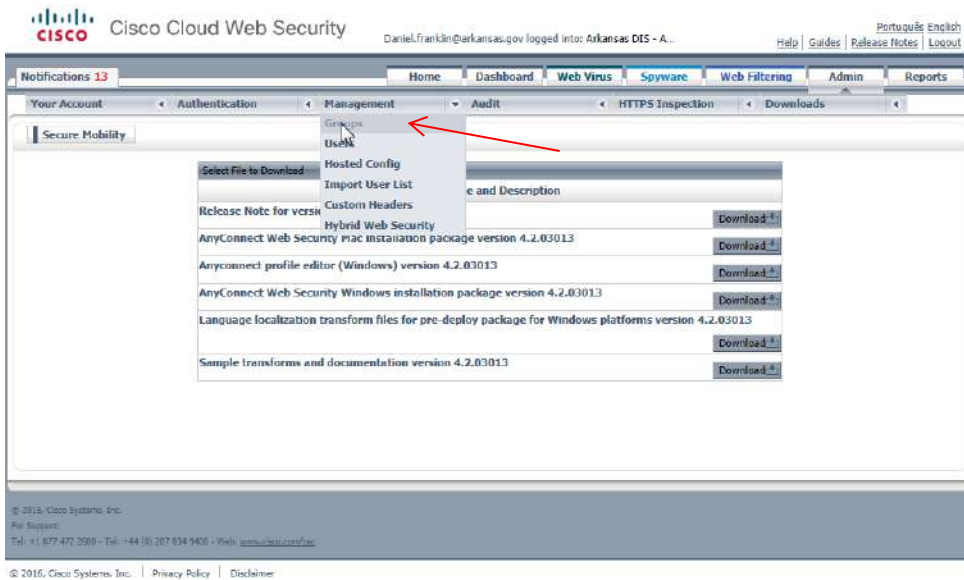
File Name and Description	Download
Release Note for version 4.2	Download
AnyConnect Web Security Mac installation package version 4.2.03013	Download
Anyconnect profile editor (Windows) version 4.2.03013	Download
AnyConnect Web Security Windows installation package version 4.2.03013	Download
Language localization transform files for pre-deploy package for Windows platforms version 4.2.03013	Download
Sample transforms and documentation version 4.2.03013	Download

At the bottom of the page, there is a footer with copyright information: © 2016, Cisco Systems, Inc. For Support: Tel: +1 877 472 2680 - Tel: +44 (0) 207 034 9400 - Web: www.cisco.com/tac. Below this is another line of footer text: © 2016, Cisco Systems, Inc. | Privacy Policy | Disclaimer.

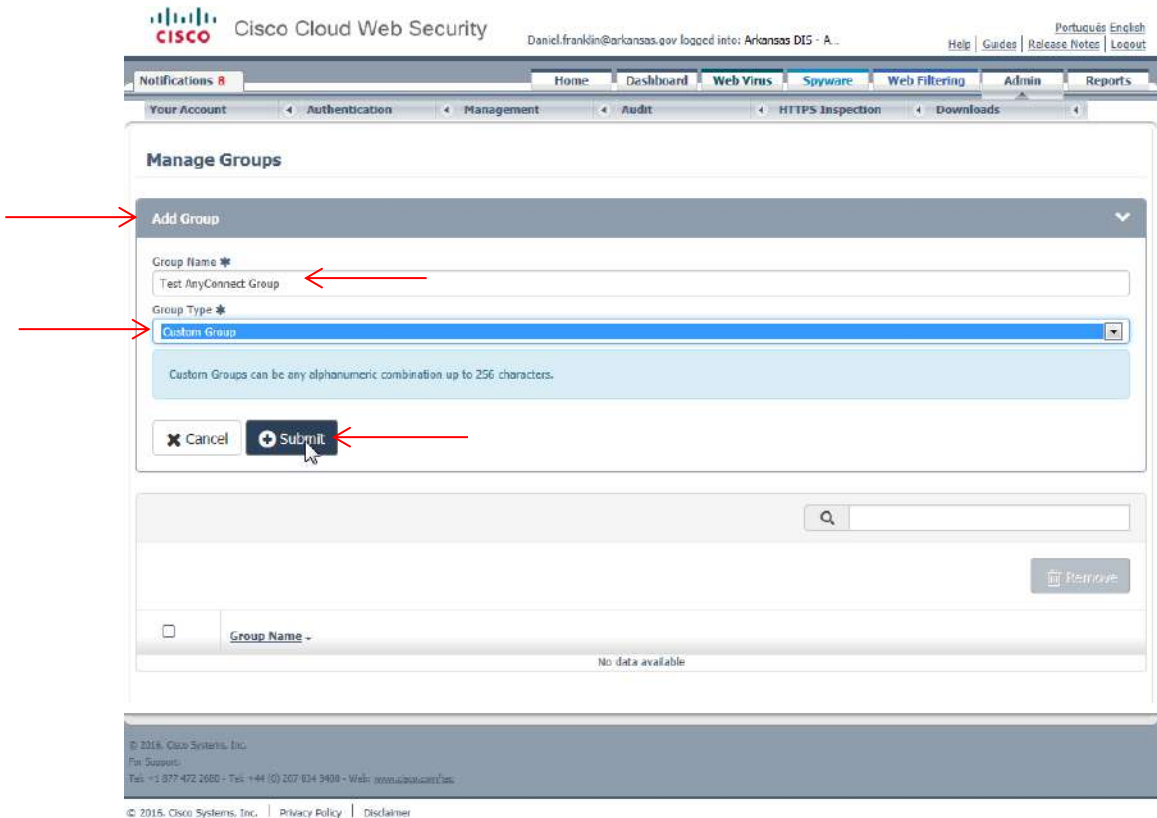
Creating AnyConnect Group

1. Click the **Admin** tab to display the administration menus.

2. In the **Management** menu, click **Groups** to display/add/edit Groups.

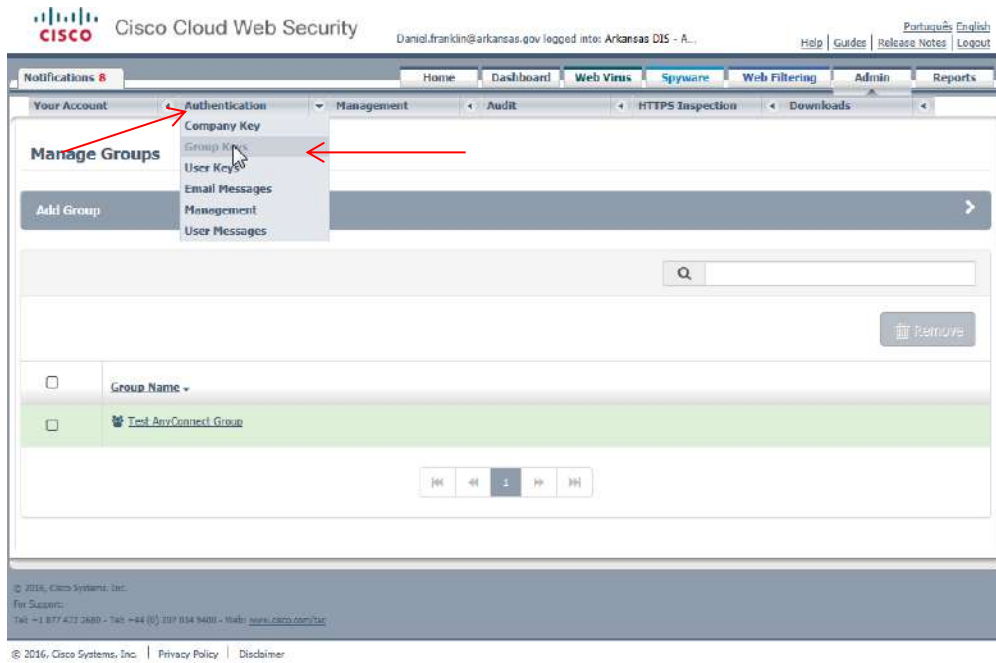


3. Click on **Add Group**, then type a Group Name.
4. For Group Type select **Custom Group**, then click **Submit**

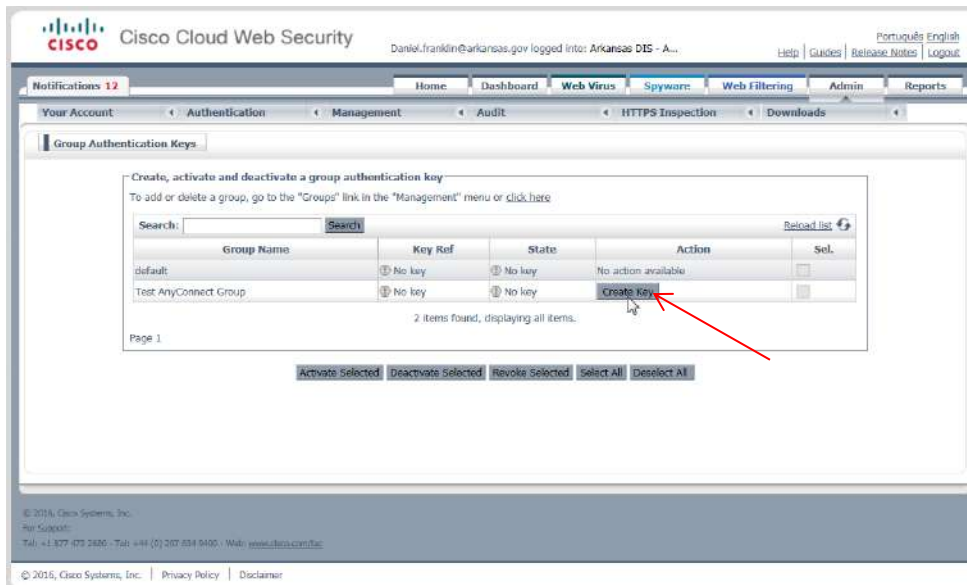


Creating Group Authentication Keys

1. Click the **Admin** tab to display the administration menus.
2. In the **Authentication** menu, click **Group Keys**.



3. Find your AnyConnect Group and click on **Create Key**



VERY IMPORTANT! SAVE THIS AUTHENTICATION KEY!

The following Authentication Keys have been created. You are advised to immediately copy these to a text file, save in a secure location, and email to the designated administrator for safe keeping. Key values are stored in an encrypted format, and it is not possible for them to be displayed again, after navigating away from this page.

Authentication Keys

The following Authentication Keys have been created. You are advised to *immediately* copy these to a text file, save in a secure location, and email to the designated administrator for safe keeping. Key values are stored in an encrypted format, and it is not possible for them to be displayed again, after navigating away from this page.

Name	Authentication Key Type	Authentication Key
Test AnyConnect Group	Group	ACECC6A6C4216BACC21966BADF80EA89

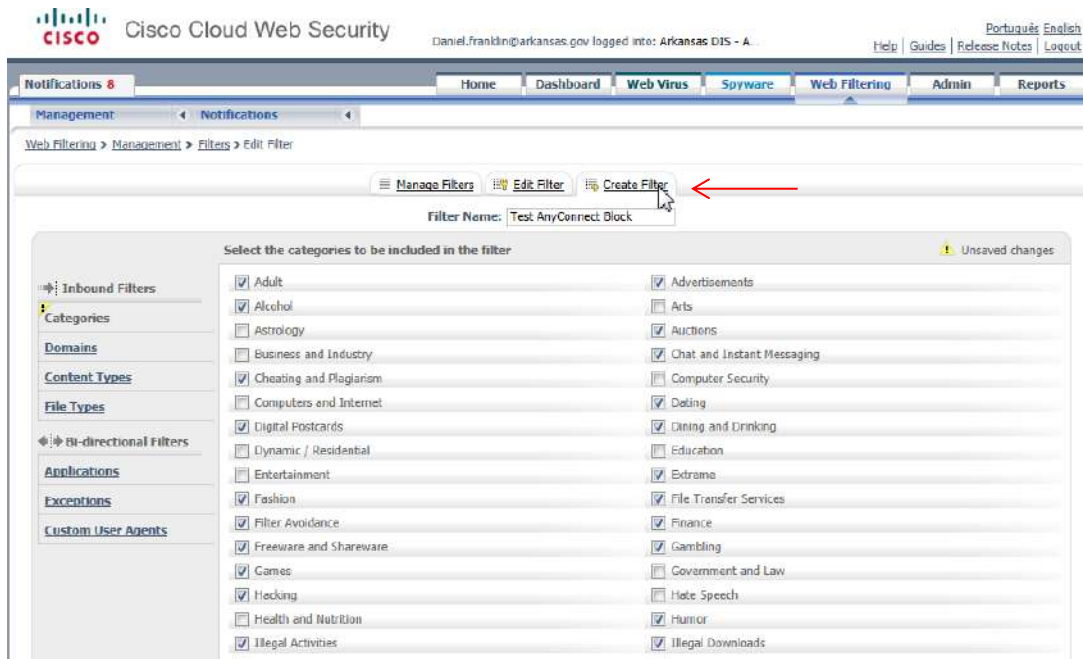
Send via email to the user x @

Creating AnyConnect Block Filter

1. Navigate to **Web Filtering > Management > Filters** to display the Manage Filters page

The screenshot shows the Cisco Cloud Web Security management console. The user is logged in as Daniel.franklin@arkansas.gov. The navigation menu is open, and the 'Filters' option is highlighted. The main content area displays the 'Manage Policy' page for a 'Company Policy'. The page includes a table with columns for '#', 'Move', 'Rules', 'Groups/Users/IPs', 'Filter', 'Schedule', 'Action', 'Active', 'Edit', 'Exceptions', and 'Delete'. The footer contains copyright information for Cisco Systems, Inc. (© 2016) and contact details for support.

2. Click on **Create Filter**, give your filter a name (IE Test AnyConnect Block)
3. Check all of the categories you want blocked
4. Click **Save** at the bottom.



Applying AnyConnect Block filter to AnyConnect Group

1. Navigate to **Web Filtering > Management > Policy** to display the Manage Policy tab.



2. Click on **Create Rule**, give it a name (IE Test AnyConnect Rule)

The screenshot shows the Cisco Cloud Web Security interface. At the top, there are navigation tabs: Home, Dashboard, Web Virus, Spyware, Web Filtering, Admin, and Reports. The current page is 'Create Rule' under 'Web Filtering > Management > Policy'. The 'Name' field contains 'Test AnyConnect Rule'. The 'Rule Action' is set to 'Block'. Below are sections for 'Define Group (\"WHO\")', 'Define Filters (\"WHAT\")', and 'Define Schedule (\"WHEN\")'. Each section has an 'Add' button. A red arrow points to the 'Create Rule' button at the top right. Another red arrow points to the 'Test AnyConnect Rule' text in the Name field. A third red arrow points to the 'Add Group' button in the Define Group section.

3. Click on **Add Group** and select your group then **Confirm Selection**

The screenshot shows a dialog box titled '2 groups of 2'. It contains a table with two rows: 'default' and 'Test AnyConnect Group'. The 'Test AnyConnect Group' row is highlighted. There are 'Select' and 'Deselect' buttons for each row. A red arrow points to the 'Deselect' button for 'Test AnyConnect Group'.

The screenshot shows a dialog box with two buttons: 'Confirm Selection' and 'Cancel'. A red arrow points to the 'Confirm Selection' button.

- Drop down **Add Filter** menu, select your AnyConnect Block Filter, then click **Add**.

Define Filters ("WHAT")
Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter	Filter	Set as Exception	Delete
Choose a filter from the list	Master - Adult Master	<input type="checkbox"/>	
Choose a filter from the list	Master - default	<input type="checkbox"/>	
Choose a filter from the list	Test AnyConnect Block	<input type="checkbox"/>	

Define Filters ("WHAT")
Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter	Filter	Set as Exception	Delete
Test AnyConnect Block	No Filter Selected	<input type="checkbox"/>	

- After all selections are complete, click **Create Rule** at the bottom.

Name **Active**

Description

Rule Action

Define Group ("WHO")
Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect. If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
Test AnyConnect Group	<input type="checkbox"/>	
Add Group	<input type="checkbox"/>	

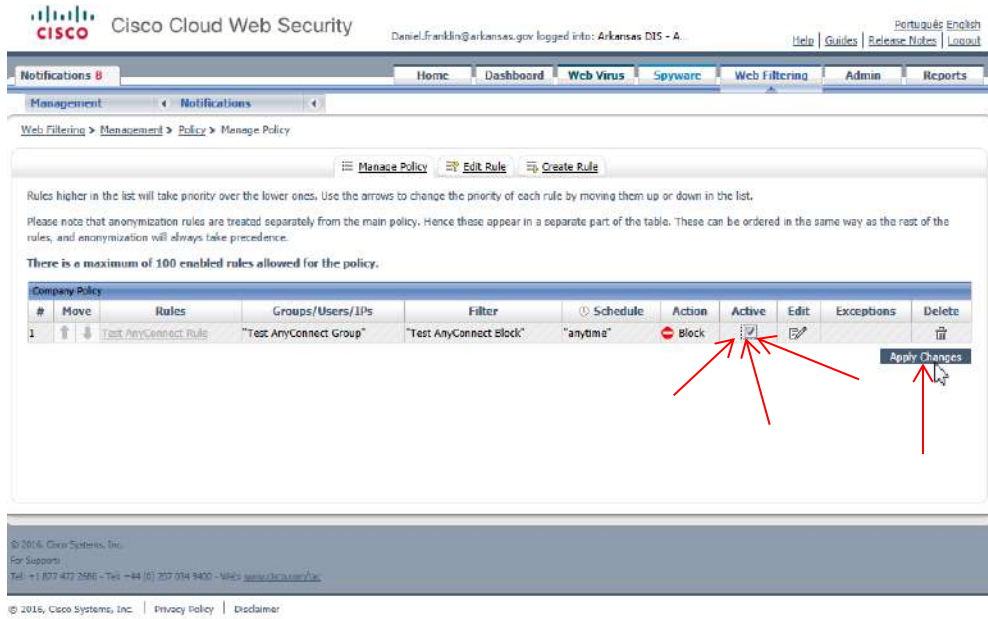
Define Filters ("WHAT")
Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter	Filter	Set as Exception	Delete
Test AnyConnect Block	Test AnyConnect Block	<input type="checkbox"/>	

Define Schedule ("WHEN")
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule	Schedule	Set as Exception	Delete
Choose a schedule from the list	anytime	<input type="checkbox"/>	

6. Check the **Active** box, then **Apply Changes**.



Installing AnyConnect Web Security Profile Editor

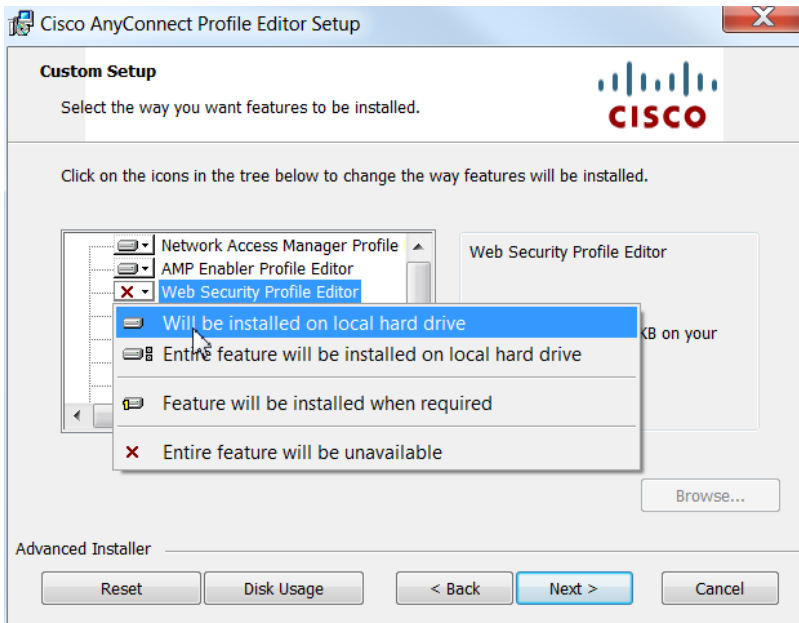
1. Open the downloaded file anyconnect-profileeditor-win-4.2.x-k9.msi



2. Select Custom



3. Click 'Web Security Profile Editor' and Select *Will be installed on local hard drive*



4. Click Install

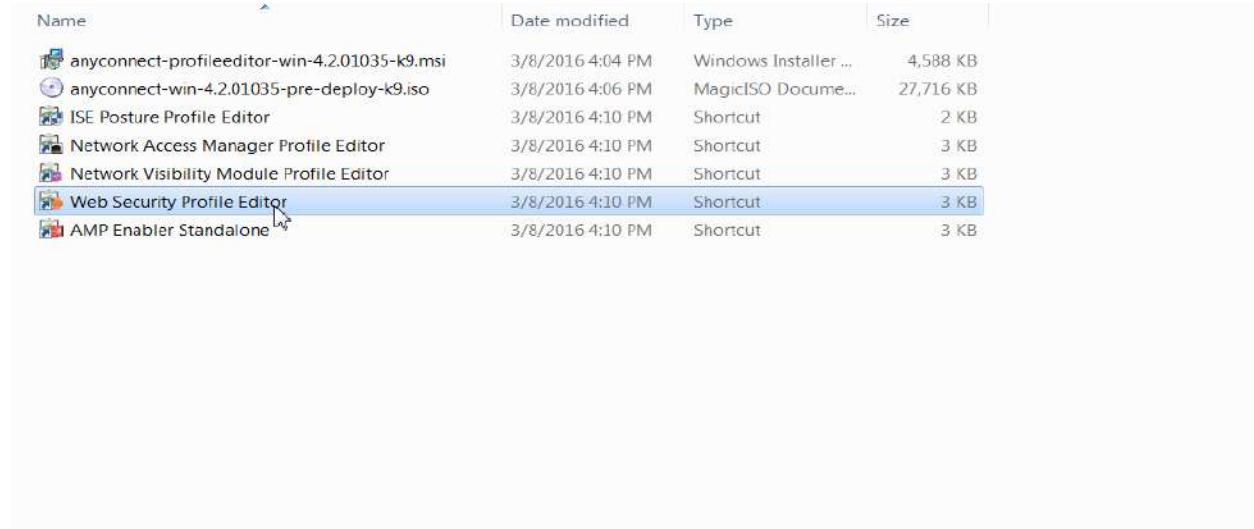


5. After Install completes, click **Finish**.

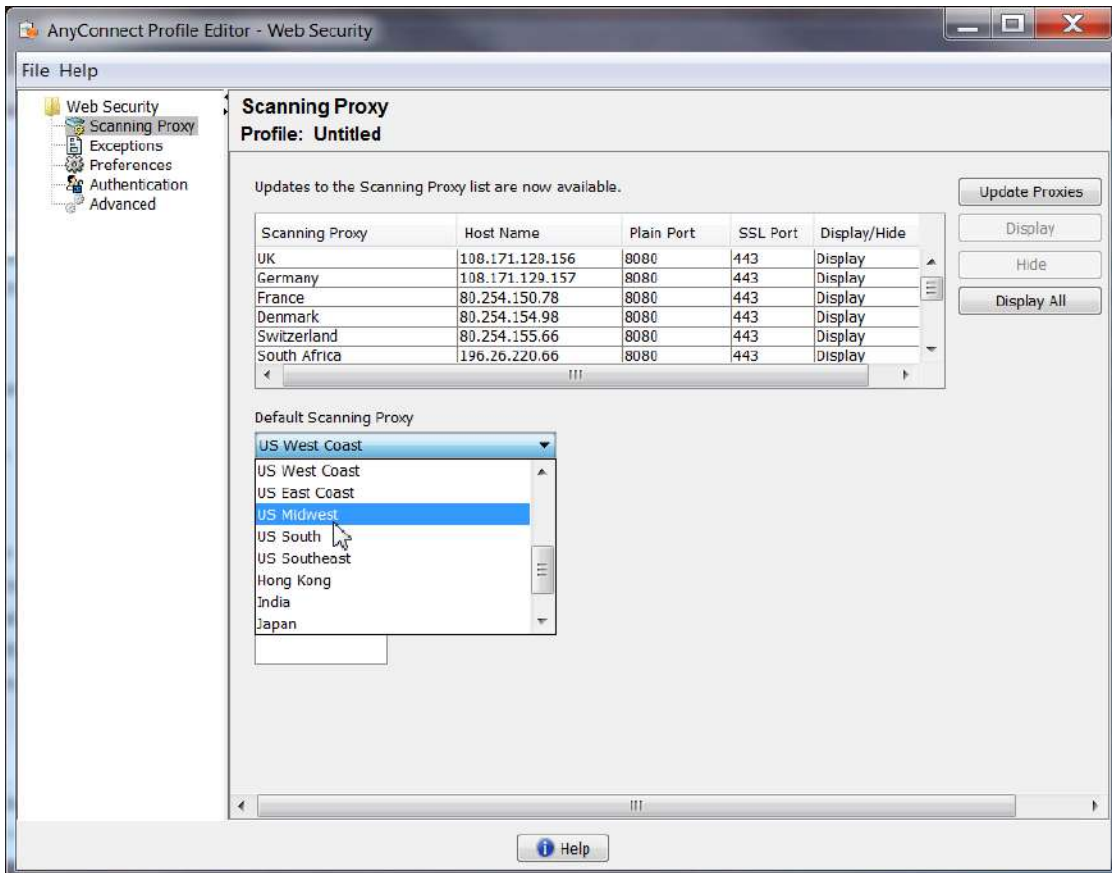


Using AnyConnect Web Security Profile Editor

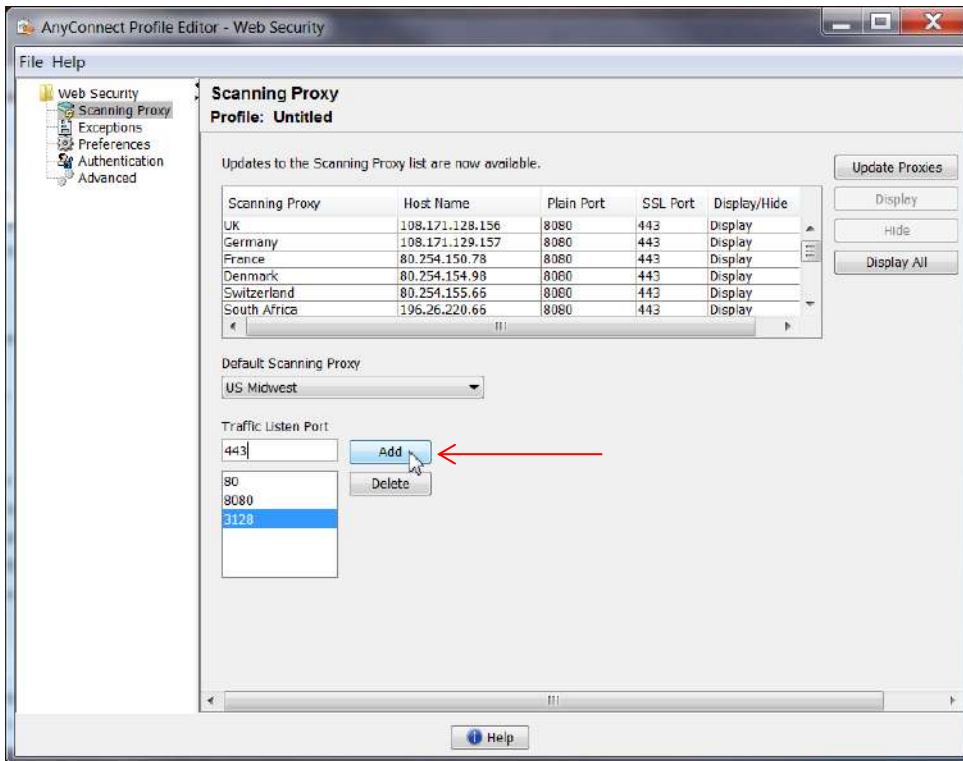
1. Open *Web Security Profile Editor*



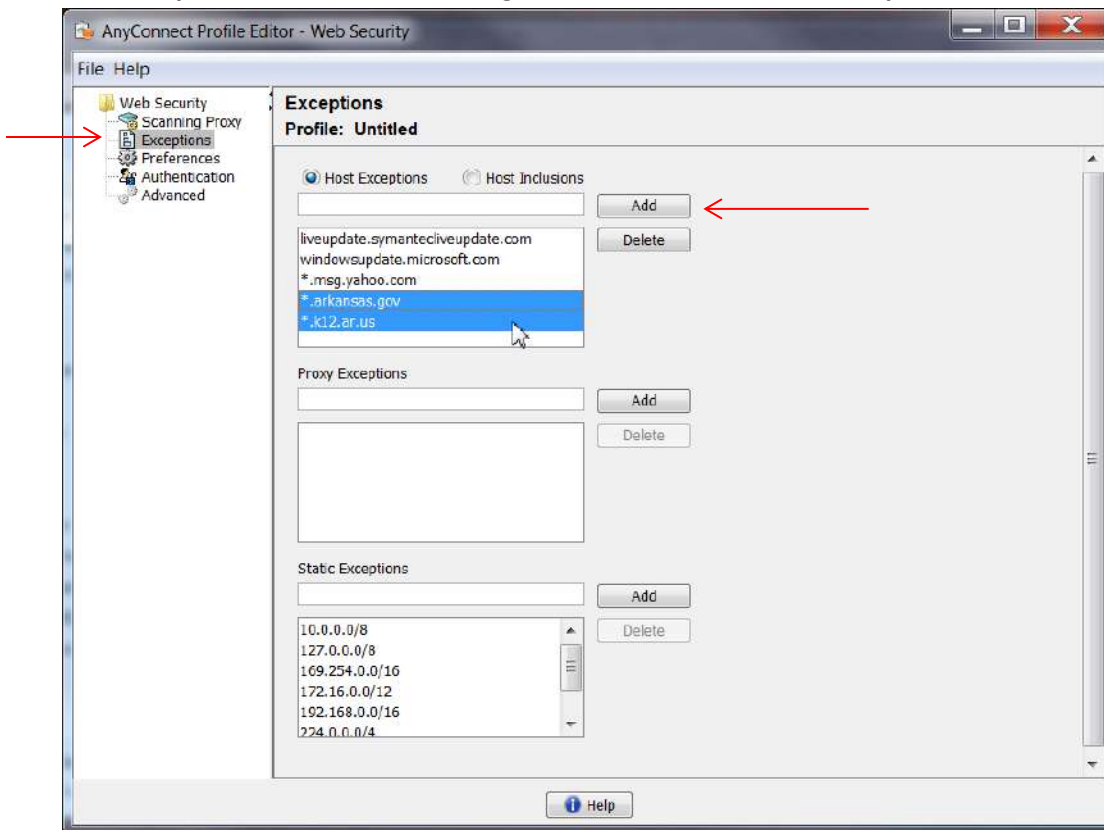
2. Change *Default Scanning Proxy* to *US Midwest*



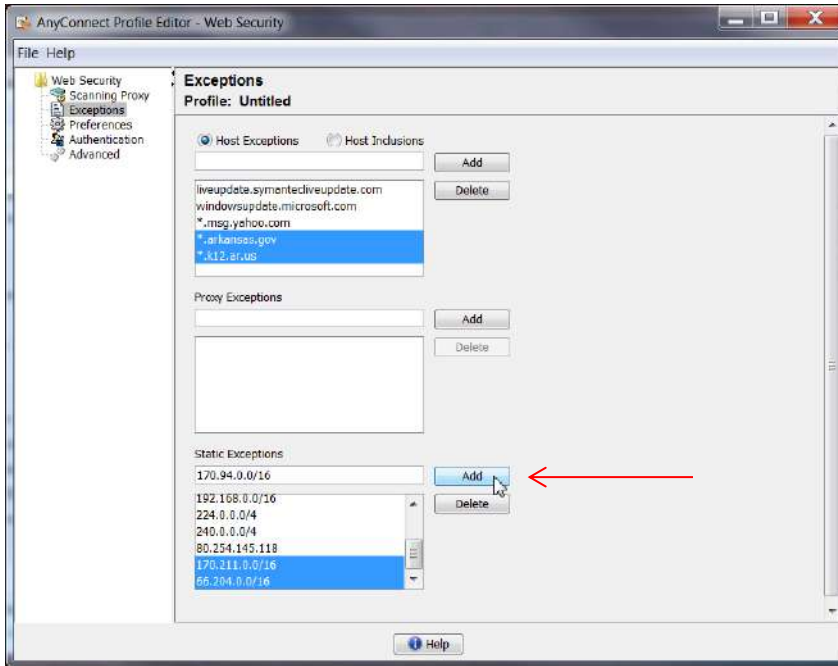
3. **Add 443 to Traffic Listen Port**



4. Click **Exceptions** and **Add *.arkansas.gov and *.k12.ar.us to Host Exceptions**

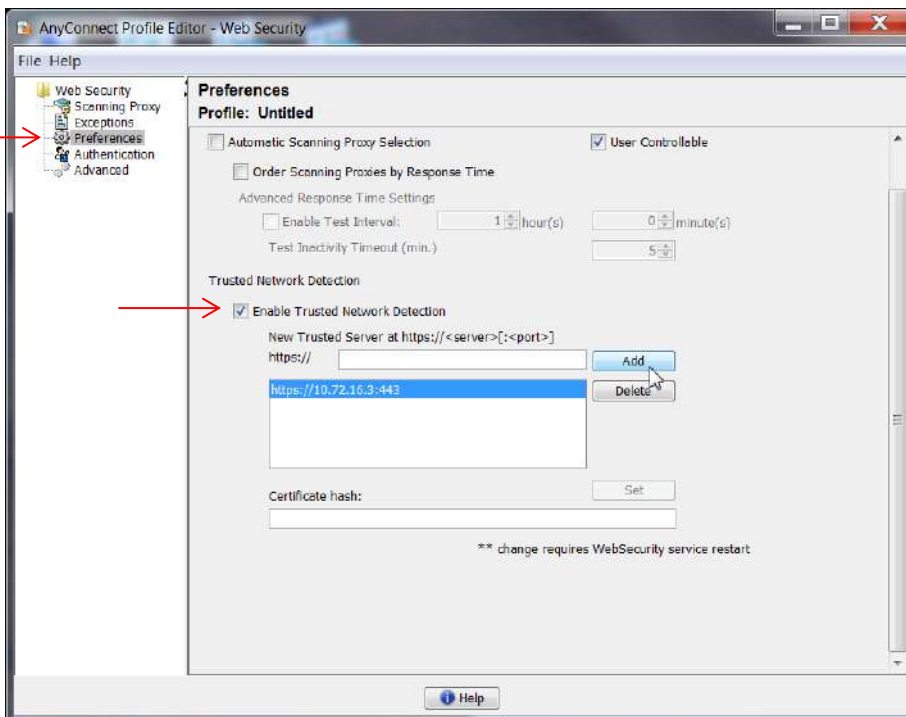


5. **Add** 170.211.0.0/16, 66.204.0.0/16, 165.29.0.0/16, and 170.94.0.0/16 to **Static Exceptions**.

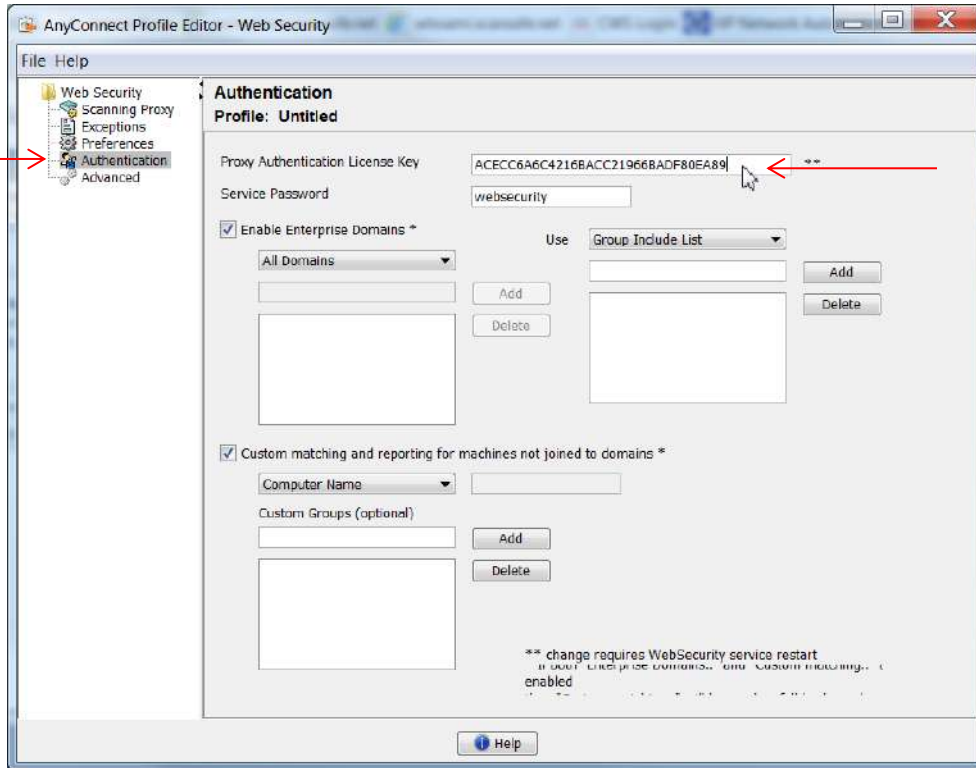


6. Click **Preferences** and **Enable Trusted Network Detection**
7. **Add** IP address of CDA (Or any **internal secure website**)

This is the trigger for AnyConnect to know if the laptop is onsite or not.



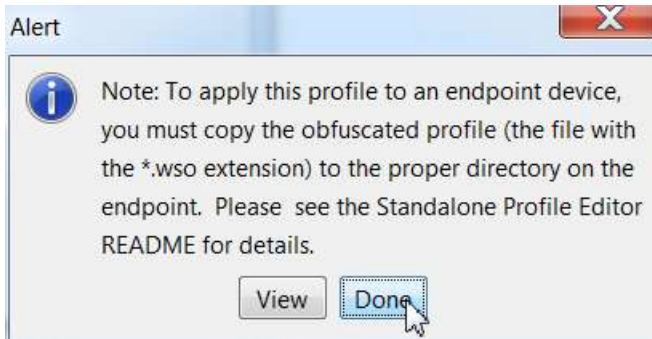
- Click **Authentication** and paste the **Group Authentication Key** you saved from your new AnyConnect Group in CWS



- Click File and Save As. Create a new folder with the AnyConnect Group Name. **Very important to save file as websecurity_serviceprofile.xml**



10. You will need the file it created with the .wso extension to copy to the client laptop after you install the AnyConnect Web Security Client

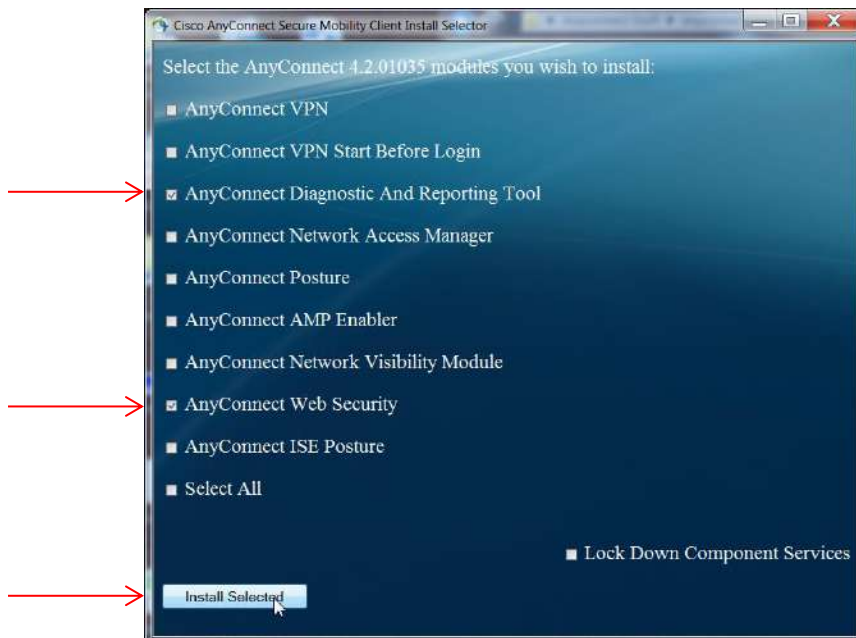


Installing AnyConnect Web Security Client

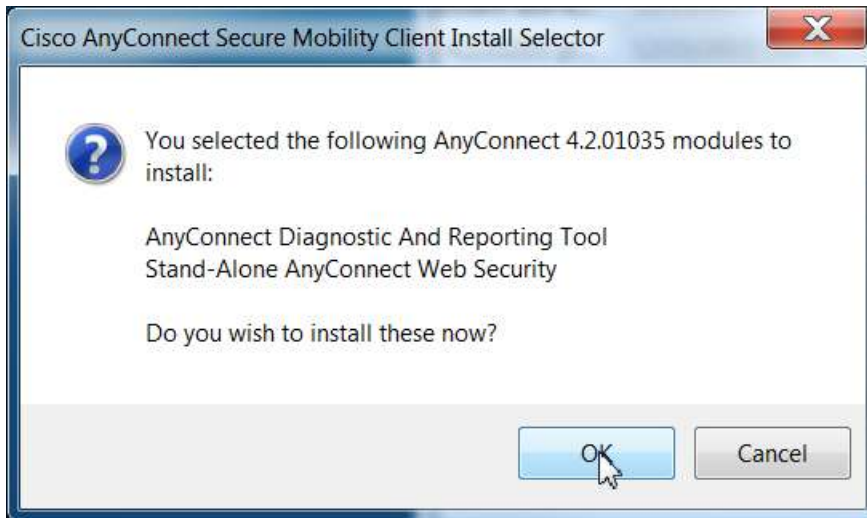
1. Burn or Extract the anyconnect-win-4.2.x-pre-deploy-k9.iso to the **client laptop** and run Setup.exe

Note: You will have to expand the screen to see all options.

2. Make sure that **ONLY** AnyConnect Diagnostic and Reporting Tool and AnyConnect Web Security are selected then click Install Selected (Optional, you can Lock Down Component Services to keep users from disabling the Secure Mobility Service)

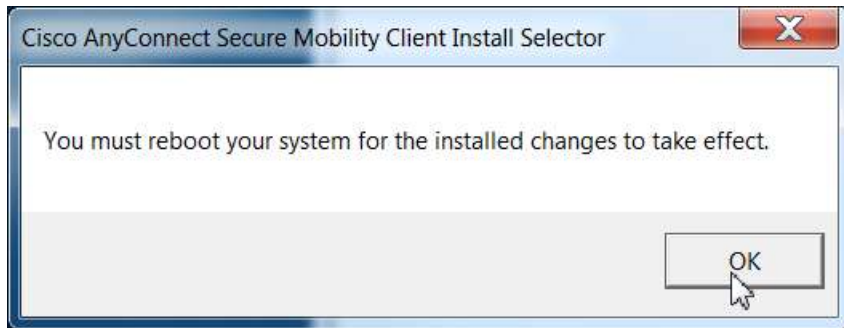


3. Click **OK** to install the 2 selected items.



4. **Accept** the EULA





VERY IMPORTANT!

Before you restart, copy the `websecurity_serviceprofile.wso` to:

`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security`

