CHAPTER 7

Configuring AnyConnect Telemetry to the WSA

The AnyConnect telemetry module for AnyConnect Secure Mobility Client sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA). The web filtering infrastructure uses this data to strengthen its web security scanning algorithms, improve the accuracy of the URL categories and web reputation database, and ultimately provide better URL filtering rules.

The AnyConnect telemetry module performs these functions:

- Monitors the arrival of content on the endpoint.
- Identifies and records the origin of any content received by the endpoint whenever possible.
- Reports detection of malicious content, and its origin to Cisco's Threat Operations Center.
- Checks the ASA every 24 hours for an updated Host Scan image. If there is an updated Host Scan image available, it pulls down the image to the endpoint.

These are the topics covered in this chapter:

System Requirements

The AnyConnect telemetry module, hereafter "telemetry module," is available for this release of AnyConnect Secure Mobility Client running on these platforms:

- Windows 7 (x86 (32-bit) and x64 (64-bit))
- Windows Vista with SP2 (x86 (32-bit) and x64 (64-bit))
- Windows XP SP3 (x86 (32-bit) and x64 (64-bit))

The telemetry module can only perform URL origin-tracing for browsers that use **wininit.dll**, such as Internet Explorer 7 and Internet Explorer 8. If you download a file using a browser which does not use **wininit.dll**, such as Firefox or Chrome, we can only identify the browser used to download the file but not the URL from which the file was downloaded.

The telemetry module requires that an antivirus application, which the AnyConnect posture module supports, be installed on the endpoint.

Note The AnyConnect posture module contains the same Host Scan image as the one delivered with CSD. The list of antivirus, antispyware, and firewall applications supported by Host Scan is the same for AnyConnect and CSD.

ASA and ASDM Requirements

The AnyConnect Secure Mobility Client with the telemetry module requires these minimum ASA components:

- ASA 8.4
- ASDM is 6.3.1

AnyConnect Secure Mobility Client Module Requirements

The telemetry module is an add-on of AnyConnect Secure Mobility Client, and it requires these modules to be installed on the endpoint in this order:

1. AnyConnect VPN Module
2. AnyConnect Posture Module
3. AnyConnect Telemetry Module

Requirements for Cisco IronPort Web Security Appliance Interoperability

You can only enable the telemetry feature if you are using the AnyConnect Secure Mobility solution with the Cisco IronPort Web Security Appliance (WSA) which requires a WSA Secure Mobility Solution license. The minimum required version of the WSA is 7.1.

The AnyConnect Telemetry functionality requires the Secure Mobility Solution to be properly configured. If you have not done so already, see the "Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution" section on page 2-46 and follow the directions to configure the ASA to work properly with the WSA.

Enable SenderBase on Cisco IronPort Web Security Appliance

The telemetry module sends virus attack incident and activity information to the WSA so that it can be forwarded to the Threat Operations Center and aggregated with other threat information. The WSA must have SenderBase network participation enabled in Standard mode for this to happen.

This is an outline of the procedure to enable the SenderBase Security Service. Consult your WSA documentation for a full description of the SenderBase Security Service.

1. Use a web browser to log into the WSA administrator GUI.

2. Select **Security Services > SenderBase.**
3. If SenderBase network participation is disabled, click **Enable**, and then click **Edit Global Settings** to configure the participation level. Cisco recommends Standard (full) participation.

Note For more information on the difference between Limited and Standard participation levels, see the *IronPort AsyncOS for Web User Guide*.

4. Submit and commit your changes.

Installing the AnyConnect Telemetry Module

You need to install the AnyConnect Secure Mobility Client and AnyConnect posture module on the endpoint before you install the telemetry module. See Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for instructions on installing the telemetry module using web-deployment and pre-deployment methods. If you would like to read just the basics about deploying the telemetry module, see Quick-Deploy of the AnyConnect Telemetry Module.

Once you install the telemetry module, it immediately begins to record the actions of any new processes that start; however, the telemetry module cannot record the actions of processes that were running on the computer before you installed it.

After you install the telemetry module, it does not track processes of Windows Explorer (explorer.exe), including file copies and renames, until the user logs out and logs back in. In addition, the telemetry module cannot record the actions of other processes that start before the user logs in until after the user reboots the computer.

Note Though it is not a requirement, we highly recommend that you reboot the endpoint after you install the telemetry module.

Quick-Deploy of the AnyConnect Telemetry Module

Here is a summary of the procedure you need to perform to deploy the telemetry module with AnyConnect. This procedure assumes that you have already configured group policies and connection profiles for your AnyConnect VPN users. To deploy the AnyConnect telemetry module, use the following procedure.

Step 1 Download the AnyConnect Windows package from Cisco.com. The file has this naming convention: anyconnect-win-<*version*>-k9.pkg.

Step 2 Upload the AnyConnect Windows package to the ASA:

a. Launch ASDM and select - **Configuration > Remote Access VPN > Network(Client) Access > AnyConnect Client Settings**.

b. Click **Add**.

c. **Upload** the AnyConnect Windows package to ASDM. When prompted, click **OK**, to use the AnyConnect package as your new current image.

d. Click **OK**. Click **Apply**.

e. Restart **ASDM**.

Step 3 Designate the AnyConnect package as the Host Scan package and enable Host Scan:

a. In ASDM select **Configuration > Remote Access VPN > Host Scan Image.**

b. Click **Browse Flash** and select the anyconnect-win-<*version*>-k9.pkg you uploaded in the previous step as the Host Scan Image.

c. Check **Enable Host Scan/CSD**.

d. Click **Apply**.

e. Restart **ASDM**.

Note This step also results in enabling Host Scan for Clientless SSL VPN Access.

Step 4 Configure a group policy to deploy telemetry as an optional module:

a. In ASDM select **Configuration > Remote Access VPN > Network(Client) Access > Group Policies**, select the group policy you want to edit and click **Edit**.

b. Select **Advanced > AnyConnect Client**.

c. Uncheck the Optional Client Modules to Download **Inherit** check box. From the drop down box, select **AnyConnect Telemetry** and **AnyConnect Posture**.

d. Click **OK**. Click **Apply**. Click **Save**.

Step 5 Configure a connection profile to specify the group policy you just configured.

a. In ASDM select **Configuration > Remote Access VPN > Network(Client) Access > AnyConnect Connection Profiles** and select the connection profile you want to configure for telemetry. Click **Edit**. The **Basic** configuration panel opens automatically.

b. In the Default Group Policy area, choose the group policy, from the previous step, that you configured to deploy telemetry.

c. Click **OK**. Click **Apply**. Click **Save**.

Step 6 Create a telemetry client profile and enable telemetry:

a. In ASDM select **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profiles**.

b. Click **Add** to create a telemetry profile. Give the profile a name and select Telemetry in the Profile Usage field.

c. In the Group Policy field, select the group policy you created to deploy telemetry as an optional module. Click **OK**.

d. From the list of Profile Names, select the telemetry client profile you just created and click **Edit**.

e. Click **Enable Service** in the Telemetry Policy panel and accept all the default values for the telemetry client profile.

f. Click **OK**. Click **Apply**. Click **Save**.

Step 7 Enable the Secure Mobility Solution:

a. In ASDM select **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution**.

b. In the Service Setup area, check **Enable Mobile User Security Service**.

c. Click **Apply**. Click **Save**.

AnyConnect Telemetry Module Interoperability

This section describes the telemetry module's interaction with other AnyConnect Secure Mobility client components:

- AnyConnect VPN Module
- AnyConnect Posture Module
- Third-Party Antivirus Software

AnyConnect VPN Module

The AnyConnect VPN module interacts with the telemetry module in these ways:

- AnyConnect's VPN service process loads and initializes the telemetry module at service starting time along with all other plug-in modules.
- The AnyConnect VPN module provides session state and AnyConnect Secure Mobility (ACSM) state information when the states have changed.
- The AnyConnect VPN module provides the XML of the secure mobility service status response from the WSA in order to get the telemetry settings from WSA.

Other than this, the telemetry module has little interaction with the VPN module and runs independently until the VPN module shuts it down or until the VPN process terminates.

AnyConnect Posture Module

The AnyConect posture module, hereafter "posture module," contains the Host Scan image. The Host Scan image passes virus detection information from the Host Scan-compatible antivirus software to the telemetry module. Host Scan can also pass system posture information to the AnyConnect telemetry module if it is needed for the telemetry report.

The telemetry module checks the ASA for an updated Host Scan image every 24 hours. If there is a an updated Host Scan image installed on the ASA, the telemetry module pulls down the image and installs the update to the endpoint automatically.

Third-Party Antivirus Software

The AnyConnect telemetry module needs a Host Scan-compliant antivirus application to detect viruses and malware. Host Scan checks the antivirus application's threat log periodically and forwards the virus detection incidents to the telemetry module.

The threat log of the antivirus application should always be enabled, otherwise Host Scan cannot trigger telemetry reporting.

Telemetry Activity History Repository

The telemetry activity history repository is a directory on the endpoint in which the telemetry module stores activity files. This is the location of the activity history repository:

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\data\

The telemetry module intercepts system operations, user operations, and API function calls, which it can use to identify the origin of the content coming into the endpoint. It aggregates this information into application activities, such as the download of a file from a URL by Internet Explorer (iexplorer.exe) or the copying of a file from a removable device by Windows Explorer (explorer.exe).

The telemetry module gathers this activity and records it in the activity.dat file. The activity.dat file is the activity history file.

When the activity.dat file reaches the size of approximately 1MB, the telemetry module saves the current activity.dat file as a new file named with the timestamp of when it was saved; for example, 20110114111312430.dat. The telemetry module then creates a new activity.dat file where it continues to store the latest activity history.

When the activity history repository reaches a certain size, the telemetry module deletes the oldest activity history files. The activity history repository size is governed by the **Maximum History Log** variable configured in the Telemetry Profile. When activity history files reach a certain age, the telemetry module deletes them from the activity history repository. Activity history file age is defined by the **Maximum History (Days)** variable configured in the Telemetry Profile. See **"Configuring the Telemetry Client Profile" section on page 7-9** for instructions on how to configure these variables.

Note The telemetry module receives its activity information from Windows functions such as winnit.dll and Kerel32.dll. If a browser or an email application does not use these functions, the telemetry module does not receive any activity data. This is why the telemetry module does not receive activity history from such browsers as Firefox and Chrome.

Note URLs stored in the activity history repository are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access. See the "URL Encryption" section on page 7-8 for more information.

Telemetry Reports

Telemetry reports contain information about viruses identified by local antivirus software and the action the antivirus software took to protect the endpoint from the virus. The telemetry module encrypts the reports and sends them to the WSA which forwards them to the Cisco Threat Operations Center (TOC). The TOC combines these reports with others and produces new URL filter and malware filter engine updates which it distributes to all WSAs.

Each telemetry report has an incident section followed by one or more activity sections. The incident section contains information about the malware, the local antivirus application, the action it took to defend against the malware, and system information about the endpoint. The activity sections contain information about the activities leading to the incident and possible origins of the virus.

When the endpoint is connected to the ASA through a virtual private network, the telemetry module sends the report to the WSA, by way of the ASA, immediately. After the telemetry module sends the reports to the WSA, it deletes the local copy.

If the endpoint is not connected to the ASA by a VPN, the telemetry module stores the reports on the endpoint here:

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\reports\

The Telemetry report filenames use the naming convention: **YYYYMMDDHHSSmmm.trt** which reflects the year, month, day, hour, minute, second, and hundredths of a second at which the report was created.

Note URLs stored in the telemetry reports are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access. See the "URL Encryption" section on page 7-8 for more information.

Possible Transference of Personal Information by Telemetry Module

The Telemetry incident reports contain the name of the malware and also the location of the malware detected on the local system. This location, the directory path, often contains the user ID of the person who downloaded the malware. For example, if Jonathan Doe downloaded "malware.txt," the directory name that could be included in the telemetry report might be "C:\Documents and Settings**jdoe**\Local Settings\Temp\Cookies**jdoe**@malware[1].txt".

Note If you agree to the Cisco End User License Agreement and install the telemetry module, you consent to Cisco's collection, use, processing and storage of personal information and non-personal information. This personal information and non-personal information is transferred to Cisco, including the transfer of such information to the United States and/or another country outside the European Economic Area, so Cisco can determine how users are interacting with our products and for the purpose of providing you technical networking support and improving our products and services. Cisco may share this information with select third parties in an anonymous aggregated form. None of this personal information and non-personal information will be used to identify or contact you, and use of the personal information and non-personal information shall be subject to Cisco's Privacy Statement, available at http://www.cisco.com/web/siteassets/legal/privacy.html. You may withdraw this consent to collection, usage, processing and storage of personal information and non-personal information at any time either by turning the telemetry module off or by uninstalling the telemetry module.

Telemetry Workflow

These steps provide an example of how the telemetry module gathers information and reports it to the WSA.

1. A user visits a web site, **http://www.unabashedevil.com**, and downloads a compressed file, **myriad_evils.zip**. The telemetry module records both activities and stores them in activity.dat.
2. Sometime later, the user extracts the content, **evil_virus.exe**, from the compressed file. The telemetry module records this activity and stores it in activity.dat.

3. A Host Scan-compliant antivirus application identifies a virus in **evil_virus.exe** and deletes the file. The antivirus application activity prompts the telemetry module to create a report on the incident.
4. The telemetry module now works backwards through the information in the activity.dat file to determine the origin of the virus. From the antivirus application incident, the telemetry module determines that **evil_virus.exe** was a virus and it was deleted by the antivirus application. From the activity.dat file, the telemetry module determines that **evil_virus.exe** was extracted from **myriad_evils.zip,** which was downloaded from **http://www.unabashedevil.com**.

   All this information is combined in a report.
5. The telemetry module forwards the telemetry report to the WSA.
   - If the endpoint is connected to the ASA through a virtual private network, the telemetry module sends the report immediately to the WSA, and it deletes the local copy of the report.
   - If the endpoint is not connected to the ASA through a VPN, the telemetry module saves the report in the report repository and sends it to the WSA at its next opportunity.
6. If the WSA enables SenderBase Network Participation, it forwards the report to the Threat Operations Center which analyzes the information along with data from other sources. The WSA receives signature updates to its URL categories and web reputation databases that have incorporated the information from multiple sources, including the telemetry data. With these new signature updates and depending on the different policies configured on the WSA, users are blocked from accessing **http://www.unabashedevil.com** and prevented from downloading **myriad_evils.zip**.

URL Encryption

URLs stored in the Activity History Repository and Telemetry Report Repository are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access.

The telemetry module treats URLs as either “internal” or “external.” An example of an internal URL might be your company’s intranet home page. An example of an external URL would be any URL that you can access on the Internet.

All domains and IP addresses configured on the WSA to be excluded from SenderBase Network Participation are defined as internal URLs by the telemetry module. If you do not exclude any domains or IP addresses from Senderbase Network Participation, the telemetry module treats all URLs as external.

Both internal and external URLs are included in the telemetry report in encrypted form and sent to the WSA.

All internal URLs specified in Telemetry reports, and in the activity history repository, are encrypted using the symmetric AES key for internal URLs. All external URLs specified in Telemetry reports, and in the activity history repository, are encrypted using the symmetric AES key for external URLs. These symmetric AES keys are randomly generated at the beginning of each VPN session or when the telemetry service starts.

The AES key used for encrypting internal URLs is encrypted with your company’s public key, and sent along with AES encrypted internal URLs in the telemetry report. You can specify your public key in the telemetry profile in the Custom Certificates area. Your public key could be any X.509 public key certificate in PEM-format provided by your company.

The AES key used for encrypting external URLs is encrypted with Cisco's public key and your company's public key. Both encrypted versions of the AES key are sent along with AES encrypted external URLs in the telemetry report. Cisco's public key is one of Cisco's public certificates and it is delivered with the telemetry module. You are not able to change Cisco's public key using the ASDM or ASA.

As a result, you can decrypt internal URLs with your company's private key. You can decrypt external URLs with Cisco's private key or your company's private key. This allows the Cisco Threat Operations Center to examine external URLs because it has Cisco's private key but it cannot decrypt your internal URLs because it does not have your company's private key.

Finally, the WSA SenderBase Participation Level determines how much of the URL gets encrypted and reported:

- **Standard.** The entire URL is encrypted with Cisco's public key and reported.
- **Limited.** The URI portion of the URL is encrypted with your private key and then the resulting URL is completely encrypted with Cisco's public key.

  For example, when telemetry reports on the URL https://www.internetdocs.example.com/Doc?docid=a1b2c3d4e5f6g7h8=en, the **Doc?docid=a1b2c3d4e5f6g7h8=en** portion is encrypted with your private key. Depending on the private key used, the resulting URL might look something like the following string:

  https://www.internetdocs.example.com/93a68d78c787d8f6sa7d09s1455623

This string is encrypted with Cisco's public key and reported. The result is that Cisco's Threat Operations Center would only be able to decrypt the domain name in the URL.

Telemetry Report Encryption

When the telemetry module is ready to send a new telemetry report to the WSA, it encrypts the report based on the configured shared secret between the endpoint, ASA, and WSA. The telemetry module then posts the encrypted report by sending a HTTP POST request to the WSA which aggregates the data and sends it to the Threat Operations Center using SenderBase Network Participation. If the POST request is successful, the telemetry module deletes the report from the local report repository.

Configuring the Telemetry Client Profile

Step 1 Open ASDM and select Configuration > Remote Access VPN > Configuration > Network (Client) Access > AnyConnect Client Profile.

Step 2 Click **Add** to create a client profile.

Step 3 Give the client profile a **name**.

Step 4 Click the **Profile Usage** field and select **Telemetry**.

Step 5 Accept the default Profile Location or click **Browse** to specify an alternate file location.

Step 6 (Optional) Select a **Group Policy** to attach the client profile or leave the client profile <Unassigned>.

Step 7 On the AnyConnect Client Profile page, select the telemetry profile you just created and click **Edit**. You can now edit your telemetry profile in the telemetry profile editor screen.

Step 8 Check the **Enable Service** checkbox to enable telemetry.

Step 9 In the **Maximum History Log (MB)** field, specify the maximum size of activity history repository.

- Range of values: 2-1,000 MB.
- Default value: 100 MB.

Step 10 In the **Maximum History (Days)** field, specify the maximum number of days to retain activity history.

- Range of values: 1-1,000 days.
- Default value: 180 days

Step 11 In the **Antivirus Check Interval (secs)** field, specify the interval at which the telemetry module prompts the posture module to check for new antivirus threat log information.

- Range of values: 5-300 seconds.
- Default value: 60 seconds

Step 12 In the **Retry Send Attempts** field, specify the number of times the telemetry module attempts to send telemetry reports to the WSA if the initial attempt fails.

- Range of values: 0-10
- Default value: 2

Step 13 In the **Administrator Defined Exceptions** field, specify an application's executable file whose behavior you want to exclude from telemetry reports. You can add the executable files in two ways:

- In the **Administration Defined Exceptions** text box, enter the file name, or the full path to the file, that you want to exclude from telemetry reporting and click **Add**. For example:

  trusted.exe

  C:\Program Files\trusted.exe

  If you specify just the file name, the behavior of that file will **not** be tracked in whatever directory it resides. If you add the full directory path and file name, the behavior of the file will **not** be tracked when it is in the directory you specify.

- Click the **Browse** button and select the local file you want to exempt from telemetry reporting. When you browse to add the file, the telemetry profile editor enters the full path to the file. The telemetry module will look for this file, at the end of this path, on all endpoints that use this telemetry profile. The path and filename must be correct for all users of this telemetry profile, not just the administrator.

  In both cases the file is listed in the **Administration Defined Exceptions** list box.

Step 14 In the **Custom Certificate Select from file** field, click **Browse** to locate a Privacy Enhanced Mail (**.pem)** type certificate to generate a profile which includes the your certificate in XML form.

Step 15 Click **OK**.

Step 16 Click **Apply**.

Configuration Profile Hierarchy

There are three client profile resources that govern telemetry behavior. The files act in an order of precedence.

Table 7-1 Telemetry Client Profile Files

File name	Location	Description and Precedence
actsettings.xml	Installed on the endpoint here: %ALLUSERSPROFILE%\Application Data \Cisco\Cisco AnyConnect Secure Mobility Client \Telemetry	File contains the base configuration for Telemetry.
telemetry_profile.tsp The name of this file is specified by the ASA administrator.	Stored on the ASA. Its location is specified on this screen: Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile	Telemetry client profile file. It is created and stored on the ASA. All elements defined in this message overwrite those in the actsettings.xml file.
Telemetry profile message sent by WSA	Not applicable. This is not a file.	There is no XML file on the WSA, but the WSA sends the message in XML format when replying to the status query request. All elements defined in this message overwrite those in the *telemetry_profile*.tsp file.