CISCO™

FireSIGHT Qualys Connector Configuration Guide

Version 1.0.1
September 29, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Using the Qualys Connector

The Qualys Connector downloads QualysGuard vulnerability reports from Qualys's cloud service, parses the data, and sends it to a Cisco Defense Center. Customers can then correlate intrusion-related vulnerabilities with QualysGuard vulnerabilities, signifying high impact events when QualysGuard identifies a host as being vulnerable to a network threat.

The Qualys Connector runs on UNIX or Linux hosts that can run Perl executables. The following steps are required to set up the Qualys Connector:

- Updates in Version 1.0.1, page 1 describes the changes made to this software since version 1.0.

- Verifying Qualys Connector Support, page 2 describes the software, license, and platform support for the Qualys Connector.

- Setting Up Your QualysGuard Account, page 2 describes what you must do in your QualysGuard account to prepare your vulnerability data to download.

- Preparing the Qualys Connector Host, page 2 describes the minimum system requirements for the host running the Qualys Connector. It also lists the steps for preparing the host so you can install the Qualys Connector.

- Installing and Configuring the Connector Software, page 4 describes how to install the Qualys Connector on the host and configure it so it will run correctly.

- Preparing the Defense Center, page 6 describes how to configure the Defense Center so it can communicate with the Qualys Connector and process QualysGuard data.

- Running the Connector, page 7 describes the steps for running the Qualys Connector so it can download QualysGuard data, process it, and send it to the Defense Center.

- Uninstalling the Qualys Connector, page 10 describes how to uninstall the Qualys Connector if you no longer need to use it.

- Troubleshooting, page 10 lists a series of steps to follow if you encounter any issues.

Updates in Version 1.0.1

The following change was made to version 1.0.1 of the Qualys Connector:

- Added support for SSL-capable web proxies. See Installing the Required Components, page 3 for the necessary Perl module and Table ii-4 on page 5 for more information on setting up proxy support.

Verifying Qualys Connector Support

The following table describes the current support for the Qualys Connector.

Table ii-1   Qualys Connector Support

FireSIGHT System Version	Supported Qualys Connector Versions	Required Licenses	Can import Qualys data to...
4.10.x	1.0+	Host	Defense Center Only
5.0+	1.0+	FireSIGHT	Defense Center Only

Setting Up Your QualysGuard Account

If you want to import QualysGuard vulnerability data into a Defense Center, you must have access to a valid QualysGuard account and its vulnerability reports. You do not need to be an administrator, but you must be able to view and download reports.

See the following sections for more information:

Creating or Identifying a QualysGuard Report Template

Log into your QualysGuard account and identify a report template you want to work with. Report templates specify parameters for a vulnerability report, such as the subnets or asset groups for the data you are interested in. If you want to learn more about report templates and creating or configuring them, consult the Qualys documentation or work with your Qualys administrator.

Initially, you may want to use a template containing a small number of hosts. Work with your Qualys administrator to figure out how many hosts are in each template. The Asset Search feature in the Qualys GUI gives you information on the size of each asset group.

Obtaining a QualysGuard Report Template ID

After you identify a report template, you need its ID. To get the ID, log into your QualysGuard account and select **Report Templates** on the lower left, in the **Tools** section. Put your pointer on the Info button of the template you are interested in. Review the URL in the status bar of the browser. The URL will look something like this:

```
https://qualsguard.qualys.com/fo/common/template_info.php?id=424242&refresh_parent=1
```
The template ID is the number after `id=` in the URL. In this example, the ID is `424242`.

Preparing the Qualys Connector Host

Find an appropriate host to run the Qualys Connector on. See the following sections for more information:

System Requirements

These are the minimum requirements for the Connector host:

- Dual core processor running at 2.4 GHz
- 2 GB RAM
- Linux or UNIX operating system
- Perl installed

If you are importing Qualys reports with a large number of hosts, it is recommended that you add more memory. A 2GB host should be able to process data for up to 10,000 hosts.

When the Connector is running, it may affect other concurrently running applications. Cisco recommends that you schedule the Connector to run when other applications are not running.

Installing the Required Components

Step 1 Verify that the Connector host has Perl installed, version 5.12.4 or later. The Qualys Connector is written in Perl, so it requires Perl on the Connector host. Consult your operating system documentation for installing Perl.

Step 2 Install or verify that the Connector host has specific Perl modules installed. These modules are:

- IO::Socket::SSL, version 1.5.3 or later
- XML::Simple, version 2.18 or later
- XML::Twig, version 3.39 or later
- Net::IP, version 1.25 or later
- YAML::XS, version 0.38 or later
- LWP::UserAgent, version 6.03 or later
- Net::SSL, version 2.84 or later

Install the following optional Perl module if IPv6 support is needed:

- IO::Socket::INET6, version 2.71 or later

Tip See Table ii-4 on page 5 for more information on proxy settings.

Cisco recommends that you use an OS-specific binary mechanism to download the modules such as apt, rpm, and so on. If you install the modules via CPAN or source code, you will also need to install a C compiler and the development version of OpenSSL on the Connector host.

Installing and Configuring the Connector Software

See the following sections for more information:

- describes how to install the software on the host.
- describes how to configure the Connector for your environment.
- describes how to display the version of the connector.

Installing the Connector

Step 1 Copy the Connector zip file that you downloaded (qualys-connector-*version*.zip) to your host.

Step 2 Extract the files using a utility that extracts `.zip` archives.

Configuring the Connector

Most configuration parameters are located in `QualysGuard.yaml` in the InputPlugins subdirectory. The parameters are stored as a set of key value pairs in the `YAML` format.

The following parameters **must** be set in `QualysGuard.yaml`:

Table ii-2   *Required Configuration Parameters*

Parameter	Type...
user_id	The username of your QualysGuard account.
password	The password of your QualysGuard account. If your password contains any punctuation, must put your password in single quotes, for example, `p@ssw0rd`.
template_id	The ID for the report template that you want to download data for.
	Note If you want to process data for multiple report templates, you can use the `process_multiple.pl` script and specify the template IDs on the command line instead of in `QualysGuard.yaml`.

You can set the following optional parameters in `QualysGuard.yaml`. If a parameter is omitted, it is set to its default value.

Table ii-3   ***Optional Configuration Parameters***

Parameter	Type
url	The URL for the QualysGuard Web service. This defaults to `https://qualysapi.qualys.com` and should be changed **only** if you have a local implementation of QualysGuard.
add_host	Either: `y` - sets the Defense Center to add a new host record to its host database when it imports vulnerability data for an IP address it does not recognize. This parameter is already set to `y` in `QualysGuard.yaml`. `n` - (the Connector default value) sets the Defense Center to ignore vulnerability data for IP addresses it does not recognize and to not add a new host record to its host database. **Note** If this parameter is set to `y`, one host from your licensed limit is used each time a new host record is created.
ip_ranges	One or more IP ranges to limit the amount of vulnerability data that is processed from the QualysGuard report. You can specify host ranges using CIDR notation or a dashed range. Example: `192.168.1.234-192.168.2.2, 192.168.1.245`. The default is `none`. **Note** If you want to reduce the amount of vulnerability data that is downloaded, you should modify the IP ranges or asset groups in the report template configuration (that is, in the QualysGuard GUI) rather than in this parameter. The Qualys Connector downloads all of the vulnerability data for the report template, even if the `ip_ranges` parameter is set.

Set the following optional parameters in `QualysGuard.yaml` for proxy support. These parameters do not have default values.

Table ii-4   ***Proxy Configuration Parameters***

Parameter	Type
proxy	The URL of the SSL-capable web proxy that will be used to connect to the QualysGuard Web service. Example: `https://192.168.1.100:443`. The proxy must be an SSL-capable web proxy, and the port number must be between `0` and `65535`.
proxy_username	The web proxy user name. This field is only necessary if the web proxy requires authentication.
proxy_password	The web proxy password. This field is only necessary if the web proxy requires authentication.

Here is a sample YAML file:

```
# Required Parameters
    user_id: dirk_g
    password: 'd0ntp@n1c'
    template_id: 424242
# Optional Parameters
    add_host: y
    ip_ranges: 192.168.1.0/24, 10.1.2.3-10.1.2.10, 42.4.2.1
    proxy: https://192.168.1.100:443
    proxy_username: zaphod
    proxy_password: 't0w3L'
```

Checking the Version of the Connector

You can display the version of the connector by running the connector script without any options:

```
./qualys_connector.pl
```

The version is in the top line of the output followed by script information, as in the following sample:

```
qualys_connector.pl Ver. 1.0.0-30
```

Preparing the Defense Center

In addition to installing and configuring the Qualys Connector, you must prepare your Defense Center so it can receive the QualysGuard vulnerability data from the Connector. See the following sections for more information:

- Configuring Host Input Client Authentication, page 6 describes how to configure the Defense Center to listen for connections from the Connector host.
- Verifying Host Connectivity, page 7 describes the process for verifying network connectivity between the Connector host and the Defense Center.
- Installing or Verifying Host Licenses, page 7 describes how to ensure the Defense Center has a sufficient number of host licenses to process QualysGuard vulnerability data.
- Configuring Vulnerability Correlation, page 7 describes how to configure the Defense Center to correlate with QualysGuard vulnerabilities.

Configuring Host Input Client Authentication

The Defense Center must be configured to listen for connections from the Qualys Connector. You must add the Connector host to the Defense Center's peers database from the Host Input Client page. You must also copy the authentication certificate generated by the Defense Center for the Connector host.

The steps required are listed in Chapter 4 of the *Host Input API Guide,* but are repeated here for convenience:

Access: Admin

Step 1 Select **Local > Registration > Host Input Client.**

Step 2 Click **Create Client**.

Step 3 In the **Hostname** field, enter the host name or IP address of the host running the host input client.

> **Note** If you use a host name, the host input server **must** be able to resolve the host to an IP address. If you have not configured DNS resolution, you should configure it first or use an IP address.

Step 4 If you want to encrypt the certificate file, enter a password in the **Password** field.

Step 5 Click **Save**.

The host input service allows the client computer to access port 8307 on the Defense Center and creates an authentication certificate to use during client-server authentication. The Host Input Client page reappears, with the new client listed under **Host Input Clients**.

Step 6 Click the download icon ( ) next to the certificate file.

Step 7 Save the certificate file to the directory used by your client computer for SSL authentication.

The client can now connect to the Defense Center.

Verifying Host Connectivity

The Connector host acts as a client and initiates a TCP connection to port 8307 on the Defense Center. You must therefore ensure that routing is properly configured between the hosts and that there is not a firewall or other network device blocking traffic to port 8307 on the Defense Center.

To test network connectivity, you can run this command on the Connector host:

```
telnet Defense_Center_IP 8307
```

You should see results similar to this:

```
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.
```

Installing or Verifying Host Licenses

You must ensure that the Defense Center has one host license for every host that has QualysGuard vulnerability data. If the Defense Center does not have enough host licenses for all the hosts containing vulnerability data, it will discard data for each new host added after the license count is exceeded.

To verify that you have enough host licenses or to install more, select **System > Licenses**. The counts of currently allocated and used license appear under **Maximum Licenses**. See "Understanding Licensing" in the FireSIGHT System *User Guide* for more information.

Configuring Vulnerability Correlation

You must ensure that the Defense Center is performing impact flag correlation with QualysGuard vulnerabilities. This should already be configured by default, but you should check the setting if you encounter any issues while correlating with QualysGuard vulnerabilities.

On the Defense Center, select **Policies > Network Discovery**, and click the **Advanced** tab. Under **Vulnerabilities to use for Impact Assessment**, the **Use Third Party Vulnerability Mappings** option should be set to **Yes**.

You must set **Use Third Party Vulnerability Mappings** to **Yes** only if you want to correlate with vulnerability mappings that you specifically created in the **User 3rd Party Mappings** section. You can leave it checked it if it is already checked.

To change the setting, click the edit icon ( ). The Edit Vulnerability Settings menu appears and shows the current selection. Change the selection and click **Save**. See "Managing System Policies" in the *FireSIGHT System User Guide* for more information about creating and editing system policies.

Running the Connector

You are now ready to run the Connector and process QualysGuard data. See the following sections for more information:

- describes how to work with one report template.

- Working with Multiple Templates, page 9 describes how to process data for multiple templates.
- Automating Connector Operation, page 10 describes how to automate the process of running the Connector.

Working with a Single Report Template

The main script to download and process QualysGuard data is `qualys_connector.pl`. Here is its syntax:

```
qualys_connector.pl [options] plugin
```

where *plugin* defaults to `QualysGuard` if it is not specified.

The following table lists the command line options. You can use the indicated option abbreviations to reduce typing. If you do not include a given option, the `qualys_connector.pl` script uses the default value. Examples that follow show the option syntax.

Table ii-5

Option	Abbreviation	Description
server	se	The Defense Center's IP address or host name.
port	po	The server port to connect to. Default is 8307.
plugininfo	pl	The file name of the YAML file used to provide configuration parameters for the QualysGuard plugin. Default is `InputPlugins/QualysGuard.yaml`.
ipv6	i	Enable IPv6 capability when connecting to the Defense Center. The Defense Center must have an IPv6 address to use this option. **Note** Even if you communicate via IPv6 with the Defense Center, the Connector host must still have an IPv4 network stack, so it can download QualysGuard vulnerability reports.
pkcs12	pk	Path name to the certificate used for host input authentication. Default is the first located file in the local directory with the .pkcs12 file extension.
password	pa	Password for the .pkcs12 file. Default is none.
syslog	sy	Enable logging to syslog. If Sys::Syslog is not installed or defined on the Connector host, logging is directed to stderr.
stderr	st	Enable logging to standard error (STDERR).
logfile	lo	Specify a log file path name to capture logging output. Default is none.
level	le	Specify a log level (3: debug, 2: info, 1: warning, 0: error). Default is 2.
csvfile	c	Specify a CSV output path name. If a CSV file is specified, the commands to transfer QualysGuard data to the Defense Center are saved as a file instead of being executed. This option and the `-server` option are mutually exclusive. If you generate CSV output, the QualysGuard data is not sent to the Defense Center. This option is useful in a testing scenario if you want to verify that the QualysGuard data is being correctly downloaded and processed. If both `-csvfile` and `-server` options are specified, the `-server` option is ignored.

Examples

This is the simplest form of the command. It assumes that a `.pkcs12` file exists in the local directory and the QualysGuard YAML file is located in `InputPlugins/QualysGuard.yaml`. The Defense Center IP address is 10.10.10.10.

```
perl qualys_connector.pl -server=10.10.10.10
```

The following is the same command with the assumed options explicitly stated:

```
perl qualys_connector.pl -server=10.10.10.10
-pkcs12=CertFile.pkcs12
-plugininfo=InputPlugins/QualysGuard.yaml
```

The following command dumps a CSV file of commands to transfer QualysGuard data instead of communicating with the Defense Center:

```
perl qualys_connector.pl -csvfile=Output.csv
-plugininfo=InputPlugins/QualysGuard.yaml
```

The previous command can also be shortened with abbreviations as follows:

```
perl qualys_connector.pl -c=Output.csv
-pl=InputPlugins/QualysGuard.yaml
```

Note that the default of all these commands is to log output to standard out. If you want to log to a file or syslog instead, you can use either the `-syslog` or `-logfile` *log_name* options or both of those options.

The default log level of 2 generates high-level log messages. You can also set the log level to 3, which generates detailed information about every vulnerability that is imported.

Working with Multiple Templates

If you want to download and process multiple report templates one at a time, you can use the `process_multiple.pl` script. The syntax is as follows:

```
perl process_multiple.pl -multiinfo
    <template_id1,template_id2,...> [options (same as for
    qualys_connector.pl)]
```

Note that the template IDs are separated by commas, but the list of IDs must not contain any spaces.

Here is an example:

```
perl process_multiple.pl -multiinfo 424242,535353
    -server=10.10.10.10
```

Also, if you specify the `-csvfile` option, the `process_multiple.pl` script prepends the template ID to the CSV file. For example, if you run this command:

```
perl process_multiple.pl -multiinfo 424242,535353
    -plugininfo=InputPlugins/QualysGuard.yaml
    -csvfile=Output.csv
```

The resulting CSV files are named `424242_Output.csv` and `535353_Output.csv`.

Automating Connector Operation

Because connector operations are performed by scripts, they can be automated by UNIX or Linux cron or launchd. See your operating system documentation for more information about how to configure these services. You are encouraged to call out file names and command line options as explicitly as possible.

For example, your crontab file can contain a command similar to the following, assuming that the Connector files are located in `/usr/local/qualys`:

```
/usr/bin/perl /usr/local/qualys/qualys_connector.pl
    -server=10.10.10.10
    -pkcs12=/usr/local/qualys/CertFile.pkcs12
    -plugininfo=/usr/local/qualys/InputPlugins/
        QualysGuard.yaml
```

Uninstalling the Qualys Connector

When you no longer need the Qualys connection, you can remove it by deleting the Connector directory and taking the Connector host out of the peer list.

Step 1 Delete the directory containing the Connector files and any subdirectories.

Step 2 In the web user interface on the Defense Center, select **Local > Registration > Host Input Client.**

Step 3 Delete the IP address or host name of the Connector host. Click the delete icon (🖥) next to the host you are removing.

🔍
Tip   When you delete the host from the list, access is revoked immediately.

Troubleshooting

Problems with using the Connector generally fall into several categories:

Problems with Initial Configuration

If you encounter problems running the connector script and downloading Qualys reports, check these items:

Step 1 You have not installed all the prerequisite Perl modules. If any library is missing, you see this error message along with the missing modules:

```
The following prerequisite Perl modules are missing :
    <Library 1>
    <etc>
```

You must install whatever modules are missing. It is highly recommended that you use an OS-specific binary mechanism to download the modules, such as apt, rpm, and so forth.

Step 2 You have not specified the correct YAML file. The default YAML file is
`InputPlugins/QualysGuard.yaml`. If you use a different file, you must explicitly specify it using the
-plugininfo command line option.

Problems with Downloading QualysGuard Reports

The first step in processing QualysGuard reports is to download them. If the Connector host generates any error messages in this stage, check the following items:

Step 1 Check that you have entered a valid user name and password in `InputPlugins/QualysGuard.yaml`. If your password has any non-alphanumeric characters, put the password in single quotes.

If your username or password is incorrect, you may see this message:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2010-01-01T12:00:00Z</DATETIME>
        <CODE>2010</CODE>
        <TEXT>Bad Login/Password</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Step 2 Check that you have entered a valid report template ID. Log into your QualysGuard account and confirm that you have the correct ID.

If your template ID is not correct, you could see this message:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2010-01-01T12:00:00Z</DATETIME>
        <CODE>999</CODE>
        <TEXT>Internal error. Please contact customer
            support.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>Incident Signature</KEY>
                <VALUE>Tried to launch invalid report.</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Step 3 Check that the Connector host has network access to download QualysGuard reports. If Qualys is storing your reports and you are not storing your data locally, the host must be able to access port 443 on qualysapi.qualys.com. Verify that network access is not being prevented by firewall, proxy, or routing policies.

Problems with Sending QualysGuard Data to the Defense Center

After the Connector host has downloaded the QualysGuard report data and processed it, the host will display this message: `QualysGuard Report Processing Complete`. At this point the Connector is ready to send data to the Defense Center and continues to generate appropriate status or log messages.

If the Connector cannot send data to the Defense Center, or if no hosts in the Defense Center network map have any QualysGuard vulnerability data, check these items:

- Verify that you have a valid network connection between the Qualys host and the Defense Center and that you can access port 8307 on the Defense Center. To test this, type `telnet` *`Defense_Center_IP`* `8307` on the host command line prompt. You should be able to establish a connection.

- Verify that you have copied a .pkcs12 certificate from the Defense Center to the directory on the Connector host containing the `qualys_connector.pl` script. You should have created this certificate on the Host Input Client page on the Defense Center. For best results, ensure that you only have a single .pkcs12 file in the directory. If you have more, the authentication process may be using the wrong one.

- Check that the Defense Center has a sufficient number of host licenses installed. The Defense Center must have one host license for every host that has QualysGuard vulnerability data.

- Open your YAML file (for example, `InputPlugins/QualysGuard.yaml`) and check the `add_host` parameter. If you are downloading vulnerability data for hosts that do not yet exist in the Defense Center network map, this parameter **must** be set to `y` or `yes`. Otherwise, these hosts are **not** added to the network map.

Obtaining Technical Support

Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco ASA devices, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance with Cisco ASA devices, please contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.