



FortiScan[®]

Version 4.1.0

Getting Started Guide



FortiScan Getting Started Guide

Version 4.1.0

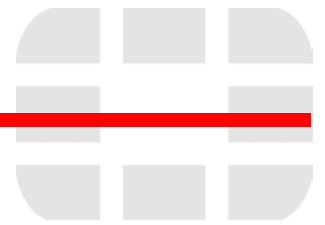
23 September 2010

17-410-96209-20100930

© Copyright 2010 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

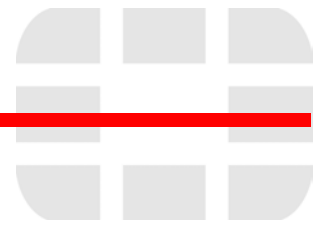
Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiAnalyzer, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiScan, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Contents

Getting Started with FortiScan VCM	5
Before you begin	6
Configuring the FortiScan Appliance.	6
Connecting to the FortiScan unit	7
Configuring basic network settings.	8
Setting the system date and time	8
Discovering host assets	10
Importing discovered hosts into the database	10
Grouping assets	11
Creating an asset group	11
Adding an asset to an asset group.	12
Installing the FortiScan Agent	12
Downloading the FortiScan Push-Installer	12
Installing agents on discovered assets.	13
Observing FortiScan agent registration behavior	14
Performing a vulnerability scan	15
Viewing detected vulnerabilities	15
Generating and viewing reports	16



Getting Started with FortiScan VCM

This document is intended to help you get started with deploying and using the FortiScan Vulnerability and Compliance Management (VCM) Platform. It assumes that you have already installed and cabled the FortiScan Appliance, as described in the FortiScan [QuickStart Guide](#) that was shipped with the device.

Here is a roadmap of the basic steps for getting started with the FortiScan VCM platform:

Table 1: A simplified roadmap for deploying FortiScan VCM

<input type="checkbox"/>	Step	Description	For the procedure...
	1	Configure the FortiScan Appliance network settings for initial operation.	See “Configuring the FortiScan Appliance” on page 6.
	2	Initiate a network asset discovery scan.	See “Discovering host assets” on page 10.
	3	Import discovered assets into the FortiScan database.	See “Importing discovered hosts into the database” on page 10.
	4	Arrange your discovered assets into asset groups.	See “Grouping assets” on page 11.
	5	Install FortiScan agents on the discovered assets.	See “Installing the FortiScan Agent” on page 12.
	6	Observe the agent registration process.	See “Observing FortiScan agent registration behavior” on page 14.
	7	Perform a vulnerability scan on the protected assets.	See “Performing a vulnerability scan” on page 15.
	8	View vulnerability alerts	See “Viewing detected vulnerabilities” on page 15.
	9	Create real-time and scheduled reports	See “Generating and viewing reports” on page 16.

You can use the above roadmap as a checklist for completing your test deployment. For more detailed procedures and explanations at any time, use the FortiScan Appliance web-based-manager context-sensitive online help, or see the [FortiScan 4.1.0 Administration Guide](#).

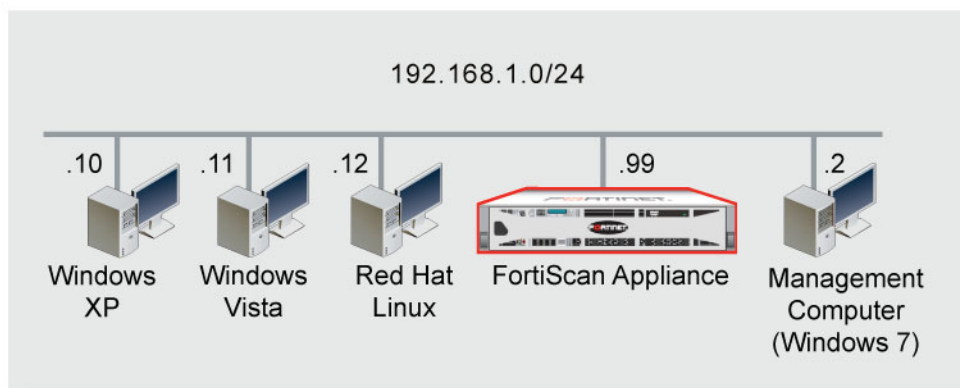
Before you begin

This guide refers to the sample network shown in [Figure 1 on page 6](#) for all procedures. It is recommended that you install the FortiScan VCM Platform on a similar test network in a lab environment to familiarize yourself with its operation, before deploying the platform on a wider scale in your enterprise network.

To set up your test installation you will need the following:

- One FortiScan Appliance, (Release 4.0.0 firmware), installed and cabled as described in the FortiScan Appliance QuickStart guide that was shipped with the device.
- Three to ten host assets, preferably with different operating system platforms, located on the same subnet as the FortiScan Appliance unit.
- A management computer (Windows) with network access to the Appliance unit.

Figure 1: Sample Test Network



Step 1: Configuring the FortiScan Appliance

The FortiScan unit ships with a factory default configuration. The default configuration enables you to connect to the FortiScan web-based manager to configure the FortiScan unit onto the network.

To configure the FortiScan unit onto the network, you must:

- change network interface IP addresses
- add DNS server IP addresses
- configure the routing table.

Once you complete the network configuration, you can perform additional configuration tasks such as setting the administrator password and setting the system time.

Connecting to the FortiScan unit

The web-based manager provides a graphical user interface (GUI) to configure, manage and maintain the FortiScan unit.

You can configure and manage the FortiScan unit using a secure HTTPS connection from any computer running Internet Explorer 7.0 and up or FireFox 3.5 and up.

Configuration changes made using the web-based manager are effective immediately without restarting the FortiScan unit or interrupting service. For all FortiScan models, use the following procedure to connect to the web-based manager for the first time.

To connect to the web-based manager, you need:

- an Ethernet connection between the FortiScan unit and management computer
- Internet Explorer 7.0 and up, or FireFox 3.5 and up.

The first time you log in to the FortiScan Appliance with the web-based manager, you must use the default administrator account settings. Fortinet recommends that you immediately configure a new password for the `admin` account.

After connecting to the web-based manager, you can configure the FortiScan unit IP address, DNS server IP address, and default gateway to connect the FortiScan unit to the network.

To connect to the web-based manager

- 1 Connect management computer's Ethernet port to the Port1 interface of the FortiScan unit, using a cross-over Ethernet cable. If you want to connect the devices through a hub or switch, use straight-through Ethernet cables.
- 2 Configure the management computer to be on the same subnet as the FortiScan LAN interface. In our example network, we have configured the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
- 3 To access the FortiScan web-based manager, start your browser and browse to ***https://192.168.1.99/*** (remember to include the "s" in https://). The Login dialog box appears.
- 4 Enter the following factory default administrator account settings and select *Login*:

Name	admin
Password	P@ssword1

- 5 For security reasons, we recommend that you immediately configure a new password for the admin account. To do this, go to *System > Admin > Administrator* and select the *Change Password* icon for the default `admin` account. Enter the password you want to use, confirm the spelling by entering it again and then select *OK*. The new password will take effect the next time you log in.



Caution: Make sure you set a strong password for the account, and change the password regularly. For security reasons, a password should contain at least one lower case letter, one upper case letter, one digit and one special character. Failure to maintain the password of the default `admin` account could compromise the security of your FortiScan Appliance unit.

Configuring basic network settings

When shipped, each network interface associated with a physical network port of the FortiScan unit has a default IP address and netmask. For Port 1, the default IP address and netmask is 192.168.1.99/255.255.255.0.

Depending on the design of your unique network, you may need to change the interface IP address settings to ensure compatibility. In addition, you must configure the FortiScan Appliance with the IP address of your DNS servers and gateway router.

To configure the FortiScan unit network interface settings

- 1 In the web-based manager, go to *System > Network > Interface*.
- 2 Select the check box for Port1 and then select *Edit* from the toolbar.
- 3 Change the IP address and netmask to an available address on the same subnet as the host assets you want to manage. Our sample network shown in [Figure 1 on page 6](#), uses subnet 192.168.1.0, so we can leave the IP address for Port1 unchanged from its default setting (192.168.1.99/255.255.255.0).
- 4 Select *OK*.

To configure the FortiScan unit DNS settings

If the FortiScan unit will be connected to the internet, perform the following steps:

- 1 Go to *System > Network > DNS*.
- 2 Enter the IP address for the *Primary DNS Server* and *Secondary DNS Server* (optional).
- 3 Select *Apply*.

To configure the FortiScan unit routing table

- 1 Go to *System > Network > Routing*.
- 2 Select *Create New* and add the *Destination IP/Mask* and *Gateway IP* address and any other routes as required.
- 3 Select *OK*.

Setting the system date and time

For many features to work, including scheduling and logging, the FortiScan Appliance system time must be accurate.

You can either manually set the FortiScan Appliance system time or configure the FortiScan unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.



Note: FortiScan Appliance units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To configure the date and time using the web-based manager

- 1 Go to *System > Dashboard*. In the *System Information* widget, in the *System Time* row, select *Change*.
- 2 From *Time Zone*, select the time zone in which the Fortinet unit is located.
- 3 Configure the following settings to either manually configure the system time, or automatically synchronize the FortiScan Appliance unit's clock with an NTP server. Then select *OK*.

System Time	The date and time according to the Fortinet unit's clock at the time that this tab was loaded, or when you last selected the <i>Refresh</i> button.
Refresh	Click to update the <i>System Time</i> field with the current time according to the Fortinet unit's clock.
Time Zone	Select the time zone in which the Fortinet unit is located.
Automatically adjust clock for daylight saving changes	Enable to automatically adjust the clock of the Fortinet unit when its time zone changes between daylight savings time (DST) and standard time.
Set Time	Select this option to manually set the date and time of the Fortinet unit's clock, then select the <i>Hour</i> , <i>Minute</i> , <i>Second</i> , <i>Year</i> , <i>Month</i> and <i>Day</i> fields before you click <i>Apply</i> .
Synchronize with NTP Server	Select this option to automatically synchronize the date and time of the Fortinet unit's clock with an NTP server, then configure the <i>Server</i> and <i>Sync Interval</i> fields before you click <i>Apply</i> .
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org .
Sync Interval	Enter how often in minutes the Fortinet unit should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.

Step 2: Discovering host assets

Once you have configured the FortiScan Appliance basic communication settings, the next step is to initiate a network discovery scan to discover the host assets in your network.

When the discovery scan job completes, the Fortinet Appliance unit creates a report listing all the hosts it discovered on the local network segment during the scan.

FortiScan automatically imports the host address information from the report into the Asset Inventory, where the discovered hosts appear in the *Unprotected* default asset group. After that, you can remotely install agents on the newly discovered assets to protect them.

To create a network discovery scan

- 1 Go to *Asset > Discovery > Schedule*. The list of scheduled network discovery scan jobs appears in the content pane.
- 2 Select *Create New*. The Create Asset Discovery (Map) Schedule dialog box appears.
- 3 In the Name field, enter a name for the network map profile.
- 4 In the *Target* section configure the following settings:

Scan Ports	The host ports to be checked. Use the default setting: TCP & UDP .
IP Range	Enter an IP range in which the scan will be executed. The IP range must be within the same subnet. For the sample network in Figure 1 on page 6 , you would enter an IP Range within the 192.168.1 subnet that covers all the test hosts, for example: 198.168.1.10-198.168.1.20.

- 5 In the *Schedule* section, select *Run Now*.
- 6 When done, select *OK* to run the new discovery scan job.

Step 3: Importing discovered hosts into the database

After running a network discovery scan, information about the discovered hosts is recorded in the network discovery scan report. This information is automatically imported into the database. If you want to use an existing discovery report from a previous version (4.0.0 and earlier) of FortiScan, you can manually import the discovered hosts into the FortiScan Appliance database so that they can be viewed and protected.

To manually import the discovered hosts

- 1 Go to *Asset > Discovery > Report*. The list of network discovery reports appears.
- 2 Select the check box for the report that contains the list of discovered assets you want to import.

- 3 In the main toolbar, select *Import*.
The list of assets contained in the report is imported to the FortiScan asset inventory database.
- 4 To view the imported assets, go to *Asset > Inventory > Asset Inventory*. Then from the asset group selection tree, select *View Filters > By Status > Unprotected*. The list of imported assets appears in the content pane.

Step 4: Grouping assets

The Asset Inventory submenu enables you to view and manage discovered assets, organize them into groups and install agents on discovered assets.

After the initial discovery scan, the FortiScan Appliance automatically places discovered assets into the following default groups:

- **All Assets** - This group contains all discovered assets.
- **Preferred Assets** - These are groups defined by the user. Assets can be dragged into the preferred asset group or cut and paste.
- **View Filters** - These are automatic groups provided by the FortiScan Appliance, as follows:
 - **By Criticality** - This group contains subgroups for each criticality level (High, Highest, Low, Lowest, Medium).
 - **By OS Family** - This group contains a subgroup for each operating system discovered in your enterprise. Assets are automatically assigned to these groups based on the asset's operating system. Assets with an undetermined operating system are placed in a default operating system group named **Other**.
 - **By Status** - This group contains a subgroup for each asset protection status category (Disconnected, Protected, Registered, Unprotected and Retired).

You cannot add assets to the default asset groups, or delete the default asset groups. You can, however, create user-defined groups and assign assets to them, to organize them by location, work group, or any other common characteristic.

Creating an asset group

To create an asset group, do the following:

- 1 Go to *Asset > Inventory > Asset Inventory*. The asset inventory view displays in the content pane.
- 2 In the asset selection tree, select the *New Asset Group* button. The New Asset Group dialog box appears.
- 3 Configure the following settings:

Name	Enter a name for the new asset group. In our example, we will use <code>test_001</code> .
Business Impact	For this example, leave the business impact rating at the default setting (High).
Asset Group Parent	Select the <i>Preferred Assets</i> group as the parent.

- 4 Select *OK* to create the new group. In the asset selection tree, our new group *test_001* appears under the *Preferred Assets* parent group.

Adding an asset to an asset group

Now that we have created our asset group, *test_001*, the next step is to add the discovered assets to this group.

An asset can be part of one group or several groups simultaneously. For example, an asset may appear in one group containing similar operating systems, and in another group containing assets for a specific work group. When you add an asset to a group, you are actually copying an existing asset from the default group and placing the copy in the group.

To add an asset to an asset group

- 1 Go to *Asset > Inventory > Asset Inventory*.
- 2 In the asset selection tree, go to *View Filters > By Status* and select the checkbox for the *Unprotected* default group. The list of unprotected assets appears in the asset group details pane.
- 3 In the asset group details pane, select the check boxes for all the discovered assets we imported earlier and then select *Copy* from the toolbar.
- 4 In the dialog box, under *Asset Group Parent* tree, select the check box for the *test_001* group and then select *OK*. The assets are added to the group.
- 5 In the asset selection tree, select the *Preferred Assets > test_001* group and verify that the discovered assets now appear in this group. Notice that the discovered assets also continue to be listed in the default groups.

We are now ready to install the FortiScan Agent on each discovered asset so that they can be protected by the VCM platform.

Step 5: Installing the FortiScan Agent

Before the FortiScan Appliance can manage and protect a host asset, the asset must have the FortiScan Agent software installed. The agent software enables communication with the FortiScan Appliance, generates periodic data surveys, and allows you to apply policies and dispatch remediations to the asset. The asset surveys generated by the FortiScan Agent keep the FortiScan Appliance database updated with the latest status about each host asset.

An administrator with a Windows platform can install the FortiScan Agent software remotely to a host asset from the *Asset Inventory* submenu, using the FortiScan Push-Installer utility. You must download the Push Installer application to your administration computer, before you can use this feature.

Downloading the FortiScan Push-Installer

You can download the FortiScan Push-Installer to an administration computer from the FortiScan web user interface. To run the FortiScan Push-Installer, an administration computer must meet the following requirements:

- It must be a Windows platform.
- It must have network access to the FortiScan Appliance and hosts.

- The Java Runtime Environment plug-in must be installed on the browser.
- The Push-Installer package must be downloaded and extracted to the following directory:

C: \FSC_Pushinstaller

To download the Push-Installer

- 1 Log in to the FortiScan Appliance web interface. The *System > Dashboard > Status* submenu appears.
- 2 Locate the *System Information* widget, and in the *Firmware Version* field, select *Update*. The Manual Upload Release dialog box appears.
- 3 In the *Download Push Installer* column, select the *Push Installer* icon.
- 4 In the file download dialog box, select *Open* to download the `FSC_Pushinstaller.zip` file.
- 5 After the file downloads, extract the contents of the zip file to the following directory:
C:\FSC_Pushinstaller
- 6 In the FortiScan Appliance web user interface, select *Cancel* to close the *Manual Upload Release* dialog box.

Installing agents on discovered assets

To install the FortiScan Agent software on a discovered host asset:

- 1 Go to *Asset > Inventory > Asset Inventory*. The asset inventory view appears.
- 2 In the asset navigation tree, go to *Preferred Assets > test_001*. The list of discovered assets appears in the asset group details pane.
- 3 Select all the check boxes for the assets in the group and then select *Installer* on the toolbar. The FortiScan Push-Installer application window appears.
The selected assets appear in the host asset list on the *Host* tab.
- 4 Configure the following settings for each asset:

Platform	Select the correct platform for each asset from the list.
Method	Install method: <ul style="list-style-type: none"> • su - For Solaris platforms • sudo - For Linux platforms • N/A - For Windows platforms
ConnectUser	The username or ID if necessary to connect to the asset.
ConnectPwd	The password corresponding to the Connect Username/ID.
InstallUser	The username or ID if necessary to install the FortiScan Agent software. This field is only required for non-Windows platforms.
InstallPwd	The password corresponding to the install username/ID. This field is only required for non-Windows platforms.

- | | |
|----------------|---|
| Task | Select install . |
| DeICEID | Select the Delete CEID option as follows: <ul style="list-style-type: none"> • Y - Enables the Push-Installer to delete the current CEID on the asset (if one exists). Specify this option when asset information in the FortiScan database is no longer applicable. For example, the asset has been wiped clean and reassigned to a new resource. In this event, the administrator may wish to disassociate any legacy data current assigned to that CEID. • N - Disables this option <p>Note: If the asset does not have a CEID then this field will not matter.</p> |

- 5 Select the *Check All* button and then select the *Push Agents* button. The progress of the installation for each asset is shown in the *Status* field.
- 6 After the agent is installed on each selected asset, the agent will immediately begin to registering itself with the FortiScan Appliance.



Note: Assets that registered during the current web session might not be visible in the web-based manager. To see them, log out and log in again to start a new session.



Note: There are other methods to install FortiScan Agents. For more options, see “About FortiScan Agent installation methods” in the [FortiScan 4.1.0 Administration Guide](#).

Step 6: Observing FortiScan agent registration behavior

Upon initial start up, the FortiScan Agent contacts the FortiScan Appliance, conducts a limited survey of the local computer system, and submits this information to the FortiScan Appliance to complete registration. The FortiScan Agent provides a detailed survey a short time later (within 15 minutes) for analysis and storage.

After successful registration with the FortiScan Appliance, the FortiScan Agent continues to conduct periodic standard and detailed surveys, and forwards this updated information to the FortiScan Appliance for analysis and storage. In addition, the FortiScan Agent completes and forwards a detailed survey each time it is started.

To observe the registration process

- 1 Go to Asset > Inventory > Asset Inventory.
- 2 In the asset group selection tree, select *Preferred Assets > test_001*. The list of discovered assets appears in the content pane.
- 3 Observe how the asset protection status for each asset changes after you first install the FortiScan agent in the host:
 - Before installing the agent, the asset status is Unprotected.
 - After installing the agent, the asset status changes to Registered.

- The asset remains in Registered status until the first detailed survey is received (typically within 10 to 20 minutes), after which the asset status changes to Protected.

For more information about asset status, see the [FortiScan 4.1.0 Administration Guide](#).

When the asset protection status changes to Protected, the asset is ready for vulnerability and compliance management.

Step 7: Performing a vulnerability scan

Once your host assets have successfully moved to Protected status, you can use the web-based manager to initiate compliance audit scans, vulnerability scans and patch scans of your enterprise network, view scan results, investigate the details for any vulnerabilities found and apply remediations. You can also easily create, apply and manage specific policies for your enterprise to ensure all assets are consistently protected.

In this guide, we'll demonstrate how to perform a vulnerability scan on the test network. For information about other operations, see the [FortiScan 4.1.0 Administration Guide](#).

To perform a vulnerability scan

- 1 Go to *Compliance > Vulnerability Scan > Perform Scan*. The wizard begins and the Benchmark page appears.
- 2 Select a vulnerability scan definition from the list of benchmarks.
- 3 Enter a unique name for the scan job and any comments, then select *Next*. The Platforms page appears.
- 4 Select the check box for each platform and then select *Next*.
- 5 Select the check box for each asset and then select *Next*.
- 6 The Perform page appears, confirming that the vulnerability scan has been scheduled.
- 7 Go to *Compliance > Vulnerability Scan > Scan Results* to view the status of the scan job. Results will not become available until the next asset survey interval. This may take several minutes depending on the survey interval selected.

Step 8: Viewing detected vulnerabilities

The *Compliance > Vulnerability Scan > Scan Results* page displays the current status and assessment results for all vulnerability scan jobs.

If you select the value in the *Job Name* field for a vulnerability scan job, the Scan Summary page for the selected job appears. This page displays the details of the selected vulnerability scan job and the results of the scan. It also enables you to view more details about each scan task (by platform) that was part of the job.

To view vulnerability alerts

- 1 Go to *Compliance > Vulnerability Scan > Scan Results*. The Scan Results page appears.
- 2 In the *Job Name* column, select the name of the vulnerability scan job that you ran in step 7. The Scan Summary page appears.
- 3 In the *Scan Task Details* list, select the *Platform* name for the scan task you want to view. The Platform Summary page appears.
- 4 The *Assets Vulnerability Result* table at the bottom of the page lists the number of vulnerability alerts that were raised by the scan task for the selected platform. To view more details about these alerts, select the value in the *# of Vulnerability Alerts* column.

Step 9: Generating and viewing reports

The FortiScan appliance enables you to generate and view a large variety of real-time and scheduled reports to monitor the activity of FortiScan platform and its effect on your enterprise.

To view real-time reports

- 1 Go to *Reports > Real-time > Real-time*. The list of available real-time reports appears.
- 2 Select *Alert View - Vulnerability Scan* to view the alerts generated by the vulnerability scan that you performed earlier.
You can export the data displayed in the report to a comma-separated-values (csv) text file, by selecting the *Export to CSV* link at the top of the page.

To schedule a report

- 1 Go to *Report > Scheduled > Scheduled*. The list of reports available for scheduling appears.
- 2 In the *Available Reports* list, select the *Schedule Report* icon next to the *Alert View - Vulnerability Scan* report. The Schedule A Report dialog box appears.
- 3 In the *Job Name* field, enter a name for the scheduled report job.
- 4 In the *Description* field, enter an optional description for the job.
- 5 In the *Schedule Type* field, configure the scheduling options you want to use for the report:

Immediate	Select to generate the report right away.
Once	Select to generate the report once. In the fields that appear, enter the date and time when you want the task to begin.
By Minute	Select to schedule a recurring report every one or more minutes. In the fields that appear, enter the date and time when you want the scheduled report to begin and the number of minutes between recurrences.

- By Hour** Select to schedule a recurring report every one or more hours. In the fields that appear, enter the date and time when you want the report generation task to begin and the number of hours between recurrences.
- By Day** Select to schedule a recurring report every one or more days. In the fields that appear, enter the date and time when you want the report generation task to begin and the number of days between recurrences.
- By Week** Select to schedule a recurring report on specific days of the week. In the fields that appear, enter the date and time to begin, the days of the week, and the time you want the report generation task to run on the selected days.
- By Month** Select to schedule a recurring report every one or more months on specific days of the month. In the fields that appear, enter the date and time to begin, the number of months between recurrences, the days of the month, and the time you want the report generation task to run on the selected days.

- 6 Select *Submit* to create the scheduled job or select *Cancel* to cancel the operation.



Note: Scheduled jobs run in sequence. That is, a scheduled job will not begin if another job is running when its start time arrives. For example, if two reports are scheduled to run at the same time, one job will start only after the other one is finished. Because some reports, like the Benchmark View, can take several hours to finish, we recommended that you avoid setting job start times close to each other.

To view a list of all scheduled reports

- 1 Go to *Report > Scheduled > Scheduled*
- 2 Select *View All Pending Scheduled Reports* in the *Available Reports* column. The list of pending scheduled reports appears.
- 3 After the scheduled job completes, select the *Alert View - Vulnerability Scan* link.

A list of completed Alert View scheduled reports appears. You can delete a report, view it online or download it to local disk as a csv file.



Note: If a scheduled report contains more than 25,000 rows of data, you can not view it online. You can only download the report.

FORTINET®

www.fortinet.com