



Configuring Active Scanning

The FireSIGHT System builds a network map through passive analysis of traffic on your network. However, you may sometimes need to actively scan a host to determine information about that host. For example, if a host has a server running on an open port but the server has not received or sent traffic during the time that the system has been monitoring your network, the system does not add information about that server to the network map. If you directly scan that host using an active scanner, however, you can detect the presence of the server.

When you actively scan a host, you send packets in an attempt to obtain information about the host. The FireSIGHT System integrates with Nmap™ 6.01, an open source active scanner for network exploration and security auditing that can be used to detect operating systems and servers running on a host. With an Nmap scan, you can check for detailed information about the operating system and servers running on the host and refine the system's vulnerability reporting based on those results.



Note

Some scanning options (such as portscans) may place a significant load on networks with low bandwidths. You should always schedule scans like these to run during periods of low network use.

For more information, see the following sections:

- [Understanding Nmap Scans, page 47-1](#)
- [Setting up Nmap Scans, page 47-9](#)
- [Managing Nmap Scanning, page 47-14](#)
- [Managing Scan Targets, page 47-17](#)
- [Working with Active Scan Results, page 47-19](#)

Understanding Nmap Scans

License: FireSIGHT

Nmap allows you to actively scan ports on hosts on your network to determine operating system and server data for the hosts, which allows you to enhance your network map and fine-tune the accuracy of the vulnerabilities mapped to scanned hosts. Note that a host must exist in the network map before Nmap can append its results to the host profile. You can also view scan results in a results file.

When you scan a host using Nmap, servers on previously undetected open ports are added to the Servers list in the host profile for that host. The host profile lists any servers detected on filtered or closed TCP ports or on UDP ports in the Scan Results section. By default, Nmap scans more than 1660 TCP ports.

Nmap compares the results of the scan to over 1500 known operating system fingerprints to determine the operating system and assigns scores to each. The operating system assigned to the host is the operating system fingerprint with the highest score.

If the system recognizes a server identified in an Nmap scan and has a corresponding server definition, the system maps vulnerabilities for that server to the host. The system maps the names Nmap uses for servers to the corresponding Cisco server definitions, and then uses the vulnerabilities mapped to each server in the system. Similarly, the system maps Nmap operating system names to Cisco operating system definitions. When Nmap detects an operating system for a host, the system assigns vulnerabilities from the corresponding Cisco operating system definition to the host.

For more information the underlying Nmap technology used to scan, refer to the Nmap documentation at <http://insecure.org>.

For more information on Nmap on your Cisco appliance, see the following topics:

- [Understanding Nmap Remediations, page 47-2](#)
- [Creating an Nmap Scanning Strategy, page 47-5](#)
- [Sample Nmap Scanning Profiles, page 47-6](#)

Understanding Nmap Remediations

License: FireSIGHT

You can define the settings for an Nmap scan by creating an Nmap remediation. An Nmap remediation can be used as a response in a correlation policy, run on demand, or scheduled to run at a specific time. In order for the results of an Nmap scan to appear in the network map, the scanned host must already exist in the network map.

Note that Nmap-supplied server and operating system data remain static until you run another Nmap scan. If you plan to scan a host for operating system and server data using Nmap, you may want to set up regularly scheduled scans to keep any Nmap-supplied operating system and server data up-to-date. For more information, see [Automating Nmap Scans, page 62-5](#). Also note that if the host is deleted from the network map, any Nmap scan results for that host are discarded.

For more information about Nmap functionality, refer to the Nmap documentation at <http://insecure.org>. The following table explains the options configurable in Nmap remediations on a FireSIGHT System.

Table 47-1 Nmap Remediation Options

Option	Description	Corresponding Nmap Option
Scan Which Address(es) From Event?	When you use an Nmap scan as a response to a correlation rule, select an option to control which address in the event is scanned, that of the source host, the destination host, or both.	N/A
Scan Types	<p>Select how Nmap scans ports:</p> <ul style="list-style-type: none"> The TCP Syn scan connects quickly to thousand of ports without using a complete TCP handshake. This options allows you to scan quickly in stealth mode on hosts where the <code>admin</code> account has raw packet access or where IPv6 is not running, by initiating TCP connections but not completing them. If a host acknowledges the Syn packet sent in a TCP Syn scan, Nmap resets the connection. The TCP Connect scan uses the <code>connect()</code> system call to open connections through the operating system on the host. You can use the TCP Connect scan if the <code>admin</code> user on your Defense Center or managed device does not have raw packet privileges on a host or you are scanning IPv6 networks. In other words, use this option in situations where the TCP Syn scan cannot be used. The TCP ACK scan sends an ACK packet to check whether ports are filtered or unfiltered. The TCP Window scan works in the same way as a TCP ACK scan but can also determine whether a port is open or closed. The TCP Maimon scan identifies BSD-derived systems using a FIN/ACK probe. 	TCP Syn: <code>-sS</code> TCP Connect: <code>-sT</code> TCP ACK: <code>-sA</code> TCP Window: <code>-sW</code> TCP Maimon: <code>-sM</code>
Scan for UDP ports	Enable to scan UDP ports in addition to TCP ports. Note that scanning UDP ports may be time-consuming, so avoid using this option if you want to scan quickly.	<code>-sU</code>
Use Port From Event	<p>If you plan to use the remediation as a response in a correlation policy, enable to cause the remediation to scan only the port specified in the event that triggers the correlation response.</p> <p>Tip You can also control whether Nmap collects information about operating system and server information. Enable the Use Port From Event option to scan the port associated with the new server.</p>	N/A
Scan from reporting detection engine	Enable to scan a host from the appliance where the detection engine that reported the host resides.	N/A
Fast Port Scan	Enable to scan only the TCP ports listed in the <code>nmap-services</code> file located in the <code>/var/sf/nmap/share/nmap/nmap-services</code> directory on the device that does the scanning, ignoring other port settings. Note that you cannot use this option with the Port Ranges and Scan Order option.	<code>-F</code>
Port Ranges and Scan Order	Set the specific ports you want to scan, using Nmap port specification syntax, and the order you want to scan them. Note that you cannot use this option with the Fast Port Scan option.	<code>-p</code>

Table 47-1 Nmap Remediation Options (continued)

Option	Description	Corresponding Nmap Option
Probe open ports for vendor and version information	Enable to detect server vendor and version information. If you probe open ports for server vendor and version information, Nmap obtains server data that it uses to identify servers. It then replaces the Cisco server data for that server.	-sV
Service Version Intensity	Select the intensity of Nmap probes for service versions. Higher service intensity numbers cause more probes to be used and result in higher accuracy, while lower intensity probes are faster but obtain less information.	--version-intensity <intensity>
Detect Operating System	Enable to detect operating system information for the host. If you configure detection of the operating system for a host, Nmap scans the host and uses the results to create a rating for each operating system that reflects the likelihood that the operating system is running on the host. For more information on when and how Nmap-identified identity data appears in the network map, see Understanding Current Identities , page 46-5.	-o
Treat All Hosts As Online	Enable to skip the host discovery process and run a port scan on every host in the target range. Note that when you enable this option, Nmap ignores settings for Host Discovery Method and Host Discovery Port List .	-PN
Host Discovery Method	Select to perform host discovery for all hosts in the target range, over the ports listed in the Host Discovery Port List , or if no ports are listed, over the default ports for that host discovery method. Note that if you also enabled Treat All Hosts As Online , however, the Host Discovery Method option has no effect and host discovery is not performed. Select the method to be used when Nmap tests to see if a host is present and available: <ul style="list-style-type: none"> • The TCP SYN option sends an empty TCP packet with the SYN flag set and recognizes the host as available if a response is received. TCP SYN scans port 80 by default. Note that TCP SYN scans are less likely to be blocked by a firewall with stateful firewall rules. • The TCP ACK option sends an empty TCP packet with the ACK flag set and recognizes the host as available if a response is received. TCP ACK also scans port 80 by default. Note that TCP ACK scans are less likely to be blocked by a firewall with stateless firewall rules. • The UDP option sends a UDP packet and assumes host availability if a port unreachable response comes back from a closed port. UDP scans port 40125 by default. 	TCP SYN: -PS TCP ACK: -PA UDP: -PU
Host Discovery Port List	Specify a customized list of ports, separated by commas, that you want to scan when doing host discovery.	port list for host discovery method

Table 47-1 Nmap Remediation Options (continued)

Option	Description	Corresponding Nmap Option
Default NSE Scripts	Enable to run the default set of Nmap scripts for host discovery and server and operating system and vulnerability detection. See http://nmap.org/nsedoc/categories/default.html for the list of default scripts.	-sC
Timing Template	Select the timing of the scan process; the higher the number you select, the faster and less comprehensive the scan.	0: T0 (paranoid) 1: T1 (sneaky) 2: T2 (polite) 3: T3 (normal) 4: T4 (aggressive) 5: T5 (insane)

Creating an Nmap Scanning Strategy

License: FireSIGHT

While active scanning can obtain valuable information, overuse of a tool such as Nmap may overload your network resources or even crash important hosts. When using any active scanner, you should create a scanning strategy to make sure that you are scanning only the hosts and ports that you need to scan.

For more information, see the following sections:

- [Selecting Appropriate Scan Targets, page 47-5](#)
- [Selecting Appropriate Ports to Scan, page 47-6](#)
- [Setting Host Discovery Options, page 47-6](#)

Selecting Appropriate Scan Targets

License: FireSIGHT

When you configure Nmap, you can create scan targets that identify which hosts you want to scan. A scan target includes a single IP address, a CIDR block or octet range of IP addresses, an IP address range, or a list of IP addresses or ranges to scan, as well as the ports on the host or hosts.

You can specify targets in the following ways:

- For IPv6 hosts:
 - an exact IP address (for example, 192.168.1.101)
- For IPv4 hosts:
 - an exact IP address (for example, 192.168.1.101) or a list of IP addresses separated by commas or spaces
 - an IP address block using CIDR notation (for example, 192.168.1.0/24 scans the 254 hosts between 192.168.1.1 and 192.168.1.254, inclusive)

For information on using CIDR notation in the FireSIGHT System, see [IP Address Conventions, page 1-22](#).

- an IP address range using octet range addressing (for example, `192.168.0-255.1-254` scans all addresses in the `192.168.x.x` range, except those that end in `.0` and `.255`)
- an IP address range using hyphenation (for example, `192.168.1.1 - 192.168.1.5` scans the six hosts between `192.168.1.1` and `192.168.1.5`, inclusive)
- a list of addresses or ranges separated by commas or spaces (for example, for example, `192.168.1.0/24, 194.168.1.0/24` scans the 254 hosts between `192.168.1.1` and `192.168.1.254`, inclusive and the 254 hosts between `194.168.1.1` and `194.168.1.254`, inclusive)

Ideal scan targets for Nmap scans include hosts with operating systems that the system is unable to identify, hosts with unidentified servers, or hosts recently detected on your network. Remember that Nmap results cannot be added to the network map for hosts that do not exist in the network map.


Caution

Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, you may want to set up regularly scheduled scans to keep any Nmap-supplied operating system and server data up to date. For more information, see [Automating Nmap Scans, page 62-5](#). Also note that if the host is deleted from the network map, any Nmap scan results are discarded. In addition, make sure you have permission to scan your targets. Using Nmap to scan hosts that do not belong to you or your company may be illegal.

Selecting Appropriate Ports to Scan

License: FireSIGHT

For each scan target you configure, you can select the ports you want to scan. You can designate individual port numbers, port ranges, or a series of port numbers and port ranges to identify the exact set of ports that should be scanned on each target.

By default, Nmap scans TCP ports 1 through 1024. If you plan to use the remediation as a response in a correlation policy, you can cause the remediation to scan only the port specified in the event that triggers the correlation response. If you run the remediation on demand or as a scheduled task, or if you do not use the port from the event, you can use other port options to determine which ports are scanned. You can choose to scan only the TCP ports listed in the `nmap-services` file, ignoring other port settings. You can also scan UDP ports in addition to TCP ports. Note that scanning for UDP ports may be time-consuming, so avoid using that option if you want to scan quickly. To select the specific ports or range of ports to scan, use Nmap port specification syntax to identify ports.

Setting Host Discovery Options

License: FireSIGHT

You can decide whether to perform host discovery before starting a port scan for a host, or you can assume that all the hosts you plan to scan are online. If you choose not to treat all hosts as online, you can choose what method of host discovery to use and, if needed, customize the list of ports scanned during host discovery. Host discovery does not probe the ports listed for operating system or server information; it uses the response over a particular port only to determine whether a host is active and available. If you perform host discovery and a host is not available, Nmap does not scan ports on that host.

Sample Nmap Scanning Profiles

License: FireSIGHT

The following scenarios provide examples of how Nmap might be used on your network:

- [Example: Resolving Unknown Operating Systems, page 47-7](#)
- [Example: Responding to New Hosts, page 47-8](#)

Example: Resolving Unknown Operating Systems

License: FireSIGHT

If the system cannot determine the operating system on a host on your network, you can use Nmap to actively scan the host. Nmap uses the information it obtains from the scan to rate the possible operating systems. It then uses the operating system that has the highest rating as the host operating system identification.

Using Nmap to challenge new hosts for operating system and server information deactivates the system's monitoring of that data for scanned hosts. If you use Nmap to discover host and server operating system for hosts the system marks as having unknown operating systems, you may be able to identify groups of hosts that are similar. You can then create a custom fingerprint based on one of them to cause the system to associate the fingerprint with the operating system you know is running on the host based on the Nmap scan. Whenever possible, create a custom fingerprint rather than inputting static data through a third-party source like Nmap because the custom fingerprint allows the system to continue to monitor the host operating system and update it as needed.

To discover operating systems with Nmap:

Access: Admin/Discovery Admin

-
- Step 1** Configure a scan instance for an Nmap module.
For more information, see [Creating an Nmap Scan Instance, page 47-9](#).
- Step 2** Create an Nmap remediation using the following settings:
- Enable **Use Port From Event** to scan the port associated with the new server.
 - Enable **Detect Operating System** to detect operating system information for the host.
 - Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
 - Enable **Treat All Hosts as Online**, because you know the host exists.
- For information on creating Nmap remediations, see [Creating an Nmap Remediation, page 47-11](#).
- Step 3** Create a correlation rule that triggers when the system detects a host with an unknown operating system.
The rule should trigger when **an discovery event occurs** and **the OS information for a host has changed** and it meets the following conditions: **OS Name is unknown**.
For information on creating correlation rules, see [Creating Rules for Correlation Policies, page 51-2](#).
- Step 4** Create a correlation policy that contains the correlation rule.
For more information on creating correlation policies, see [Creating Correlation Policies, page 51-46](#).
- Step 5** In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.
- Step 6** Activate the correlation policy.
- Step 7** Purge the hosts on your network map to force network discovery to restart and rebuild the network map.

Step 8 After a day or two, search for events generated by the correlation policy. Analyze the Nmap results for the operating systems detected on the hosts to see if there is a particular host configuration on your network that the system does not recognize.

For more information on analyzing Nmap results, see [Analyzing Scan Results, page 47-21](#).

Step 9 If you find hosts with unknown operating systems whose Nmap results are identical, create a custom fingerprint for one of those hosts and use it to identify similar hosts in the future.

For more information, see [Fingerprinting Clients, page 46-8](#).

Example: Responding to New Hosts

License: FireSIGHT

When the system detects a new host in a subnet where intrusions may be likely, you may want to scan that host to make sure you have accurate vulnerability information for it.

You can accomplish this by creating and activating a correlation policy that detects when a new host appears in this subnet, and that launches a remediation that performs an Nmap scan on the host.

After you activate the policy, you can periodically check the remediation status view (**Policy & Response > Responses > Remediations > Status**) to see when the remediation launched. The remediation's dynamic scan target should include the IP addresses of the hosts it scanned as a result of the server detection. Check the host profile for those hosts to see if there are vulnerabilities that need to be addressed for the host, based on the operating system and servers detected by Nmap.



Caution

If you have a large or dynamic network, detection of a new host may be too frequent an occurrence to respond to using a scan. To prevent resource overload, avoid using Nmap scans as a response to events that occur frequently. In addition, note that using Nmap to challenge new hosts for operating system and server information deactivates Cisco monitoring of that data for scanned hosts.

To scan in response to the appearance of a new host:

Access: Admin/Discovery Admin

Step 1 Configure a scan instance for an Nmap module.

For more information, see [Creating an Nmap Scan Instance, page 47-9](#).

Step 2 Create an Nmap remediation using the following settings:

- Enable **Use Port From Event** to scan the port associated with the new server.
- Enable **Detect Operating System** to detect operating system information for the host.
- Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
- Enable **Treat All Hosts as Online**, because you know the host exists.

For information on creating Nmap remediations, see [Creating an Nmap Remediation, page 47-11](#).

Step 3 Create a correlation rule that triggers when the system detects a new host on a specific subnet.

The rule should trigger when **a discovery event occurs** and **a new host is detected**.

For information on creating correlation rules, see [Creating Rules for Correlation Policies, page 51-2](#).

Step 4 Create a correlation policy that contains the correlation rule.

For more information on creating correlation policies, see [Creating Correlation Policies, page 51-46](#).

- Step 5** In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.
- Step 6** Activate the correlation policy.
- Step 7** When you are notified of a new host, check the host profile to see the results of the Nmap scan and address any vulnerabilities that apply to the host.
-

Setting up Nmap Scans

License: FireSIGHT

To scan using Nmap, you must first configure a scan instance and a scan remediation. If you plan to schedule Nmap scans, you must also define a scan target.

For more information, see the following sections:

- [Creating an Nmap Scan Instance, page 47-9](#)
- [Creating an Nmap Scan Target, page 47-10](#)
- [Creating an Nmap Remediation, page 47-11](#)

Creating an Nmap Scan Instance

License: FireSIGHT

You can set up a separate scan instance for each Nmap module that you want to use to scan your network for vulnerabilities. You can set up scan instances for the local Nmap module on your Defense Center and for any devices you want to use to run scans remotely. The results of each scan are always stored on the Defense Center where you configure the scan, even if you run the scan from a remote device. To prevent accidental or malicious scanning of mission-critical hosts, you can create a blacklist for the instance to indicate the hosts that should never be scanned with the instance.

Note that you cannot add a scan instance with the same name as any existing scan instance.

To create a scan instance:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Click **Add Nmap Instance**.
The Instance Detail page appears.
- Step 3** In the **Instance Name** field, enter a name that includes 1 to 63 alphanumeric characters, with no spaces and no special characters other than underscore (_) and dash (-).
- Step 4** In the **Description** field, specify a description with 0 to 255 alphanumeric characters, which can include spaces and special characters.
- Step 5** Optionally, in the **Black Listed Scan hosts** field, specify any hosts or networks that should *never* be scanned with this scan instance, using the following syntax:

- For IPv6 hosts, an exact IP address (for example, `2001:DB8::fedd:eeff`)
- For IPv4 hosts, an exact IP address (for example, `192.168.1.101`) or an IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between `192.168.1.1` and `192.168.1.254`, inclusive)
- Note that you cannot use an exclamation mark (!) to negate an address value.

If you specifically target a scan to a host that is in a blacklisted network, that scan will not run.

Step 6 Optionally, to run the scan from a remote device instead of the Defense Center, specify the IP address or name of the device as it appears in the Information page for the device in the Defense Center web interface, in the **Remote Device Name** field.

Step 7 Click **Create**.

The scan instance is created.

Creating an Nmap Scan Target

License: FireSIGHT

You can create and save scan targets that identify specific hosts and ports. Then, when you perform an on-demand scan or schedule a scan, you can use one of the saved scan targets.

For scans of targets with IPv4 addresses, you can use an IP address, a list of IP addresses, CIDR notation, or Nmap scan octets to select the hosts to scan. You can also specify a range of addresses using a hyphen. Separate addresses and ranges in a list with commas or spaces.

For scans of IPv6 addresses, use an IP address. Ranges are not supported.

Note that Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, you may want to set up regularly scheduled scans to keep any Nmap-supplied operating system and server data up to date. For more information, see [Automating Nmap Scans, page 62-5](#). Also note that if the host is deleted from the network map, any Nmap scan results for that host are discarded.

To create a scan target:

Access: Admin/Discovery Admin

Step 1 Select **Policies > Actions > Scanners**.

The Scanners page appears.

Step 2 On the toolbar, click **Targets**.

The Scan Target List page appears.

Step 3 Click **Create Scan Target**.

The Scan Target page appears.

Step 4 In the **Name** field, type the name you want to use for this scan target.

Step 5 In the **IP Range** text box, specify the host or hosts you want to scan, using the following syntax:

- for IPv6 hosts, an exact IP address (for example, `2001:DB8::fedd:eeff`)
- for IPv4 hosts, an exact IP address (for example, `192.168.1.101`) or comma-separated list of IP addresses

- for IPv4 hosts, an IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between 192.168.1.1 and 192.168.1.254, inclusive)

For information on using CIDR notation in the FireSIGHT System, see [IP Address Conventions, page 1-22](#).

- for IPv4 hosts, an IP address range using octet range addressing (for example, `192.168.0-255.1-254` scans all addresses in the `192.168.x.x` range, except those that end in `.0` and `.255`)
- for IPv4 hosts, an IP address range using hyphenation (for example, `192.168.1.1 - 192.168.1.5` scans the 6 hosts between 192.168.1.1 and 192.168.1.5, inclusive)
- for IPv4 hosts, a list of addresses or ranges separated by commas or spaces (for example, for example, `192.168.1.0/24, 194.168.1.0/24` scans the 254 hosts between 192.168.1.1 and 192.168.1.254, inclusive and the 254 hosts between 194.168.1.1 and 194.168.1.254, inclusive)

**Note**

The **IP Range** text box accepts up to 255 characters. In addition, note that if you use a comma in a list of IP addresses or ranges in a scan target, the comma converts to a space when you save the target.

Step 6 In the **Ports** field, specify the ports you want to scan.

You can enter any of the following, using values from 1 to 65535:

- a port number
- a list of ports separated by commas
- a range of port numbers separated by a dash
- ranges of port numbers separated by dashes, separated by commas

Step 7 Click **Save**.

The scan target is created.

Creating an Nmap Remediation

License: FireSIGHT

You can define the settings for an Nmap scan by creating an Nmap remediation. An Nmap remediation can be used as a response in a correlation policy, run on demand, or scheduled to run at a specific time. In order for the results of an Nmap scan to appear in the network map, the scanned host must already exist in the network map.

For more information on the specific settings in an Nmap remediation, see [Understanding Nmap Remediations, page 47-2](#).

Note that Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host for operating system and server data using Nmap, you may want to set up regularly scheduled scans to keep any Nmap-supplied operating system and server data up-to-date. For more information, see [Automating Nmap Scans, page 62-5](#). Also note that if the host is deleted from the network map, any Nmap scan results for that host are discarded.

For general information about Nmap functionality, refer to the Nmap documentation at <http://insecure.org>.

To create an Nmap remediation:**Access:** Admin/Discovery Admin**Step 1** Select **Policies > Actions > Scanners**.

The Scanners page appears.

Step 2 Click **Add Remediation** next to the scan instance where you want to add a remediation.

The Edit Remediation page appears.

Step 3 In the **Remediation Name** field, type a name for the remediation that includes 1 to 63 alphanumeric characters, with no spaces and no special characters other than underscore (_) and dash (-).**Step 4** In the **Description** field, type a description for the remediation that includes 0 to 255 alphanumeric characters, including spaces and special characters.**Step 5** If you plan to use this remediation in response to a correlation rule that triggers on an intrusion event, a connection event, or a user event, configure the **Scan Which Address(es) From Event?** option:

- Select **Scan Source and Destination Addresses** to scan the hosts represented by the source IP address and the destination IP address in the event.
- Select **Scan Source Address Only** to scan the host represented by the event's source IP address.
- Select **Scan Destination Address Only** to scan the host represented by the event's destination IP address.

If you plan to use this remediation in response to a correlation rule that triggers on a discovery event or a host input event, by default the remediation scans the IP address of the host involved in the event; you do not need to configure this option.

**Note**

Do **not** assign an Nmap remediation as a response to a correlation rule that triggers on a traffic profile change.

Step 6 Configure the **Scan Type** option:

- To scan quickly in stealth mode on hosts where the `admin` account has raw packet access or where IPv6 is not running, by initiating TCP connections but not completing them, select **TCP Syn Scan**.
- To scan by using a system `connect()` call, which can be used on hosts where the `admin` account on your Defense Center does not have raw packet access or where IPv6 is running, select **TCP Connect Scan**.
- To send an ACK packet to check whether ports are filtered or unfiltered, select **TCP ACK Scan**.
- To send an ACK packet to check whether ports are filtered or unfiltered but also to determine whether a port is open or closed, select **TCP Window Scan**.
- To identify BSD-derived systems using a FIN/ACK probe, select **TCP Maimon Scan**.

Step 7 Optionally, to scan UDP ports in addition to TCP ports, select **On** for the **Scan for UDP ports** option.**Tip**

A UDP portscan takes more time than a TCP portscan. To speed up your scans, leave this option disabled.

Step 8 If you plan to use this remediation in response to correlation policy violations, configure the **Use Port From Event** option:

- Select **On** to scan the port in the correlation event, rather than the ports you specify in step 11.

If you scan the port in the correlation event, note that the remediation scans the port on the IP addresses that you specified in step 5. These ports are also added to the remediation's dynamic scan target.

- Select **Off** to scan only the ports you will specify in step 11.

Step 9 If you plan to use this remediation in response to correlation policy violations and want to run the scan using the appliance running the detection engine that detected the event, configure the **Scan from reporting detection engine** option:

- To scan from the appliance running the reporting detection engine, select **On**.
- To scan from the appliance configured in the remediation, select **Off**.

Step 10 Configure the **Fast Port Scan** option:

- To scan only the ports listed in the `nmap-services` file located in the `/var/sf/nmap/share/nmap/nmap-services` directory on the device that does the scanning, ignoring other port settings, select **On**.
- To scan all TCP ports, select **Off**.

Step 11 In the **Port Ranges and Scan Order** field, type the ports you want to scan by default, using Nmap syntax, in the order you want to scan those ports.

Specify values from 1 to 65535. Separate ports using commas or spaces. You can also use a hyphen to indicate a port range. When scanning for both TCP and UDP ports, preface the list of TCP ports you want to scan with a T and the list of UDP ports with a U. For example, to scan ports 53 and 111 for UDP traffic, then scan ports 21-25 for TCP traffic, enter `U:53,111,T:21-25`.

Note that the **Use Port From Event** option overrides this setting when the remediation is launched in response to a correlation policy violation, as described in step 8.

Step 12 To probe open ports for server vendor and version information, configure **Probe open ports for vendor and version information**:

- Select **On** to scan open ports on the host for server information to identify server vendors and versions.
- Select **Off** to continue using Cisco server information for the host.

Step 13 If you choose to probe open ports, set the number of probes used by selecting a number from the **Service Version Intensity** drop-down list:

- To use more probes for higher accuracy with a longer scan, select a higher number.
- To use fewer probes for less accuracy with a faster scan, select a lower number.

Step 14 To scan for operating system information, configure **Detect Operating System** settings:

- Select **On** to scan the host for information to identify the operating system.
- Select **Off** to continue using Cisco operating system information for the host.

Step 15 To determine whether host discovery occurs and whether port scans are only run against available hosts, configure **Treat All Hosts As Online**:

- To skip the host discovery process and run a port scan on every host in the target range, select **On**.
- To perform host discovery using the settings for **Host Discovery Method** and **Host Discovery Port List** and skip the port scan on any host that is not available, select **Off**.

Step 16 Select the method you want Nmap to use when it tests for host availability:

- To send an empty TCP packet with the SYN flag set and elicit an RST response on a closed port or a SYN/ACK response on an open port on available hosts, select **TCP SYN**.

Note that this option scans port 80 by default and that TCP SYN scans are less likely to be blocked by a firewall with stateful firewall rules.

- To send an empty TCP packet with the ACK flag set and elicit an RST response on available hosts, select **TCP ACK**.

Note that this option scans port 80 by default and that TCP ACK scans are less likely to be blocked by a firewall with stateless firewall rules.

- To send a UDP packet to elicit port unreachable responses from closed ports on available hosts, select **UDP**. This option scans port 40125 by default.

- Step 17** If you want to scan a custom list of ports during host discovery, type a list of ports appropriate for the host discovery method you selected, separated by commas, in the **Host Discovery Port List** field.
- Step 18** Configure the **Default NSE Scripts** option to control whether to use the default set of Nmap scripts for host discovery and server, operating system, and vulnerability discovery:
- To run the default set of Nmap scripts, select **On**.
 - To skip the default set of Nmap scripts, select **Off**.
- See <http://nmap.org/nsedoc/categories/default.html> for the list of default scripts.
- Step 19** To set the timing of the scan process, select a timing template number; select a higher number for a faster, less comprehensive scan and a lower number for a slower, more comprehensive scan.
- Step 20** Click **Save**, then click **Done**.
The remediation is created.
-

Managing Nmap Scanning

License: FireSIGHT

You can modify or delete Nmap scan instances and remediations as needed. You can also run an on-demand Nmap scan. You can also view or download Nmap results for previous scans. For more information, see the following sections:

- [Managing Nmap Scan Instances, page 47-14](#)
- [Managing Nmap Remediations, page 47-15](#)
- [Running an On-Demand Nmap Scan, page 47-16](#)

Managing Nmap Scan Instances

License: FireSIGHT

You can edit or delete Nmap scan instances. For more information, see the following sections:

- [Editing an Nmap Scan Instance, page 47-14](#)
- [Deleting an Nmap Scan Instance, page 47-15](#)

Editing an Nmap Scan Instance

License: FireSIGHT

Use the following procedure to modify scan instances. Note that you can view, add, and delete remediations associated with the instance when you modify it.

To edit a scan instance:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Click **View** next to the instance you want to edit.
The Instance Detail page appears.
- Step 3** Optionally, click **View** next to the remediation you want to view or edit.
For more information on editing remediations, see [Editing an Nmap Remediation, page 47-16](#).
- Step 4** Optionally, click **Delete** next to the remediation you want to delete.
For more information on deleting remediations, see [Deleting an Nmap Remediation, page 47-16](#).
- Step 5** Optionally, click **Add** to add a new remediation to this scan instance.
For more information on creating new remediations, see [Managing Nmap Remediations, page 47-15](#).
- Step 6** Optionally, make changes to the scan instance settings, then click **Save**.
- Step 7** Click **Done**.
The scan instance is modified.
-

Deleting an Nmap Scan Instance

License: FireSIGHT

Delete an Nmap scan instance when you no longer want to use the Nmap module profiled in the instance. Note that when you delete the scan instance, you also delete any remediations that use that instance.

To delete a scan instance:

Access: Admin/Discovery Admin

-
- Step 1** Click **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Click **Delete** next to the scan instance you want to delete.
The instance is deleted.
-

Managing Nmap Remediations

License: FireSIGHT

You can edit or delete Nmap remediations. For more information, see the following sections:

- [Editing an Nmap Remediation, page 47-16](#)

- [Deleting an Nmap Remediation, page 47-16](#)

Editing an Nmap Remediation

License: FireSIGHT

Modifications you make to Nmap remediations do not affect scans in progress. The new settings take effect when the next scan starts.

To edit an Nmap remediation:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Next to the remediation you want to edit, click **View**.
The Remediation Edit page appears.
- Step 3** Make modifications as necessary.
For information on the settings you can change, see [Creating an Nmap Remediation, page 47-11](#).
- Step 4** Click **Save**, then click **Done**.
The remediation is modified.
-

Deleting an Nmap Remediation

License: FireSIGHT

Delete an Nmap remediation if you no longer need it.

To delete an Nmap remediation:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Next to the remediation you want to delete, click **Delete**.
- Step 3** Confirm that you want to delete the remediation.
The remediation is deleted.
-

Running an On-Demand Nmap Scan


License: FireSIGHT

You can launch on-demand Nmap scans whenever needed. You can specify the target for an on-demand scan by entering the IP addresses and ports you want to scan or by selecting an existing scan target.

Note that Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, you may want to set up regularly scheduled scans to keep any Nmap-supplied operating system and server data up to date. For more information, see [Automating Nmap Scans, page 62-5](#). In addition, note that if the host is deleted from the network map, any Nmap scan results are discarded.

To run an on-demand Nmap scan:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** Next to the Nmap remediation you want to use to perform the scan, click **Scan**.
The Nmap Scan Target dialog box appears.
- Step 3** Optionally, to scan using a saved scan target, select a target from the **Saved Targets** drop-down list and click **Load**.
The IP addresses and ports associated with the scan target populate the **IP Range(s)** and **Ports** fields.
-
-  **Tip** To create a scan target, click **Edit/Add Targets**. For more information, see [Creating an Nmap Scan Target, page 47-10](#).
-
- Step 4** In the **IP Range(s)** field, specify the IP address for hosts you want to scan or modify the loaded list, up to 255 characters.
For hosts with IPv4 addresses, you can specify multiple IP addresses separated by commas or use CIDR notation. You can also negate IP addresses by preceding them with an exclamation point (!). For information on using CIDR notation in the FireSIGHT System, see [IP Address Conventions, page 1-22](#).
For hosts with IPv6 addresses, use an exact IP address. Ranges are not supported.
- Step 5** In the **Ports** field, specify the ports you want to scan or modify the loaded list.
You can enter a port number, a list of ports separated by commas, or a range of port numbers separated by a dash. For details on entering ports, see [Specifying Ports in Searches, page 60-7](#).
- Step 6** Click **Scan Now**.
The Nmap server performs the scan.
Note that Nmap validates IP address ranges and displays an error message if the range is invalid. If this occurs, correct the contents of the **IP Range(s)** field to indicate a valid IP address range.
-

Managing Scan Targets

License: FireSIGHT

When you configure an Nmap module, you can create and save scan targets that identify the hosts and ports you want to target when you perform an on-demand or a scheduled scan, so that you do not have to construct a new scan target every time. A scan target includes a single IP address or a block of IP

addresses to scan, as well as the ports on the host or hosts. For Nmap targets, you can also use Nmap octet range addressing or IP address ranges. For more information on Nmap octet range addressing, refer to the Nmap documentation at <http://insecure.org>.

Note that scans for scan targets containing a large number of hosts can take an extended period of time. As a workaround, scan fewer hosts at a time.

After you create a scan target, you can modify or delete it.

For more information, see the following sections:

- [Creating an Nmap Scan Target, page 47-10](#)
- [Editing a Scan Target, page 47-18](#)
- [Deleting a Scan Target, page 47-18](#)

Editing a Scan Target

License: FireSIGHT

You can modify scan targets you created.



Tip

You might want to edit a remediation's dynamic scan target if you do not want to use the remediation to scan a specific IP address, but the IP address was added to the target because the host was involved in a correlation policy violation that launched the remediation.

To edit an existing scan target:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** On the toolbar, click **Targets**.
The Scan Target List page appears.
- Step 3** Click **Edit** next to the scan target you want to edit.
The Scan Target page appears.
- Step 4** Make modifications as necessary and click **Save**.
The scan target is updated.
-

Deleting a Scan Target

License: FireSIGHT

Delete a scan target if you no longer want to scan the hosts listed in it.

To delete a scan target:

Access: Admin/Discovery Admin

-
- Step 1** Select **Policies > Actions > Scanners**.
The Scanners page appears.
- Step 2** On the toolbar, click **Targets**.
The Scan Target List page appears.
- Step 3** Next to the scan target you want to delete, click **Delete**.
The scan target is deleted.
-

Working with Active Scan Results

License: FireSIGHT

For information on how to monitor Nmap scans in progress, import results from scans previously performed through the FireSIGHT System or results performed outside the FireSIGHT System, and view and analyze scan results, see the following sections:

- [Viewing Scan Results, page 47-19](#)
- [Understanding the Scan Results Table, page 47-21](#)
- [Analyzing Scan Results, page 47-21](#)
- [Monitoring Scans, page 47-21](#)
- [Importing Scan Results, page 47-22](#)
- [Searching for Scan Results, page 47-22](#)

Viewing Scan Results

License: FireSIGHT

You can view a table of scan results, and then manipulate the event view depending on the information you are looking for.

The page you see when you access scan results differs depending on the workflow you use. You can use the predefined workflow, which includes a table view of scan results.

You can also create a custom workflow that displays only the information that matches your specific needs. For information on creating a custom workflow, see [Creating Custom Workflows, page 58-39](#).

The following table describes some of the specific actions you can perform on a scan results workflow page.

Table 47-2 *Scan Results Table Functions*

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Scan Results Table, page 47-21 .
modify the time and date range for the scan result	click the time range link. For more information, see Setting Event Time Constraints, page 58-23 .

Table 47-2 Scan Results Table Functions (continued)

To...	You can...
sort scan results	click the column title. Click the column title again to reverse the sort order.
constrain the columns that appear	<p>click the close icon (✕) in the column heading that you want to hide. In the pop-up window that appears, click Apply.</p> <p>Tip To hide or show other columns, select or clear the appropriate check boxes before you click Apply. To add a disabled column back to the view,</p> <p>Click the expand arrow (▶) to expand the search constraints, then click the column name under Disabled Columns.</p>
drill down to the next page in the workflow, constraining on a specific value	<p>use one of the following methods:</p> <ul style="list-style-type: none"> on a drill-down page that you created in a custom workflow, click a value within a row. Note that clicking a value within a row in a table view constrains the table view and does not drill down to the next page. To drill down to the next workflow page constraining on some users, select the check boxes next to the users you want to view on the next workflow page, then click View. To drill down to the next workflow page keeping the current constraints, click View All. <p>Tip Table views always include “Table View” in the page name.</p> <p>For more information, see Constraining Events, page 58-31.</p>
configure scan instances and remediations	<p>Click Scanners in the toolbar.</p> <p>For more information, see Setting up Nmap Scans, page 47-9.</p>
navigate within and between workflow pages	find more information in Using Workflow Pages, page 58-18 .
navigate to other event views to view associated events	the name of the event view you want to see from the Jump to drop-down list. For more information, see Navigating Between Workflows, page 58-36 .
search for scan results	click Search . For more information, see Searching for Scan Results, page 47-22 .

To view scan results:

Access: Admin/Discovery Admin

Step 1 Select **Policies > Actions > Scanners**.

Step 2 Click **Scan Results**.

The first page of the default scan results workflow appears. To use a different workflow, including a custom workflow, click (**switch workflows**) by the workflow title. For information on specifying a different default workflow, see [Configuring Event View Settings, page 71-3](#).

Understanding the Scan Results Table

License: FireSIGHT

When you run an Nmap scan, the Defense Center collects the scan results in a database. The fields in the scan results table are described in the following table.

Table 47-3 Scan Results Fields

Field	Description
Start Time	The date and time that the scan that produced the results started.
End Time	The date and time that the scan that produced the results ended.
Scan Target	The IP address (or host name, if DNS resolution is enabled) of the scan target for the scan that produced the results.
Scan Type	Either <code>Nmap</code> or the name of the third-party scanner to indicate the type of the scan that produced the results.
Scan Mode	The mode of the scan that produced the results: <ul style="list-style-type: none"> • <code>On Demand</code> — results from scans run on demand. • <code>Imported</code> — results from scans on a different system and imported onto the Defense Center. • <code>Scheduled</code> — results from scans run as a scheduled task.

Analyzing Scan Results

License: FireSIGHT

You can view scan results that you create using the local Nmap module as a rendered page in a pop-up window. You can also download the Nmap results file in raw XML format.

You can also view operating system and server information detected by Nmap in host profiles and in the network map. If a scan of a host produces server information for servers on filtered or closed ports, or if a scan collects information that cannot be included in the operating system information or the servers section, the host profile includes those results in an Nmap Scan Results section. For more information, see [Viewing Host Profiles, page 49-5](#).

Monitoring Scans

License: FireSIGHT

You can check the progress of an Nmap scan and cancel scan jobs currently in progress. Scan results provide the start time and end time of each scan. Also, after a scan is completed, you can also view the scan results as a rendered page in a pop-up window. Nmap results you can download and view using the Nmap Version 1.01 DTD, available at <http://insecure.org>. You can also clear scan results.

To monitor a scan:

Access: Admin/Discovery Admin

Step 1 Select **Policies > Actions > Scanners**.

Step 2 Click **Scan Results**.

The first page of the default scan results workflow appears. To use a different workflow, including a custom workflow, click (**switch workflows**) by the workflow title. For information on specifying a different default workflow, see [Configuring Event View Settings, page 71-3](#).

**Tip**

If you are using a custom workflow that does not include the table view of scan results, click (**switch workflows**) by the workflow title, then select **Scan Results**.

Step 3 You can perform the following actions:

- To view the scan results as a rendered page in a pop-up window, click **View** next to the scan job.
- To save a copy of the scan results file so that you can view the raw XML code in any text editor, click **Download** next to the scan job.

Importing Scan Results

License: FireSIGHT

You can import XML results files created by an Nmap scan performed outside of the FireSIGHT System. You can also import XML results files that you previously downloaded from the FireSIGHT System. To import Nmap scan results, the results file must be in XML format and adhere to the Nmap Version 1.01 DTD. For more information on creating Nmap results and on the Nmap DTD, refer to the Nmap documentation at <http://insecure.org>. For information on downloading XML results from the FireSIGHT System, see [Monitoring Scans, page 47-21](#).

Note that a host must exist in the network map before Nmap can append its results to the host profile.

To import results:

Access: Admin/Discovery Admin

Step 1 Select **Policies > Actions > Scanners**.

The Scan Instances page appears.

Step 2 On the toolbar, click **Import Results**.

The Import Results page appears.

Step 3 Click **Browse** to navigate to the results file.**Step 4** After you return to the Import Results page, click **Import** to import the results.

The results file is imported.

Searching for Scan Results

License: FireSIGHT

You can search for Nmap or third-party scan results for any scans run on an appliance or managed appliance in your FireSIGHT System.

Table 47-4 Scan Results Search Criteria

Field	Search Criteria Rules
Start Time	Type the date and time that the scan that produced the results started. See Specifying Time Constraints in Searches, page 60-5 for the syntax for entering time.
End Time	Type the date and time that the scan that produced the results ended. See Specifying Time Constraints in Searches, page 60-5 for the syntax for entering time.
Scan Target	Type the IP address (or host name, if DNS resolution is enabled) of the scan target for the scan that produced the results. Use a specific IP address or CIDR notation to specify a range of IP addresses. See Specifying IP Addresses in Searches, page 60-6 for a full description of the syntax allowed for IP addresses.
Scan Type	Type <code>Nmap</code> or a third-party scanner ID to indicate the type of the scan that produced the results.
Scan Mode	Type the mode of the scan that produced the results: <ul style="list-style-type: none"> • Type <code>On Demand</code> to retrieve results from scans run on demand. • Type <code>Imported</code> to retrieve results from scans on a different system and imported onto the Defense Center. • Type <code>Scheduled</code> to retrieve results from scans run as a scheduled task.

For more information on searching, including how to load and delete saved searches, see [Searching for Events, page 60-1](#).

To search for scan results:

Access: Admin/Discovery Admin

- Step 1** Select **Analysis > Search**, then select **Scan Results** from the table drop-down list.
The Scan Results search page appears.



Tip To search the database for a different kind of event, select it from the table drop-down list.

- Step 2** Enter your search criteria in the appropriate fields, as described in the [Scan Results Search Criteria](#) table.
If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields.

- Step 3** Optionally, if you plan to save the search, you can select the **Private** check box to save the search as private so only you can access it. Otherwise, leave the check box clear to save the search for all users.



Tip If you want to save a search as a restriction for custom user roles with restricted privileges, you **must** save it as a private search.

- Step 4** Optionally, you can save the search to be used again in the future. You have the following options:
- Click **Save** to save the search criteria.

For a new search, a dialog box appears prompting for the name of the search; enter a unique search name and click **Save**. If you save new criteria for a previously-existing search, no prompt appears. The search is saved (and visible only to your account if you selected **Private**) so that you can run it at a later time.

- Click **Save As New** to save a new search or assign a name to a search you created by altering a previously-saved search.

A dialog box appears prompting for the name of the search; enter a unique search name and click **Save**. The search is saved (and visible only to your account if you selected **Private**) so that you can run it at a later time.

Step 5 Click **Search** to start the search.

Your search results appear.
