Working with Discovery Events

Discovery events alert you to the activity on your network and provide you with the information you need to respond appropriately. They are triggered by the changes that your managed devices detect in the network segments they monitor. Your *network discovery policy* specifies the kinds of data the system collects, the monitored network segments, and the specific hardware interfaces that your system uses to monitor traffic. For more information on network discovery, see Understanding Discovery Data Collection, page 45-1.

As a simple example of a discovery event, you may have conference rooms or spare work spaces where visiting employees attach to your network. You would expect to see New Host events generated on these segments on a regular basis, and you would not suspect malicious intent. However, if you see a New Host event on a network segment that is locked down, then you can escalate your response accordingly.

User discovery events provide information about users logged into the hosts on your network. You can view events that catalog user activity on the network and drill down to view information on a particular user. For example, if you want to see what user is associated with a new host, you can check the host profile to find out what users have been detected in traffic going to or from that host.

Discovery events provide you with much greater depth of insight into the activity on your network and with much more granularity than this simple example shows. For each monitored host, you can configure the system to detect related application protocols, network protocols, clients, users, and potential vulnerabilities. The system can also provide information on vulnerabilities detected by third-party scanners that you import onto the Defense Center using the host input feature. Indications of compromise (IOC) use intrusion, malware, and other data to identify hosts whose security may be compromised. In addition, you can track any changes in host criticality, host attribute, or vulnerability settings that users enter via the user interface.

The system provides a set of predefined workflows that you can use to analyze the discovery events that your system generates. You can also create custom workflows that display only the information that matches your specific needs.

To collect and store network discovery data for analysis, make sure that your network discovery policy is configured to discover the appropriate data on the networks and zones where your Cisco-managed devices and NetFlow-enabled devices monitor traffic. To exclude monitored areas from discovery, configure that in the network discovery policy. Note that an access control policy must be applied to the managed device before you can apply a network discovery policy. For more information, see Creating a Network Discovery Policy, page 45-22.

For more information, see:

- Viewing Discovery Event Statistics, page 50-2
- Viewing Discovery Performance Graphs, page 50-5
- Understanding Discovery Event Workflows, page 50-6

Viewing Discovery Event Statistics

License: FireSIGHT

The Discovery Statistics page displays a summary of the hosts, events, protocols, application protocols, and operating systems detected by the system:

- The statistics summary provides general statistics about the total events, application protocols, hosts, network devices, and information about your host limit usage; see Statistics Summary, page 50-3.
- The event breakdown provides statistics about the types of events occurring on the system; see Event Breakdown, page 50-4.
- The protocol breakdown provides statistics about the protocols that detected hosts are using. See Protocol Breakdown, page 50-4.
- The application protocol breakdown provides statistics about the application protocols running on the network; see Application Protocol Breakdown, page 50-4.
- The operating system breakdown lists the operating systems that are running on the network and how many hosts are using each operating system; see OS Breakdown, page 50-5.

The page lists statistics for the last hour and the total accumulated statistics. You can select statistics for a particular device, or all devices. You can also view events that match the entries on the page by clicking the event, server, operating system, or operating system vendor listed within the summary.

To view the Discovery Statistics Summary:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Summary > Discovery Statistics**.

The statistics summary page appears.

Step 2 From the **Select Device** list, select the device whose statistics you want to view. Select **All** to view statistics for all devices managed by the Defense Center.

Statistics Summary

License: FireSIGHT

The statistics summary provides general statistics about the total events, application protocols, hosts, network devices, and information about your host limit usage.

Descriptions of the rows of the Statistics Summary section follow.

Total Events

Total number of discovery events stored on the Defense Center.

Total Events Last Hour

Total number of discovery events generated in the last hour.

Total Events Last Day

Total number of discovery events generated in the last day.

Total Application Protocols

Total number of application protocols from servers running on detected hosts.

Total IP Hosts

Total number of detected hosts identified by unique IP address.

Total MAC Hosts

Total number of detected hosts not identified by IP address.

Note that the Total MAC Hosts statistic remains the same whether you are viewing discovery statistics for all devices or for a specific device. This is so because managed devices discover hosts based on their IP addresses. This statistic gives the total of all hosts that are identified by other means and is independent of a given managed device.

Total Routers

Total number of detected nodes identified as routers.

Total Bridges

Total number of detected nodes identified as bridges.

Host Limit Usage

Total percentage of the host limit currently in use. The host limit is defined by your FireSIGHT license. Note that the host limit usage only appears if you are viewing statistics for all managed devices. For more information on monitoring host usage, see Configuring FireSIGHT Host Usage Monitoring, page 68-16.

Note If the host limit is reached and a host is deleted, the host will not reappear on the network map until you restart network discovery on all managed devices configured to perform discovery.

Last Event Received

The date and time that the most recent discovery event occurred.

Last Connection Received

The date and time that the most recent connection was completed.

Event Breakdown

License: FireSIGHT

The Event Breakdown section lists a count of each type of network discovery and host input event that occurred within the last hour, as well as a count of the total number of each event type stored in the database. For full descriptions of each event type, see Understanding Discovery Event Types, page 50-9 and Understanding Host Input Event Types, page 50-13.

You can also use the Event Breakdown section to view details on discovery and host input events.

To view network discovery and host input events by type:

Access: Admin/Any Security Analyst

Step 1 Click the type of event you want to view.

The first page of the default discovery events workflow appears, constrained by the event type you picked. To use a different workflow, including a custom workflow, click **(switch workflow)** by the workflow title. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3. If no events appear, you may need to adjust the time range; see Setting Event Time Constraints, page 58-23.

For information on working with discovery events, see Working with Discovery and Host Input Events, page 50-8.

Protocol Breakdown

License: FireSIGHT

The Protocol Breakdown section lists the protocols currently in use by detected hosts. It displays each detected protocol name, its “layer” in the protocol stack, and the total number of hosts that communicate using the protocol.

Application Protocol Breakdown

License: FireSIGHT

The Application Protocol Breakdown section lists the application protocols that are currently in use by detected hosts. It lists the protocol name, the total number of hosts running the application protocol in the past hour, and the total number of hosts that have been detected running the protocol at any point.

You can also use the Application Protocol Breakdown section to view details on servers using the detected protocols.

To view servers that use a listed application protocol:

Access: Admin/Any Security Analyst

Step 1 Click the name of the application protocol you want to view.

The first page of the default servers workflow appears, constrained by the application protocol you picked. To use a different workflow, including a custom workflow, click **(switch workflow)** by the workflow title. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

For information on working with servers, see Working with Servers, page 50-35.

OS Breakdown

License: FireSIGHT

The OS Breakdown section lists the operating systems currently running on the monitored network, along with their vendors and the total number of hosts running each operating system.

A value of `unknown` for the operating system name or version means that the operating system or its version does not match any of the system's fingerprints. A value of `pending` means that the system has not yet gathered enough information to identify the operating system or its version.

You can use the OS Breakdown section to view details on the detected operating systems.

To view hosts by operating system or vendor:

Access: Admin/Any Security Analyst

Step 1 You have two options:

- To view all hosts running a specific operating system, under **OS Name**, click the operating system name.
- To view all hosts running any operating system from a specific vendor, under **OS Vendor**, click the vendor name.

The first page of the default hosts workflow appears, constrained by the operating system or vendor you picked. To use a different workflow, including a custom workflow, click **(switch workflow)** by the workflow title. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

For information on working with hosts, see Working with Hosts, page 50-18.

Viewing Discovery Performance Graphs

License: FireSIGHT

You can generate graphs that display performance statistics for managed devices with discovery events.

Note New data is accumulated for statistics graphs every five minutes. Therefore, if you reload a graph quickly, the data may not change until the next five-minute increment occurs.

Descriptions of the available graph types follow.

Processed Events/Sec

Displays a graph that represents the number of events that the Data Correlator processes per second

Processed Connections/Sec

Displays a graph that represents the number of connections that the Data Correlator processes per second

Generated Events/Sec

Displays a graph that represents the number of events that the system generates per second

Mbits/Sec

Displays a graph that represents the number of megabits of traffic that are analyzed by the discovery process per second

Avg Bytes/Packet

Displays a graph that represents the average number of bytes included in each packet analyzed by the discovery process

K Packets/Sec

Displays a graph that represents the number of packets analyzed by the discovery process per second, in thousands

To generate discovery performance graphs:

Access: Admin/Maint

Step 1 Select **Overview > Summary > Discovery Performance.**

The Discovery Performance page appears.

Step 2 From the **Select Device** list, select the Defense Center or managed devices you want to include.

Depending on which appliance you select, the **Select Graph(s)** list adjusts to display the available graphs.

Step 3 From the **Select Graph(s)** list, select the type of graph you want to create.

Tip You can select multiple graphs by holding down the Ctrl or Shift keys while clicking on the graph type.

Step 4 From the **Select Time Range** list, select the time range you would like to use for the graph. You can choose from last hour, last day, last week, or last month.

Step 5 Click **Graph** to graph the selected statistics.

The selected graph appears.

Understanding Discovery Event Workflows

License: FireSIGHT

The Defense Center provides a set of workflows that you can use to analyze the discovery events that are generated for your network. The workflows are, along with the network map, a key source of information about your network assets. These workflows contain tables that are populated with discovery data generated by the system.

Access network discovery workflows from the **Analysis > Hosts** menu. The Defense Center provides predefined workflows for discovery events, as well as for detected hosts and their host attributes, servers, applications, application details, vulnerabilities, user activities, and users. You can also create custom workflows. For more information on workflows, see Understanding and Using Workflows, page 58-1.

Tip Select **Analysis > Custom > Custom Tables** to access workflows based on custom tables.

When you are using a network discovery workflow, you can perform many common actions, whatever the type of event. These common functions are described in the Common Discovery Event Actions table.

Table 50-1 Common Discovery Event Actions

To...	You can...
view the host profile for an IP address	click the host profile icon ( ) or, for hosts with active indications of compromise (IOC) tags, the compromised host icon ( ) that appears next to the IP address. For information on IOC, see Working with Indications of Compromise, page 50-31.
view user profile information	click the user icon ( ) that appears next to the user identity. For more information, see Understanding User Details and Host History, page 50-62.
sort data	click the column title. Click the column title again to reverse the sort order.
drill down to the next page in the workflow	use one of the following methods: • To drill down to the next workflow page constraining on a specific value, click a value within a row. Note that this only works on drill-down pages. Clicking a value within a row in a table view only constrains the table view and does not drill down to the next page. • To drill down to the next workflow page constraining on some events, select the check boxes next to the events 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**. **Tip** Table views always include “Table View” in the page name. For more information, see Constraining Events, page 58-31.
constrain the columns that appear	click the close icon (✖) in the column heading that you want to hide. In the pop-up window that appears, click **Apply**. **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, click the expand arrow to expand the search constraints, then click the column name under Disabled Columns.
navigate within the current workflow page	find more information in Navigating to Other Pages in the Workflow, page 58-35.
navigate between pages in the current workflow, keeping the current constraints	click the appropriate page link at the top left of the workflow page. For more information, see Using Workflow Pages, page 58-18.

Table 50-1 Common Discovery Event Actions (continued)

To...	You can...
delete items from the system, including: • discovery and host input events from discovery event workflows • hosts and network devices from host workflows • host attributes from host attribute workflows • servers from server workflows • applications from application workflows • third-party vulnerabilities from third-party vulnerability workflows • users from user workflows	use one of the following methods: • To delete some items, select the check boxes next to items you want to delete, then click **Delete**. • To delete all items in the current constrained view, click **Delete All**, then confirm you want to delete all the items. These items remain deleted until the system's discovery function is restarted, when they may be detected again. **Tip** See Purging Discovery Data from the Database, page B-1 for information on deleting all discovery events from the database and also for information on how to restart discovery. Note that you **cannot** delete Cisco (as opposed to third-party) vulnerabilities; you can, however, mark them reviewed. For more information, see Working with Vulnerabilities, page 50-49.
navigate to other event views to view associated events	find more information in Navigating Between Workflows, page 58-36.

Working with Discovery and Host Input Events

License: FireSIGHT

The system generates discovery events that communicate the details of changes in your monitored network segments. *New* events are generated for newly discovered network features, and change events are generated for any change in previously identified network assets.

During its initial network discovery phase, the system generates new events for each host and any TCP or UDP servers discovered running on each host. Optionally, you can configure the system to use data exported by NetFlow-enabled devices to generate these new host and server events.

In addition, the system generates new events for each network, transport, and application protocol running on each discovered host. When you create a discovery rule configured to include NetFlow-enabled devices, you can disable detection of application protocols. However, you cannot disable application detection in discovery rules that do not use a configured NetFlow-enabled device. If you enable host or user discovery in non-NetFlow discovery rules, applications are automatically discovered.

After the initial network mapping is complete, the system continuously records network changes by generating change events. Change events are generated whenever the configuration of a previously discovered asset changes.

When a discovery event is generated, it is logged to the database. You can use the Defense Center web interface to view, search, and delete discovery events.You can also use discovery events in correlation rules. Based on the type of discovery event generated as well as other criteria that you specify, you can build correlation rules that, when used in a correlation policy, launch remediations and syslog, SNMP, and email alert responses when network traffic meets your criteria.

You can add data to the network map using the host input feature. You can add, modify, or delete operating system information, which causes the system to stop updating that information for that host. You can also manually add, modify, or delete application protocols, clients, servers, and host attributes or modify vulnerability information. When you do this, the system generates host input events.

See the following sections for more information:

Understanding Discovery Event Types

License: FireSIGHT

There are many types of discovery events. For example, the system generates and logs a New Host event when it detects a new host on your monitored network segment. When you view a table of discovery events, the event type is listed in the **Event** column. For more information, see Viewing Discovery and Host Input Events, page 50-14.

Contrast discovery events, which are generated when the system detects a change in your monitored network (such as detecting traffic from a previously undetected host), with host input events, which are generated when a user takes a specific action (such as manually adding a host). For more information on host input events, see Understanding Host Input Event Types, page 50-13.

You can configure the types of discovery events the system logs by modifying your network discovery policy. By default, the system logs all types of discovery events. For more information, see Configuring Database Event Limits, page 63-15.

If you understand the information the different types of discovery events provide, you can more effectively determine which events you want to log and alert on, and how to use these alerts in correlation policies. In addition, knowing the names of the event types can help you craft more effective event searches. Descriptions of the different types of discovery events follow.

Additional MAC Detected for Host

This event is generated when the system detects a new MAC address for a previously discovered host.

This event is often generated when the system detects hosts passing traffic through a router. While each host has a different IP address, they all appear to have the MAC address associated with the router. When the system detects the actual MAC address associated with the IP address, it displays the MAC address in bold text within the host profile and displays an “ARP/DHCP detected” message within the event description in the event view.

Client Timeout

This event is generated when the system drops a client from the database due to inactivity.

Client Update

This event is generated when the system detects a payload (that is, a specific type of content, such as audio, video, or webmail) in HTTP traffic.

DHCP: IP Address Changed

This event is generated when the system detects that a host IP address has changed due to DHCP address assignment.

DHCP: IP Address Reassigned

This event is generated when a host is reusing an IP address; that is, when a host obtains an IP address formerly used by another physical host due to DHCP IP address assignment.

Hops Change

This event is generated when the system detects a change in the number of network hops between a host and the device that detects the host.

This may happen if the device sees host traffic through different routers and is able to make a better determination of the host's location. This may also happen if the device detects an ARP transmission from the host, indicating that the host is on a local segment.

Host Deleted: Host Limit Reached

This event is generated when the host limit on the Defense Center is exceeded and a monitored host is deleted from the Defense Center's network map.

Host Dropped: Host Limit Reached

This event is generated when the host limit on the Defense Center is reached and a new host is dropped. Compare this with the previous event where old hosts are deleted from the network map when the host limit is reached.

To drop new hosts when the host limit is reached, go to **Policies > Network Discovery > Advanced** and set **When Host Limit Reached** to **Drop hosts**. See Configuring Data Storage, page 45-35 for more information.

Host IOC Set

This event is generated when an IOC (Indications of Compromise) is set for a host and generates an alert.

Host Timeout

This event is generated when a host is dropped from the network map because the host has not produced traffic within the interval defined in the network discovery policy. Note that individual host IP addresses and MAC addresses time out individually; a host does not disappear from the network map unless all of its associated addresses have timed out. See Configuring Data Storage, page 45-35 for information about configuring the host timeout value.

If you change the networks you want to monitor in your network discovery policy, you may want to manually delete old hosts from the network map so that they do not count against your FireSIGHT license. For more information, see Working with the Hosts Network Map, page 48-2.

Host Type Changed to Network Device

This event is generated when the system detects that a detected host is actually a network device.

Identity Conflict

This event is generated when the system detects a new server or operating system identity that conflicts with a current active identity for that server or operating system.

If you want to resolve identity conflicts by rescanning the host to obtain newer active identity data, you can use Identity Conflict events to trigger an Nmap remediation. For more information, see Configuring Nmap Remediations, page 54-11.

For more information, see Understanding Identity Conflicts, page 46-6 and Configuring Identity Conflict Resolution, page 45-32. For information on manually resolving conflicts, see Resolving Operating System Identity Conflicts, page 49-14 and Resolving Server Identity Conflicts, page 49-19.

Identity Timeout

This event is generated when identity data that was added to the network map through an active source times out.

If you want to refresh identity data by rescanning the host to obtain newer active identity data, you can use Identity Conflict events to trigger an Nmap remediation. For more information, see Configuring Nmap Remediations, page 54-11.

For more information, see Resolving Server Identity Conflicts, page 49-19.

MAC Information Change

This event is generated when the system detects a change in the information associated with a specific MAC address or TTL value.

This event often occurs when the system detects hosts passing traffic through a router. While each host has a different IP address, they will all appear to have the MAC address associated with the router. When the system detects the actual MAC address associated with the IP address, it displays the MAC address in bold text within the host profile and displays an "ARP/DHCP detected" message within the event description in the event view. The TTL may change because the traffic may pass through different routers or if the system detects the actual MAC address of the host.

NETBIOS Name Change

This event is generated when the system detects a change to a host's NetBIOS name. This event will only be generated for hosts using the NetBIOS protocol.

New Client

This event is generated when the system detects a new client.

Note To collect and store client data for analysis, make sure that you enable application detection in your discovery rules in the network discovery policy. For more information, see Understanding Application Detection, page 45-10.

New Host

This event is generated when the system detects a new host running on the network.

If you select the **Discover** option and select **Hosts** in a network discovery rule where a NetFlow device is selected, this event is also generated when a device processes NetFlow data that involves a new host.

New Network Protocol

This event is generated when the system detects that a host is communicating with a new network protocol (IP, ARP, and so on).

New OS

This event is generated when the system either detects a new operating system for a host, or a change in a host's operating system.

New TCP Port

This event is generated when the system detects a new TCP server port (for example, a port used by SMTP or web services) active on a host. Note that this event is not used to identify the application protocol or the server associated with it; that information is transmitted in the TCP Server Information Update event.

If you select the **Discover** option and select **Applications** in a network discovery rule for NetFlow data, this event is also generated when a device processes NetFlow data involving a server on your monitored networks that does not already exist in the network map.

New Transport Protocol

This event is generated when the system detects that a host is communicating with a new transport protocol, such as TCP or UDP.

New UDP Port

This event is generated when the system detects a new UDP server port running on a host.

If you select the **Discover** option and select **Applications** in a network discovery rule for NetFlow data, this event is also generated when a device processes NetFlow data involving a server on your monitored networks that does not already exist in the network map.

TCP Port Closed

This event is generated when the system detects that a TCP port has closed on a host.

TCP Port Timeout

This event is generated when the system has not detected activity from a TCP port within the interval defined in the system's network discovery policy. See Configuring Data Storage, page 45-35 for information about configuring the server timeout value.

TCP Server Information Update

This event is generated when the system detects a change in a discovered TCP server running on a host.

This event may be generated if a TCP server is upgraded.

UDP Port Closed

This event is generated when the system detects that a UDP port has closed on a host.

UDP Port Timeout

This event is generated when the system has not detected activity from a UDP port within the interval defined in the network discovery policy. See Configuring Data Storage, page 45-35 for information about configuring the server timeout value.

UDP Server Information Update

This event is generated when the system detects a change in a discovered UDP server running on a host.

This event may be generated if a UDP server is upgraded.

VLAN Tag Information Update

This event is generated when the system detects a change in the VLAN tag attributed to a host. For more information about VLAN tags, see Working with VLAN Tags in the Host Profile, page 49-21.

Understanding Host Input Event Types

License: FireSIGHT

There are many types of host input events. For example, the system generates and logs an Add Host event when a user adds a host using the host import feature. When you view a table of discovery events, the event type is listed in the **Event** column. For more information, see Viewing Discovery and Host Input Events, page 50-14.

Contrast host input events, which are generated when a user takes a specific action (such as manually adding a host), with discovery events, which are generated when the system itself detects a change in your monitored network (such as detecting traffic from a previously undetected host). For more information on host input events, see Understanding Discovery Event Types, page 50-9.

You can configure the types of host input events that the system logs by modifying your network discovery policy. By default, the system logs all types of host input events. For more information, see Configuring Database Event Limits, page 63-15.

If you understand the information the different types of host input events provide, you can more effectively determine which events you want to log and alert on, and how to use these alerts in correlation policies. In addition, knowing the names of the event types can help you craft more effective event searches. Descriptions of the different types of host input events follow.

Add Client

This event is generated when a user adds a client.

Add Host

This event is generated when a user adds a host.

Add Protocol

This event is generated when a user adds a protocol.

Add Scan Result

This event is generated when the system adds the results of an Nmap scan to a host.

Add Port

This event is generated when a user adds a server port.

Delete Client

This event is generated when a user deletes a client from the system.

Delete Host/Network

This event is generated when a user deletes an IP address or subnet from the system.

Delete Protocol

This event is generated when a user deletes a protocol from the system.

Delete Port

This event is generated when a user deletes a server port or group of server ports from the system.

Host Attribute Add

This event is generated when a user creates a new host attribute.

Host Attribute Delete

This event is generated when a user deletes a user-defined host attribute.

Host Attribute Delete Value

This event is generated when a user deletes a value assigned to a host attribute.

Host Attribute Set Value

This event is generated when a user sets a host attribute value for a host.

Host Attribute Update

This event is generated when a user changes the definition of a user-defined host attribute.

Set Host Criticality

This event is generated when a user sets or modifies the host criticality value for a host.

Set Operating System Definition

This event is generated when a user sets the operating system for a host.

Set Server Definition

This event is generated when a user sets the vendor and version definitions for a server.

Set Vulnerability Impact Qualification

This event is generated when a vulnerability impact qualification is set.

When a vulnerability is disabled at a global level from being used for impact qualifications, or when a vulnerability is enabled at a global level, this event is generated.

Vulnerability Set Invalid

This event is generated when a user invalidates (or reviews) a vulnerability or vulnerabilities.

Vulnerability Set Valid

This event is generated when a user validates a vulnerability that was previously marked as invalid.

Viewing Discovery and Host Input Events

License: FireSIGHT

Both discovery events and host input events can be viewed using Discovery Events workflows. Discovery events record the detection of network discovery data based on the configured network discovery policy for an appliance. Host input events record the input of host data into the network map through the host input feature. For more information, see Understanding Discovery Event Types, page 50-9 and Understanding Host Input Event Types, page 50-13.

You can use the Defense Center to view a table of discovery or host input events. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access events differs depending on the workflow you use. You can use the predefined workflow, which includes the table view of discovery events and a terminating host view page. 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 Discovery Event Actions table below describes some of the specific actions you can perform on a discovery events workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-2 Discovery Event Actions

To...	You can...
modify the time and date range for displayed events	find more information in Setting Event Time Constraints, page 58-23. Note that events that were generated outside the appliance's configured time window (whether global or event-specific) may appear in an event view if you constrain the event view by time. This may occur even if you configured a sliding time window for the appliance.
learn more about the contents of the columns in the table	find more information in Understanding the Discovery Events Table, page 50-15.

To view discovery events:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Discovery Events**.

The first page of the default discovery events workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3. If no events appear, you may need to adjust the time range; see Setting Event Time Constraints, page 58-23.

Understanding the Discovery Events Table

License: FireSIGHT

The system generates discovery events that communicate the details of changes in your monitored network segments. *New* events are generated for newly discovered network features, and change events are generated for any change in previously identified network assets.

During its initial network discovery phase, the system generates new events for each host and any TCP or UDP servers it discovers on each host. In addition, the system generates new events for each network, transport, or application protocol running on each discovered host. For NetFlow-related traffic, you can control whether the system generates new events when it detects application protocols running on a host. After the initial network mapping is complete, the system continuously records network changes by generating change events. Change events are generated whenever the configuration of a previously discovered host, server, or client changes.

Descriptions of the fields in the discovery events table follow.

Time

The time that the system generated the event.

Event

The event type. See Understanding Discovery Event Types, page 50-9 and Understanding Host Input Event Types, page 50-13 for a description of each available event.

IP Address

The IP address associated with the host involved in the event.

User

The last user to log into the host involved in the event before the event was generated. If only non-authoritative users log in after an authoritative user, the authoritative user remains the current user for the host unless another authoritative user logs in.

MAC Address

The MAC address of the NIC used by the network traffic that triggered the discovery event. This MAC address can be either the actual MAC address of the host involved in the event, or the MAC address of a network device that the traffic passed through.

MAC Vendor

The MAC hardware vendor of the NIC used by the network traffic that triggered the discovery event.

Port

The port used by the traffic that triggered the event, if applicable.

Description

The text description of the event.

Device

The name of the device that generated the event. For new host and new server events based on NetFlow data, this is the device that processed the NetFlow data.

Searching for Discovery Events

License: FireSIGHT

You can search for specific discovery events. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.

  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.

- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation.
- Use the device field to search for specific devices as well as devices in groups, stacks, or clusters. For more information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

Special Search Syntax for Discovery Events

The following table notes search information specific to particular discovery event fields. For more information on discovery event fields, see Understanding the Hosts Table, page 50-20.

Table 50-3 Discovery Event Search Criteria Notes

Field	Search Criteria Notes
Event	The range of event names is listed in Understanding Discovery Event Types, page 50-9 and Understanding Host Input Event Types, page 50-13
MAC Vendor	To search for virtual MAC vendors, that is, for events that involve virtual machines, type `virtual_mac_vendor`. To search for a vendor whose name includes a comma, enclose the entire search term in quotes. Otherwise, the Defense Center treats the term as two searches and returns events that match each search term.
Port	Note that you cannot: • enter a port/protocol combination as you can when searching for other kinds of events • use spaces when specifying port numbers or ranges.

To search for discovery events:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Discovery Events** from the table drop-down list.

The page updates with the appropriate constraints.

Step 3 Enter your search criteria in the appropriate fields, as described in General Search Syntax, page 50-16 and Special Search Syntax for Discovery Events, page 50-17.

If you enter criteria for multiple fields, the search returns only the records that match search cirteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 use the search as a data restriction for a custom user role, you **must** save it as a private search.

Step 5 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 6 Click **Search** to start the search.

Your search results appear in the default discovery events workflow, constrained by the current time range. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Hosts

License: FireSIGHT

The system generates an event when it detects a host and collects information about it to build the host profile. You can use the Defense Center web interface to view, search, and delete hosts.

While viewing hosts, you can create traffic profiles and compliance white lists based on selected hosts. You can also assign host attributes, including host criticality values (which designate business criticality) to groups of hosts. You can then use these criticality values, white lists, and traffic profiles within correlation rules and policies.

Although you can configure the network discovery policy to add hosts to the network map based on data exported by NetFlow-enabled devices, the available information about these hosts is limited. For example, there is no operating system data available for these hosts, unless you provide it using the host input feature. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

For more information, see the following sections:

- Viewing Hosts, page 50-19

Viewing Hosts

License: FireSIGHT

You can use the Defense Center to view a table of hosts that the system has detected. Then, you can manipulate the view depending on the information you are looking for.

The page you see when you access hosts differs depending on the workflow you use. Both predefined workflows terminate in a host view, which contains a host profile for every host that meets your constraints. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The Host Actions table below describes some of the specific actions you can perform on an hosts workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-4 Host Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Hosts Table, page 50-20.
assign a host attribute to selected hosts	find more information in Setting Host Attributes for Selected Hosts, page 50-28.
create traffic profiles for selected hosts	find more information in Creating a Traffic Profile for Selected Hosts, page 50-23.
create a compliance white list based on selected hosts	find more information in Creating a Compliance White List Based on Selected Hosts, page 50-23.

To view hosts:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Hosts**.

The first page of the default hosts workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 hosts, click **(switch workflow)**, then select **Hosts**.

Understanding the Hosts Table

License: FireSIGHT

When the system discovers a host, it collects data about that host. That data can include the host's IP addresses, the operating system it is running, and more. You can view some of that information in the table view of hosts. For more information on the data that the system collects about detected hosts, see Using Host Profiles, page 49-1.

Descriptions of the fields in the hosts table follow below.

Although you can configure the network discovery policy to add hosts to the network map based on data exported by NetFlow-enabled devices, the available information about these hosts is limited. For example, there is no operating system data available for these hosts, unless you provide it using the host input feature. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

Last Seen

The date and time any of the host's IP addresses was last detected by the system. The Last Seen value is updated at least as often as the update interval you configured in the network discovery policy, as well as when the system generates a new host event for any of the host's IP addresses.

For hosts with operating system data updated using the host input feature, the Last Seen value indicates the date and time when the data was originally added.

IP Address

The IP addresses associated with the host.

MAC Address

The host's detected MAC address of the NIC.

The MAC Address field appears in the Table View of Hosts, which you can find in the Hosts workflow. You can also add the MAC Address field to:

- custom tables that include fields from the Hosts table
- drill-down pages in custom workflows based on the Hosts table

MAC Vendor

The host's detected MAC hardware vendor of the NIC.

The MAC Vendor field appears in the Table View of Hosts, which you can find in the Hosts workflow. You can also add the MAC Vendor field to:

- custom tables that include fields from the Hosts table
- drill-down pages in custom workflows based on the Hosts table

Current User

The user identity (username) of the currently logged in user on the host.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Host Criticality

The user-specified criticality value assigned to the host. See the description of the Host Criticality column in Understanding the Host Attributes Table, page 50-27 for more information about this field.

NetBIOS Name

The NetBIOS name of the host. Only hosts running the NetBIOS protocol will have a NetBIOS name.

VLAN ID

VLAN ID used by the host. For more detailed information about VLAN IDs, see Working with VLAN Tags in the Host Profile, page 49-21.

Hops

The number of network hops from the device that detected the host to the host.

Host Type

The type of host (host, mobile device, jailbroken mobile device, router, bridge, NAT device, or load balancer). The methods the system uses to distinguish network devices include:

- the analysis of Cisco Discovery Protocol (CDP) messages, which can identify network devices and their type (Cisco devices only)
- the detection of the Spanning Tree Protocol (STP), which identifies a device as a switch or bridge
- the detection of multiple hosts using the same MAC address, which identifies the MAC address as belonging to a router
- the detection of TTL value changes from the client side, or TTL values that change more frequently than a typical boot time, which identify NAT devices and load balancers

If a device is not identified as a network device, it is categorized as a host.

Hardware

The hardware platform for a mobile device.

OS

The detected operating system (name, vendor, and version) running on the host, or updated using Nmap or the host input feature. This field appears when you invoke the hosts event view from the Custom Analysis widget on the dashboard. It is also a field option in custom tables based on the Hosts table.

Note if the system detects multiple identities, it displays those identities in a comma-separated list.

In this field, a value of `unknown` means that the operating system does not match any of the known fingerprints. A value of `pending` means that the system has not yet gathered enough information to identify the operating system.

OS Vendor

The vendor of the operating system detected on the host or updated using Nmap or the host input feature.

Note if the system detects multiple vendors, it displays those vendors in a comma-separated list.

In this field, a value of `unknown` means that the operating system does not match any of the known fingerprints. A value of `pending` means that the system has not yet gathered enough information to identify the operating system.

OS Name

The detected operating system running on the host or updated using Nmap or the host input feature.

Note if the system detects multiple names, it displays those names in a comma-separated list.

In this field, a value of `unknown` means that the operating system does not match any of the known fingerprints. A value of `pending` means that the system has not yet gathered enough information to identify the operating system.

OS Version

The version of the operating system detected on the host or updated using Nmap or the host input feature.

Note if the system detects multiple versions, it displays those versions in a comma-separated list.

In this field, a value of `unknown` means that the operating system does not match any of the known fingerprints. A value of `pending` means that the system has not yet gathered enough information to identify the operating system.

Source Type

One of the following values for the source of the host's operating system identity:

- User: *`user_name`*
- Application: *`app_name`*
- Scanner: *`scanner_type`* (Nmap or scanner added through network discovery configuration)
- FireSIGHT, for operating systems detected by the system

The system may reconcile data from multiple sources to determine the identity of an operating system; see Understanding Current Identities, page 46-5.

Confidence

One of:

- the percentage of confidence that the system has in the identity of the operating system running on the host, for hosts detected by the system
- 100%, for operating systems identified by an active source, such as the host input feature or Nmap scanner
- `unknown`, for hosts for which the system cannot determine an operating system identity, and for hosts added to the network map based on NetFlow data

Notes

The user-defined content of the Notes host attribute.

Device

Either the managed device that detected the traffic or the device that processed the NetFlow or host input data that added the host to the network map.

If this field is blank, either the host was added to the network map by a device that is not explicitly monitoring the network where the host resides, as defined in the network discovery policy, or the host was added using the host input feature and has not also been detected by the system.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Creating a Traffic Profile for Selected Hosts

License: FireSIGHT

A traffic profile is a profile of the traffic on your network, based on connection data collected over a timespan that you specify. After you create a traffic profile, you can detect abnormal network traffic by evaluating new traffic against your profile, which presumably represents normal network traffic.

You can use the Hosts page to create a traffic profile for a group of hosts that you specify. The traffic profile will be based on connections detected where one of the hosts you specify is the initiating host. Use the sort and search features to isolate the hosts for which you want to create a profile.

To create a traffic profile for selected hosts:

Access: Admin

Step 1 On a table view in the hosts workflow, select the check boxes next to the hosts for which you want to create a traffic profile.

Step 2 At the bottom of the page, click **Create Traffic Profile**.

The Create Profile page appears, populated with the IP addresses of the hosts you specified as the hosts to be monitored.

Step 3 Modify and save the traffic profile according to your specific needs.

For more information on creating traffic profiles, see Creating Traffic Profiles, page 53-1.

Creating a Compliance White List Based on Selected Hosts

License: FireSIGHT

Compliance white lists allow you to specify which operating systems, clients, and network, transport, or application protocols are allowed on your network.

You can use the Hosts page to create a compliance white list based on the host profiles of a group of hosts that you specify. Use the sort and search features to isolate the hosts that you want to use to create a white list.

To create a compliance white list based on selected hosts:

Access: Admin

Step 1 On a table view in the hosts workflow, select the check boxes next to the hosts for which you want to create a white list.

Step 2 At the bottom of the page, click **Create White List**.

The Create White List page appears, populated with the information in the host profiles of the hosts you specified.

Step 3 Modify and save the white list according to your specific needs.

For more information on creating compliance white lists, see Creating Compliance White Lists, page 52-7.

Searching for Hosts

License: FireSIGHT

You can search for specific hosts by using one of the predefined searches or by using your own search criteria.

When searching for hosts, you should keep in mind that although you can configure the network discovery policy to add hosts to the network map based on data exported by NetFlow-enabled devices, the available information about these hosts is limited. For example, there is no operating system data available for these hosts, unless you provide it using the host input feature. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

You can search for specific discovery events. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IP addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.

Note When you search for hosts by IP address, the results include all hosts for which at least one IP address matches your search conditions, that is, a search for an IPv6 address may return hosts whose primary address is IPv4.

- Use the device field to search for specific devices as well as devices in groups, stacks, or clusters. For more information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

Special Search Syntax for Hosts

The following table notes search information specific to particular host fields. For more information on host fields, see Understanding the Hosts Table, page 50-20.

Table 50-5 Host Search Criteria

Field	Search Criteria Notes
Host Type	To search for all network devices, type `!host`.
MAC Vendor	To search for virtual MAC vendors, that is, for events that involve virtual machines, type `virtual_mac_vendor`. To search for a vendor whose name includes a comma, enclose the entire search term in quotes. Otherwise, the Defense Center treats the term as two searches and returns events that match each search term.
OS Vendor/Name/Version	Type `unknown` to search for hosts where the operating system is unknown. Type `n/a` to search for hosts where the operating system has not yet been identified.
Confidence	You can precede the confidence with greater than (`>`), greater than or equal to (`>=`), less than (`<`), less than or equal to (`<=`), or equal to (`=`) operators. Matches to an `n/a` search include hosts added to the network map based on NetFlow data.
OS Conflict	Note that the OS Conflict column does not appear in search results. To determine whether you are viewing hosts with or without operating system conflicts, expand the search constraints on the workflow page. For more information on resolving operating system conflicts, see Resolving Operating System Identity Conflicts, page 49-14.

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

To search for hosts:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Hosts** from the table drop-down menu.

The page updates with the appropriate constraints.

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

Step 3 Enter your search criteria in the appropriate fields, as described in the Host Search Criteria table.

If you enter criteria for multiple fields, the Defense Center returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default hosts workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Host Attributes

License: FireSIGHT

The FireSIGHT System collects information about the hosts it detects and uses that information to build host profiles. However, there may be additional information about the hosts on your network that you want to provide to your analysts. You can add notes to a host profile, set the business criticality of a host, or provide any other information that you choose. Each piece of information is called a host attribute.

You can use host attributes in host profile qualifications, which constrain the data you collect while building a traffic profile, and also can limit the conditions under which you want to trigger a correlation rule. You can also set attribute values in response to a correlation rule.

For more information, see:

- Viewing Host Attributes, page 50-27
- Understanding the Host Attributes Table, page 50-27

- Setting Host Attributes for Selected Hosts, page 50-28
- Searching for Host Attributes, page 50-29
- Configuring Set Attribute Remediations, page 54-15

Viewing Host Attributes

License: FireSIGHT

You can use the Defense Center to view a table of hosts detected by the system, along with their host attributes. Then, you can manipulate the view depending on the information you are looking for.

The page you see when you access host attributes differs depending on the workflow you use. You can use the predefined workflow, which includes a table view of host attributes that lists all detected hosts and their attributes, and terminates in a host view page, which contains a host profile for every host that meets your constraints.

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 Host Attribute Actions table below describes some of the specific actions you can perform on a host attributes workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-6 Host Attribute Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Host Attributes Table, page 50-27.
assign a host attribute to selected hosts	find more information in Setting Host Attributes for Selected Hosts, page 50-28

To view host attributes:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Host Attributes**.

The first page of the default host attributes workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 host attributes, click **(switch workflow)**, then select **Attributes**.

Understanding the Host Attributes Table

License: FireSIGHT

The FireSIGHT System collects information about the hosts it detects and uses that information to build host profiles. However, there may be additional information about the hosts on your network that you want to provide to your analysts. You can add notes to a host profile, set the business criticality, or provide any other information that you choose. Each piece of information is called a host attribute.

You can use host attributes in host profile qualifications, which constrain the data you collect while building a traffic profile, and also can limit the conditions under which you want to trigger a correlation rule.

Note that the host attributes table does not display hosts identified only by MAC addresses.

For more information on host attributes, see Working with the Predefined Host Attributes, page 49-30 and Working with User-Defined Host Attributes, page 49-31.

Descriptions of the fields in the host attributes table follow.

IP Address

The IP addresses associated with a host.

Current User

The user identity (username) of the currently logged in user on the host.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Host Criticality

The user-assigned importance of a host to your enterprise. You can use the host criticality in correlation rules and policies to tailor policy violations and their responses to the importance of a host involved in an event. You can assign a host criticality of low, medium, high, or none.

For information on setting a host's criticality, see Working with the Predefined Host Attributes, page 49-30 and Setting Host Attributes for Selected Hosts, page 50-28.

Notes

Information about the host that you want other analysts to view. For information on how to add a note, see Working with the Predefined Host Attributes, page 49-30.

Any user-defined host attribute, including those for compliance white lists

The value of the user-defined host attribute.

The host attributes table contains a field for each user-defined host attribute. For more information, see Working with User-Defined Host Attributes, page 49-31.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Setting Host Attributes for Selected Hosts

License: FireSIGHT

There are two predefined host attributes that you can assign to each host: host criticality and host-specific notes.

Use the host criticality to designate the business criticality of a given host. You can tailor correlation policies and alerts based on host criticality. For example, your organization's mail servers are more critical to your business than a typical user workstation. You can assign a high host criticality value to your mail servers and other business-critical servers and medium or low values to other hosts. You could then create a correlation policy that launches different alerts based on the criticality of an affected host.

Use notes to record information about a host that you want other analysts to view. For example, if you have a computer on the network that has an older, unpatched version of an operating system that you use for testing, you can use the notes feature to indicate that the system is intentionally unpatched.

You can also create user-defined host attributes. For example, you could create a host attribute that assigns physical location identifiers to hosts, such as a facility code, city, or room number. For more information on created user-defined host attributes, see Creating User-Defined Host Attributes, page 49-32.

You can also set the host criticality of selected hosts in a host workflow, and from within a host profile, or set it through a remediation. For more information, see Working with the Predefined Host Attributes, page 49-30 or Configuring Set Attribute Remediations, page 54-15.

To set host attributes for selected hosts:

Access: Admin/Any Security Analyst

Step 1 Select the check boxes next to the hosts to which you want to add a host attribute.

Tip Use the sort and search features to isolate the hosts to which you want to assign particular attributes.

Step 2 At the bottom of the page, click **Set Attributes**.

The Host Attributes pop-up window appears.

Step 3 Optionally, set the host criticality for the hosts you selected.

You can select **None**, **Low**, **Medium**, or **High**.

Step 4 Optionally, add notes to the host profiles of the hosts you selected by entering up to 255 alphanumeric characters, special characters, and spaces in the text box.

Step 5 Optionally, set any user-defined host attributes you have configured.

Step 6 Click **Save**.

The host attributes you specified are assigned to the selected hosts.

Searching for Host Attributes

License: FireSIGHT

You can search for hosts that have specific host attributes. For example, if your company has several regional offices, you could configure a host attribute that tells you which city any one host resides in. You could then search for hosts in specific regions. For more information on host attributes, see Working with User-Defined Host Attributes, page 49-31.

You may want to create searches customized for your network environment, then save them to reuse later. For more information on the host attribute fields, see Understanding the Host Attributes Table, page 50-27.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for host attributes:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 From the table drop-down list, select **Host Attributes**.

The page updates with the appropriate constraints.

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

Step 3 Enter your search criteria in the appropriate fields, as described in Understanding the Host Attributes Table.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default host attributes workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Indications of Compromise

License: FireSIGHT

The FireSIGHT System correlates various types of data (intrusion events, Security Intelligence, connection events, and file or malware events) associated with hosts to determine whether a host on your monitored network is likely to be compromised by malicious means. Certain combinations and frequencies of event data trigger indications of compromise (IOC) tags on affected hosts. IOC-tagged host IP addresses appear in event views with a special compromised host icon ( ); you also can write compliance rules that account for IOC-tagged hosts.

To use this feature, you must have IOC rules enabled in your network discovery policy. You can enable any or all of the predefined rules to trigger IOC tags on compromised hosts. For more information, see Setting Indications of Compromise Rules, page 45-33.

See the following sections for detailed information about indications of compromise:

Viewing Indications of Compromise

License: FireSIGHT

You can use the Defense Center to view a table of triggered Indications of Compromise (IOC). Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access IOC depends on the workflow you use. Both predefined IOC workflows terminate in a host view, which contains a host profile for every host that meets your constraints. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The following table describes some of the specific actions you can perform on an IOC workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-7 Indication of Compromise Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Indications of Compromise Table, page 50-32.
view the host profile for a compromised host	click the compromised host icon ( ) in the **IP Address** column.
mark selected IOC events resolved so they no longer appear in the list	select the check boxes next to the IOC events you want to edit, then click **Mark Resolved**. For more information, see Resolving Indications of Compromise, page 49-10.
view details of events that triggered the IOC	click the view icon ( ) in the **First Seen** or **Last Seen** columns.

To view indications of compromise:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Indications of Compromise**.

The first page of the default indications of compromise (IOC) workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 IOC table view, click **(switch workflow)**, then select **Indications of Compromise**.

Understanding the Indications of Compromise Table

License: FireSIGHT

The FireSIGHT System correlates various types of event data associated with hosts to determine whether a host on your monitored network is likely to be compromised by malicious means. These correlations appear, associated with the host, as indications of compromise (IOC). You can mark a host IOC as resolved, which removes that IOC tag from the host. A host can trigger multiple IOC tags; you can view

all IOC tags associated with a host in the Indications of Compromise section of the host profile. For more information on IOC data in the host profile, see Working with Indications of Compromise in the Host Profile, page 49-8.

Descriptions of the fields in the IOC table follow below.

IP Address

The IP address associated with the host that triggered the IOC.

Category

Brief description of the type of compromise indicated, such as `Malware Executed` or `Impact 1 Attack`.

Event Type

Identifier associated with a specific Indication of Compromise (IOC), referring to the event that triggered it.

Description

Description of what the IOC means for the potentially compromised host, such as `This host may be under remote control` or `Malware has been executed on this host`.

First/Last Seen

The first (or most recent) date and time that events triggering a host's IOC occurred.

Searching for Indications of Compromise

License: FireSIGHT

You can search for specific indications of compromise (IOC) tags triggered on monitored hosts by using one of the predefined searches or by using your own search criteria. The predefined searches serve as examples and can provide quick access to important information about your network.

You may want to modify specific fields within the default searches to customize them for your network environment, then save them to reuse later. The fields you can use to retrieve data are described in Understanding the Indications of Compromise Table, page 50-32.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.

  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for indications of compromise:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Indications of Compromise** from the table drop-down list.

The page updates with the appropriate constraints.

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

Step 3 Enter your search criteria in the appropriate fields, as described in Understanding the Indications of Compromise Table, page 50-32.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default IOC workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Servers

License: FireSIGHT

The FireSIGHT System collects information about all servers running on hosts on monitored network segments. The information that the system collects includes the name of the server, the application and network protocols used by the server, the vendor and version of the server, the IP address associated with the host running a server, and the port on which the server communicates.

When the system detects a server, it generates a discovery event unless the associated host has already reached its maximum number of servers. For more information, see Host Limits and Discovery Event Logging, page 45-13. You can use the Defense Center web interface to view, search, and delete server events.

You can also base correlation rules on server events. For example, you could trigger a correlation rule when the system detects a chat server, such as ircd, running on one of your hosts.

Although you can configure the network discovery policy to add servers to the network map based on application data exported by NetFlow-enabled devices, the available information about these servers is limited. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

See the following sections for more information:

Viewing Servers

License: FireSIGHT

You can use the Defense Center to view a table of detected servers. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access servers differs depending on the workflow you use. All the predefined workflows terminate in a host view, which contains a host profile for every host that meets your constraints. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The Server Actions table below describes some of the specific actions you can perform on an servers workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-8 Server Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Servers Table, page 50-36.
edit server identities	select the check boxes next to the events for servers you want to edit, then click **Set Server Identity**. For more information, see Editing Server Identities, page 49-18.

To view servers:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Servers**.

The first page of the default servers workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 servers, click **(switch workflow)**, then select **Servers**.

Understanding the Servers Table

License: FireSIGHT

The FireSIGHT System collects information about servers running on hosts on monitored network segments.

Descriptions of the fields in the servers table follow below.

Although you can configure the network discovery policy to add servers to the network map based on data exported by NetFlow-enabled devices, the available information about these servers is limited. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

Last Used

The date and time the server was last used on the network or the date and time that the server was originally updated using the host input feature. The Last Used value is updated at least as often as the update interval you configured in the network discovery policy, as well as when the system detects a server information update. For information on setting the update interval, see Configuring Data Storage, page 45-35.

IP Address

The IP address associated with the host running the server.

Port

The port where the server is running.

Protocol

The network or transport protocol used by the server.

Application Protocol

The application protocol, as indicated by one of the following:

- the name of the application protocol for the server
- `pending`, if the system cannot positively or negatively identify the server for one of several reasons
- `unknown`, if the system cannot identify the server based on known server fingerprints or if the server was added through host input and did not include the application protocol

Category, Tags, Risk, or Business Relevance for Application Protocols

The categories, tags, risk level, and business relevance assigned to the application protocol. These filters can be used to focus on a specific set of data. For more information, see Table 45-2 on page 45-11.

Vendor

One of:

- the server vendor as identified by the system, Nmap or another active source, or that you specified using the host input feature
- blank, if the system cannot identify its vendor based on known server fingerprints, or if the server was added to the network map using NetFlow data

Version

One of:

- the server version as identified by the system, Nmap or another active source, or that you specified using the host input feature
- blank, if the system cannot identify its version based on known server fingerprints, or if the server was added to the network map using NetFlow data

Web Application

The web application based on the payload content detected by the system in the http traffic. Note that if the system detects an application protocol of `HTTP` but cannot detect a specific web application, the system supplies a generic web browsing designation.

Category, Tags, Risk, or Business Relevance for Web Applications

The categories, tags, risk level, and business relevance assigned to the web application. These filters can be used to focus on a specific set of data. For more information, see Table 45-2 on page 45-11.

Hits

The number of times the server was accessed. For servers added using the host input feature, this value is always 0.

Source Type

One of the following values:

- User: *user_name*
- Application: *app_name*
- Scanner: *scanner_type* (Nmap or scanner added through network discovery configuration)
- FireSIGHT, FireSIGHT Port Match, or FireSIGHT Pattern Match, for servers detected by the FireSIGHT System
- NetFlow, for servers added to the network map based on NetFlow data

The system may reconcile data from multiple sources to determine the identity of a server; see Understanding Current Identities, page 46-5.

Device

The name of the device that either detected the server or processed the NetFlow or host input data that added the server to the network map.

Current User

The user identity (username) of the currently logged in user on the host.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Searching for Servers

License: FireSIGHT

You can search for specific servers that are running on monitored hosts by using one of the predefined searches or by using your own search criteria. The predefined searches serve as examples and can provide quick access to important information about your network.

You may want to modify specific fields within the default searches to customize them for your network environment, then save them to reuse later. The fields you can use to retrieve data are described in Understanding the Servers Table, page 50-36.

When searching for servers, you should keep in mind that although you can configure the network discovery policy to add applications, including servers, to the network map based on data exported by NetFlow-enabled devices, the available information about these servers is limited. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (!).

- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Use the device field to search for specific devices as well as devices in groups, stacks, or clusters. For more information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for servers:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 From the table drop-down list, select **Servers**.

The page updates with the appropriate constraints.

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

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default servers workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Applications

License: FireSIGHT

When a monitored host connects to another host, the system can, in many cases, determine what application was used. The FireSIGHT System detects the use of many email, instant messaging, peer to peer, web applications, as well as other types of applications.

For each detected application, the system logs the IP address that used the application, the product, the version, and the number of times its use was detected. You can use the web interface to view, search, and delete application events. You can also update application data on a host or hosts using the host input feature.

If you know which applications are running on which hosts, you can use that knowledge to create host profile qualifications, which constrain the data you collect while building a traffic profile, and also can limit the conditions under which you want to trigger a correlation rule. You can also base correlation rules on the detection of application. For example, if you want your employees to use a specific mail client, you could trigger a correlation rule when the system detects a different mail client running on one of your hosts.

You should carefully read the release notes for each FireSIGHT System update as well as the advisories for each VDB update for information on updated detectors.

To collect and store application data for analysis, make sure that you enable application detection in your network discovery policy. For more information, see Understanding Discovery Data Collection, page 45-1.

See the following sections for more information:

- Viewing Application Details, page 50-45
- Understanding the Application Detail Table, page 50-46
- Searching for Application Details, page 50-47

Viewing Applications

License: FireSIGHT

You can use the Defense Center to view a table of detected applications. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access applications differs depending on the workflow you use. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The Application Actions table below describes some of the specific actions you can perform on an application workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-9 Application Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Applications Table, page 50-41.
open the Application Detail View for a specific application	click the application detail view icon ( ) next to a client, application protocol, or web application.

To view applications:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Application Details**.

The first page of the default application details workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 application details, click **(switch workflow)**, then select **Clients**.

Understanding the Applications Table

License: FireSIGHT

When a monitored host connects to another host, the FireSIGHT System can, in many cases, determine what application was used. The system detects various web browsers or servers, email clients or servers, instant messengers, peer-to-peer applications, and so on. When the system detects traffic for a known client, application protocol, or web application, it logs information about the application and the host running it.

The FireSIGHT System classifies application data into three types: client, web application, and application protocol. The applications table provides a list combining all three types of detected applications on the appliance.

Descriptions of the fields in the applications table follow.

Application

The name of the detected application.

IP Address

The IP address associated with the host using the application.

Category

A general classification for the application that describes its most essential function. Each application belongs to at least one category.

Tag

Additional information about the application. Applications can have any number of tags, including none.

Risk

How likely the application is to be used for purposes that might be against your organization's security policy. An application's risk can range from `Very Low` to `Very High`.

Of Application Protocol Risk, Client Risk, and Web Application Risk, the highest of the three detected, when available, in the traffic that triggered the intrusion event.

Business Relevance

The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally. An application's business relevance can range from `Very Low` to `Very High`.

Of Application Protocol Business Relevance, Client Business Relevance, and Web Application Business Relevance, the lowest of the three detected, when available, in the traffic that triggered the intrusion event.

Current User

The user identity (username) of the currently logged in user on the host.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Type

The type of application:

- **Application Protocols** represent communications between hosts.
- **Client Applications** represent software running on a host.
- **Web Applications** represent the content or requested URL for HTTP traffic.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Searching for Applications

License: FireSIGHT

You can search for hosts that are running specific clients, application protocols, or web applications. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for applications:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Applications** from the table drop-down list.

The page updates with the appropriate constraints.

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default clients workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Application Details

License: FireSIGHT

When a monitored host connects to another host, the system can, in many cases, determine what application was used. The FireSIGHT System detects the use of many email, instant messaging, peer to peer, web applications, as well as other types of applications.

For each detected application, the system logs the IP address that used the application, the product, the version, and the number of times its use was detected. You can use the web interface to view, search, and delete application events. You can also update application data on a host or hosts using the host input feature.

If you know which applications are running on which hosts, you can use that knowledge to create host profile qualifications, which constrain the data you collect while building a traffic profile, and also can limit the conditions under which you want to trigger a correlation rule. You can also base correlation

rules on the detection of application. For example, if you want your employees to use a specific mail client, you could trigger a correlation rule when the system detects a different mail client running on one of your hosts.

You should carefully read the release notes for each FireSIGHT System update as well as the advisories for each VDB update for information on updated detectors.

To collect and store application data for analysis, make sure that you enable application detection in your network discovery policy. For more information, see Understanding Application Detection, page 45-10.

See the following sections for more information:

- Viewing Application Details, page 50-45
- Understanding the Application Detail Table, page 50-46
- Searching for Application Details, page 50-47

Viewing Application Details

License: FireSIGHT

You can use the Defense Center to view a table of detected application details. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access application details differs depending on the workflow you use. There are two predefined workflows. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The Application Details Actions table below describes some of the specific actions you can perform on an application details workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-10 Application Details Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Application Detail Table, page 50-46.
open the Application Detail View for a specific application	click the application detail view icon ( ) next to a client.

To view application details:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Application Details**.

The first page of the default application details workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 application details, click **(switch workflow)**, then select **Clients**.

Understanding the Application Detail Table

License: FireSIGHT

When a monitored host connects to another host, the FireSIGHT System can, in many cases, determine what application was used. The system detects various web browsers, email clients, instant messengers, peer-to-peer applications, and so on.

When the system detects traffic for a known client, application protocol, or web application, it logs information about the application and the host running it. Descriptions of the fields in the application details table follow.

Last Used

The time that the application was last used or the time that the application data was updated using the host input feature. The Last Used value is updated at least as often as the update interval you configured in the network discovery policy, as well as when the system detects an application information update. For information on setting the update interval, see Configuring Data Storage, page 45-35.

IP Address

The IP address associated with the host using the application.

Client

The name of the application. Note that if the system detected an application protocol but could not detect a specific client, `client` is appended to the application protocol name to provide a generic name.

Version

The version of the application.

Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications

The categories, tags, risk level, and business relevance assigned to the application. These filters can be used to focus on a specific set of data. For more information, see Table 45-2 on page 45-11.

Application Protocol

The application protocol used by the application. Note that if the system detected an application protocol but could not detect a specific client, `client` is appended to the application protocol name to provide a generic name.

Web Application

The web application based on the payload content or URL detected by the system in the http traffic. Note that if the system detects an application protocol of `HTTP` but cannot detect a specific web application, the system supplies a generic web browsing designation here.

Hits

The number of times the system detected the application in use. For applications added using the host input feature, this value is always `0`.

Device

The device that generated the discovery event containing the application detail.

Current User

The user identity (username) of the currently logged in user on the host.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Searching for Application Details

License: FireSIGHT

You can search for hosts that are running specific clients, application protocols, or web applications. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.

- Use the device field to search for specific devices as well as devices in groups, stacks, or clusters. For more information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for application details:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Application Details** from the table drop-down list.

The page updates with the appropriate constraints.

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

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default application details workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Vulnerabilities

License: FireSIGHT

The FireSIGHT System includes its own vulnerability tracking database which is used, in conjunction with the system's fingerprinting capability, to identify the vulnerabilities associated with the hosts on your network.

The operating systems, servers, and clients running on your hosts have different sets of associated vulnerabilities. You can deactivate vulnerabilities for a host after you patch the host or otherwise judge it immune to a vulnerability. You can use the Defense Center to track and review the vulnerabilities for each host.

Note that vulnerabilities for vendorless and versionless servers are not mapped unless the applications protocols used by the servers are mapped in the system policy. Vulnerabilities for vendorless and versionless clients cannot be mapped. For more information, see Mapping Vulnerabilities for Servers, page 63-30.

For more information, see:

Viewing Vulnerabilities

License: FireSIGHT

You can use the Defense Center to view a table of vulnerabilities. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access vulnerabilities differs depending on the workflow you use. You can use the predefined workflow, which includes a table view of vulnerabilities. The table view contains a row for each vulnerability in the database, regardless of whether any of your detected hosts exhibit the vulnerabilities. The second page of the predefined workflow contains a row for each vulnerability (that you have not deactivated) that applies to detected hosts on your network. The predefined workflow terminates in a vulnerability detail view, which contains a detailed description for every vulnerability that meets your constraints.

Tip If you want to see the vulnerabilities that apply to a single host or set of hosts, perform a search for vulnerabilities, specifying an IP address or range of IP addresses for the hosts. For more information on searching for vulnerabilities, see Searching for Vulnerabilities, page 50-52.

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 an vulnerabilities workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-11 Vulnerability Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Vulnerabilities Table, page 50-50.
view the vulnerability details for a vulnerability	click the view icon ( ) in the SVID column. Alternatively, constrain on the vulnerability ID and drill down to the vulnerability details page. For more information, see Viewing Vulnerability Details, page 49-27.
deactivate selected vulnerabilities so they are no longer used for intrusion impact correlation for currently vulnerable hosts	find more information in Deactivating Vulnerabilities, page 50-52.
view the full text of a vulnerability title	right-click the title and select **Show Full Text**.

To view vulnerabilities:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Vulnerabilities > Vulnerabilities**.

The first page of the default vulnerabilities workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 vulnerabilities, click **(switch workflow)**, then select **Vulnerabilities**.

Understanding the Vulnerabilities Table

License: FireSIGHT

The FireSIGHT System includes its own vulnerability tracking database which is used, in conjunction with the system's fingerprinting capability, to identify the vulnerabilities associated with the hosts on your network.

The operating systems, servers, and clients running on your hosts have different sets of associated vulnerabilities. You can deactivate vulnerabilities for a host after you patch the host or otherwise judge it immune to a vulnerability. You can use the Defense Center to track and review the vulnerabilities for each host.

For more information on vulnerabilities, see Working with the Vulnerabilities Network Map, page 48-7 and Working with Vulnerabilities in the Host Profile, page 49-25.

Descriptions of the fields in the vulnerabilities table follow.

SVID

The Cisco vulnerability identification number that the system uses to track vulnerabilities.

Click the view icon ( ) to access the vulnerability details for the SVID. See Viewing Vulnerability Details, page 49-27 for more information.

Bugtraq ID

The identification number associated with the vulnerability in the Bugtraq database. (http://www.securityfocus.com/bid/)

Snort ID

The identification number associated with the vulnerability in the Snort ID (SID) database. That is, if an intrusion rule can detect network traffic that exploits a particular vulnerability, that vulnerability is associated with the intrusion rule's SID.

Note that a vulnerability can be associated with more than one SID (or no SIDs at all). If a vulnerability is associated with more than one SID, the vulnerabilities table includes a row for each SID.

Title

The title of the vulnerability.

IP Address

The IP address associated with the host affected by the vulnerability.

Date Published

The date the vulnerability was published.

Vulnerability Impact

Displays the severity assigned to the vulnerability in the Bugtraq database on a scale of 0 to 10, with 10 being the most severe. The vulnerability impact is determined by the writer of the Bugtraq entry based on his or her best judgment and guided by SANS Critical Vulnerability Analysis (CVA) criteria.

Remote

Indicates whether the vulnerability is remotely exploitable.

Available Exploits

Indicates whether there are known exploits for the vulnerability.

Description

A brief description of the vulnerability.

Technical Description

A detailed technical description of the vulnerability.

Solution

Information about repairing the vulnerability.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Deactivating Vulnerabilities

License: FireSIGHT

Deactivate a vulnerability after you patch the hosts on your network or otherwise judge them immune. Deactivated vulnerabilities are not used for intrusion impact correlation. Note that if the system discovers a new host that is affected by that vulnerability, the vulnerability is considered valid (and is not automatically deactivated) for that host.

You can deactivate vulnerabilities within the vulnerabilities workflow **only** on a workflow page that shows vulnerabilities for specific hosts on your network, that is:

- on the second page of the default vulnerabilities workflow, **Vulnerabilities on the Network**, which shows only the vulnerabilities that apply to the hosts on your network
- on any page in a vulnerabilities workflow, custom or predefined, that you constrained based on IP address using a search.

Deactivating a vulnerability within a vulnerabilities workflow that is not constrained on IP addresses deactivates the vulnerability for *all* detected hosts on your network. To deactivate a vulnerability for a single host, you have three options:

- Use the network map.

  For more information, see Working with the Vulnerabilities Network Map, page 48-7.
- Use the host's host profile.

  For more information, see Setting Vulnerabilities for Individual Hosts, page 49-30.
- Constrain the vulnerabilities workflow based on the IP addresses of the host or hosts for which you want to deactivate vulnerabilities. For hosts with multiple associated IP addresses, this function applies only to the single, selected IP address of that host.

To constrain the view based on IP address, perform a search for vulnerabilities, specifying an IP address or range of IP addresses for the hosts for which you want to deactivate vulnerabilities. For more information on searching for vulnerabilities, see Searching for Vulnerabilities, page 50-52.

To deactivate vulnerabilities:

Access: Admin/Any Security Analyst

Step 1 On the Vulnerabilities on the Network page, select the check boxes next to vulnerabilities you want to deactivate, then click **Review**.

Searching for Vulnerabilities

License: FireSIGHT

You can search for vulnerabilities that affect the hosts on your network. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (!).

- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

Specific Search Criteria for Vulnerabilities

Note the following information specific to searching for vulnerabilities:

- Find Bugtraq ID numbers at http://www.securityfocus.com/bid.
- Enter `TRUE` to search for vulnerabilities that are exploited, or `FALSE` to exclude such vulnerabilities.

To search for vulnerabilities:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Vulnerabilities** from the table drop-down list.

The page updates with the appropriate constraints.

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 use the search as a data restriction for a custom user role, you **must** save it as a private search.

Step 5 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 6 Click **Search** to start the search.

Your search results appear in the default vulnerabilities workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Third-Party Vulnerabilities

License: FireSIGHT

The FireSIGHT System includes its own vulnerability tracking database which is used, in conjunction with the system's fingerprinting capability, to identify the vulnerabilities associated with the hosts on your network.

If your organization can write scripts or create command line import files to import network map data from third-party applications, you can import third-party vulnerability data to augment the system's vulnerability data. For more information, see the *FireSIGHT System Host Input API Guide.*

To include imported data in impact correlations, you must map third-party vulnerability information to the operating system and application definitions in the database. You cannot map third-party vulnerability information to client definitions.

For more information, see:

- Viewing Third-Party Vulnerabilities, page 50-54
- Understanding the Third-Party Vulnerabilities Table, page 50-55
- Searching for Third-Party Vulnerabilities, page 50-56

Viewing Third-Party Vulnerabilities

License: FireSIGHT

After you use the host input feature to import third-party vulnerability data, you can use the Defense Center to view a table of third-party vulnerabilities. Then, you can manipulate the event view depending on the information you are looking for.

The page you see when you access third-party vulnerabilities differs depending on the workflow you use. There are two predefined workflows. You can also create a custom workflow that displays only the information that matches your specific needs. For more information, see Creating Custom Workflows, page 58-39.

The following table describes some of the specific actions you can perform on a third-party vulnerabilities workflow page. You can also perform the tasks described in the Common Discovery Event Actions table.

Table 50-12 Third-Party Vulnerability Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Third-Party Vulnerabilities Table, page 50-55.
view the vulnerability details for a third-party vulnerability	click the view icon ( ) in the SVID column. Alternatively, constrain on the vulnerability ID and drill down to the vulnerability details page. For more information, see Viewing Vulnerability Details, page 49-27.

To view third-party vulnerabilities:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Vulnerabilities > Third-Party Vulnerabilities**.

The first page of the default third-party vulnerabilities workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 third-party vulnerabilities, click **(switch workflow)**, then select **Vulnerabilities by Source** or **Vulnerabilities by IP Address**.

Understanding the Third-Party Vulnerabilities Table

License: FireSIGHT

When you import third-party vulnerability information using the host input feature, the system stores that information in its database. The fields in the third-party vulnerabilities table are described in the following table.

Vulnerability Source

The source of the third-party vulnerabilities, for example, QualysGuard or NeXpose.

Vulnerability ID

The ID number associated with the vulnerability for its source.

IP Address

The IP address associated with the host affected by the vulnerability.

Port

A port number, if the vulnerability is associated with a server running on a specific port.

Bugtraq ID

The identification number associated with the vulnerability in the Bugtraq database. (http://www.securityfocus.com/bid/)

CVE ID

The identification number associated with the vulnerability in MITRE's Common Vulnerabilities and Exposures (CVE) database (http://www.cve.mitre.org/).

SVID

The legacy vulnerability identification number that the system uses to track vulnerabilities

Click the view icon ( ) to access the vulnerability details for the SVID. See Viewing Vulnerability Details, page 49-27 for more information.

Snort ID

The identification number associated with the vulnerability in the Snort ID (SID) database. That is, if an intrusion rule can detect network traffic that exploits a particular vulnerability, that vulnerability is associated with the intrusion rule's SID.

Note that a vulnerability can be associated with more than one SID (or no SIDs at all). If a vulnerability is associated with more than one SID, the vulnerabilities table includes a row for each SID.

Title

The title of the vulnerability.

Description

A brief description of the vulnerability.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Searching for Third-Party Vulnerabilities

License: FireSIGHT

You can search for third-party vulnerabilities that affect the hosts on your network. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (!).

- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

Specific Search Criteria for Vulnerabilities

Note the following information specific to searching for vulnerabilities:

- Find Bugtraq ID numbers at http://www.securityfocus.com/bid.
- Enter `TRUE` to search for vulnerabilities that are exploited, or `FALSE` to exclude such vulnerabilities.

To search for third-party vulnerabilities:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Third-Party Vulnerabilities** from the table drop-down list.

The page updates with the appropriate constraints.

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 use the search as a data restriction for a custom user role, you **must** save it as a private search.

Step 5 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 6 Click **Search** to start the search.

Your search results appear in the default third-party vulnerabilities workflow. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with Users

License: FireSIGHT

When either an Active Directory Agent or a managed device detects a user login for a user who is not already in the database, the user is added to the database, unless you have specifically restricted that login type (see Restricting User Logging, page 45-29).

Note Although the system detects SMTP logins, the system does not record them unless there is already a user with a matching email address in the database; users are **not** added to the database based on SMTP logins.

The type of login that the system detected determines what information is stored about the new user, as described in the following table.

Table 50-13 Login Types and User Data Stored

Login Type	User Data Stored
LDAP AIM Oracle SIP HTTP FTP MDNS	• username • current IP address • login type (`aim`, `ldap`, `oracle`, `sip`, `http`, `ftp`, or `mdns`)
POP3 IMAP	• username • current IP address • email address • login type (`pop3` or `imap`)

If you configured Defense Center-LDAP server connections, the Defense Center queries the LDAP servers every five minutes and obtains metadata for the new users in the user database. At the same time, the Defense Center also queries the LDAP servers for updated information on users whose records in the Defense Center database are more than 12 hours old. It may take five to ten minutes for the Defense Center database to update with user metadata after the system detects a new user login. From the LDAP servers, the Defense Center obtains the following information and metadata about each user:

- LDAP username
- first and last names
- email address
- department
- telephone number

The number of users the Defense Center can store in its database depends on your FireSIGHT license. Note that AIM, Oracle, and SIP logins create duplicate user records because they are not associated with any of the user metadata that the system obtains from LDAP servers. To prevent overuse of user count because of duplicate user records from these protocols, disable logging of the protocols in the network discovery policy. For more information, see Restricting User Logging, page 45-29.

You can search, view, and delete users from the database; you can also purge all users from the database. For more information, see the following sections:

- Viewing Users, page 50-59
- Understanding the Users Table, page 50-60
- Understanding User Details and Host History, page 50-62
- Searching for Users, page 50-62

Viewing Users

License: FireSIGHT

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

The page you see when you access users differs depending on the workflow you use. You can use the predefined workflow, which includes a table view of users that lists all detected users, and terminates in a user details page. The user details page provides information on every user that meets your constraints.

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.

For more information about the contents of the columns in the table, see Understanding the Users Table, page 50-60.The following table, see describes some of the specific actions you can perform on an users workflow page. You can also perform the actions in the Common Discovery Event Actions table.

To view users:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Users > Users**.

The first page of the default users workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. 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 users, click **(switch workflow)**, then select **Users**.

Understanding the Users Table

License: FireSIGHT

When the system discovers a user, it collects data about that user and stores it in the database. Descriptions of the fields in the users table follow.

User

One of:

- the first name, last name, and username of the user as collected via the optional Defense Center-LDAP server connections
- the username only, if you have not configured Defense Center-LDAP server connections, or for users that the Defense Center cannot correlate with an LDAP record

The Defense Center also displays the protocol used to detect the user.

Note that because unsuccessful AIM login attempts are recorded, the Defense Center can store invalid AIM users (for example, if a user misspelled his or her username).

Current IP

The IP address associated with the host that the user is logged into. This field is blank if another authoritative user logs into the host with the same IP address after the user's login, unless the user is an authoritative user and the new user is a non-authoritative user. (The system associates the IP address with the last authoritative user that logged in with the host.) For more information on authoritative vs. non-authoritative users, see Users Database, page 45-7.

First Name

The user's first name, as obtained from the optional Defense Center-LDAP server connections. This field is blank if:

- you have not configured a Defense Center-LDAP server connection
- the Defense Center cannot correlate the user in the Defense Center database with an LDAP record (for example, for users added to the database via an AIM, Oracle, or SIP login)
- there is no first name associated with the user on your LDAP servers

Last Name

The user's last name, as obtained from the optional Defense Center-LDAP server connections. This field is blank if:

- you have not configured a Defense Center-LDAP server connection
- the Defense Center cannot correlate the user in the Defense Center database with an LDAP record (for example, for users added to the database via an AIM, Oracle, or SIP login)
- there is no last name associated with the user on your LDAP servers

E-Mail

The user's email address. This field is blank if:

- the user was added to the database via an AIM login
- the user was added to the database via an LDAP login and there is no email address associated with the user on your LDAP servers

Department

The user's department, as obtained from the optional Defense Center-LDAP server connections. If there is no department explicitly associated with the user on your LDAP servers, the department is listed as whatever default group the server assigns. For example, on Active Directory, this is `Users (ad)`. This field is blank if:

- you have not configured a Defense Center-LDAP server connection
- the Defense Center cannot correlate the user in the Defense Center database with an LDAP record (for example, for users added to the database via an AIM, Oracle, or SIP login)

Phone

The user's telephone number, as obtained from the optional Defense Center-LDAP server connections. This field is blank if:

- you have not configured a Defense Center-LDAP server connection
- the Defense Center cannot correlate the user in the Defense Center database with an LDAP record (for example, for users added to the database via an AIM, Oracle, or SIP login)
- there is no telephone number associated with the user on your LDAP servers

User Type

The protocol used to detect the user. For example, for users added to the database when detects a POP3 login, the user type is `pop3`.

Count

The number of users that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Understanding User Details and Host History

License: FireSIGHT

From any event view that associates user identity data with other kinds of events, as well as from a table view of users, you can display the User Identity pop-up window to learn more about a specific user. User information also appears in the terminating page for users workflows.

The user data you see is the same as you would see in the table view of users; for more information, see Understanding the Users Table, page 50-60.

The host history provides a graphic representation of the last twenty-four hours of the user's activity. A list of IP addresses of the hosts that the user logged into and logged off of approximates login and logout times with bar graphs. A typical user might log on to and off of multiple hosts in the course of a day. For example, periodic automated logins to a mail server would display as multiple short sessions, while longer logins (such as during working hours) display longer sessions.

Note that when a non-authoritative user login to a host is detected, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user login is detected for that host, only another authoritative user login changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control. If you configure capture of failed logins in the network discovery policy, the host history also includes hosts where the user failed to log in.

The data used to generate the host history is stored in the user history database, which by default stores 10 million user login events. If you do not see any data in the host history for a particular user, either that user is inactive, or you may need to increase the database limit. For more information, see Configuring Database Event Limits, page 63-15.

To view user details and host history:

Access: Admin/Any Security Analyst

Step 1 You have two options:

- In any event view that lists users, click the user icon () that appears next to a user identity.
- In any users workflow, click the Users terminating page.

User details appear.

Searching for Users

License: FireSIGHT

You can search for specific users. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (!).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.

  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.

- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

Specific User Search Criteria

For **User Type**, valid search criteria are `ldap`, `pop3`, `imap`, `oracle`, `sip`, `http`, `ftp`, `mdns`, and `aim`; because users are not added to the database based on SMTP logins, entering `smtp` will not return any results.

To search for users:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **Users** from the table drop-down list.

The Users search page appears.

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

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default users workflow. To use a different workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.

Working with User Activity

License: FireSIGHT

The FireSIGHT System generates events that communicate the details of user activity on your network. Descriptions of the four types of user activity follow.

New User Identity

This event is generated when the system detects a user login for a user that is not in the database.

User Login

This event is generated when any of the following occur:

- an Active Directory Agent that you installed on an Active Directory server detects an LDAP login
- a managed device detects an LDAP, POP3, IMAP, SMTP, AIM, Oracle, FTP, HTTP, MDNS or SIP login
- There are several points to keep in mind regarding user login events:
- SMTP logins are not recorded unless there is already a user with a matching email address in the database.
- Failed logins are only for LDAP, IMAP, FTP, and POP3, and only when detected in traffic. Users are not added to the detected users database as a result of a failed login, but the activity is optionally recorded in the user activity database, based on the user logging configuration in the network discovery policy.

– A user login is not recorded if you have specifically restricted its login type; see Restricting User Logging, page 45-29.

Note that when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user. In addition, when a non-authoritative user is the current user on a host, that user still cannot be used for user control.

Delete User Identity

This event is generated when you manually delete a user from the database.

User Identity Dropped: User Limit Reached

This event is generated when the system detects a user that is not in the database, but cannot add the user because you have reached the maximum number of users in the database as determined by your FireSIGHT license.

The total number of detected users the Defense Center can store depends on your FireSIGHT license. After you reach the licensed limit, in most cases the system stops adding new users to the database. To add new users, you must either manually delete old or inactive users from the database, or purge all users from the database.

However, the system favors authoritative users. If you have reached the limit and the system detects a login for a previously undetected authoritative user, the system deletes the non-authoritative user who has remained inactive for the longest time, and replaces it with the new authoritative user.

When the system detects user activity, it is logged to the database. You can view, search, and delete user activity; you can also purge all user activity from the database.

Whenever possible the FireSIGHT System correlates user activity with other types of events. For example, intrusion events can tell you the users who were logged into the source and destination hosts at the time of the event. This can tell you who owns the host that was targeted by an attack, or who initiated an internal attack or portscan.

You can also use user activity in correlation rules. Based on the type of user activity as well as other criteria that you specify, you can build correlation rules that, when used in a correlation policy, launch remediations and alert responses when network traffic meets your criteria. For more information on user activity, see Understanding User Data Collection, page 45-3.

For more information, see the following sections:

- Viewing User Activity Events, page 50-65
- Understanding the User Activity Table, page 50-66
- Searching for User Activity, page 50-67

Viewing User Activity Events

License: FireSIGHT

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

The page you see when you access user activity differs depending on the workflow you use. You can use the predefined workflow, which includes the table view of user activity and terminates in a user details page, which contains user details for every user that meets your constraints. 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.

For more information about the contents of the columns in the table, see Understanding the User Activity Table, page 50-66.The following table, see describes some of the specific actions you can perform on an user activity workflow page. You can also perform the actions in the Common Discovery Event Actions table.

To view user activity:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Users > User Activity**.

The first page of the default user activity workflow appears. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3. If no events appear, you may need to adjust the time range; see Setting Event Time Constraints, page 58-23.

Tip If you are using a custom workflow that does not include the table view of user activity, click **(switch workflow)**, then select **User Activity**.

Understanding the User Activity Table

License: FireSIGHT

When the system detects user activity, it is logged to the database. Descriptions of the fields in the users table follow.

Time

The time that the system detected the user activity.

Event

The user activity type. For more information, see Working with User Activity, page 50-64.

User

The user associated with the activity. At a minimum, this field contains a username and the protocol used to detect the user. If there is LDAP metadata on the user, this field may also contain the first name and last name of the user.

User Type

The protocol used to detect the user. For example, for users added to the database when the system detects a POP3 login, the user type is `pop3`.

IP Address

For User Login activity, the IP address involved in the login, which can be an IP address of the user's host (for LDAP, POP3, IMAP, FTP, HTTP, MDNS, and AIM logins), the server (for SMTP and Oracle logins), or the session originator (for SIP logins).

Note that an associated IP address does not mean the user is the current user for that IP address; when a non-authoritative user logs into a host, that login is recorded in the user and host history. If no authoritative user is associated with the host, a non-authoritative user can be the current user for the host. However, after an authoritative user logs into the host, only a login by another authoritative user changes the current user.

For other types of user activity, this field is blank.

Description

For Delete User Identity and User Identity Dropped activity, the username of the user who was deleted from the database or failed to be added to the database. For logins to network resources, `network login` is displayed. For other types of user activity, this field is blank.

Device

For user activity detected by a managed device, the name of the device. For other types of user activity, the managing Defense Center.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows.

Searching for User Activity

License: FireSIGHT

You can search for specific user activity. You may want to create searches customized for your network environment, then save them to reuse later.

General Search Syntax

The system displays examples of valid syntax next to each search field. When entering search criteria, keep the following points in mind:

- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.

  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Searches return only records that match the search criteria specified for all fields.
- Many fields accept one or more asterisks (`*`) as wild cards.
- For some fields, you can specify `n/a` or `blank` in the field to identify events where information is not available for that field; use `!n/a` or `!blank` to identify the events where that field is populated.
- Most fields are case-insensitive.
- IP addresses may be specified using CIDR notation. For information on entering IPv4 and IPv6 addresses in the FireSIGHT System, see IP Address Conventions, page 1-22.
- Use the device field to search for specific devices as well as devices in groups, stacks, or clusters. For more information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.
- Click the add object icon (+) that appears next to a search field to use an object as a search criterion.

For detailed information on search syntax, including using objects in searches, see Searching for Events, page 60-1.

To search for user activity:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Search**.

The Search page appears.

Step 2 Select **User Activity** from the table drop-down menu.

The User Activity search page appears.

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

Step 3 Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields. Click the add icon (+) that appears next to a search field to use an object as a search criterion.

Step 4 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 5 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 6 Click **Search** to start the search.

Your search results appear in the default user activity workflow, constrained by the current time range. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.