Nuix Adaptive Security

Nuix Adaptive Security 2.16.1

User Guide

March 2023

nuix

Content

Introduction

Welcome to the Nuix Adaptive Security User Guide.

About Nuix Adaptive Security

Visibility into the security of your environment is crucial to your organization's success. Nuix Adaptive Security can help you answer questions about your organization, such as:

- Is my organization compromised?
- Has someone taken critical data out of my organization?
- How was someone able to access our environment?
- Is something about to happen?

When you don't have visibility, it leaves your organization in a precarious position, at a decision-making disadvantage, and open to greater risk.

Nuix Adaptive Security delivers a proactive approach that provides the kind of *visibility, adaptability,* and *control* that is missing with traditional endpoint products. By leveraging endpoint analytics, Nuix Adaptive Security reduces the time it takes to detect impending or ongoing attacks. Nuix Adaptive Security accelerates recovery time, easily adapts to changing environments, regulations, and attack vectors. Ultimately, Nuix Adaptive Security stops incidents in real-time.

Nuix Adaptive Security has perfected the art of continuous monitoring and response to isolate the important (and often small) signals from the noise and identify when behaviors exhibit uncharacteristic patterns. Nuix Adaptive Security relies on two fundamental and unique elements to drive the *protect-detect-response-remediate* process:

- The Digital Behavior Recorder (TM) continuously monitors and records key digital behaviors.
- The patent-pending logic engine provides customizable logic on the endpoint, enabling it to recognize and act on threats in real-time.

Additional product documentation

Some information found in this guide is available in greater detail in other documents. These include:

- *Nuix Adaptive Security Installation Guide, Version 2.16.1*
- *Nuix Adaptive Security Quick Start Guide, Version 2.16.0*
- *Nuix Adaptive Security Release Notes, Version 2.16.1*
- *Nuix Adaptive Security Administration Guide, Version 2.16.0*
- *Nuix Adaptive Security Rule Language Reference Guide, Version 2.16.0*

Access Nuix Adaptive Security

The installation process creates a shortcut on the desktop called **Adaptive Security**.

Use this shortcut to access the Nuix Adaptive Security application, using the user credentials and server address provided by the System Administrator.

Individuals with appropriate permissions can perform the administration of users and groups. For more information about this, see the *Nuix Adaptive Security Installation Guide*.

Sign in

To access Nuix Adaptive Security:

1. Go to the Desktop and double-click the **Adaptive Security** shortcut. The **Nuix Adaptive Security Login** window appears, as shown in the following image.

Note: When entering data in the window, an exclamation point is displayed until you enter data that meets the criteria.

2. In the **Server** list, enter the Nuix Adaptive Security Server IP address provided by your system administrator.
3. In the **User Name** box, verify that the user name defaults to your user name.
4. In the **Password** box, enter the password that you received from your system administrator.

Note: The password is case-sensitive.

5. Click **Login**.
6. The Nuix Adaptive Security Dashboard appears.

The Nuix Adaptive Security application interface

After logging in, the Nuix Adaptive Security application interface opens to the Dashboard.

The following sections describe how to deploy agents, interact with the endpoints, and investigate the collected information.

Main navigation bar

The tasks on the left side of the application in the main navigation bar provide easy access to configurations and monitoring.

The functions described in the following table allow for interaction with your data.

Button	Description	Function
	Dashboard	Provides a visual summary of alerts and activity in the environment.
	Alerts	Displays all alerts from the endpoint agents.
	Collections	Use Collections to obtain specific files from endpoints across the network.
	Search	Allows you to find specific information within the Nuix Adaptive Security application.
	Investigate	Provides easy access to the information collected from the endpoint agents.
	Configuration	Access and manage endpoint agent configuration.
	Endpoints	Shows a list of all the endpoints.
	Event Statistics	View daily event details about the endpoints in your environment.
	Tasks	Shows the list of tasks created on all the endpoints.
	User Profile	Provides information about the currently logged-in user, including the user name, server address, server status, and the application version.
	System	Provides the ability to make changes to how data is stored. Information about your instance of Nuix Adaptive Security is also available.

Work with tabs

This section discusses options that are common across multiple tabs of Nuix Adaptive Security.

Quick filter lists

The Alerts, Collections, Search, Investigate, Configuration, Endpoints, Event Statistics, and Tasks tabs have quick filters that allow you to refine your data.

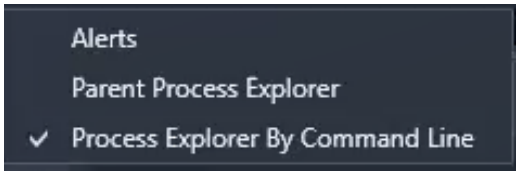
The available filters are described in the sections of this guide that discuss the individual tabs.

For all the Quick Filter lists, **Show Advanced** is displayed by default. Click **Hide Advanced** to make the quick filters disappear, except for the Quick Filter setting. Click **Show Advanced** to view alerts.

Close and switch open tabs

Note: This option is not available on the Dashboard or the Search tab.

The arrow above the context menu on the right side shows a list of all the tabs currently open. A check mark shows the tab in the list being viewed, as shown in the following image. If it is necessary to switch to a different tab, select that tab here.



To close all open tabs, click the **X** next to the arrow. The **Close All** dialog box is displayed. Click the box next to **Delete Insight from Workspace permanently** to remove the open Insights. Click **OK** when you are finished.

Tab options

Right-clicking any of the tabs created on the right tab displays a context menu with the following options:

- **Dock**: Keeps the tab in a stationary place and ensures that the data shown is the most current. Selected by default.
- **Float**: Moves the tab, allowing for a better look at the data by moving it, for example, to a different window from where the Nuix Adaptive Security application is open.
- **Auto Hide**: Moves the tab into the background automatically.
- **Hide**: Moves the tab into the background.
- **Close all but this**: Closes all tabs but the selected one.
- **Pin Tab**: Keeps the open tab on the right tab permanently. Unpin the tab to allow it to move within Nuix Adaptive Security or remove the tab from the view.

The following options appear when there is more than one tab open:

- **New horizontal tab group**: The selected tab is displayed in a new horizontal grouping.
- **New vertical tab group**: The selected tab is displayed in a new vertical grouping.

Current filter bar

A filter bar is displayed at the bottom of the open tab of data.

The current filter bar shows the query being used. Edit the filter by clicking the **Edit Filter** link on the right side of the bar. For more information about the Edit Filter link, see Filter Editor. Stop the use of a filter by clicking the **X** in the filter bar.

To use a filter, select the checkbox next to the filter name. If there is no current filter in use, the menu in the current filter bar lists the previously used filters. To use one of the filters, select that filter from the list.

Results List

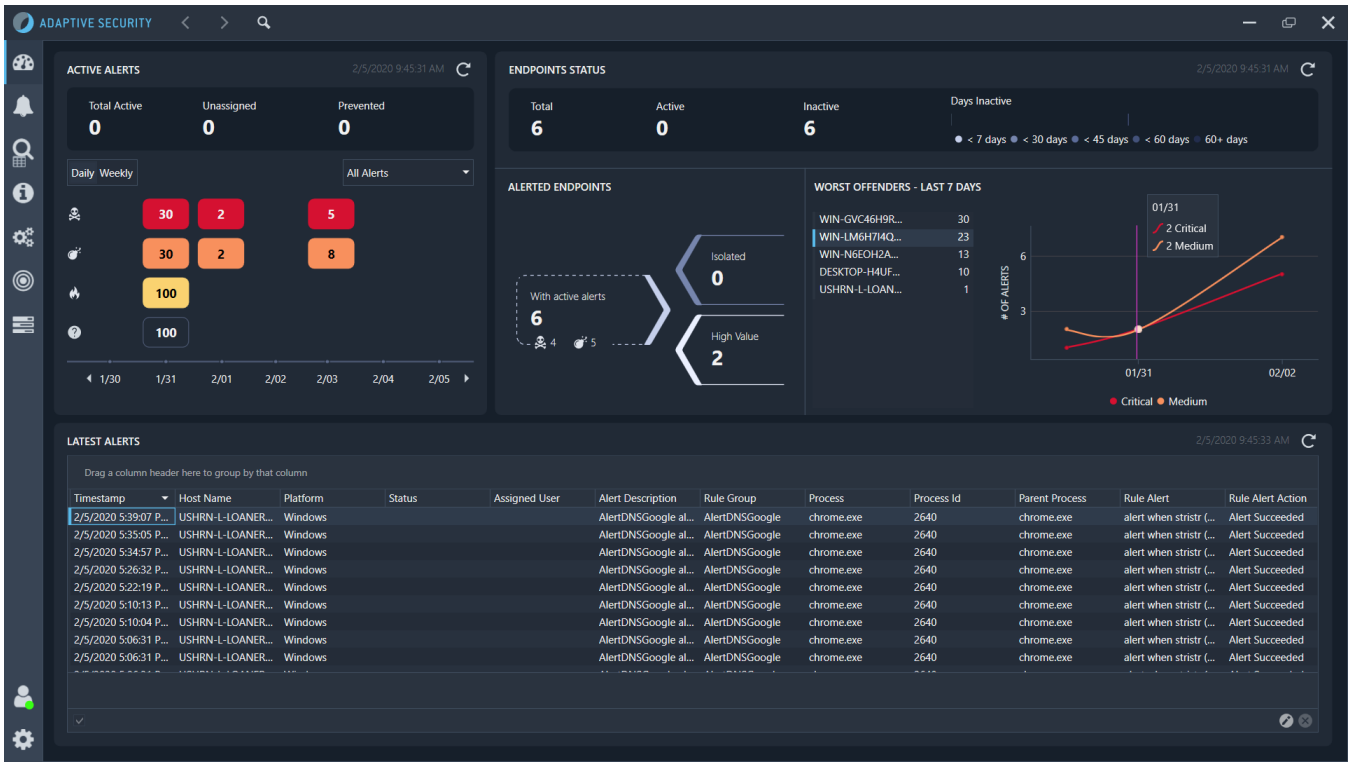
The Results List is located under the Quick Filter list on the Alerts, Endpoints, and Tasks tabs. The options in this section depend on what tab you are viewing. The available options are described in the sections of this guide that discuss the individual tabs.

These lists share the following common characteristics:

- **Show in Groups**: If selected, use this option along with any of the previously listed categories.
- A checkmark next to any of these options indicates the selected option.
- You can organize alerts in ascending or descending order.

Dashboard

The Nuix Adaptive Security Dashboard provides quick and easy access to the most relevant alerts, endpoints, and activity in the Nuix Adaptive Security environment.

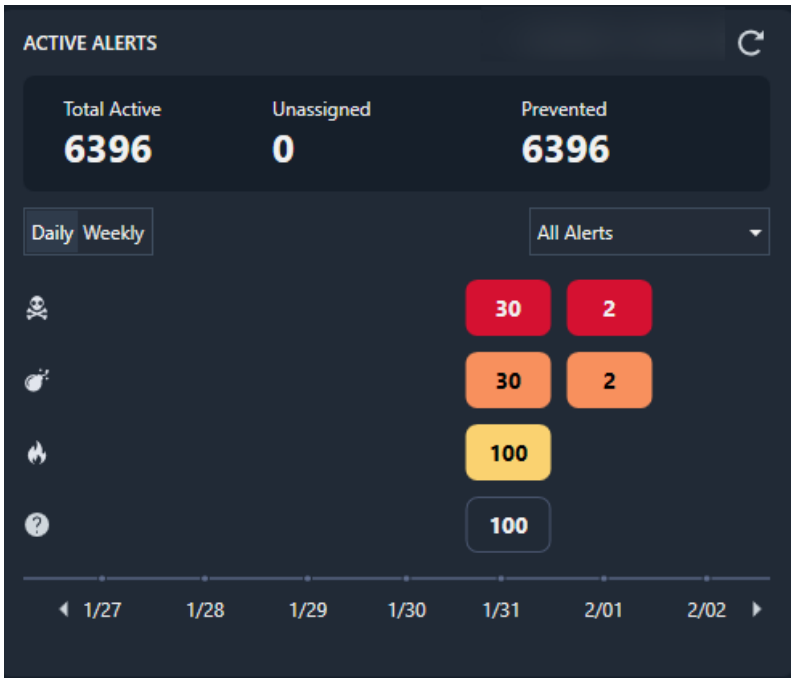


The Dashboard page consists of three sections:

- Active Alerts
- Endpoints Status
- Latest Alerts

Active Alerts

The Active Alerts section displays a summary of alerts in Nuix Adaptive Security, as shown in the following image.



On the right side of the tab, there is a **Refresh** button that shows a menu that allows you to update data at selected intervals. The default option is **Disabled**.

The alerts are classified into the following categories:

- **Total Active**: Displays the total number of alerts across all endpoints with a status of Active, which includes alerts with a status of Unassigned, Pending Investigation, Investigation in Progress, Investigation on Hold, or Investigation in Review.
- **Unassigned**: Displays the number of alerts not assigned to a user.
- **Prevented**: Displays the number of alerts that have resulted in a process being blocked.

Clicking on any of these categories opens the Alert insight on the Investigate page, with the appropriate filters set, so you can see how the alerts are categorized (Active, Prevented, Unassigned).

Active Alerts chart

The alerts can be further examined in the chart found underneath the alert summary.

Click the **Daily** or **Weekly** button to display the alerts for a day or a week. Use the menu on the right to display the alerts by **All alerts** or **Assigned to me**.

Use the arrows on the bottom of the chart to change the dates.

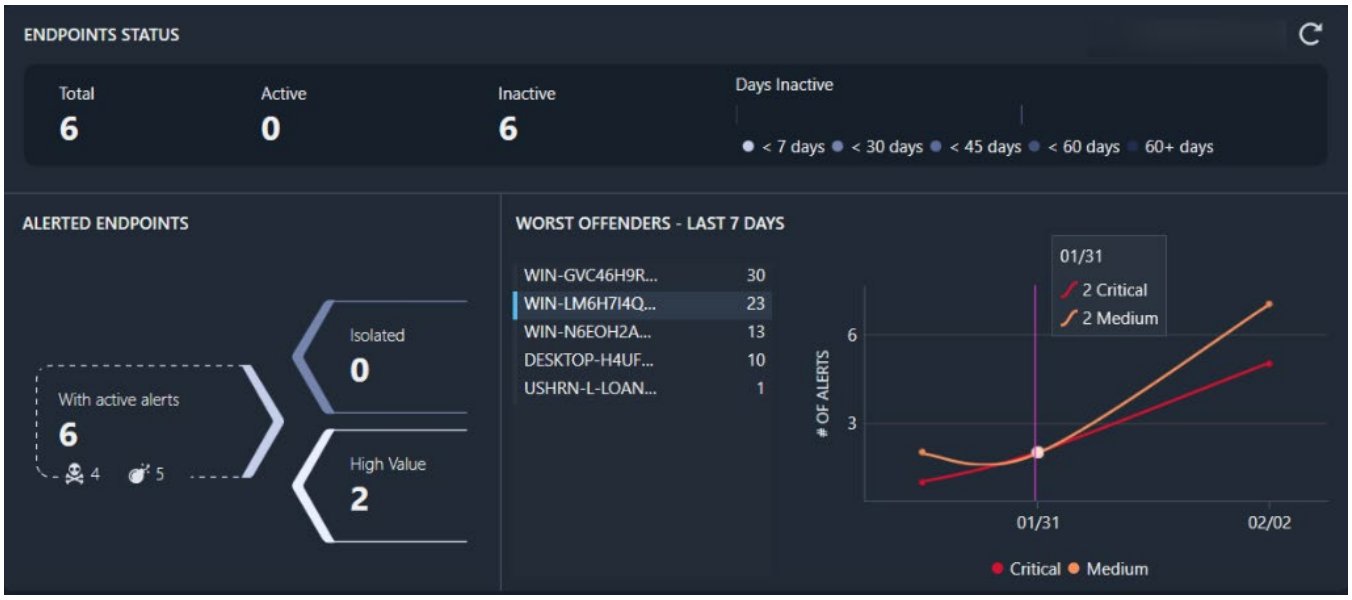
Alert severity and category

The alerts are organized using the severity categories in the following table to analyze the data. Category and Severity are Alert metadata fields that are persisted along with alert data when the alert is triggered.

Button	Description
	**Critical**: Displays the alerts defined in a logic rule as severity=critical.
	**Medium**: Displays the alerts defined in a logic rule as severity=medium.
	**Low**: Displays the alerts defined in a logic rule as severity=low.
	**Unknown**: Displays the alerts defined in a logic rule as severity=unknown. Any alerts without a category are also listed here.

Endpoints Status

This section displays information about your endpoints, including the number of inactive endpoints, the number of endpoints with open alerts, and the endpoints that have generated the most alerts in the past 7 days.



This section consists of three areas:

- Endpoint Status
- Alerted Endpoints
- Worst Offenders - Last 7 Days

On the right side of the section, there is a **Refresh** button that shows a menu that allows you to update data at selected intervals. The default option is **Disabled**.

Endpoint Status chart

This section displays the alerts as they relate to the endpoint.

The alerts are divided into the following categories:

- **Total**: Displays the total number of endpoints connected to Nuix Adaptive Security.
- **Active**: Displays the total number of connected endpoints with an active alert.
- **Inactive**: Displays the total number of endpoints not currently connected to Nuix Adaptive Security.

To the right of the total, active, and inactive endpoints status is a chart that displays a count of endpoints and the number of days an endpoint has been offline.

Alerted endpoints

The Alerted Endpoints area displays the number of endpoints with one or more active alerts.

An example of this is shown in the following image.

The alerts are divided into the following categories:

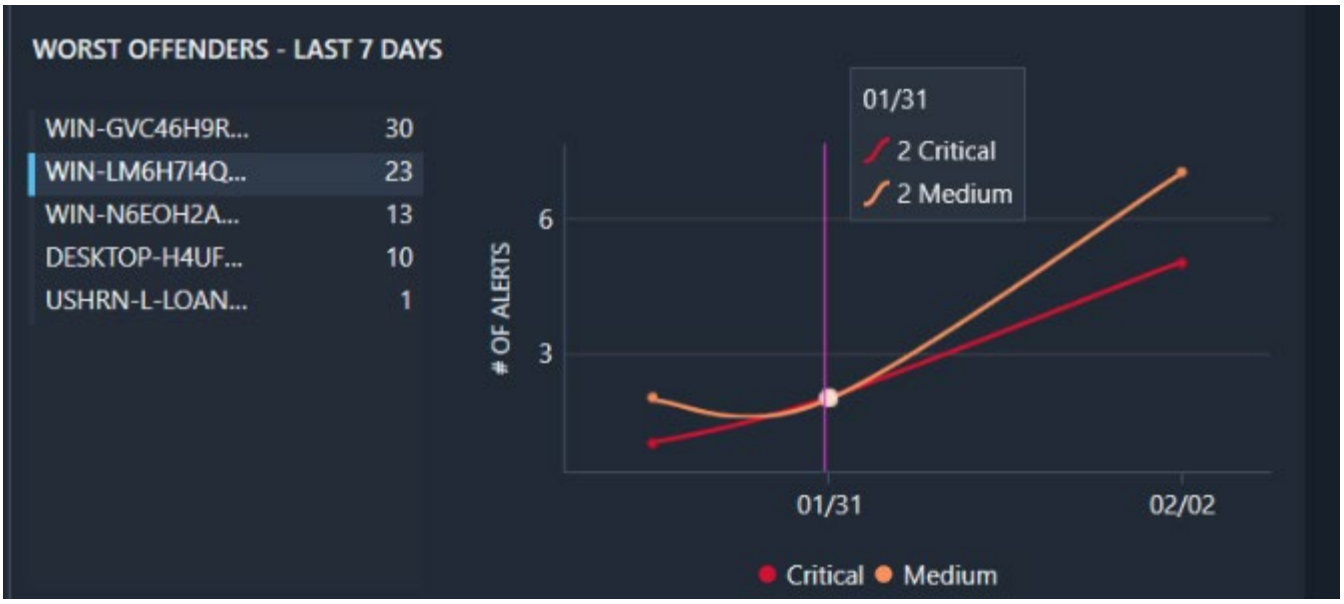
- **With Active Alerts**: Displays the number of endpoints with active alerts. The number next to the **Critical** icon is the number of endpoints with one or more critical alerts, and the number next to the **Medium** icon is the number of endpoints with one or more medium alerts. These categories are defined by how you set up your Logic Rules. For more information about Logic Rules, see Logic Rule.
- **Isolated**: Displays the total number of isolated endpoints. If there are isolated endpoints, the arrow is red.
- **High Value**: Displays the total number of endpoints in the High Value group. For more information about the High Value group, see Groups.

Click on any of the categories to display the endpoint details.

Worst Offenders - Last 7 Days

This section lists the endpoints generating the most alerts over the last 7 days.

An example of this is shown in the following image.

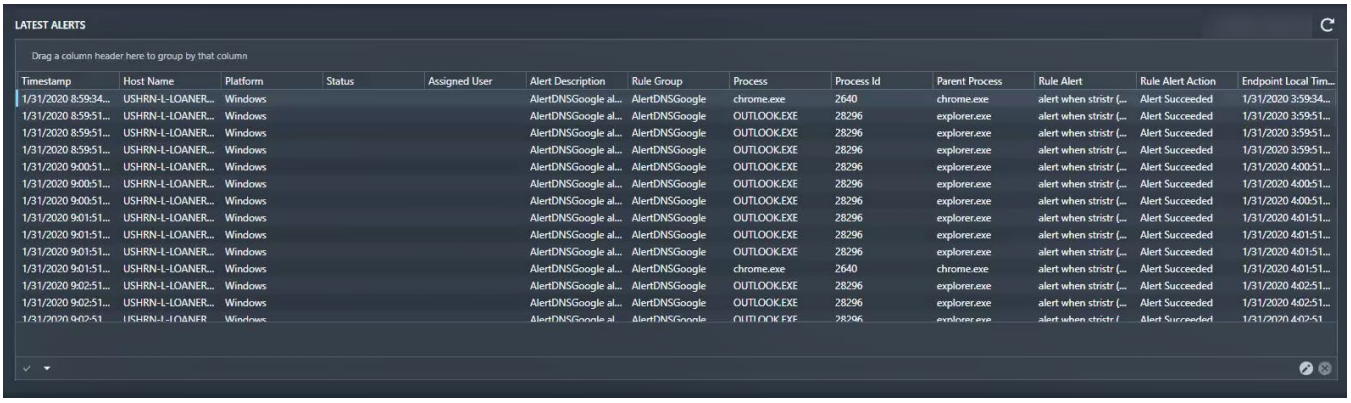


The chart displays the endpoints in the order of the number of alerts generated. The graph to the right displays the Critical and Medium alerts generated on the endpoint during the time period.

Latest Alerts

The Latest Alerts section displays the 1,000 most recent alerts occurring in the Nuix Adaptive Security environment.

Sort, search, and filter the alerts to quickly identify anomalous network activity.



On the right side of the section, there is a **Refresh** button. Select the Refresh button to select your refresh interval. For example, refresh the alerts every 30 seconds. The default option is **Disabled**.

Context menus for alerts

The context menus and options allow you to view your data in greater detail.

Right-click an alert row to show a menu with the following options:

Investigate: These options allow you to examine the data.

- **External Threat**: Opens a series of insights to help determine if the alert is from an external threat.
- **Insider Threat**: Opens a series of insights to help determine if the alert is from an insider threat.
- **Events**: Select from one of the following: Process, DNS, Network, Files, Loaded Modules, Sessions, Media, Keystrokes, Print, Registry to open the alert insight. The categories displayed depend on your selection.
- **Visualize**: Displays a process tree for the alert. For a discussion of this option in greater detail, see Visualize Option - Process Tree.

Respond: These options allow you to react to the threat found on the Investigate tab.

- **View Endpoint**: Shows the status of the endpoint on the Endpoint tab.
- **View File System**: Opens the File System tab on the endpoint that is the source of the alert.
- **Network Isolation**: Separates an endpoint from the network for further investigation. Use the arrow next to the menu option to click **Enable** or **Disable**.
- **Terminate Process**: Ends the process that triggered the alert.

Collect: These options allow you to gather data from the threat and their response to it.

- **Screenshot**: Creates a screenshot as a JPG or PNG by selecting the corresponding box. Adjust the image quality setting from 0 to 100. The default is 75.
- **Collect from Host**: Allows you to create and run a collection on the selected endpoint.
- **Collect this File**: Allows you to collect a specific file on the selected endpoint. Requires the file full path or file path and name.
- **Execute Command**: Runs a command on an endpoint using a command shell.

Alert: These options allow you to take a detailed look at and act upon individual alerts.

- **View Alert:** Provides more details on the alert.
- **Change Status**: Shows the current status of the alert and allows you to make changes to the status by choosing a value from one of the following categories:
  - **Active**: Unassigned, Pending Investigation, Investigation in Progress, Investigation on Hold, Investigation in Review.
  - **Closed**: Resolved, False Alert, No Investigation, Archive.
- **Assign User:** Assigns an alert to one of the users in the list.
- **Copy:** Copies the selection to the clipboard.

Filtering

Filter the data in the Latest Alerts section of the Dashboard.

Right-click any of the column headers to display the following pop-up menu options:

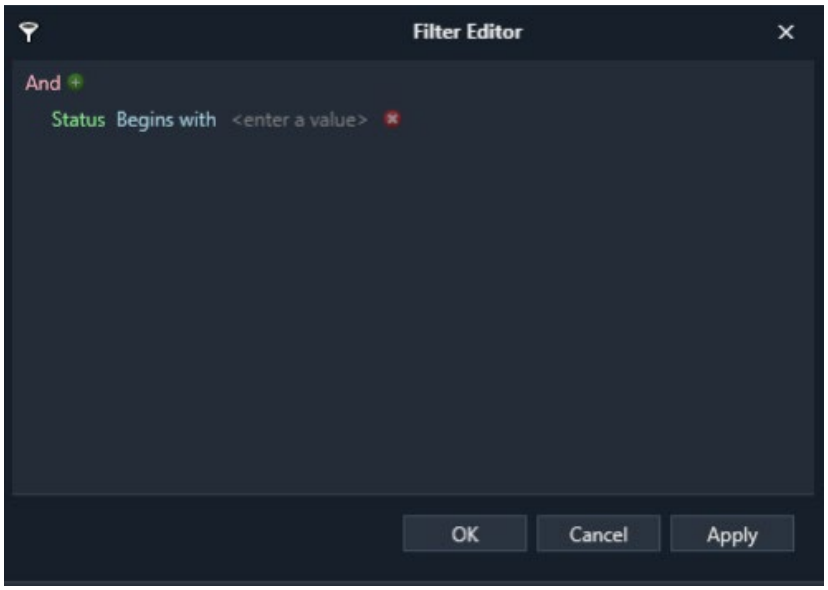
- **Sort Ascending**: Sorts the items in the column in ascending order.
- **Sort Descending**: Sorts the items in descending order.
- **Clear Sorting**: Returns the data to its default sorting.
- **Group by This Column**: Groups the data by the selected column.
- **Show/Hide Group Panel**: Shows the **Group** panel that allows you to group the data by column, or, if selected, to hide the group panel.
- **Show/Hide Column Chooser**: Opens a pop-up menu to select the columns to display. Use the search bar to find a column and it shows that column. A deselected column in this pop-up menu is displayed in the Latest Alerts section. For selected columns, this changes to **Hide** and removes the column. To close this box, click the **X** in the corner of the box.
- **Best Fit**: Shows the data with extra space removed from the column.
- **Best Fit (all columns)**: Shows the data with extra space removed from all the columns.
- **Filter Editor**: Creates filters manually, once you enter the criteria.

Dragging a column header to the **Group** panel above the data groups the data by column and shows the following options, in addition to those described in the previous section.

- **Full Expand**: Fully expands the data contained in the entire alert into a more readable format.
- **Full Collapse**: Collapses the data contained in the entire alert, allowing more to appear in the window.
- **Ungroup**: Removes any columns the data is grouped by. This replaced **Group by This Column**.
- **Group Summary Editor**: Provides a list of columns. This dialog box has two tabs:
  - **Items**: Select any of the values to use as a column header. Select the check boxes next to Min, Max, Average, or Sum to select one or all the values.
  - **Order**: Lists the values selected. Use the arrows to move the value up or down in the list. Selecting a value populates the boxes that appear below the list. These values can be set as follows:
    - **Prefix**: Lists the prefix selected in the list, for example, select Count and Count is displayed in the box.
    - **Display format text**: Uses one of the following options:
      - **Default**: None
      - **Number**: #.00, #, #, E2, n, n1, n2, e, e1, f, f1
      - **Percent**: 0.00, 0%
      - **Suffix**: Add a means of identifying the data.
      - **Example**: This renders based on what is in the Prefix, Display format text, and Suffix boxes.
  - To save the changes, click **OK.**

Filter Editor

The Filter Editor allows you to create queries you can use to refine your data.

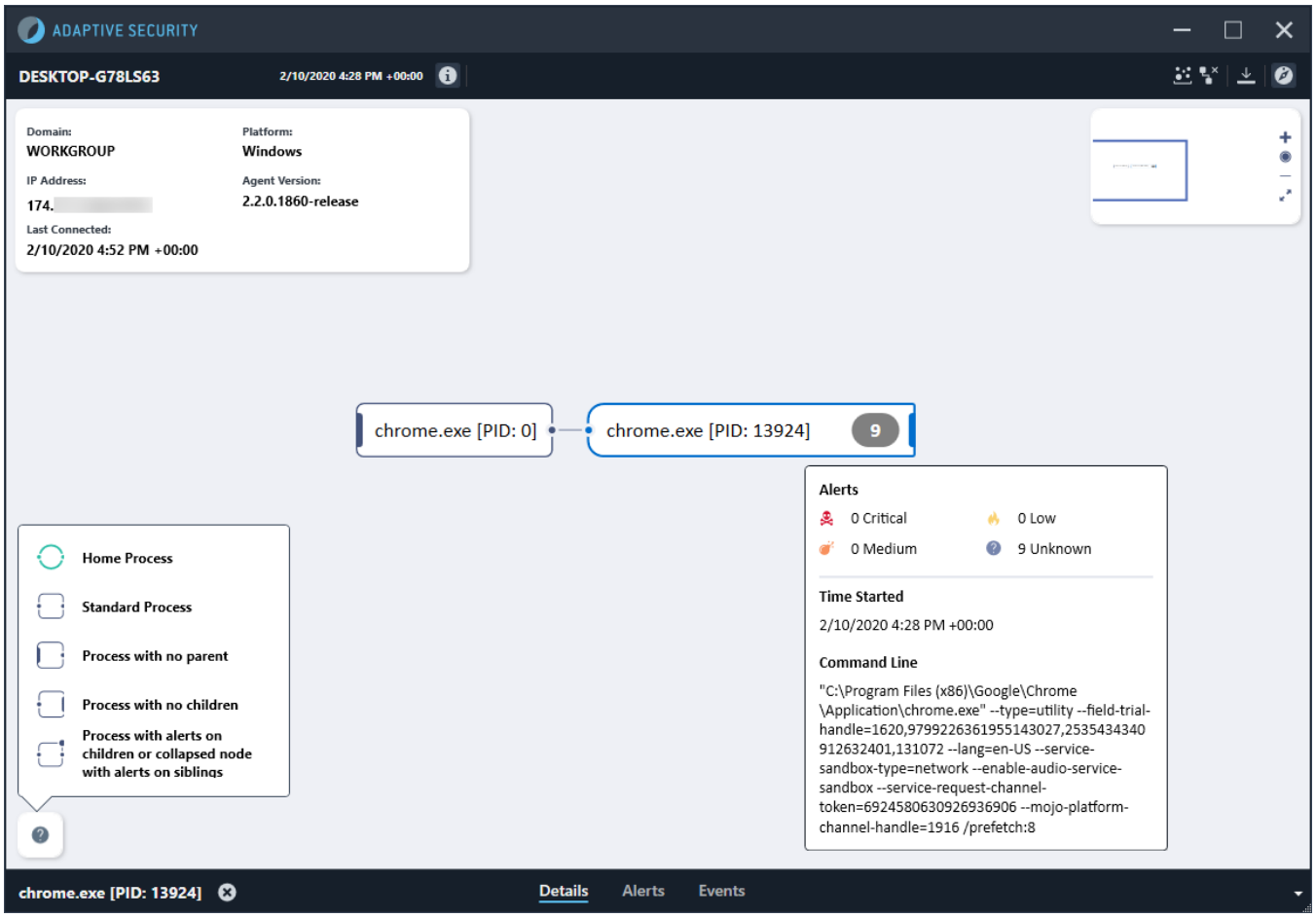


To create a filter using the Filter Editor:

1. Click the conditional operator, the word **And** shown in the previous image, and select one from the list.
2. Click the category and select one from the list.
3. Click the conditional operator, the word **And** shown in the previous image, and select one from the list.
4. Use the menu that is displayed or the search dialog box to find a variable category.
5. Once you have created your filter, click **Apply**.
6. Click **OK** to close the dialog box once you are finished.

Visualize option – Process Tree

Clicking this option allows you to visualize the execution of a threat as it happened on your endpoints. The Process Tree shows the relationship of the selected process to other processes on the endpoint and provides an interactive exploration of the current and past processes running on an endpoint. Use the Process Tree to gain quick and easy access to all the events that a given process executed to perform investigative or remediation actions, for example, to isolate a process.



Use the toolbar

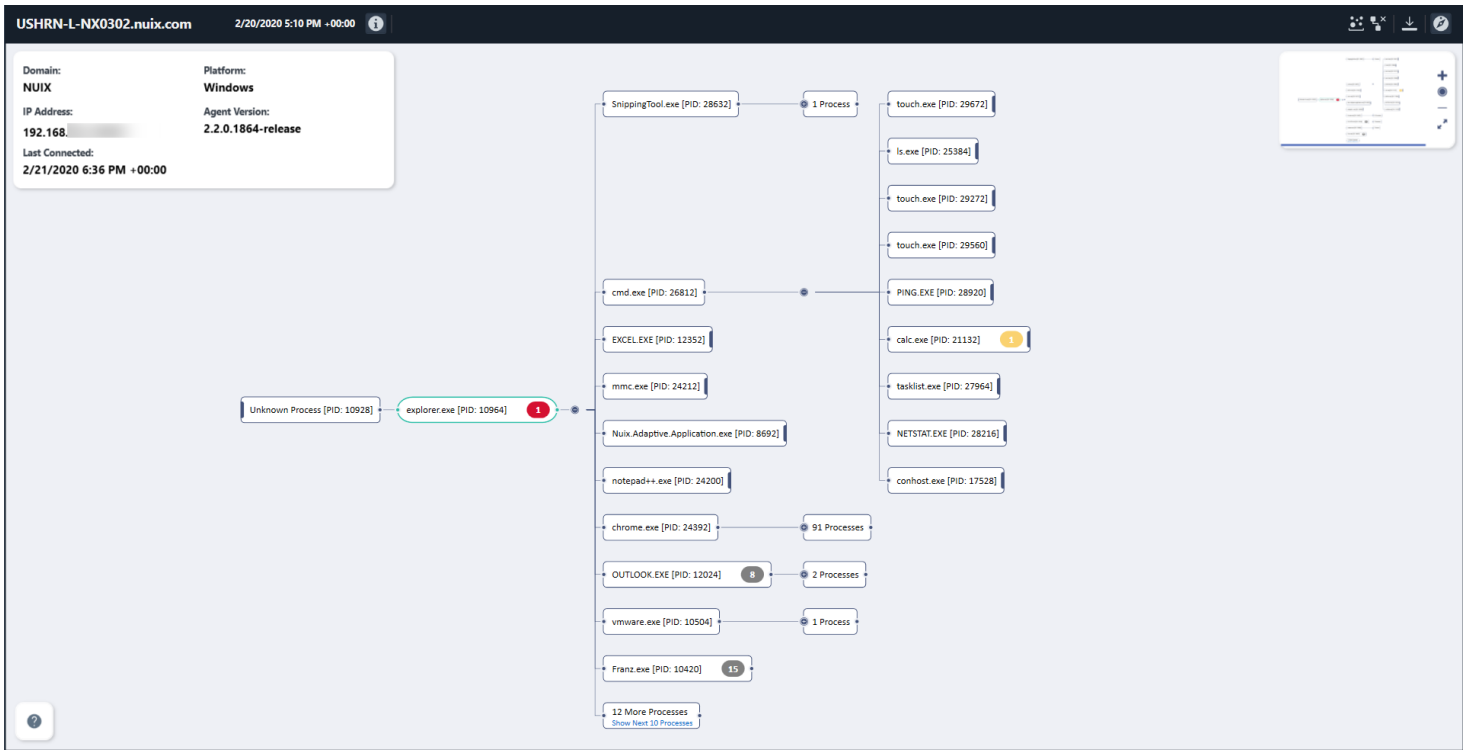
The host name for the computer (for example, computername.place.com) and the timestamp are listed on the left side of the toolbar. Clicking on the information button toggles the host information window that contains information about the endpoint.

The right side of the toolbar includes buttons for the options described in the following table.

Button	Description
	**Isolate Endpoint:** Displays the **Isolate Endpoint** dialog box. If you want to isolate this endpoint, click **OK**. For more information about this topic see Network Isolation.
	**Download Diagram**: Displays the **Export As**…dialog box. Use this window to save a JPEG copy of the diagram to your machine.
	**Toggle Navigation:** Shows or hides the navigation pane.

Use the canvas

The canvas displays the process interactions with other processes on the endpoint. An example canvas is shown in the following image.



Host Information Window

View the host information window in the upper-left corner of the canvas. You can view the following information:

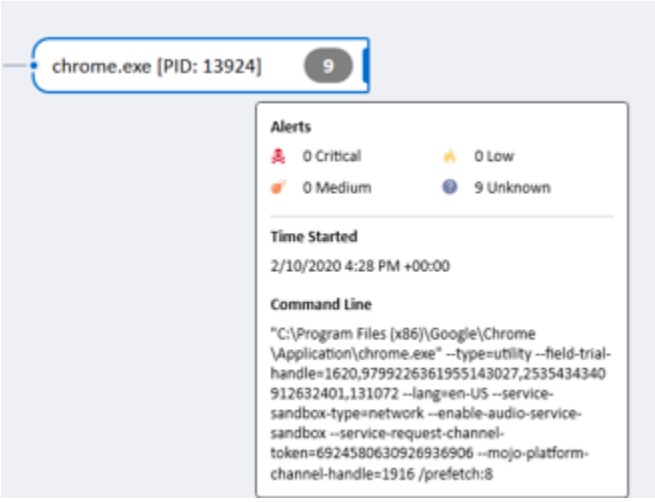
- **Domain**: Displays the endpoint's domain name.
- **IP Address**: Displays the IP address of the endpoint.
- **Last Connected**: Displays the time that the latest connection to the endpoint was established with Nuix Adaptive Security. For example, if you initiate a connection at 10:30 AM but are viewing the process tree at 11:15 AM and the connection is still open, the time displayed will be 10:30 AM.
- **Platform**: Displays the platform installed on the endpoint.
- **Agent Version**: Displays the version of the Nuix Adaptive Security Agent running on the endpoint.

Legend

Click the information button in the lower-left corner of the canvas to display the legend that contains the information found in the following table.

Button	Description
	**Home Process**: This is the root process node currently being visualized.
	**Standard Process**: This is a standard process and may or may not be a descendant of the home process.
	**Process with no parent**: This is a process without a parent process.

Button	Description
	**Process with no children**: This is a process that spawned no other processes.
	**Process with alerts on children or collapsed node with alerts on siblings**: This is a process whose children have one or more alerts. If the process is a collapsed node, the red dot appears if one of the processes in the collapsed node has an alert.

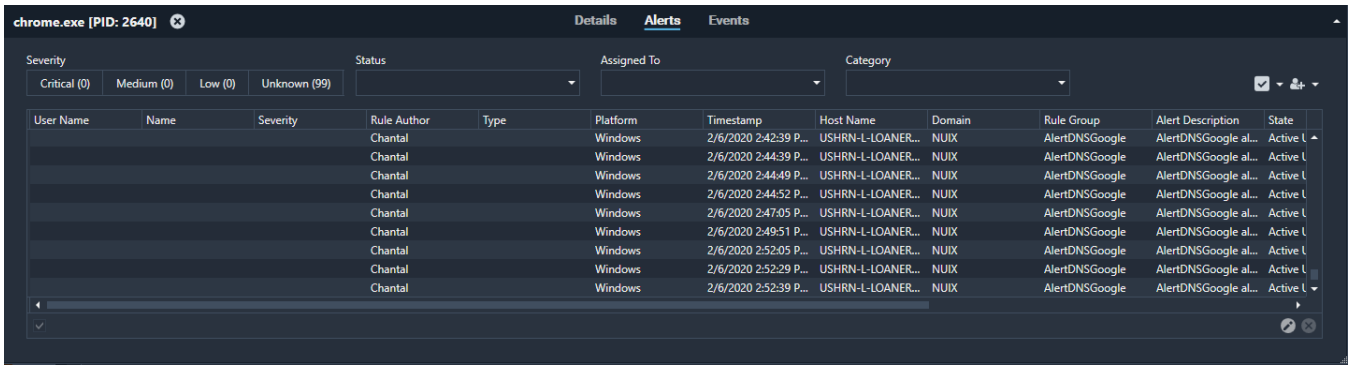


Hover over a node in the process tree to display more information about the node. In the example shown in the previous image, the node has more than 99 alerts classified as Unknown. These alerts can be viewed by clicking on the Alerts tab of the Process Information pane.

Note: If there are over 100 nodes, you see a message that says “100+ more nodes.” Nuix Adaptive Security does not open all these nodes, because doing so may impact performance.

Use the Process Information pane

Clicking one of the nodes or processes in the process tree shows a tab in the bottom part of the window, as shown in the following image. The data for the process is displayed on one of the following tabs:



- **Details**: Lists the Process, User, and Parent Process data for the process. The following process information is in each category:
  - **Process:** PID, Command Line, MD5, Create State, Exit Time, Signature Status, Directory, and Full Path.
  - **User:** User SID, User ID, and Process User.
  - **Parent Process:** Parent Process ID, Parent Name, Parent Exe File Path, and Parent Path.
- **Alerts**: Lists alerts triggered by the selected process. Use Severity, Status, Assignee, and Category to filter the alerts.
  - Set Severity to Critical, Medium, Low, or Unknown. For more information about this topic, see Alert Categories.
  - For more information about Statuses and Assignees, see Context Menus for Alerts.
  - For more information about the options found under Category, see Results List.
- **Events**: Lists the events triggered by the selected process. Events are shown by type. Select one of the following from the menu: Agent Shutdowns, Processes, Loaded Modules, Key Logs, Files, Registry, Network, Removable Media, Namespace Queries, and Print. These are discussed in greater detail in Insight data sources. You can reorder the data in ascending or descending order by clicking on the arrow at the top of the column. You can also filter the data by right-clicking on any of the column headers. The options in this menu are discussed in greater detail in Filtering.

Note: The option to drag column headers is not available when using the Visualize option.

Click on the **X** next to the name of the process to terminate that process.

Warning: You can terminate any Process or Parent Process from this window but doing so to some processes may cause the impacted endpoint to display an exception error or forcibly reboot itself.

Click the arrow on the bottom right side of the box to hide or show the bottom part of the window.

Alerts

The Alerts tab lists alerts generated by Nuix Adaptive Security. The alerts are generated by the logic rules in the agent that are executed on the endpoint. Alerts are notifications that specific events occurred on the endpoint.

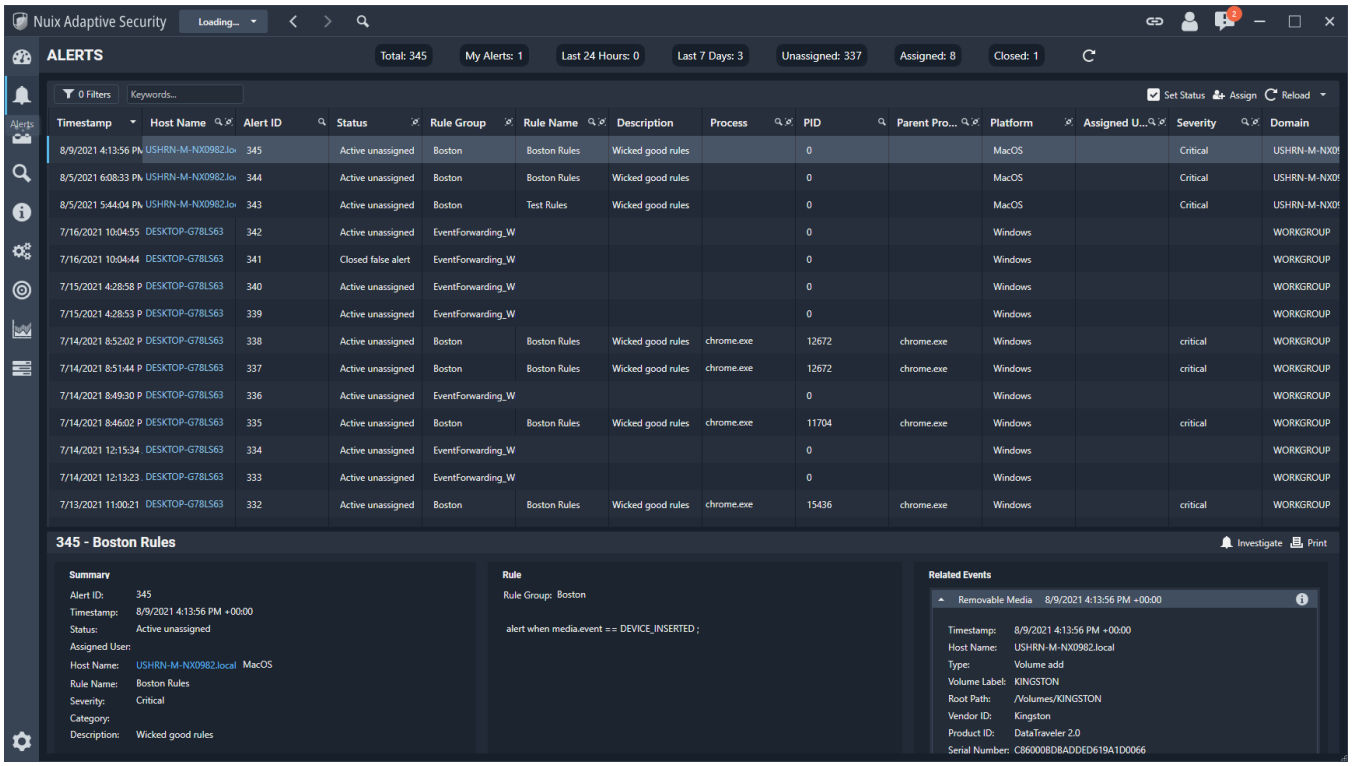
Note: Logic rules that generate many alerts lead to decreased performance of the application at startup. This degradation will continue until the database times out.

You can set alert limits to avoid performance issues.

- Add ViewLimitAlert with a value of 10000 in web.config and make the following edit to the my.ini file:

```
Innodb_adaptive_hash_index_parts=64
```

Filter the data by using the filters in the Alerts pane on the top-left corner of the tab. View the alerts in the Alerts pane. View the alert's detailed description on the bottom pane. An example alert is shown in the following image.



Quick Filter options

The Quick Filter options are available to further refine the data.

Refine the data using the following options:

- **Quick Filter**: Filter the results, using any of the following categories: My Alerts, Last 24 Hours, Last 7 Days, Assigned, Unassigned, Total, and Closed. **Total** is the default value.
- **Date Range**: The first box defaults to **From Date**. To make a change to this value, click the menu arrow to show the calendar, and click a date. The second box is the **To Date**. To make a change to this value, click the menu arrow to show the calendar, and modify the value.
- **Assigned**: Click **Select a User** to show the list of users and select one from the menu.
- **Status**: Use **Select a Status** to show all the data. Click the menu to select from one of the following statuses:
  - **Active**: Unassigned, Pending Investigation, Investigation in Progress, Investigation on Hold, or Investigation in Review.
  - **Closed**: Resolved, False Alert, No Investigation, or Archived.
- **Endpoints**: For more information about this topic, see Endpoint Selector.
- **Keywords**: Enter a search term and the results will contain just the term. Click **Reset** to clear the search bar. Click **Filter** to narrow the results by search term.

Results list

Located under the Quick Filter list, this section shows all the generated alerts.

Refine the results by selecting from one of the following categories:

- **Timestamp**: Displays alerts by their timestamp, with the earliest ones first.
- **Type**: Displays alerts by their type. Shows all the results.
- **State**: Alerts are organized by the status listed under Filter Options in Quick Filter Options.
- **Process**: Displays alerts by Process. In the detailed view of the alert, you can use the X next to the process name to terminate the process.
- **Assigned User**: Displays alerts by the Assigned User. Alerts with no user assigned will be listed first.
- **Host Name**: Displays the name of the endpoint where the alert takes place.
- **Domain**: Displays the alerts by their domain.

Alert options

Right-click any of the alerts listed on the bottom-left side of the pane, and a menu appears with the following options:

- **Change Status**: View the status of the alerts and make changes to the alerts by choosing a value from one of the following categories:
  - **Active**: Unassigned, Pending Investigation, Investigation in Progress, Investigation on Hold, Investigation in Review.
  - **Closed**: Resolved, False Alert, No Investigation, Archive.
- **Assign User**: Assign an alert to one of the users in the list by selecting the user.

Detailed view of an alert

The alerts are organized using the following filters at the top of the tab:

- **Total**: Shows the total number of alerts logged by Nuix Adaptive Security.
- **My Alerts**: Shows the alerts assigned to you.
- **Last 24 Hours**: Shows the number of alerts logged within the last 24 hours.
- **Last 7 Days**: Shows the number of alerts logged within the last 7 days.
- **Unassigned**: Shows the number of alerts not assigned to a user.
- **Assigned**: Shows the number of alerts assigned to ablo user.
- **Closed**: Shows the number of alerts that have any of the Closed statuses discussed in Quick Filter Options.

Warning: You can terminate any Process or Parent Process from this window but doing so for some processes may cause the impacted endpoint to display a bluescreen or forcibly reboot itself.

To terminate the process if the alert has negative consequences for an endpoint:

1. Navigate to the alert that contains the process.
2. Select the related Process or Parent Process.
3. Terminate the process by clicking the **X** next to the process.
4. Confirm this action by clicking **Execute** in the dialog box.

Alert information

Alert information contains more detailed data about the specific alert. An example is shown in the following image.

The following information is available on the Alert Information section of the tab:

- **Timestamp**: The date and time of the alert's generation.
- **Host Name**: Name of the endpoint where the alert takes place.
- **Alert ID**: Displays the alert identification number.
- **Status**: Current status of the alert. For more information about this topic, see Context Menus for Alerts.
- **Rule Group**: Name of the rule group generating the alert.
- **Rule Name**: Name of the logic rule that generated the alert.
- **Description**: Description of what causes the alert to generate. An example description is "more than *n* files copied in *n* seconds to removable media."
- **Process**: Name of the process that generated the alert.
- **PID**: ID of the process that generated the alert.
- **Parent Process**: Name of the parent process that generated the alert.

Warning: While you can terminate any Process or Parent Process from this window, doing so for some processes may cause the impacted endpoint to display a bluescreen or forcibly reboot itself.

- **Platform**: Operating system of the endpoint.
- **Assigned User**: For alerts assigned to a user, the assignee appears here.

- **Severity**: Alert severity level as 1, low, medium, and critical.
- **Domain**: Domain of the endpoint.

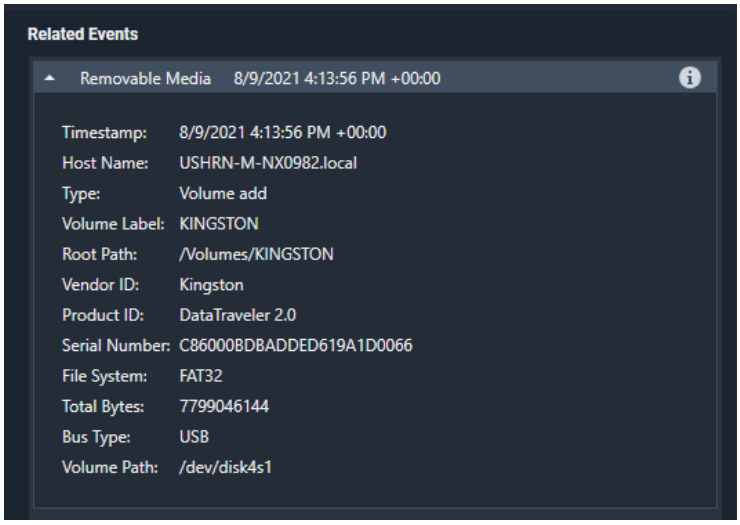
Summary

The Summary section provides detailed information for the alert including:

- **Alert ID**: Displays the alert identification number.
- **Timestamp**: The date and time of the alert's generation.
- **Status**: Current status of the alert. For more information about this topic, see Context Menus for Alerts.
- **Assigned User**: For alerts assigned to a user, the assignee appears here.
- **Host Name**: Name of the endpoint where the alert takes place.
- **Severity**: Alert severity level as 1, low, medium, and critical.
- **Category**: The category as defined by the user.
- **Description**: Description of what causes the alert to generate. An example description is "more than *n* files copied in *n* seconds to removable media."
- Rule
  - **Rule Name**: Name of the logic rule that generated the alert.
  - **Rule Group**: Name of the rule group generating the alert.

Related events

This section provides information related to the generation of the alert, as shown in the following image.



The information here varies depending on the type of event. For example, if the related event is about removable media, the information listed includes information such as the serial number and the amount of free space on the device.

Screenshots

When an alert has an associated screenshot, you can view the screenshot under Alert Details > Screenshot. You can view, resize, save, and open the screenshot in the viewer.

Collection

When an alert has triggered a collection associated with it, you can view in under Alert Details > Collection. For more information, see Collections.

Content inspection

View the matched content including:

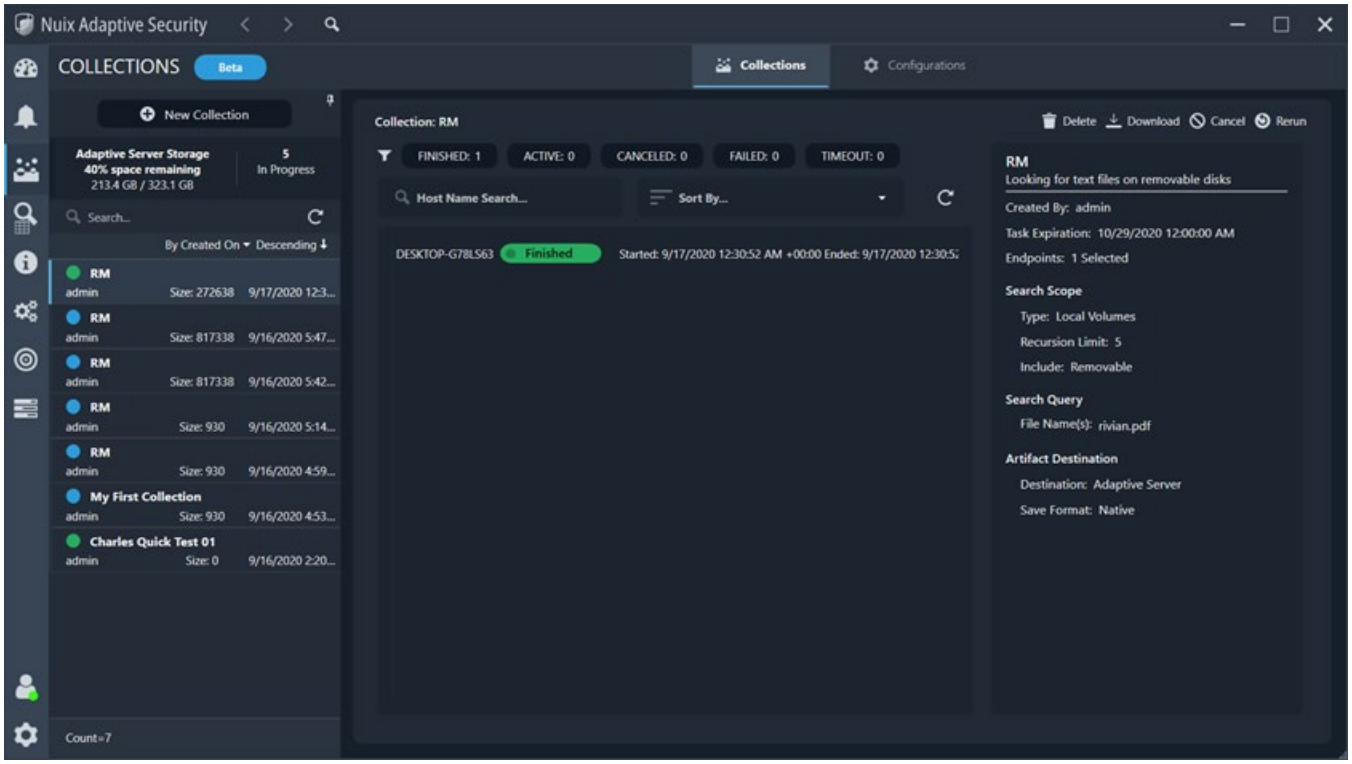
- File full path
- Rule name
- Rule group
- Rule
- File name and expression details

Collections

The Collections tab is where you can manage, configure, and schedule collections in the Nuix Adaptive Security application. Run targeted collections to obtain specific files from endpoints across the network. Types of targeted file collections include:

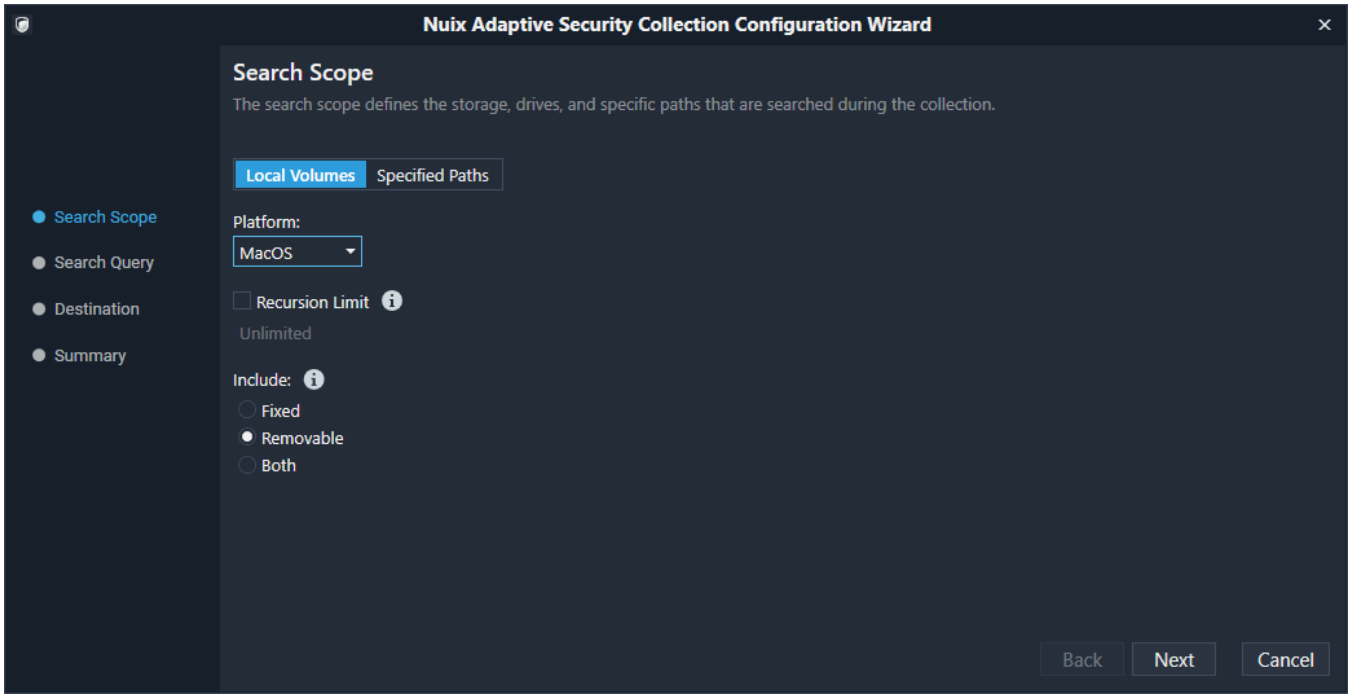
- Incident Response Collection
- Browser History Files
- User Documents
- Email Stores and Archives
- All Image and Media Files

In the Nuix Adaptive Security application, there are two wizards, the collection wizard and the configuration wizard. You can create and save configurations for running the collection. The configuration defines what you are searching for and how you want to search during a targeted collection. You can collect specific files by using the full path and file name. Create and run the collection using the collection wizard. A collection is a group of tasks to send to the endpoint. In the collection wizard, you can select from a list of saved configurations or create one in real time.



Collection configurations

Create configurations using the Collection Configuration Wizard, shown in the following image. The configuration acts as a template for the collection. The configuration defines what you are searching for and how you want to search during a collection.



The collection configuration fields are described in the following table.

Collection configuration	Description
Search Scope	The search scope defines the storage, drives, and specific paths that are searched during the collection. Select the endpoint platform for the collection which includes Windows, macOS, and Linux. The recursion limit sets the maximum depth of subfolders to be searched within the specified directory paths.
Search Query	The search query defines the types of files, file location, date of the file, and file size for the collection. Comma-delimited string expressions inside the **File Name**, **File Path**, and **MD5s** boxes are used as search criteria to find files in the Search Scope. For example, in the File Name box, enter docfile1, docfile2, and docfile3, and the collection will match on any of these specific file names. The **Date Range** defines when the file was created, accessed, or written. The **File Size** range is limited to 10 characters. Use the up arrow to type additional characters.
Destination	The destination is where you save and store the collected data. You can save the collection to the Nuix Adaptive Security server, a network drive, the endpoint local drive, or an Amazon S3 bucket. Save the file as a native file or compressed in a password-protected .zip. **Note**: Due to the type of encryption, use 7-Zip to extract the encrypted files.
Summary	The summary includes the configuration name and description. Set the **Task Expiration,** which will cancel the task if the task takes longer than the set date.

Create collection configurations

To create the collection configuration:

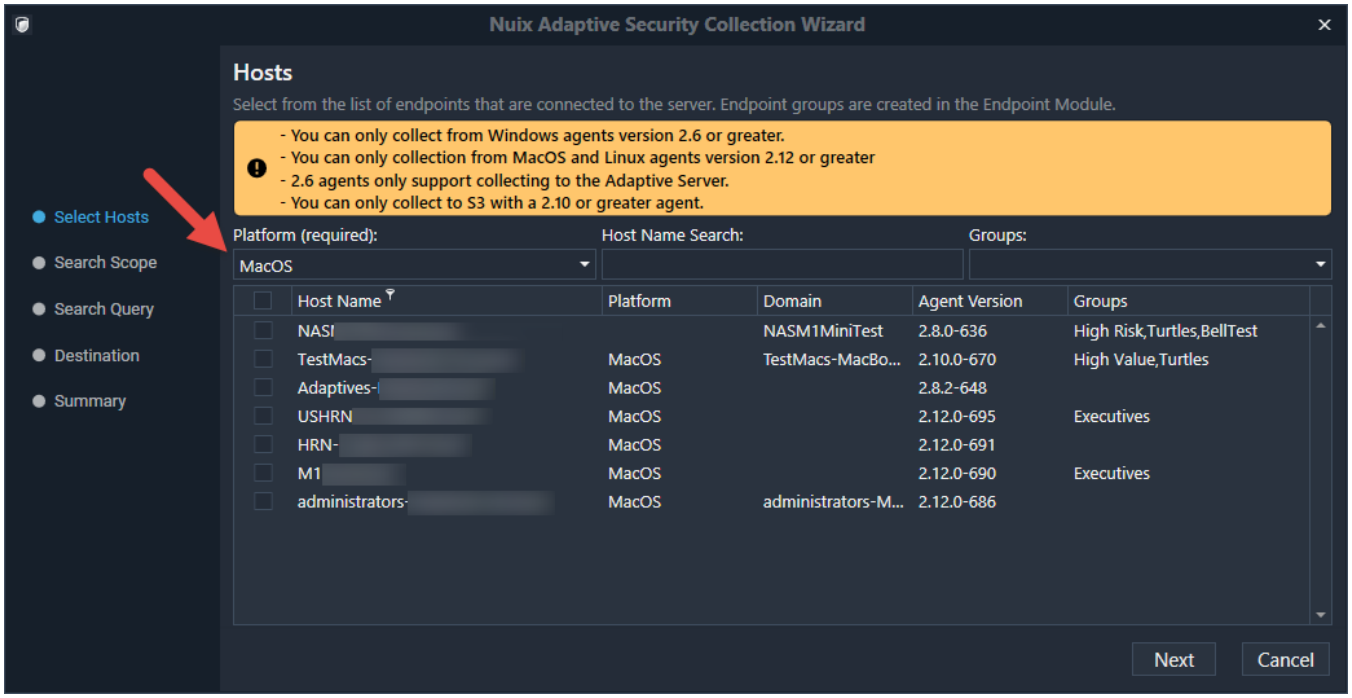
1. On the **Collections** tab, select the **Configurations** tab and select **+ New Configuration**.
2. Enter the **Search Scope**. Click **Next**.
3. Enter the **Search Query**. Click **Next**.
4. Enter the **Destination**. Click **Next**.
5. Enter the **Summary**. Click **Save**.

Create collections

Create and run collections using the Collection Wizard, as shown in the following image. In the Collection Wizard, you can select from one of the saved configurations, create a new configuration, or edit an existing configuration.

Warning: Consider limiting your search query, specifically the number of files you collect. This will directly affect your bandwidth, disk space, and the length of time it takes to collect the files.

Consider using a network drive instead of the local drive when performing large collections.



Collections limitations

The collections feature has some limitations depending on the agent versions.

- You can only collect from Windows agents version 2.6 or greater.
- You can only collect from macOS and Linux agents version 2.12 or greater.

To create the collection:

1. On the **Collections** tab, select **+ New Collection**.
2. Select from the list of saved configurations. For more about creating collection configurations, see Collection Configurations. Click **Next**.
3. Click on **Select Hosts**, you must select the **Platform** to populate the list of hosts with the corresponding platform. Then select hosts or groups of hosts to collect data. Endpoint groups are created in the Endpoint Module. For more information, see Groups. Click **Next**.
4. Verify the remaining configuration settings. Click **Next**.
5. Select to **Run** the collection.

Work with collections

The Collections tab is where you can manage, configure, and schedule collections. After a collection is complete, you can save it as a .zip file. You can also cancel, rerun, download, or delete collections.

In the Collections Explorer, you can do the following:

- **+ New Collection**: Create and run a new collection.
- **Adaptive Server Storage**: View the available server storage.
- **In Progress**: View the number of collections in progress.
- **Search**: Search for saved collections.

In the Collections List, you can do the following:

- **View collection status**: The status options include Finished, Active, Canceled, Failed, and Timeout.

- **Search**: Search for collections using the host name.
- **Sort by**: Filter collections based on specified criteria.

In the Collections Details, you can do the following:

- **Collections Toolbar**: Delete, Download, Cancel, and Rerun the selected collections.
- **Configuration Details**: View the selected host's Collection Configuration details.

Example collection use cases

This section describes real-world use cases for Collections.

Collect all files from a directory

This example is for collecting all files from the c:\temp directory.

In this example, you know the absolute path of the directory so you can use that as the search root. This means the search will start here and traverse the directory structure. Collecting all files is simple as you will leave all search conditions blank.

To collect all files from a directory:

1. Open the **Collection Wizard**.
2. Select the hosts for the search.
3. In **Search Scope**, select the **Specified Paths** and enter the path c:\temp into the text box.
4. In **Search Query**, leave all fields blank and click **Next**.
5. Check the Name, Description, and Task Expiration, update them if desired, and click the **Run** button.

Collect executable files from a directory

This example is for collecting executable files (.exe) from the c:\windows\system32 directory.

In this example, you know the root directory for the search, so you can specify the path.

To collect executable files from a directory:

1. Open the **Collection Wizard**.
2. Select the hosts for the search.
3. In **Search Scope**, select the **Specified Paths** and enter the path c:\windows\system32 into the text box.
4. In **Search Query**, in the **File Names** box enter *.exe to match on the file name. The * will match any number of characters before the .exe part of the file name.
5. Check the Name, Description, and Task Expiration, update them if desired, and click the **Run** button.

Collect from endpoints

You can run a collection by selecting a specific endpoint on the **Endpoint Insight** page. Right-click on the endpoint and choose **Collect from Host** or **Collect this File** to open the Collection wizard.

File content inspection and collection

Rule based file content inspection allows you to write rules to perform regular expression pattern matching against file content. The file inspection action in the rule language will trigger a regular expression search against a single file, and if any of the supplied regular expressions result in matches an InspectFileMatch event containing all the match details for that inspection is generated and sent through the filter engine.

Rule Base File Collection allows you to write rules to retrieve files from an endpoint back to the server.

While these two capabilities can be used independently, there are many use cases in which they are used together to collect evidence from the endpoint.

An example use case is detecting exfiltration of sensitive data using removable media devices like thumb drives. When files are written to a USB thumb drive, the files are searched for sensitive content and, if found, collected back to the server for further analysis.

Here is a simplified rule example.

```
uses "Nuix Base";

Rulegroup ThumbdriveExfil
{

global string g_Regexes[]=
{
      "(?i)proprietary and confidential",
      "(?i)project x"
};

 inspectfile(file.path, g_Regexes, "ThumbdriveExfil") when
nias::bRemovableMediaWrite == true;
 collectfile(inspectfilematch.path) when
strcmp(inspectfilematch.label,"ThumbdriveExfil", false);
}
```

The file inspection rule above will trigger a regular expression search against any file that is written to a removable media device such as a thumb drive. The parameters of the InspectFile action include the path of the file to inspect, a variable supplying a list of regular expressions to search, and a label string. The label string is used to differentiate the InspectFileMatch events when there are multiple InspectFile rules. Multiple InspectFile rules could exist, and you may desire to process matches differently from each of those InspectFile rules.

The regular expressions in use in this example include data classification markings and specific project names. If any matches are found, an InspectFileMatch event is generated. The CollectFile rule will match InspectFileMatch events with the label “ThumbDriveExfil”.

A second similar use case is detecting web browser exfiltration. If Microsoft Office or PDF files are opened by a web browser (presumably for uploading the file to the cloud) they are scanned for sensitive content. If sensitive content is found, you can collect a copy of the file and also take a screenshot of the desktop to gain further context about where the file was being uploaded.

Here is a simplified rule example.

```
Rulegroup BrowserExfil
{

global string g_Regexes[]=
{
      "(?i)proprietary and confidential",
      "(?i)project x"
};

global string gBrowserList[]=
{
      "msedge.exe",
      "chrome.exe"
};

global string gWatchedExtensions[]={
      ".pdf",
      ".docx",
      ".doc",
      ".ppt",
```



```
      ".pptx",
      ".xls",
      ".xlsx"
};

inspectfile(file.path, g_Regexes, "BrowserExfil") when
      file.event == FILE_OPEN and
      endswith(file.path, gWatchedExtensions, FALSE) and
      endswith(curproc.path, gBrowserList, false);

collectfile(inspectfilematch.path) when
strcmp(inspectfilematch.label,"BrowserExfil", false);
screenshot(inspectfilematch.pid, 2, 10) when
strcmp(inspectfilematch.label,"BrowserExfil", false);

}
```

File inspection algorithm

The algorithm employed by the File Inspection feature determines the type of file being scanned based on the file extension. It then parses the file based on file type and generates a normalized text stream. Regular expression pattern matching is then performed against the normalized text stream. The following file extensions are recognized: PDF, DOCX, DOCM, PPTX, XLSX, ZIP, TXT, ZIP, DWG, DWF, DXF, DWXF.

Specific file types

Files with ".txt" extensions are checked for byte order marks and then parsed appropriately as either Unicode or ASCII.

In the case of files with unrecognized extensions (ones that are not listed above) a best effort is made to search the file by treating it as if it were a ".txt" file.

In the case of files with a ".zip" extension, they can only be processed if they are not encrypted and not password protected. When processing a zip file the files contained in the archive are enumerated and searched individually based on their file extensions.

Due to the nature of Office documents, the text stream produced for searching will sometimes include special meta data. See Notes on Searching Office Documents below for more information.

Regular expression engine

The regular expression engine used for searching is the Microsoft .Net regular expression engine. It is compatible with Perl 5 regular expressions and adds some additional features. A regular expression language reference guide can be found here: external link - Regular Expression Language - Quick Reference.

Search office documents

Office documents are archive files containing numerous XML files that are processed and assembled by Office applications to "build" the document on screen. In addition to the actual content of the document body, there is also metadata. One such case of metadata is the Microsoft Sensitivity Label data.

The text stream generated for Office documents by the Adaptive File Inspection algorithm represents sensitivity label data in a special format to provide for easier matching and for a better contextual understanding of result data.

For example, here is a custom.xml file from a docx file.

Each of the properties are represented in the generated text stream using the following format:

```
MSIP_Label_[name]=[value]
```

The specific strings generated for this example are:

```
MSIP_Label_Sensitivity=Confidential Restricted
MSIP_Label_Enabled=true
MSIP_Label_SetDate=2020-05-06T14:12:36Z
MSIP_Label_Method=Privileged
MSIP_Label_Name=Not Encrypted
MSIP_Label_SiteId=fd799da1-bfc1-4234-a91c-72b3a1cb9e26
MSIP_Label_ActionId=eb48ec5b-23b1-4808-9c79-00006793cf1c
MSIP_Label_ContentBits=0
```

An example regular expression to match a particular label would look like this:

```
MSIP_Label_Name=Not Encrypted
```

Search

The Search tab lets you find specific information by searching for specific files in a directory.

Files can be located using their root path and the file name or MD5 values. To search by multiples of these values, separate the values with a comma. These searches run recursively from a point in the path through the rest of the directory.

Note: Searches performed using MD5 can cause high disk read times.

You can perform file searches on Windows, Mac, and Linux endpoints. This creates a task in the Nuix Adaptive Security server. View this task in the Task Explorer while the query is ongoing or active. Go to the **Tasks** tab to view the task and further examine the information generated. For more information about what you can view on the Tasks tab, see Tasks.

Using the following file path example, with the root path `/folder` as the search term, the search checks any data that appears in `/folder` through the end of the file path.

Examples:

- **Root path**: In the following example, the user's name is User 1: *C:\Users\User 1*
- **MD 5 Value**: 8cf52f8ad0c0d7230ac53b6fa64b0327

Wildcards are used to represent one or more other characters. You can perform file searches using wildcard characters. The Nuix Adaptive Security wildcard syntax supports the asterisk (*) and question mark (?) characters. The asterisk (*) represents any number of characters in a file name search. For example, search for all document files using ***.doc**. The question mark (?) matches one character in a file name search. For example, search for XML-style office documents using ***.???x**.

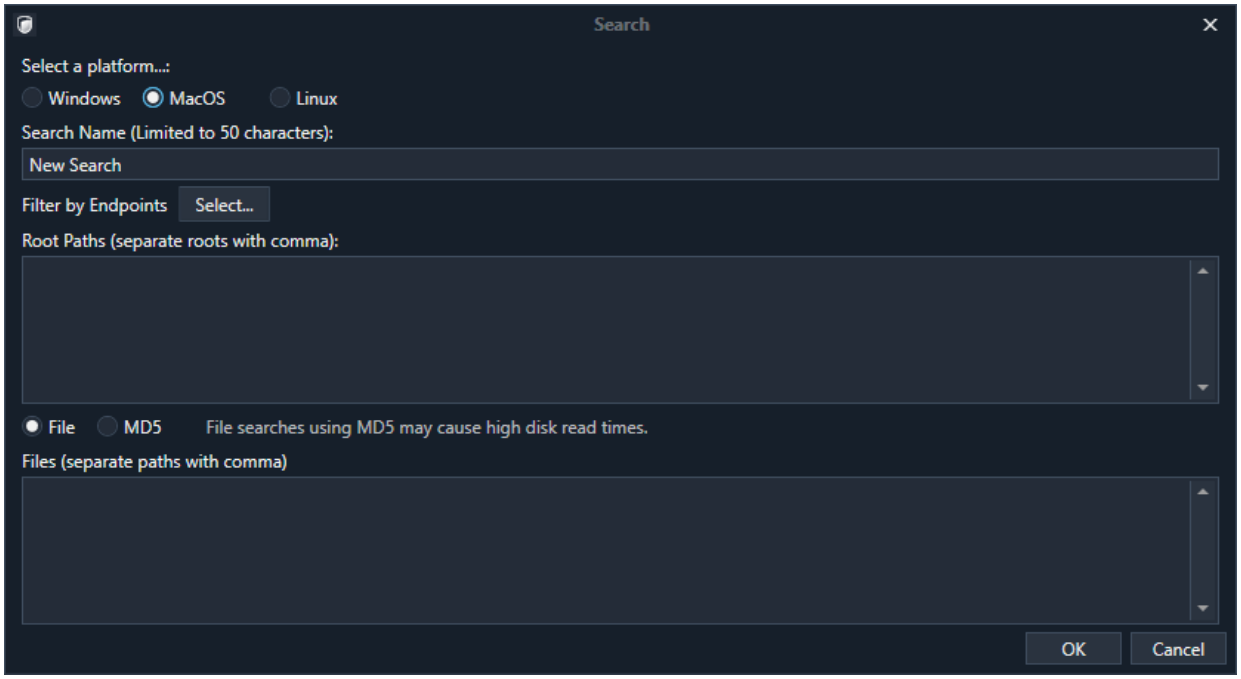
Wildcards cannot be used in file path searches.

Search for files

To access the **Search** dialog box, click the **Search** button at the top of the application or on the main vertical navigation bar.

To start a search:

1. Click the **Search** button at the top of the application. The **Search** dialog box appears, as shown in the following image.



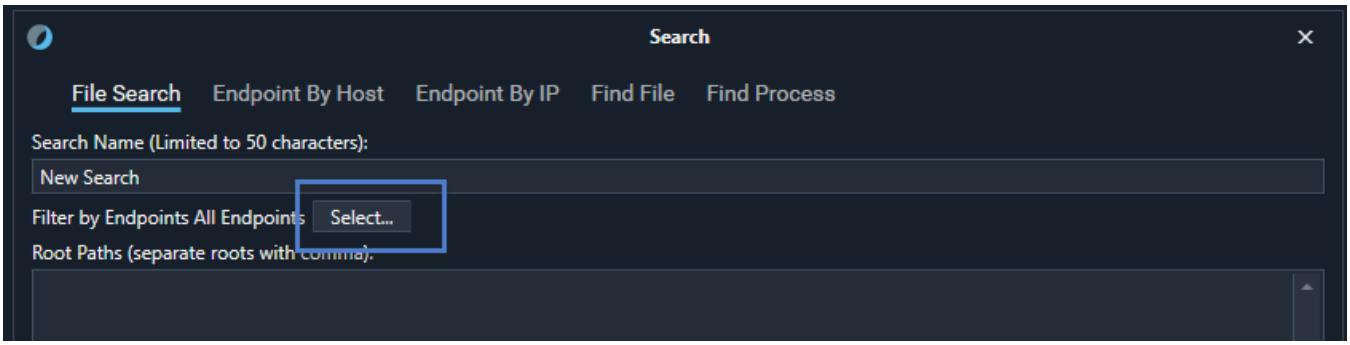
2. (*Optional*) Enter a name in the **Search Name** box. The search name is limited to 50 characters. If you do not enter a new name for a search, the search name defaults to **New Search.**
3. To select a specific endpoint or all endpoints, click **Select**. In the **Select Endpoints** dialog box, you can select a single endpoint from the list, or select all the endpoints in your instance. For more information about this, see Endpoint Selector.
4. Click **OK**.

Endpoint Selector

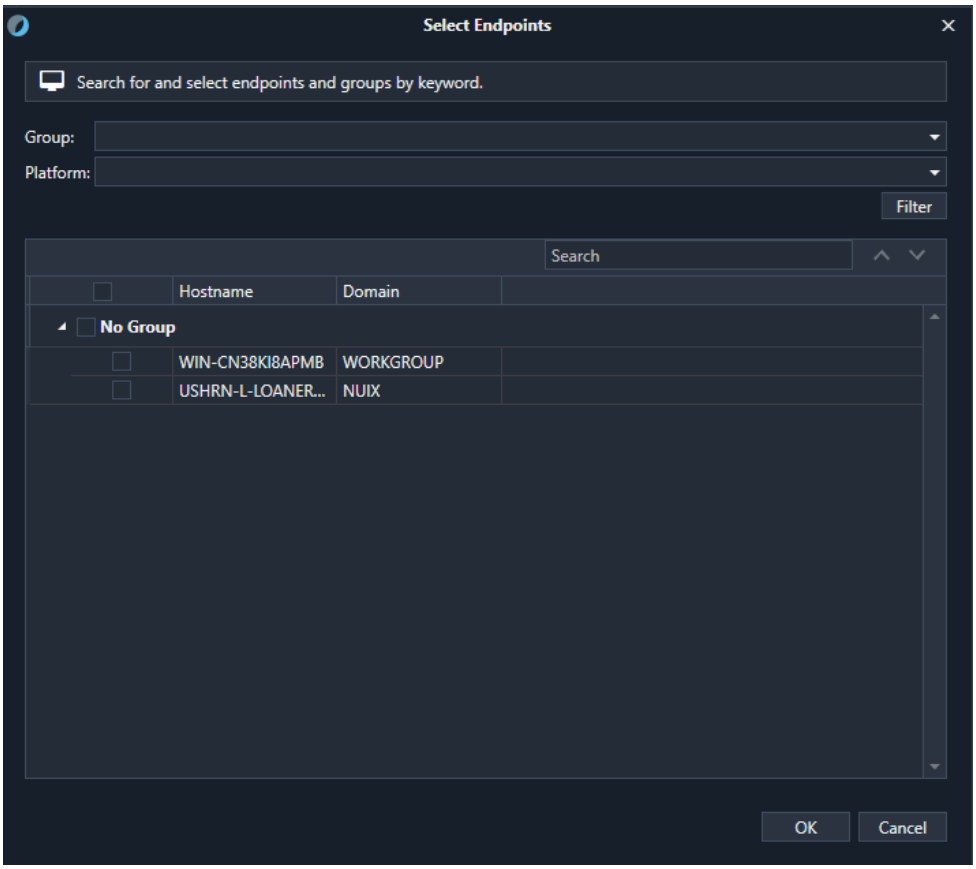
Use the **Endpoint Selector** to search for and select endpoints and groups by keyword.

To access the **Select Endpoints** dialog box:

1. In the **Search** dialog box, click the **Select** button, as shown in the following image.



2. The **Select Endpoints** dialog box appears, as shown in the following image.



The following options are available for working with your endpoints:

- **Group**: The application provides five groups by default (Servers, Desktops, Laptops, High Risk, and Executives). Endpoint groups appear here. To filter the endpoints by group, select one or all the groups from the list, and then click **OK**. Then click the **Filter** button.
- **Platform**: To filter the endpoints by platform, select one of the platforms from the list, and then click the **Filter** button.

- **Search**: This is useful if your list has many endpoints. Start typing the endpoint name into the search box, and the list updates based on what you type.
- **Previous/Next**: Use these buttons to navigate between the search results.

To select one or more endpoints in a search:

1. To select a single endpoint, select the check box next to one of the endpoints in the list. To select multiple endpoints, select the check boxes next to the endpoints in the list. The number of endpoints included in the search is displayed in the Search dialog box.

   For example, if there are seven endpoints in the application, but you select three, the interface will display "Selected Endpoints: 3." If there are endpoint groups, restrict the searches to a specific group by selecting that group from the list. To include all groups in the search, select **Select All**. For more information about groups and how groups can be organized, see Groups.

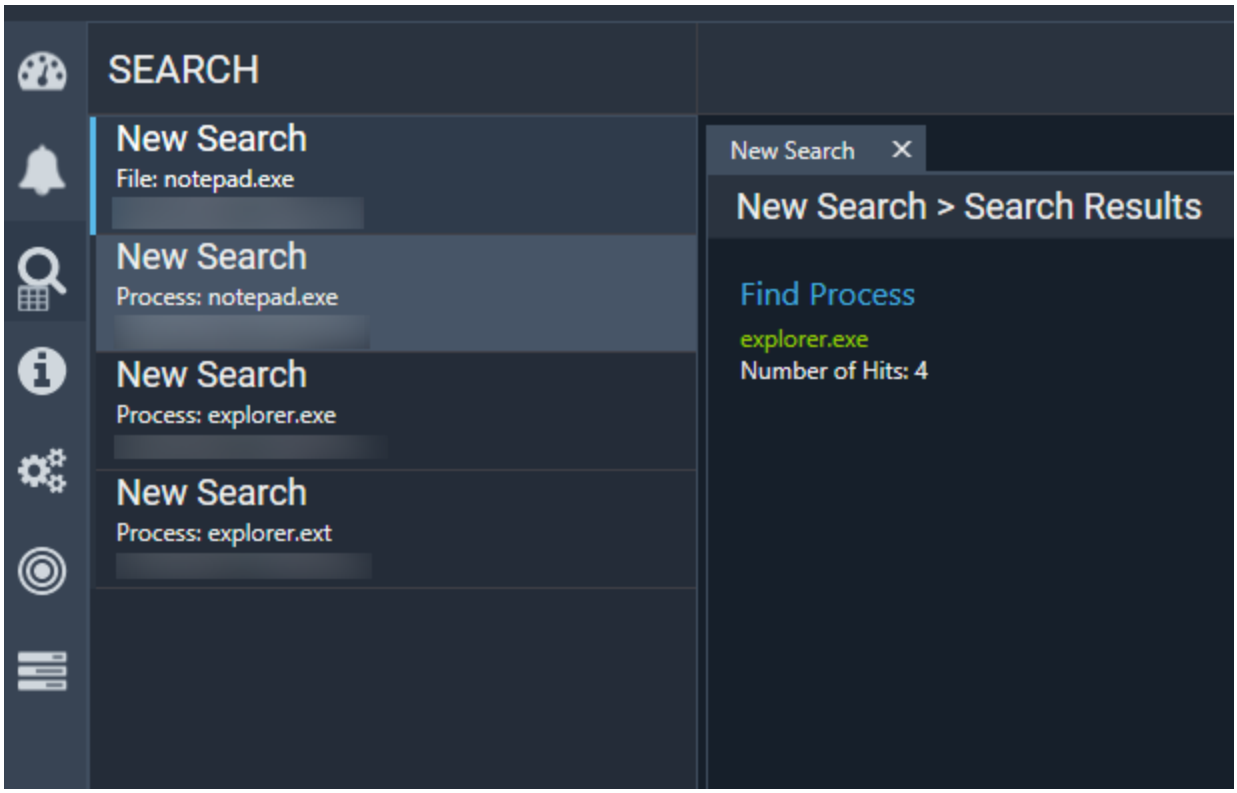
2. Click **OK** when finished.
3. To search for an endpoint name in your list, begin typing the name, and the results update based on what you type.

Stored searches

This is useful for frequently used or otherwise important searches.

Nuix Adaptive Security stores all searches until you clear the local storage. For more information about clearing local storage, see Preferences.

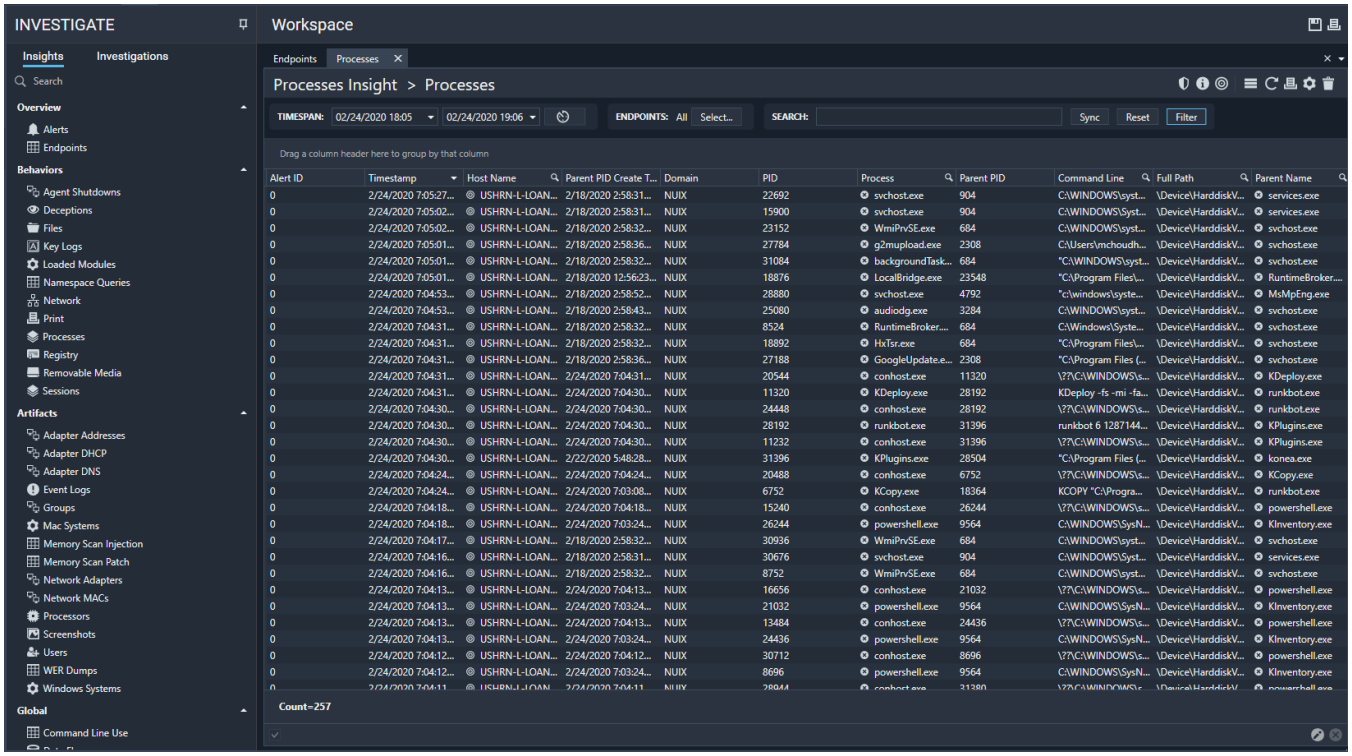
Previous searches appear on the left side of the tab under **Recent Searches**. Selecting a search from the left side of the Search tab shows the data in the search on the right side of the Search tab. An example is shown in the following image.



Investigate

Use the Investigate tab to examine data in more detail.

Use the pin next to Insights or Investigations on the left side to display the selected Insight in the full window. Select from the two tabs on the tab, **Insights** or **Investigations**, and click the pin again to make that part of the navigation reappear. An example of this tab is shown in the following image.



Workspace options

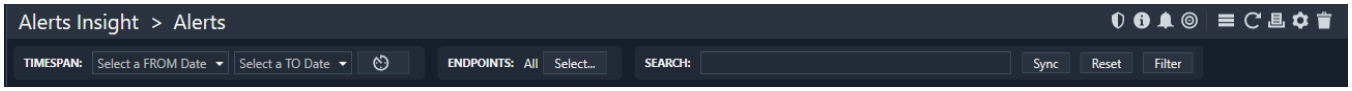
In the Workspace on the right side of the pane, the **Save** and **Print** options, shown in the following image, are available.

The **Save** and **Print** options are described in the following table.

Button	Description
	**Save**: Save work as part of a new or existing investigation. In the dialog box, enter a name, which must be at least eight (8) characters. Under **Insights**, select (**Select All**) to select all insights, or select the check boxes next to an insight for individual insights. Click **Add** to add the insight.
	**Print**: Prints the selected workspace. Confirm this action by clicking **Yes** in the dialog box.

Using the options on the horizontal toolbar

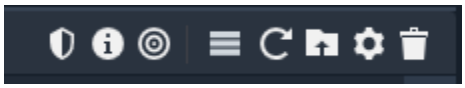
The following image shows the options available in the right pane of the Investigate tab.



These options are described in the following tables.

Top part of the horizontal toolbar

On the upper part of the toolbar, the options in the following table are available.



Button	Description
	**Microsoft Defender**: View whether Microsoft Defender is enabled or disabled on an endpoint. This option is for Windows and does not appear if the endpoint is a Mac or Linux.
	**Investigate**: Click this option to further examine the data, using one of the following options on the menu: • **External Threat**: Opens a series of insights to help determine if the alert is from an external threat. • **Insider Threat**: Opens a series of insights to help determine if the alert is from an insider threat. • **Events**: Select from the list of events to open the alert insight. The categories that appear depend on your selection. • **Visualize**: Displays a process tree for the alert. For more information on this topic, see Visualize Option - Process Tree.

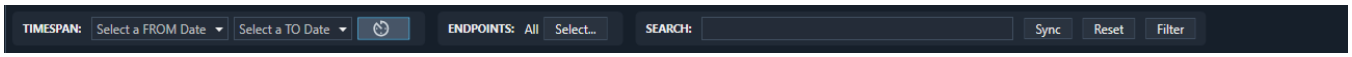
	**Alert**: Click this option to do the following:
	Note: This option is only available when viewing the Alert Insight.
	• **Click to view in Alert Module**: The alert is shown as it appears on the Alert tab.
	• **Change Status**: Select a value from one of the following categories:
	  ○ **Active**: Unassigned, Pending Investigation, Investigation in Progress, Investigation on Hold, and Investigation in Review.
	  ○ **Closed**: Resolved, False Alert, No Investigation, and Archived.
	• **Assign User**: Assign an alert to one of the users in the list by clicking the user.

	**Endpoint**: Click an endpoint from the list, and examine the data, using one of the following options found on the menu: **Respond**: These options allow you to react to the threat. • **View Endpoint**: Shows the status of the endpoint on the Endpoint tab. • **Network Isolation**: Separates an endpoint from the network for further investigation. Use the arrow next to the menu option to click **Enable** or **Disable**. • **Terminate Process**: Ends the process that triggered the alert. **Collect**: These options allow you to gather data from the threat and their response to it. • **Screenshot**: Creates a screenshot as a JPG or PNG by selecting the corresponding box. Adjust the image quality setting from 0 to 100. The default is 75. • **View File System**: Shows the **Overview** tab on the endpoint that is the source of the alert. • **Collect from Host**: Allows you to create and run a collection on the selected endpoint.

Button	Description
	• **Collect this File**: Allows you to collect a specific file on the selected endpoint. Requires the file full path or file path and name. • **Execute Command**: Runs a command on an endpoint using the command shell. • **Upload and Execute**: Allows you to select, upload, and execute a file on the selected endpoint. • **Query Event Log**: Allows you to select one of the event logs listed in more detail. • **Survey**: Performs an endpoint survey, updating the data available on the endpoint details tab. **Manage**: These options allow you to administer the endpoint. For more information about each of the actions found under Manage on this menu, see Manage endpoints. • **Configure**: Open the configure endpoints dialogue. The configuration defines the agent settings, logic rule set, namespaces, and hash lists. • **Upgrade**: Open the upgrade dialogue. Next to Installer, select a version of the Nuix Adaptive Security Endpoint Agent to apply to the endpoint. To use this option, the platform (Windows, Mac, or Linux) must match that of the installer configuration. • **Uninstall**: Removes Nuix Adaptive Security from the endpoint. • **Add to Group**: Opens the Assign a Group dialogue. Select a group to add the endpoint to. • **Copy**: Copies the data in the column to the clipboard.
	Click to expand the row height.
	Click to refresh data.
	Click to export data to CSV.
	**Grid Controls**: Shows the Grid Controls to make the following changes to the data settings: • **Poll Rate**: Sets the time interval at which Nuix Adaptive Security selects data from the endpoints. Click one of the following options: ○ Disabled ○ 15 Seconds ○ 30 Seconds ○ 1 Minute ○ 3 Minutes ○ 5 Minutes ○ 30 Minutes ○ 1 Hour • **Show Group Panel**: Take one of the columns and drag the column to this area, so that the data is sorted by column, or to hide the option if the option is clicked. Clicking the option a second time removes the panel.
	• **Delete**: Deletes the Insight. Click **Yes** in the dialog box to confirm the deletion.

Bottom part of the horizontal toolbar

In the bottom part of the toolbar, the options described in the following table are available.



Option	Description
Timespan	**Timespan**: In the first list, select a **FROM** date. In the second list, select a **TO** date. Change these dates and times by clicking on the calendar and adjusting the calendar or time. Click **Offset** at the bottom of the calendar and select one of the following options from the menu: • MIN (1 or 30) • HRS (1, 3, 12 or 24) • DAYS (3, 7 or 30) • MONTHS (6 or 12) Update the time by clicking the plus (+) or minus (–) sign.
	**Quick Timespan**: Use this option to select one of the following quick timespans: • None • Now+ (defined as one hour before the current time) • Hours (-3, -12 or -24) • Days (-3 or -7) • + Hours (+ 3 or +24) • +/- Hours (+/- 3 or +/-24)
Endpoints	**Endpoints**: Use **Select** to select an endpoint from the list by selecting the check box next to it or select all the endpoints in the instance by clicking the check box above the list and clicking **OK**. The number selected is displayed here. For example, if there are seven endpoints in the Nuix Adaptive Security instance, but you select three, then the window will say "**Selected Endpoints: 3.**" For more information about this, see the Endpoint Selector topic.
Search	**Search**: Enter a term in the Search box and the results appear on the bottom tab. This may take a few seconds.
Sync	**Sync**: Allows for the synchronizing of data.
Reset	**Reset**: Returns the data to the default parameters and resets the Timespan to **Now+**.
Filter	**Filter**: Narrows the results based on the search term.

Filter in the context menus

Use the column header to organize the data on the Investigate tab. For more information about this topic, see Filtering.

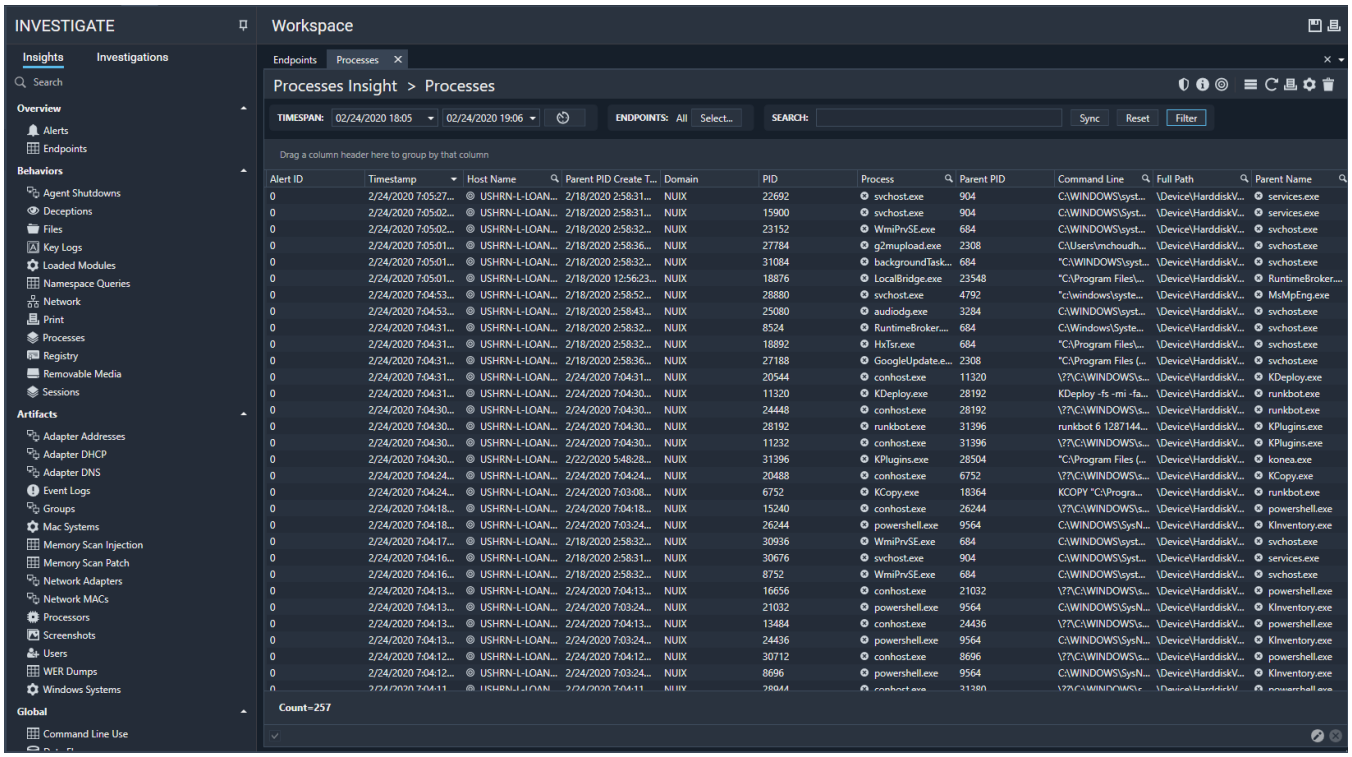
Insights

Insights are the data sources generated through the alerts and endpoints displayed on the Dashboard.

To view data, click a specific insight, and any data that Nuix Adaptive Security has gathered appears on the right side of the tab, as shown in the following image.

You can navigate from the Insight toolbar to find related information. This is useful during an investigation when you need to pivot from one specific insight to another specific insight. The menu is context-sensitive and changes based on the selected field.

In the application, right-click on the insight to select to pivot to a different related insight.



An alert generates each time you trigger a condition set up in the Logic Rules.

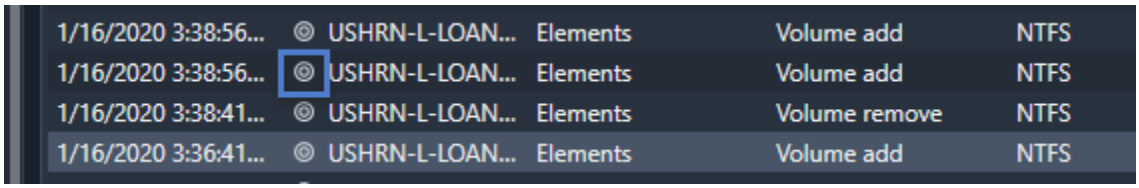
To terminate the process if the alert has negative consequences for an endpoint:

1. Navigate to the alert that contains the process.
2. Select the related **Process Name** or the **Parent Name**.
3. Terminate the process by clicking the **X** next to the process.
4. Confirm this action by clicking **Execute** in the dialog box.

Warning: You can terminate any Process or Parent Process from this window but doing so for some processes may cause the impacted endpoint to display a bluescreen or forcibly reboot itself.

Drag any of the column headers into the area above the data for closer examination. Right-clicking on a column shows a menu. For more information about the actions available for column headers and column menus, see Filtering.

If you are viewing an insight that displays the host name, click the endpoint button next to the host name, as shown in the following image. Doing this opens the **Overview** tab for the selected endpoint on the **Endpoints** tab.



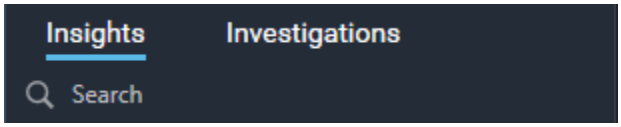
Insight data sources

Nuix Adaptive Security presents its data in categories called Insights. These insights are further divided into three categories:

- Overview
- Behaviors
- Artifacts

Note: Nuix Adaptive Security lists a maximum of 10,000 results for the Registry, Network, and Namespace Queries grids. To show data that is beyond 10,000, you must reverse the data. Flipping the data shows items from the end of the list and shows up to 10,000 items. For example, if you are viewing the latest data for an insight, flipping it shows the oldest data first. If you group items in any grid, the number at the bottom can be over 10,000 items.

Use the **Search** box, as shown in the following image, to find specific information in the Insight Data Sources.



The data sources are explained in greater detail in the following sections.

Overview

The data sources described in the following table are found in the Overview group of insights.

Data source	Description	Additional information
Alerts	Notable activity triggered by rules occurring on the endpoints.	You can customize alerting criteria for various business needs including the ability to update logic rules to reduce false positives or adjust to new threats.
Screenshots	List of screenshot actions.	Visual proof of an issue.
Endpoints	View all endpoints reporting into the system. Information includes connection status, connection address, operating system, and configurations.	Ability to obtain endpoint OS information, troubleshoot unresponsive endpoints, and confirm the configuration applied to an endpoint.

Events

The data sources described in the following table are found in the Events group of insights.

Note: Consider the following when capturing Namespace insights:

- All namespace events appear in the Insights list, including blocked namespace events.
- You can find out if you have blocked a namespace by adding an alert.
- You cannot capture or block some namespace events, for example, ns lookup.exe or ping.exe.

Data source	Description	Additional information
Clipboard	Record of copy and paste events. This is used to capture content when a user copies and pastes data on an endpoint.	The timestamp is the time the data was pasted. Supports Microsoft standard clipboard formats. Includes the name of the source window title. Supported for Windows endpoints only.
Files	Record of file writes and deletes throughout the enterprise.	Ability to identify file activity including file writes or deletes. You can download files for review in support of an investigative matter or as part of an Incident Response matter for reverse engineering.
Key Logs	Recorded keystroke activity on selected endpoints.	Monitor the use of specific typed keywords as part of an investigation.
Loaded Modules	List of dynamic link libraries (DLLs) in use by applications.	Understand process capabilities.
Namespace Queries	List of Domain Name Service (DNS) lookups.	Identify server callouts including the initiating process. For example, C2 and data exfiltration.
Network	Network activity including information about connection status and data sent or received.	Identify network activity focusing on active connections with data transfers. Important for data exfiltration and potential lateral movement.

Data source	Description	Additional information
Print	Record of all print activity on endpoints including printing to PDF files.	Identify data leaving the network as file copies (data exfiltration by insider threats).
Processes	Application activity including parent/child process relationships.	Ability to identify relationships between parent/child processes and further correlate any additional processes initiating.
Registry	A listing of registry activity throughout the enterprise.	Ability to store data files with unique keys.
Removable Media	Record of removable media use across the enterprise.	Ability to get identifiable device information from removable media, including when you attach or detach the removable media, and the ability to download files for review when connected.
Sessions	User account activity throughout the enterprise.	Correlate activity to user accounts.
URL Event	Record of URL browser data events. This is used to capture URL browsing data when a user is web browsing on an endpoint.	Supports Firefox, Chrome, Edge, and Vivaldi web browsers. Internet Explorer is not supported.
Windows Event Logs	List of event logs from Windows machines across the enterprise.	Identify illegal or unwanted events.
Agent Shutdowns	Record of shutdowns of the Nuix Adaptive Security Endpoint Agent on the endpoints.	Agent shutdown messages are generated for the following reasons: • Stop Request – The agent stopped. • Restart – The agent restarted; this is usually for a configuration change. • Shutdown – The endpoint is shutdown. • Self – The agent is uninstalled.

Note: When using the Removable Media insight, be aware that “Volume Serial Number” is a Windows-only value. If the Agent is a Mac or Linux, this column is empty.

Collections

The data sources described in the following table are found in the Collections group of insights.

Data source	Description	Additional information
Collected Files	Collect targeted files.	Identification of possible data exfiltration.
Content Inspection	Scans a file to look for possible sensitive data.	Identification of possible data exfiltration.
Memory Scan Injection	Scans the memory of a process looking for covertly injected modules.	Identification of possible malware.

Data source	Description	Additional information
Memory Scan Patch	Scans the memory of a process to identify code patches and inline hooks.	Identification of possible malware.

Surveys

The date sources described in the following table are found in the Surveys group of insights.

Data source	Description	Additional information
Users	A survey of account users on endpoints.	View illegal or unwanted connections.
Groups	A survey of account groups on endpoints.	View illegal or unwanted network connections.

Other

The date sources described in the following table are found in the Other group of insights.

Data source	Description	Additional information
Linux Systems	Linux endpoint system information across the enterprise.	View rogue or outdated software.
Mac Systems	Mac endpoint system information across the enterprise.	View rogue or outdated software.
Windows Systems	System information of Windows endpoints across the enterprise.	View rogue or outdated software.
Adapter DNS	List of DNS addresses by the adapter.	View unwanted connections to the network adapter.
Network Adapters	List of network adapters endpoints that have connected across the enterprise.	View illegal or unwanted network connections.
Adapter DHCP	List of DHCP addresses by adapter across the enterprise.	View unwanted connections to the network adapter.
Adapter Addresses	Physical address and additional information about the network adapters used on endpoints throughout the enterprise.	View unwanted connections to the network adapter.
Network MACs	List of network MAC addresses endpoints that are communicating with across the enterprise.	View rogue devices.
Processors	Details on processors used by endpoints in the enterprise.	View rogue or outdated software.
WER Dumps	List of Windows Error Reporting (WER) dumps requested by the operator.	Collect a group of error reporting files for future review or create dumps to free up space on an endpoint.

Insight data options

Right-click a data item in a column to show a menu with the following options:

Investigate: These options allow you to begin an investigation into the threat.

- **External Threat**: Opens a series of insights to help determine if the alert is from an external threat.
- **Insider Threat**: Opens a series of insights to help determine if the alert is from an insider threat.
- **Events**: Select from one of the following: Process, DNS, Network, Files, Loaded Modules, Sessions, Media, Keystrokes, Print, Registry to open the alert insight. The categories that appear depend on your selection.
- **Visualize**: Displays a process tree for the alert. For a discussion of this option in greater detail, see Visualize Option - Process Tree.

Respond: These options allow you to react to the threat found in Investigate.

- **View Endpoint**: Shows the status of the endpoint on the Endpoint tab.
- **Network Isolation**: Separates an endpoint from the network for further investigation. Use the arrow next to the menu option to click **Enable** or **Disable**.
- **Terminate Process**: Ends the process that triggered the alert.
- **Add to MD5 Hash List**: Adds the selected MD5 to one or more Hash Lists.

Note: This option is available only in the Processes insight.

- **Delete Files**: Allows you to delete the selected file on the endpoint. Click **OK** in the dialog box to confirm the action.

Note: This option is available only in the Files insight.

Collect: These options allow you to gather data from the threat and their response to it.

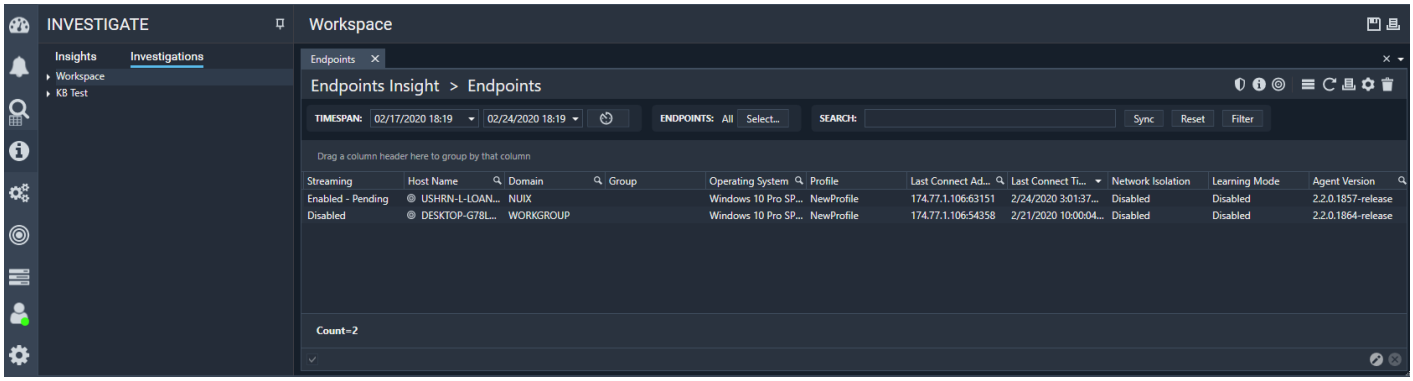
- **Screenshot**: Creates a screenshot as a JPG or PNG by selecting the corresponding box. Adjust the image quality setting from 0 to 100. The default is 75.
- **View File System**: Shows the Overview tab on the endpoint that is the source of the alert.
- **Collect from Host**: Allows you to create and run a collection on the selected endpoint.
- **Execute Command**: Runs a command on an endpoint using the command shell.
- **Upload and Execute**: Allows you to select a file, and upload and execute it on the selected endpoint.
- **Query Event Log**: Allows you to select one of the event logs listed to examine the logs in more detail.
- **Survey**: Performs an endpoint survey, updating the data available on the endpoint details tab.

Manage: These options allow you to administer the endpoint. For more information about each of the actions found under Manage on this menu, see Manage endpoints .

- **Configure**: Open the configure endpoints dialogue. The configuration defines the agent settings, logic rule set, namespaces, and hash lists.
- **Upgrade**: Open the upgrade dialogue. Next to Installer, select a version of the Nuix Adaptive Security Endpoint Agent to apply to the endpoint. To use this option, the platform (Windows, Mac, or Linux) must match that of the installer configuration.
- **Uninstall**: Removes Nuix Adaptive Security from the endpoint.
- **Add to Group**: Opens the Assign a Group dialogue. Select a group to add the endpoint to.

Investigations

This tab provides an easy way to gather all investigations in one place, using the same features described in Insights for further examination of the data, including selecting an investigation and editing the name, as shown in the following image.



Work with screenshots

Write rules to capture screenshots on endpoints to find out more details on suspicious endpoint activity. Capture and view activities performed on the endpoint to gain a better understanding of what the end-user was doing at the time of an alert. Screenshots may help to determine the severity of the alert and the next steps for triage.

The minimum interval for screenshot captures is one per second or up to four per ten seconds.

In the Nuix Adaptive Security application, you can access screenshots in the following modules:

- Investigate
- Insights
- Alerts
- Endpoints

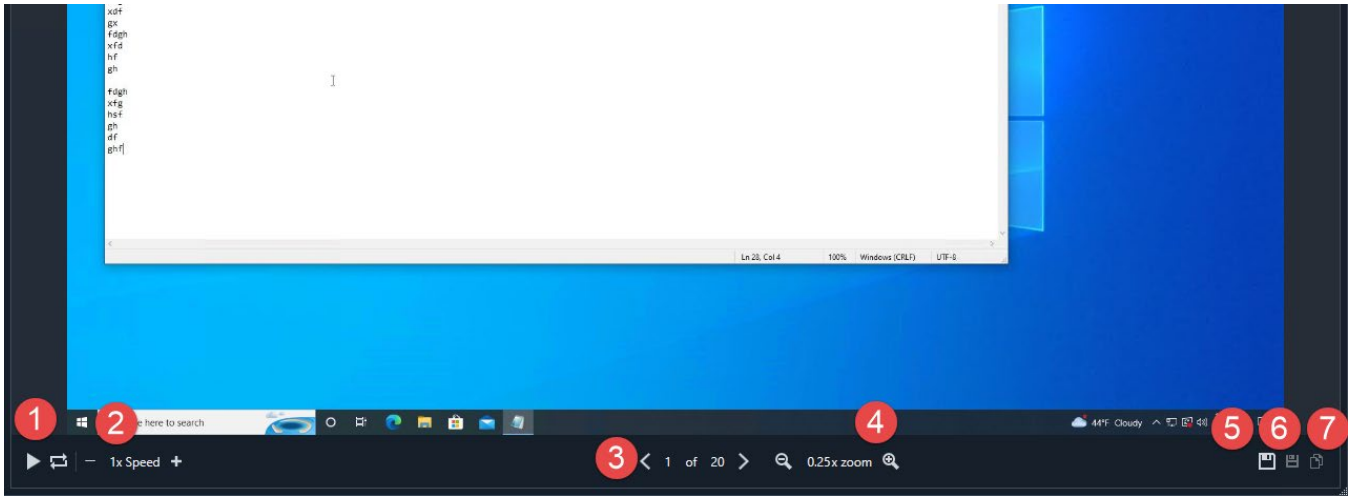
- For investigating insight data sources, see screenshots in Artifacts.
- For more information on capturing screenshots on endpoints, see Capturing Screenshots.
- To capture screenshots for a group of endpoints, see Capture screenshots for a group of endpoints.
- For more information about screenshots as forward events, see Forward events.
- For more information about **screenshot rules**, see the *Nuix Adaptive Security Rule Language Reference Guide*.

Screenshot Playback

In the Nuix Adaptive Security application, click on an alert to view screenshots related to the alert with an animated slideshow.

Screenshots are captured at a minimum of four frames per second and a maximum of up to four minutes in length. The screenshot identification information includes the title, ID, date, and time.

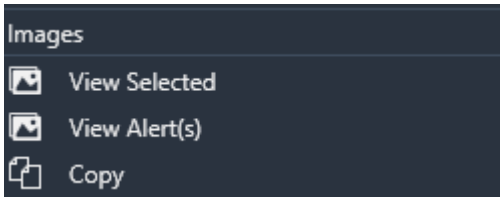
Select the alert IDs and view all screenshots in a loop, as shown in the following image.



The information and functions that are available in the animated screenshot viewer are described in the following table.

Number	Function	Description
1	Play/Pause	Select to Play or Pause the animated screenshot loop.
2	Frame rate	The frame rate of all selected screenshots. You can increase or decrease the speed of the loop.
3	Forward and Backward	Navigate forward and backward with arrow buttons which are also tied to the keyboard arrow buttons.
4	Zoom	Zoom in to get a closer look at the screenshot to view details.
5	Save All	Save and download all screenshots. Use this to download all screenshots after reviewing them with the viewer.
6	Save	Select **Save** to download and share the selected screenshot.
7	Copy	Click **Copy to Clipboard** to copy and paste the selected file to the local system.

There is a right-click menu option under the Images header, as shown in the following image.



Click **View Selected** to open a list of selected images or click **View Alert(s)** to open all the images for the selected alert ID. You can also select to **Copy** the text from any focused or selected grid cell. From the Screenshot Insight, you can pivot to the alert ID.

Screenshots are supported on Windows, macOS, and Linux endpoints.

Screenshots are captured on the endpoint based on the logic rules and then sent to the Nuix Adaptive Security database.

Screenshot Rule Examples

The following rule example will take four screenshots per second for 10 seconds when the word screenshot is typed.

```
Screenshot(keystroke.pid, 10) when stristr(keystroke.keydata,"Screenshot");
```

The following rule example takes a screenshot every 5 seconds for the next 60 seconds resulting in a capture of 12 screenshots. The rule fires when chrome is started with the incognito option. The screenshots are taken from the desktop of the session where the chrome browser was started.

```
screenshot(process.pid, 5, 60) when process.state == PROCESS_STARTED and
stristr(process.cmdline, "chrome") and stristr(process.cmdline, "-incognito");
```

Warning: Consider your database space and limit your screenshots when writing rules. This will directly affect your bandwidth, disk space, and the length of time it takes to view the files.

Rolling Screenshots

Rolling screenshots allows you to capture a movie of an endpoint's desktop for a time span starting before and continuing after the occurrence of a particular suspicious event on the endpoint.

Rolling screenshots are enabled through the use of an EFL rule. Once enabled, screenshots are captured at a rate of four per second and stored in a circular screenshot log on the endpoint. The EFL rule specifies the maximum number of seconds of screenshots to maintain in the circular screenshot log. As the circular screenshot log fills, the oldest screenshots are continually overwritten by newer screenshots.

Another EFL rule is then used to trigger the collection of these screenshots to the server, for example, upon detection of a suspicious event. This rule can specify the number of seconds worth of screenshots both before and after the suspicious event that will be returned to the server.

Once collected to the server, you can use the Nuix Adaptive Security application to view the collected screenshots as a slide show. This provides a movie of the endpoint's desktop for a time range surrounding the occurrence of a suspicious event as determined by custom EFL rule logic.

The startrss rule action is used to enable rolling screenshots. The example below enables rolling screenshots for a session based on the user name.

```
startrss(session.id, 20) when session.event == SESSION_LOGON and
strstr(session.username,   "oscar",false);
```

The rule example below sends back 20 seconds worth of screenshots in response to a particular file written on the endpoint: 10 screenshots are from before the file write and 10 screenshots are from after.

```
capturerss(file.pid, 10 ,10) when strstr(file.path, "captureit",false);
```

Use the stoprss rule action to turn off rolling screenshots. If you don't turn off rolling screenshots with the stoprss rule action, rolling screenshots will remain enabled until that session exits. One use case might be to enable rolling screenshots and then disable them after a set period of time. This helps to manage the resource consumption associated with rolling screenshots.

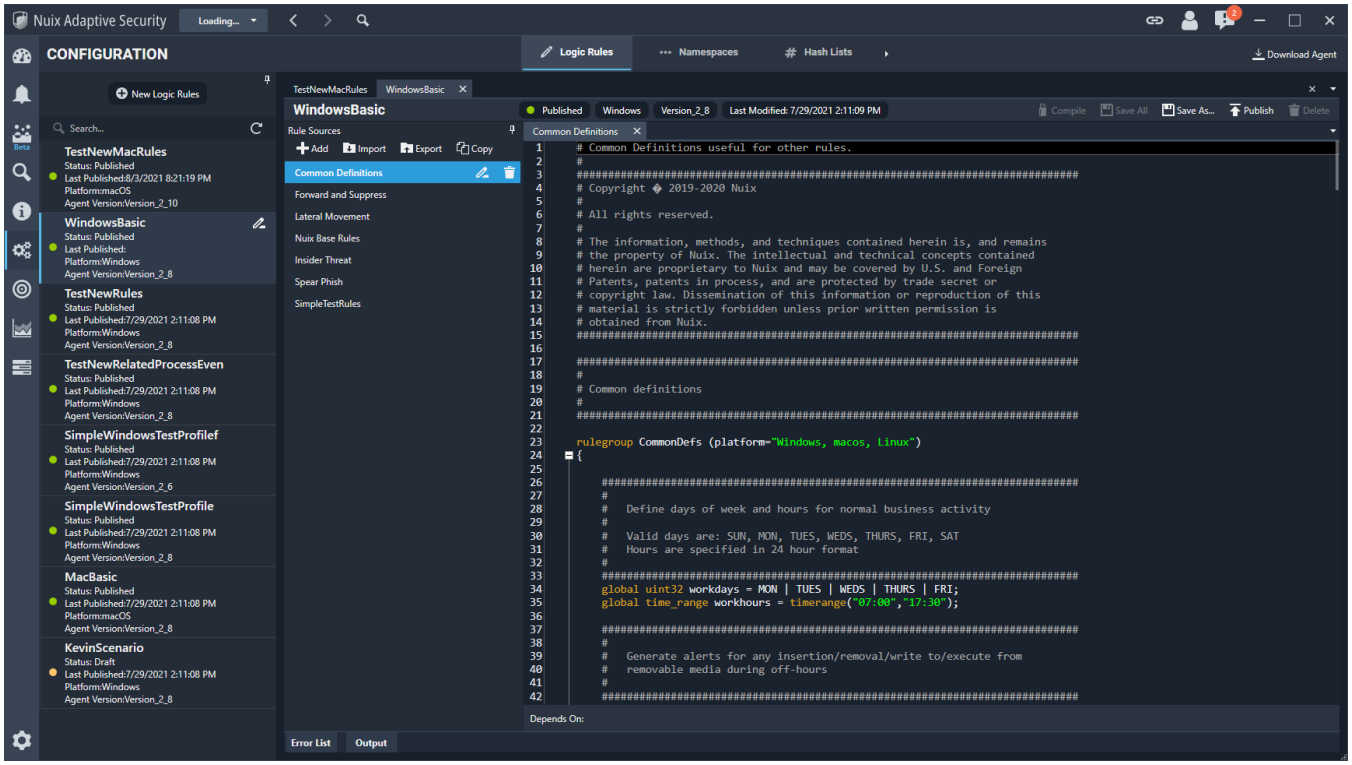
Enabling rolling screenshots will result in the consumption of additional CPU and disk resources on the endpoint. In general, the amount of disk resources consumed scales linearly with the number of seconds worth of rolling screenshots maintained in the circular screenshot log as well as the screen resolution on the endpoint. The amount of CPU usage consumed by rolling screenshots is affected primarily by screen resolution.

Configuration

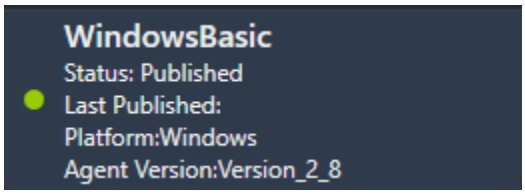
The configuration module is where you can make dynamic changes to agents by manipulating the rules in real time. The configuration defines the agent settings, logic rule set, namespaces, and hash lists.

There are two parts to the agent configuration. The first part is set up in the System module. This is where you will do the system settings for the initial configuration. Once configured, these settings are not likely to change very often. See System for more details. The second part is the configuration settings which are more dynamic and can change throughout the investigation process. Manipulate the logic rules to go from broad to very targeted rules for specific agents or groups of agents.

The following image shows an example of a configuration.



Information is available for each configuration listed on the left side, as shown in the following image.



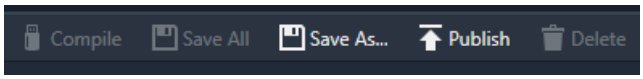
- **Status**: Published or draft. Draft versions have not been sent out to endpoints. You cannot delete published configurations. Any changes to a published set will be saved as a subsequent draft.
- **Last Published**: Date and timestamp of when the agent configuration was last sent out to endpoints.
- **Platform**: Displays the OS for the configuration. The configuration in the example is for Windows agents.
- **Agent Version**: The Nuix Adaptive Security agent version.

Mac agent settings

- The Mac agent needs the following permissions.
  - The Mac agent must be granted full disk access in the Mac security settings to operate properly.
  - The Mac agent must be granted screen recording permission to use the screen shot feature.

Use the options on the horizontal toolbar

On the right side of the tab, the **Compile**, **Save All**, **Save As…**, **Publish,** and **Delete** options, shown in the following image, are available.



The options are described in the following list.

- **Compile**: Compiles the logic rules which is required for the rules to become effective. Any errors in your rules appear in **Error List**.
- **Save All**: Save the created configuration.
- **Save as**: Save as a different file.
- **Publish**: Send out configuration to endpoints.
- **Delete:** Delete the configuration. You cannot delete a published configuration.

Create a configuration

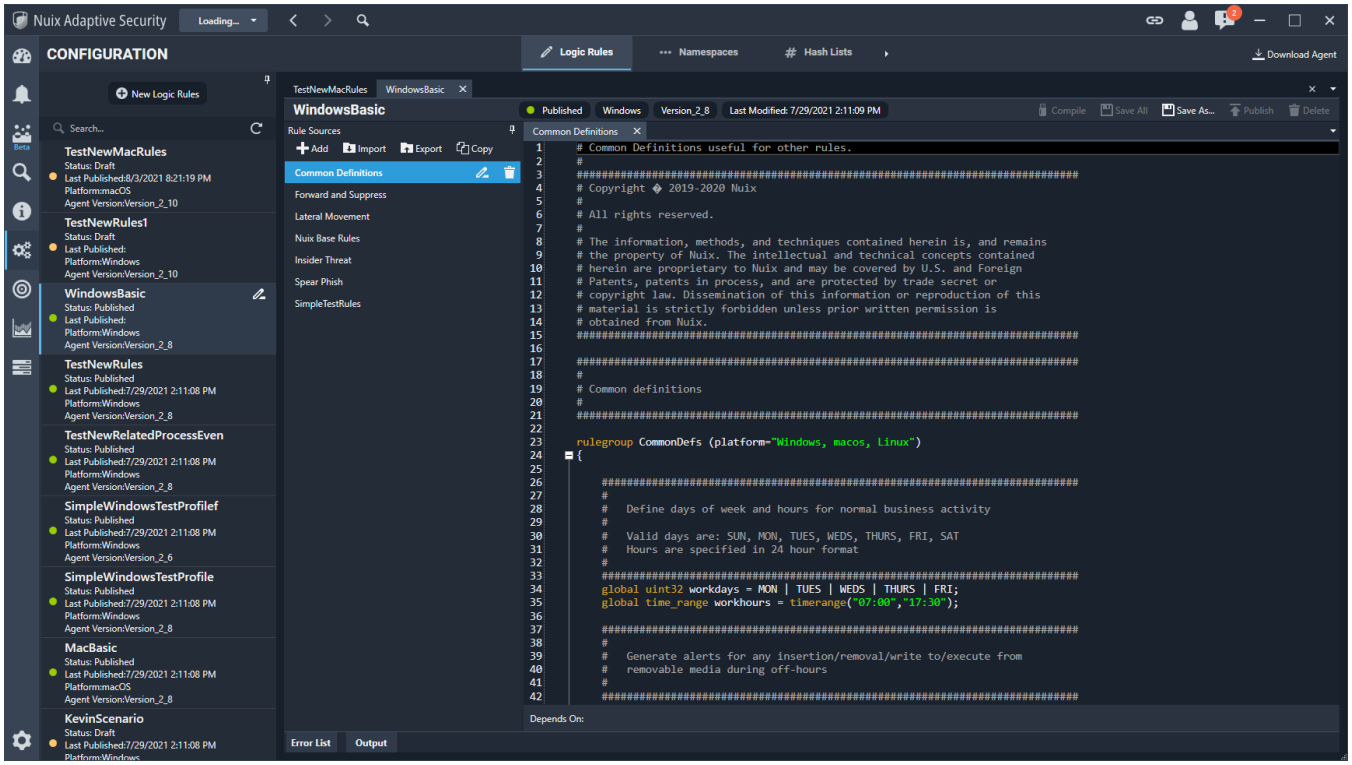
To create a new configuration:

1. Go to the **Configuration** tab.
2. Select **+ New Logic Rules** and enter a name.
3. Select a version from the **Target Version** list.
4. Click **OK** to save the new configuration.
5. Select the configuration from the list to open the logic rules.
6. Add logic rules, namespaces, and hash lists to the configuration.

Logic rules

Logic rules are used to perform actions based on events generated by the endpoint.

The information that appears on this tab provides a summary of your Logic Rules, as shown in the following image.



The summary includes the following information:

- **Name**: Displays the name of the ruleset.
- **Status**: Published or draft. Draft versions have not been sent out to endpoints. You cannot delete published configurations. Any changes to a published set will be saved as a subsequent draft.
- **Platform**: Displays the platform targeted by the ruleset.
- **Agent Version**: Displays the version of the Nuix Adaptive Security Endpoint Agent that the ruleset is targeting.

Perform the actions described in the following table using the buttons in the Rule Set section in the Logic Rule Editor window.

Action	Function
Compile	Compiles the created logic rules. This is required for the rules to become effective.
Save All	Saves the created logic rules
Save As	Saves the created logic rules as a new file.
Publish	Pushes the rules out to the agents.
Delete Logic Rules	Deletes the selected logic rules.

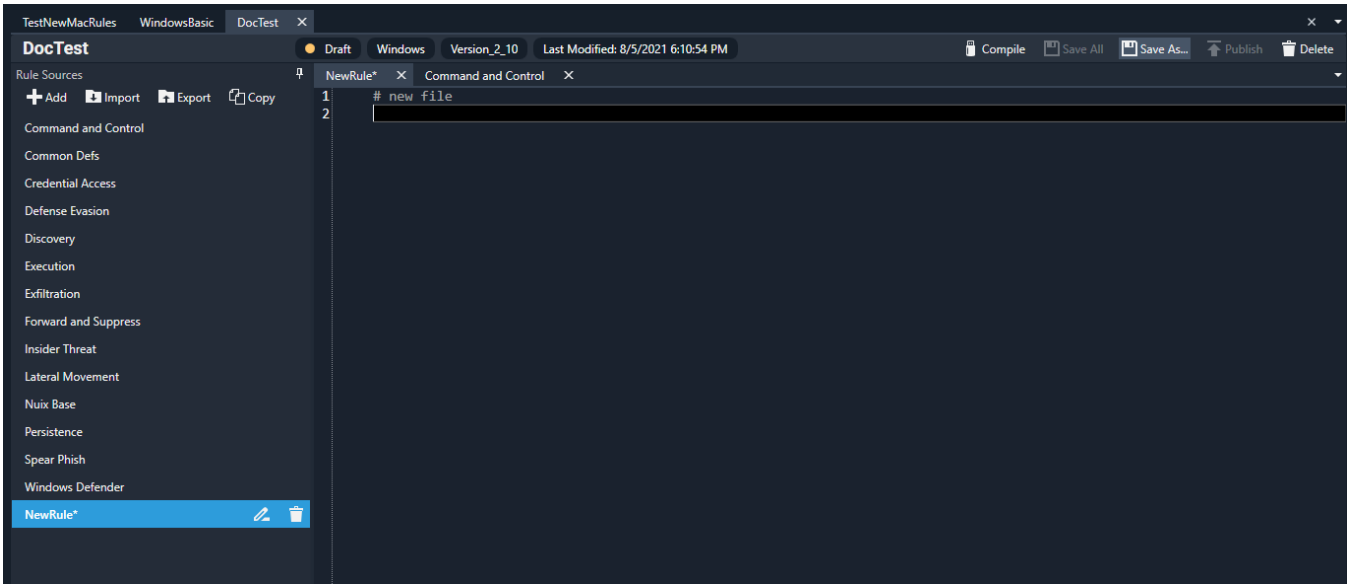
Perform the actions described in the following table using the buttons in the Rule Set section in the Logic Rule Editor window.

Action	Function
+Add	Creates a new source file.
Import	Import saved rule set from an ERF file saved on your local system.
Export	Export a saved rule set as an ERF file to your local system.
Copy	Copies rules from a source file into the current rule set.

Create a logic rule

To create a new logic rule:

1. Select a **Logic Rule Set** from the list. Double-click on a rule to view it in the logic rule editor.
2. Click the **+ADD** to add a new source file to write new rules.
3. Enter a name in the **New Rule Source** dialog box.
4. Click **OK** to continue. The name of the new rule source appears under Rule Sources and the empty source appears on the right side of the tab, as shown in the following image.



5. Enter the text of your rule in the window.
6. When you complete the new rule, in the **Rule Set** section, click **Compile**. Any errors in your rules appear in **Error List,** found following the rule.
7. Fix any errors and click **Compile** again, if necessary. Errors are shown line by line.
8. After the rules have successfully compiled, click **Save All**. The source files appear in the list of existing rules in the **Rule Sources** section.

Create a new rule by copying sources

To create a new rule by copying source files:

1. In the Rules Sources section, click **Copy**.
2. In the **Select Rule Groups To Copy** dialog box, click the plus (+) button to expand a configuration, select the check box for one or more sources, and then click **OK**. You can select multiple source files from this window.
3. When you complete the new rule, in the Rule Set section, click **Compile**.
4. After the rules have successfully compiled, click **Save Logic Rules**. The source files appear in the list of existing rules in the Rule Sources section.

For rules added to an existing configuration, the current logic rules are also listed and appear at the top of the list.

Note: To move a rule from an older version of the software to a newer one, copy the rule before removing it from the older version and paste it into the newer version. Rules are forward compatible but not backward compatible.

Export logic rules

Nuix Adaptive Security supports logic rule export and generates a zipped ERF file for exported rules. The generated file contains a separate EFL file for each of the exported rules. Rule export is beneficial for further examination of the rules or for rules you are copying elsewhere.

To export a rule set:

1. Go to the **Configuration** tab.
2. Open a logic rule set and select **Export** on the menu under Rules Sources.
3. In the **Rule File Export** dialog box that appears, select the file save location.
4. (*Optional*) Under **File name**, change the name of the file. By default, the name of the file matches the name of the logic rules set containing the rules.
5. Select **Save** when you have selected the location for the file and the file name.
6. When completed, the saved file will appear in the file location.

Import logic rules

You can import logic rules from your local system.

Note: The only supported file type for import is an ERF file.

To import a rule set:

1. Go to the **Configuration** tab and open an existing rule set or create a new one.
2. Select **Import** on the menu under Rules Sources.
3. Next to the **Select File to Import** that appears, select the location on your local machine where the imported files are located.
4. Select the rules that you wish to import by checking the boxes.
5. Click **OK** to start the import.
6. When completed, the imported rules are displayed in the logic rule set.

Memory scanning

The Nuix Adaptive Security endpoint agent can scan live user space process memory on Windows endpoints to look for evidence of techniques associated with malicious code. Memory scanning can only be initiated from rules written in the Nuix Adaptive Security Event Filter Language.

For more information about the memscan rule action, see the *Nuix Adaptive Security Rule Language Reference Guide*.

Two specific types of scans can be initiated.

- Module Injection Scans

- Patch Scans

Module Injection Scans

The module injection scan identifies instances of modules covertly loaded into the address space of a process using reflective injection. Modules loaded through reflective injection bypass the operating system loader. Because the modules are not loaded by the operating system loader, the operating system is not aware of their presence and their presence will not be reported by standard APIs and system tools. In addition, modules loaded through reflective injection are not reported by Nuix Adaptive Security's image load events.

When a scan finds an instance of a reflectively injected module in a process, the agent carves the injected module from memory and then generates a memory scan injection event. The event data includes the module that was carved from memory, the process ID and executable path for the process where the injected module was found, the base virtual address at which the injected module was loaded, and a number of fields taken from the PE header of the injected image including SizeOfImage, CheckSum, Characteristics, and Magic number.

Because the Nuix Adaptive Security Agent may perform patching as part of its monitoring capabilities, an owner designation field is also included in the event data to identify instances of module injection performed by the Nuix Adaptive Security agent.

The memory scan injection event is sent through the filter engine on the endpoint agent allowing rules to operate on the event. Memory scan injection events that the Agent sends back to the Server as the result of rule matches are viewable as Memory Scan Injection Artifacts from the Investigate tab in the Nuix Adaptive Security interface.

Patch Scans

The patch scan identifies modifications to executable modules in memory by performing a byte-by-byte comparison between modules loaded in memory and their corresponding on-disk files. When a process is scanned, this comparison is performed for the process executable and all DLLs loaded into that process space. Because some portions of an image are expected to change during the load time or runtime of a process, these comparisons are only performed against portions of executable images that are determined to be read-only based on section characteristics in the PE header. This typically applies to executable code and certain Portable Executable (PE) data structures such as the export address table.

Patching of code in memory is often performed by malicious code to subvert or modify intended behavior. However, patches are not always a sign of malicious activity. Google Chrome and Adobe Acrobat, for example, use sandboxing techniques in their applications which require inline hooking of functions exported from various Windows system DLLs.

When a discrepancy between an in-memory image and the backing disk file is identified, the agent generates a memory scan patch event. The event data includes the process ID and executable path for the process in which the patch was found, the executable path for the specific module containing the patch, the base address where the patch begins, and the length of the patch. In addition, the patched bytes from memory and the original bytes from the disk file are included.

The event data also indicates whether this patch represents an inline hook, an export address table hook, or neither. In the event of an inline hook or export address table hook, the target address of the hook is also supplied if the agent can determine it.

To provide more context about a patch, the event data includes symbolic information to represent the location of the start of the patch, and the target for an inline hook or export address table hook. This provides greater context than simply supplying a virtual memory address alone. The following is an example of the symbolic information for a patch that was applied to an exported function from a system DLL:

```
\Device\HarddiskVolume3\Windows\System32\ntdll.dll!NtMapViewOfSection+0x00000000
```

Similarly, the symbolic information for the target of an inline hook that points into the heap is given in the following example:

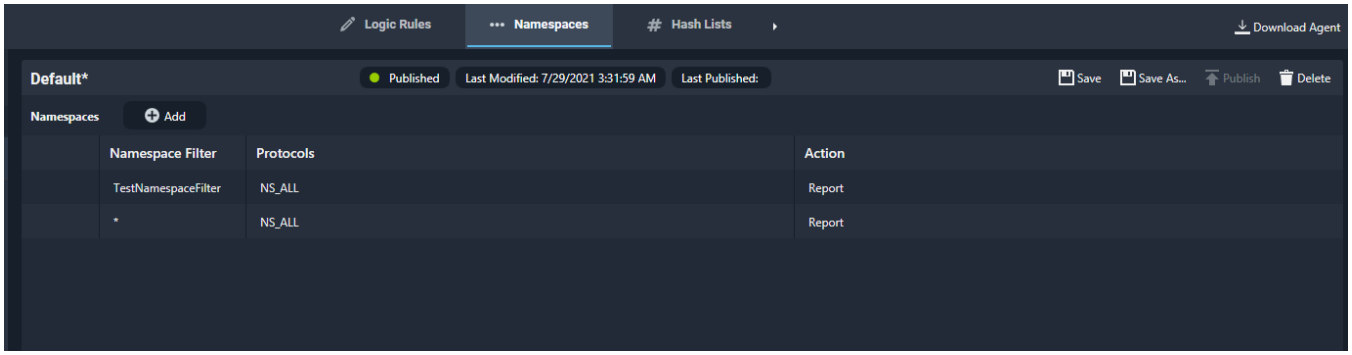
```
[heap]0x00007ff8fafb0300
```


Because the Nuix Adaptive Security Agent may perform patching as part of its monitoring capabilities, an owner designation is also included in the event data to identify instances of inline hooks installed by the Nuix Adaptive Security agent.

The memory scan patch event is sent through the filter engine on the endpoint agent allowing rules to operate on the event. Memory scan patch events that the agent sends back to the server as the result of rule matches are viewable as Memory Scan Patch Artifacts from the Investigate tab in the Nuix Adaptive Security application interface.

Namespaces

This tab lists the namespace filters for the Nuix Adaptive Security Endpoint Server, as shown in the following image.



Note: This option is available only for a Windows endpoint.

Order is important when setting up a namespace filter. The first match Nuix Adaptive Security finds is the accepted match, and that is the one recorded by the software.

For example, set up a namespace filter with two rules and try to block access to nuix.com. The first rule is an *(asterisk) filter set to **Report**, and the second one is for the intended action, *nuix.com set to **Block**. As a user, try and access nuix.com on an endpoint running the agent configuration containing this namespace filter. If you created the rules as described, the block does not occur. Instead, Nuix Adaptive Security records the attempt to access nuix.com, because it is the accepted match. This is the incorrect way to set up a namespace filter if the goal is to block something.

To block something before reporting it, for example, the scenario described in the previous example, have the Block namespace filter set first, as shown in the following image.

Doing this blocks access to *nuix.com as intended, because the **Block** rule is now the accepted match.

The following settings are displayed on this tab:

- **Namespace Filter**: Enter a name for the filter.
- **Protocols**: Select one of the following from the list:
  - All
  - NetWare Service Advertising Protocol (SAP)
  - Novell Directory Services
  - Peer Browse
  - Service Location Protocol (SLP)
  - Dynamic Host Configuration Protocol (DHCP)

- Local TCPIP Lookup
- Host File TCPIP Lookup
- Domain Name System (DNS)
- NetBIOS over TCP/IP
- Windows Internet Naming Service (WINS)
- Network Location Awareness (NLA)
- Bluetooth
- **NBP**: Stands for Name Binding Protocol.
- **MS**: Stands for Mail Server.
- **STDA**: Stands for Stochastic Time Demand Analysis.
- Email
- Peer Name Resolution Protocol (PNRP)
- Peer Name Resolution Protocol Cloud (PNRP)

- **Action**: Select **Report** or **Block** from the menu.

Add a namespace

To enter a namespace filter for a new agent configuration or make changes to an existing namespace filter:

1. Open the **Namespace** tab.
2. Select **+Add** to add a new row.
3. Enter your **Namespace Filter**.
4. Select a **Protocol** from the list.
5. Select an **Action** from the list.

Next to each row you can click to **Edit** the namespace or click the **X** button to delete the row.

Hash lists

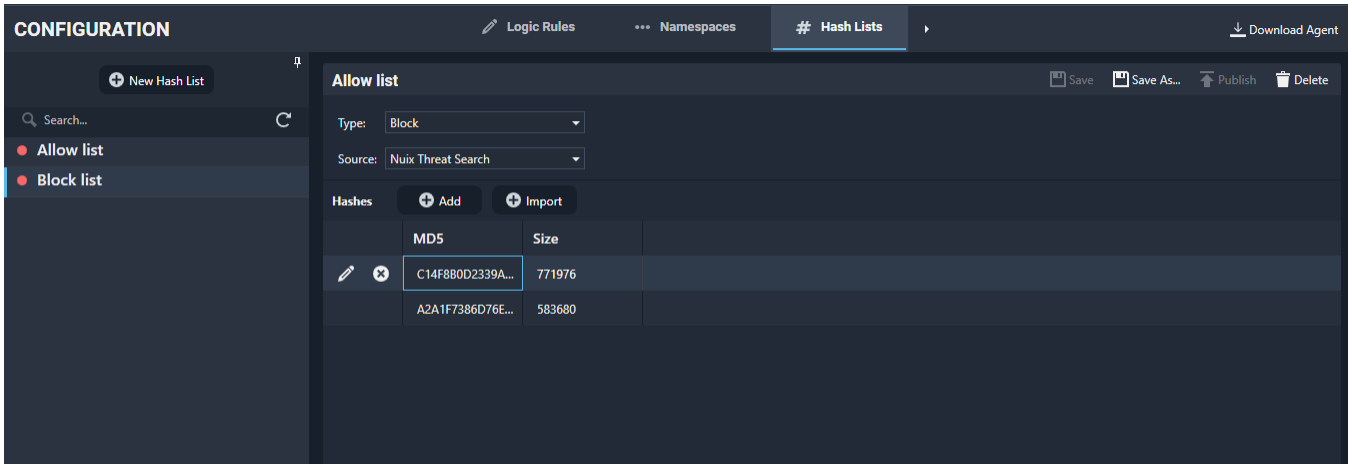
A hash is a string representation of a file and its contents at a specific point in time.

If the content of the file changes, so does the hash. You can use many different algorithms to create a hash. The most commonly used hash in Nuix Adaptive Security is the MD5 Message-Digest Algorithm (MD5).

The hash list shows the hashes that belong to various lists, including **Block** (Block list) and **Allow** (Allow list).

Hash lists tab

Use the Hash Lists tab to maintain and manage hash lists as shown in the following image.



It is best practice to maintain a block list (list of prohibited hashes). Block lists allow investigators to limit the number of programs to execute on endpoints within the enterprise by prohibiting the programs from running.

The following settings are displayed on this tab:

- **Name**: Add a name for the new hash list.
- **Type**: Select what the hash list type should do:
  - **Unknown**: List of programs with an unknown hash list type.
  - **Ignore**: List of programs ignored by Nuix Adaptive Security.
  - **Allow**: A program can run if the appropriate rule is enabled. For information about rules, see the *Nuix Adaptive Security Rule Language Reference Guide.*

    Warning: Use this feature with caution. The hash list type is based on the file's hash, if the program updates, the hash will also be different, and the program cannot run on the endpoint.
  - **Block**: List of programs prohibited from running.
- **Source**: Select the source of the hash list. This setting can be set to Nuix Threat Search, Nuix Endpoint Server, Nuix Adaptive Security Endpoint, Nuix Adaptive Security Enterprise Server, or other additional sources.

Work with hash lists

You can perform the following functions when working with hash lists.

- + Add
- + Import
- Edit
- Delete

Import a hash list

Use the National Software Reference Library (NSRL) format and a comma-separated value (CSV) file to bulk import hashes. The hash list files must be in a CSV format and must have the following field:

- **MD5**: The MD5 hash of a file.

The following fields are optional:

- **File Size**: The size of the file.
- **SHA-256**: Secure hash algorithm with the digest length of 256 bits.

The order of the columns is not important.

Example:

```
"SHA-
1","MD5","CRC32","FileName","FileSize","ProductCode","OpSystemCode","SpecialCode"
"000006CD8F63343893C52830FC36118124131E25","41D0DD202B31F022CDB92802567058A5","7AD2
4105","redbull.erp",8663417,201453,"362",""
"000006E81C829F654163696578D9B1841E8CE167","3F4894B0A067111BC862608E3B6D6205","21AB
6D9F","dy3246416.htm",11366,14693,"362",""
"000007B928F4C211CC8ED3C9707196A7C5BA3AF8","68563E2BFC732E10E885BD2DCF49F2EF","3494
0E24","microsoft-windows-businessscanning-feature-
package~31bf3856ad364e35~amd64~pt-br~6.1.7601.17514.mum",1541,201424,"362",""
```

To import a file:

1. Click **Import** to open the file search.
2. Find the file on your local machine and click **Open**.
3. Click **Load**.

4. To add the file to an existing Target Hash List, select the list from the menu. If you want to add the file to a new hash list, click **New.**
5. The **Status** area at the bottom shows the progress of the hashes loaded.
6. Once the load is complete, click **Import** to import the file into Nuix Adaptive Security.

Configure the agent

There are three workflows for configuring the agent.

- Configuring the agent for the first time for a new Nuix Adaptive Security installation.
- Changing the logic rules on an existing agent that is running on an endpoint.
- Upgrading the agent version on an endpoint.

Configure the agent for the first time

This section describes configuring a new agent for the first time in a new system setup. When configuring the agent all the settings below are required except for the hash list and logic rules.

Prerequisites

Set up the configuration parameters which include:

System Settings

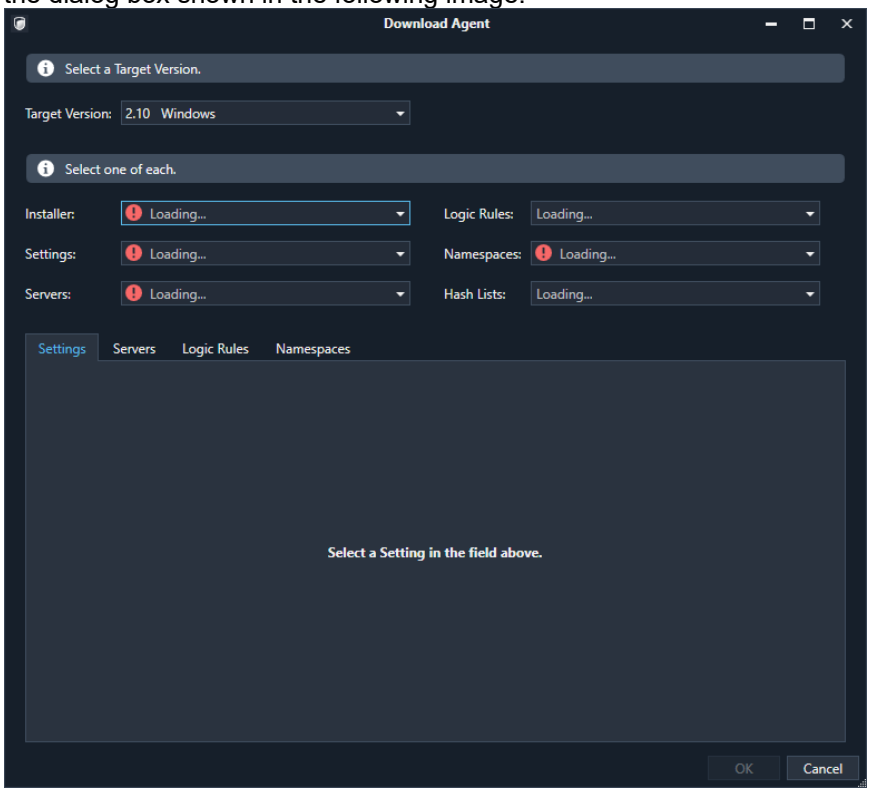
The following settings are in the **System** module.

- target version
- installer
- settings
- servers
-
- Configuration Settings

The following settings are in the **Configuration** module.

- logic rules
- namespace
- hash lists

Clicking on **Download Agent** on the menu at the top of the **Configuration** module or System module displays the dialog box shown in the following image.



To select the agent configuration:

1. Click the **Download Agent** button to display the **Download Agent** dialog box.
2. Select one of the available **Target Versions** to embed in the file from the **configuration**.
3. Select one of the available **Installers** to embed in the file from the **Installers** list.
4. Select the **Settings** as set from the System Settings configuration.
5. Select the **Server** as set from the System Servers configuration**.**
6. Select the **Logic Rules**.
7. Select the **Namespaces**.
8. Select the **Hash Lists**.
9. Click **OK** to create the installer and place it in a local directory, using the **Browse for Folder** dialog box. The agent is saved as an .exe file.

Change the Logic Rules for an existing agent

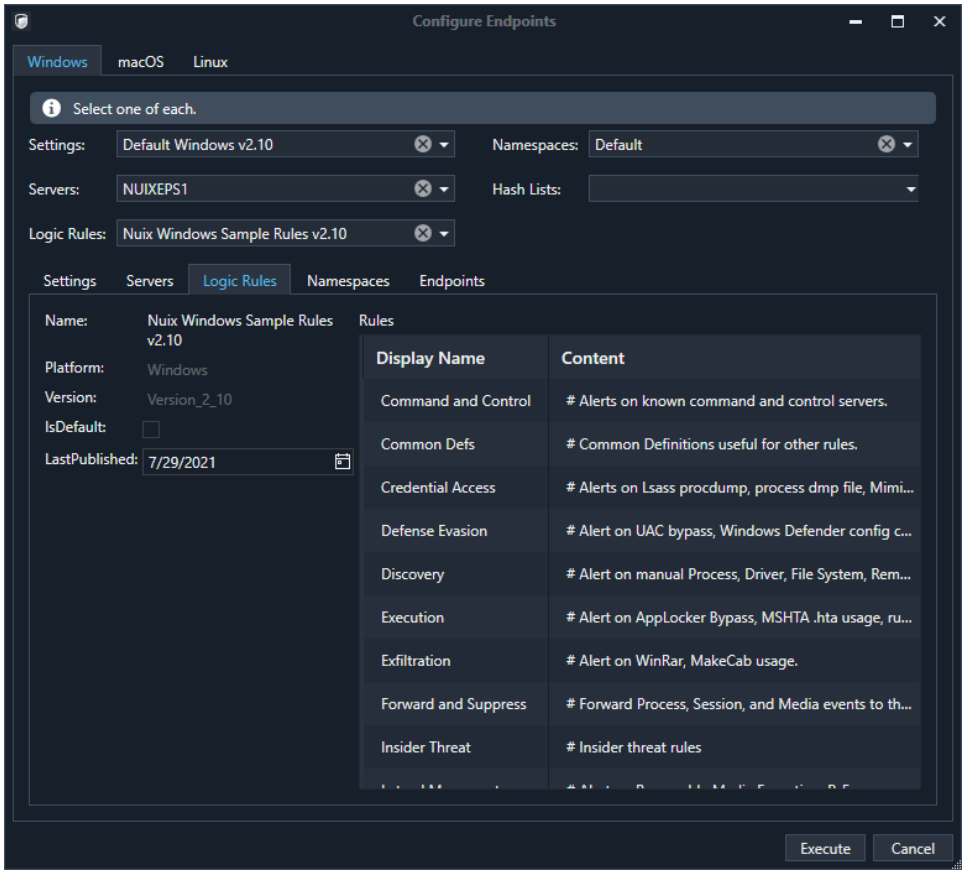
During an investigation, you can change the logic rules on an agent running on an endpoint.

Note: When you change the endpoint configuration, you only have to select the new logic rule set.

During an endpoint change or update, the endpoint details text will display in orange until the change is made and then the text returns to white.

To change the logic rules for an existing agent:

1. Go to the Endpoint module, right-click on an endpoint and select **Configure**.
2. Select the new logic rules set.
3. Select **Execute** and the rules are automatically updated on the agent.



Upgrade the agent

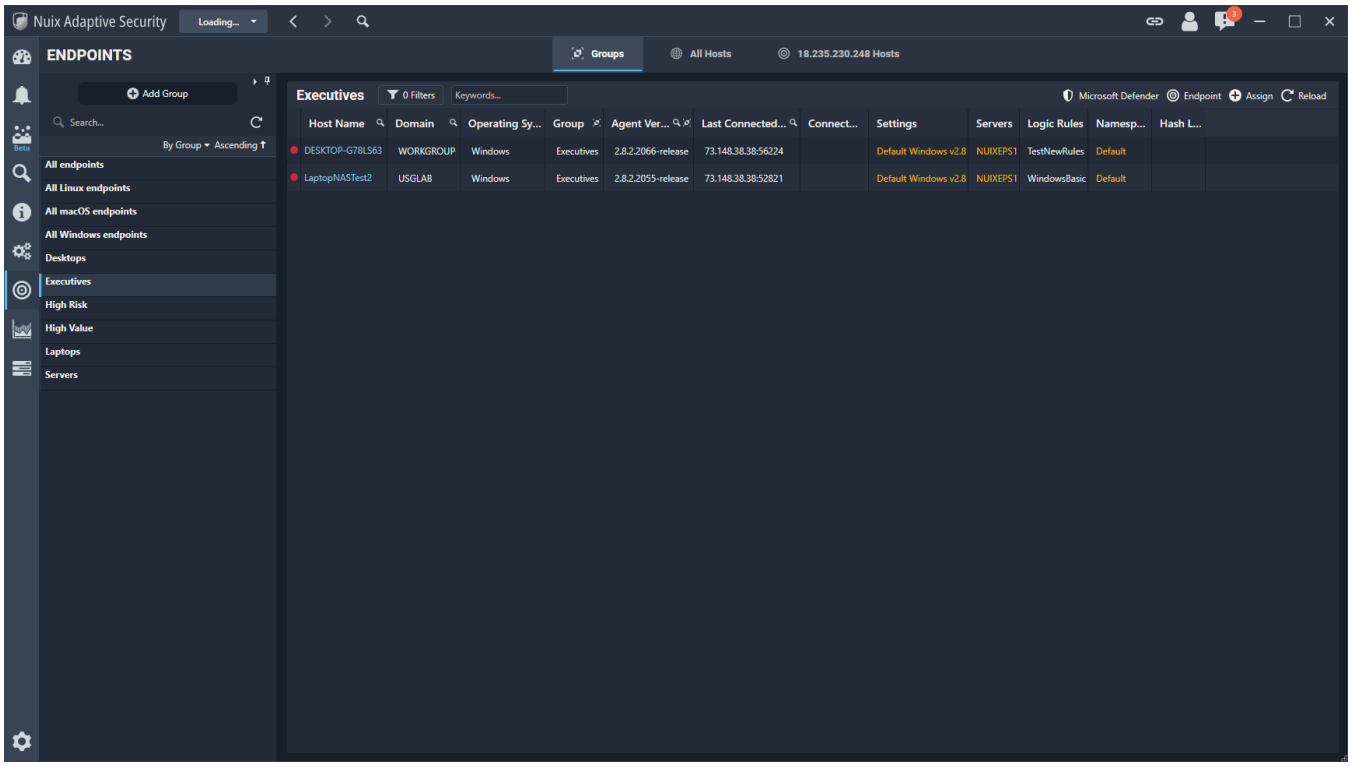
Upgrade agents from the Endpoint module.

To upgrade an agent version running on an endpoint:

1. Go to the Endpoint module, right-click on an endpoint and select **Upgrade**.
2. Select the new version from the **Installer** list.
3. Select execute and the agent is upgraded with the new version.

Endpoints

In the Endpoints module, as shown in the following image, view the endpoints by groups, all hosts in a global environment, and hosts associated with the server.



Groups

Group endpoints based on their functions in the environment. Different groups of endpoints may need different logic rules. In the Groups tab, you can add a new group and filter endpoints in a group.

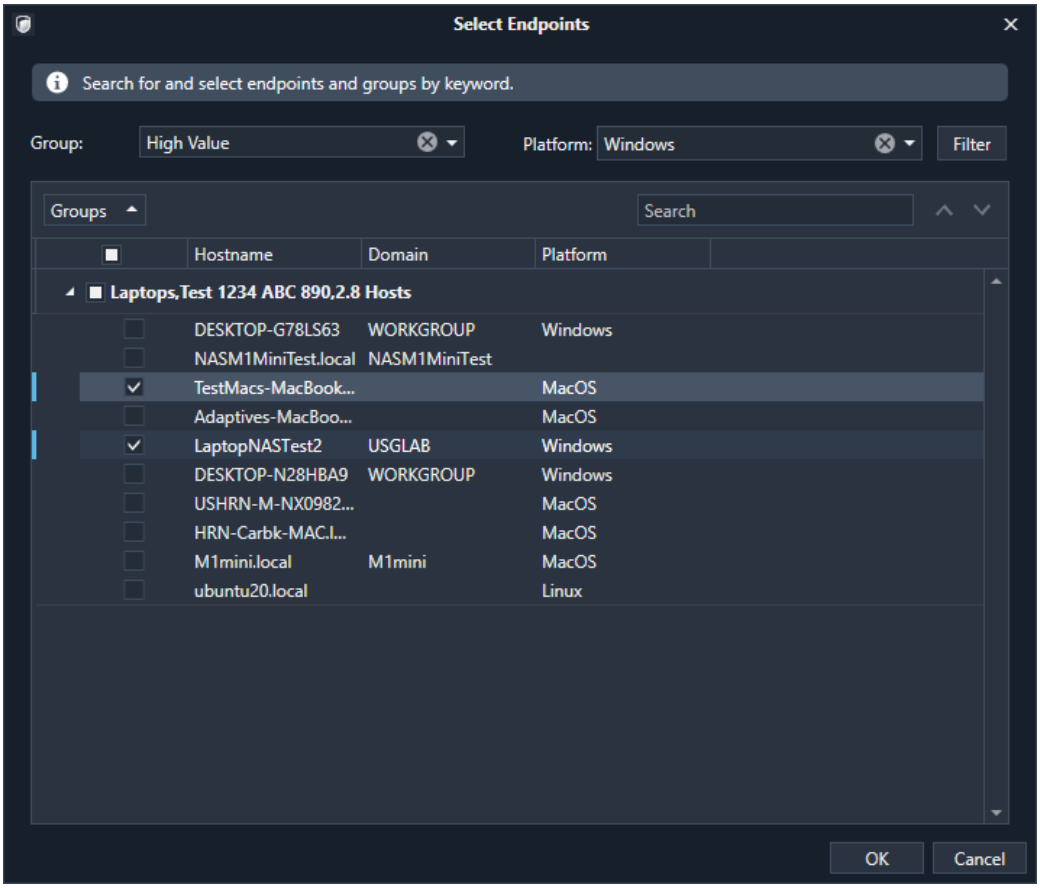
When working with groups you can perform the following group tasks:

- Configure
- Upgrade
- Uninstall
- Screenshot

Create an endpoint group

To create a new endpoint group:

1. Select **+ Add Group** to open the New Group dialog box.
1. In the **New Group** dialog box, provide a new group name. There are no rules for the name of the group, but it should be something memorable or that conforms to a previously established naming convention.
2. To assign an endpoint to the group, select **+Add** which opens a dialogue box to select endpoints.
3. Select a parent **Group** to select a set of endpoints and then select the **Platform**.
4. Select the hostnames of the endpoints to add to the group, as shown in the following image.



5. Click **OK**.

The selected endpoints are added to the new group.

Assign an endpoint to a group

To assign an endpoint to a group:

1. Select a group of endpoints.
2. Select **+Add**.
3. In the dialog box, select a group and platform.
4. Select the hostname to add to the group.
5. Click **OK**.

The selected endpoint is added to the group.

Configure endpoints in a group

To configure endpoints in a group:

1. Select a group of endpoints.
2. Select **Endpoints** > **Configure**.
3. In the dialog box, select the configuration settings.
4. Click **Execute**.

The selected configuration settings are added to the endpoints in the group.

Upgrade endpoints in a group

To upgrade endpoints in a group:

1. Select a group of endpoints.
2. Select **Endpoints** > **Upgrade**.
3. In the dialog box, select the new installer for each platform.
4. Click **Execute**.

The endpoints in the group are upgraded to the selected installer.

Uninstall endpoints in a group

To uninstall endpoints in a group:

1. Select a group of endpoints.
2. Select **Endpoints** > **Uninstall**.
3. In the dialog box, select the endpoints you wish to uninstall.
4. Click **Execute**.

The endpoints in the group are uninstalled.

Capture screenshots for a group of endpoints

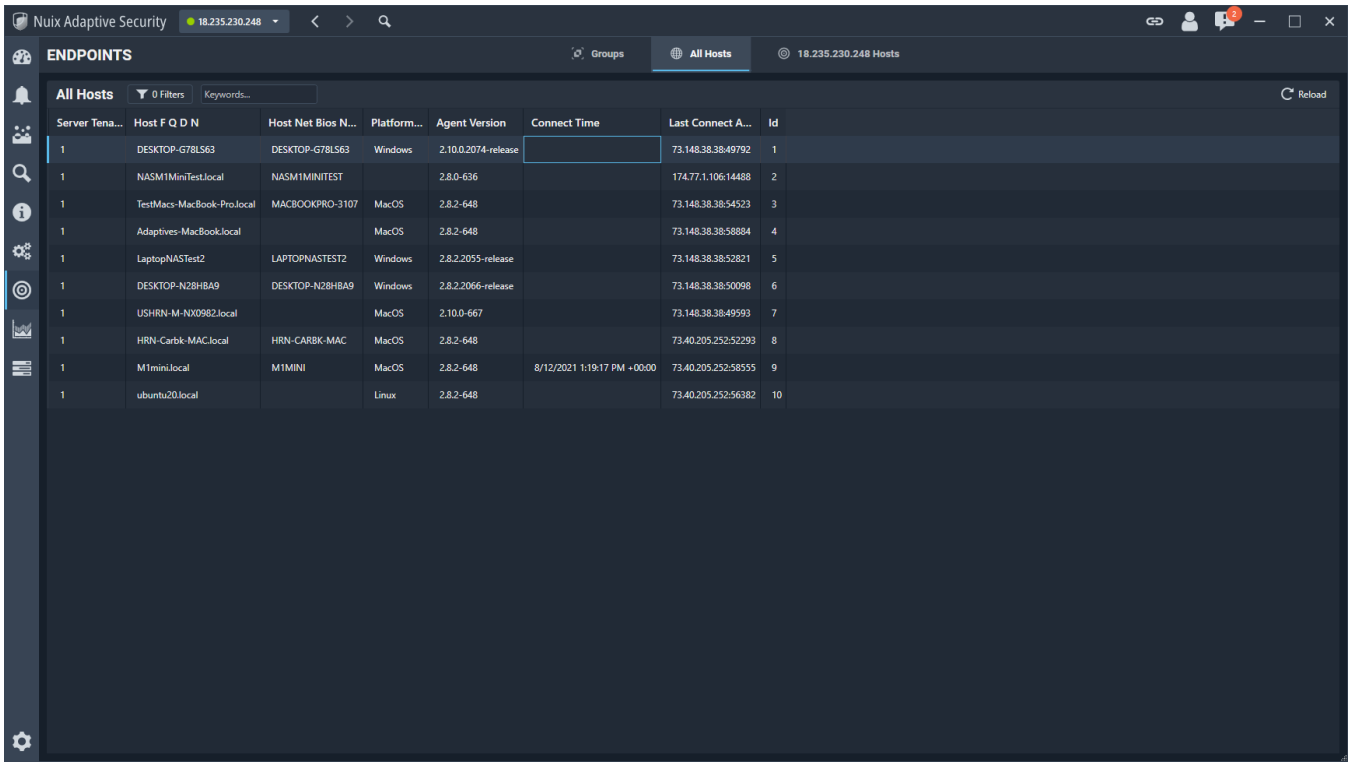
To take screenshots of endpoints in a group:

1. Select a group of endpoints.
2. Select **Endpoints** > **Screenshot**.
3. In the dialog box, select the **Format** and **Image Quality**.
4. Click **Execute**.

Screenshots are captured for the endpoints in the group. The screenshots are stored in the database and you can view it in the **Screenshot Insight** or the **Task Result** view.

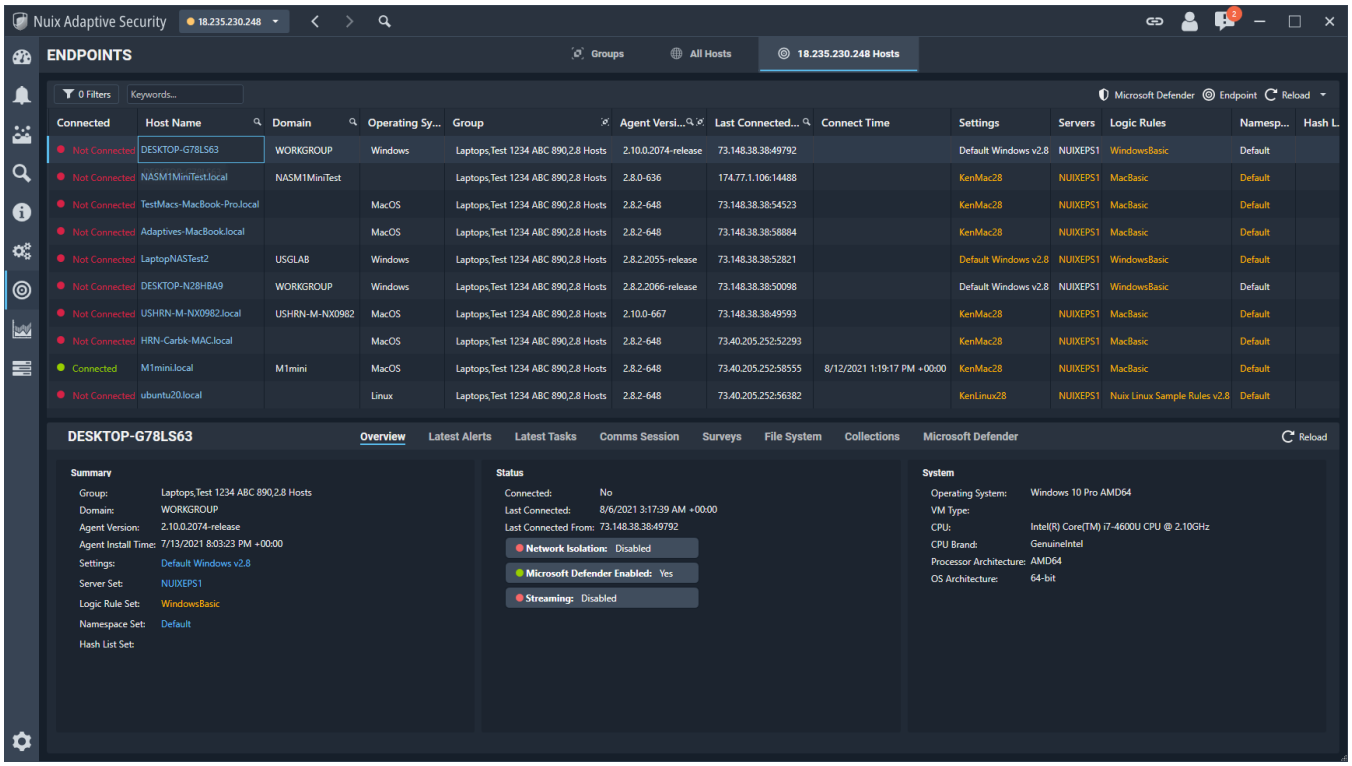
All Hosts

View all hosts in your environment in the **Endpoint** module in the **All Hosts** tab, as shown in the following image. Use the filters to search for endpoints by using the following categories: Group By, Agent Versions, and Platform. Use **Clear** to clear the filters. Click **Apply** to update the list of results based on the **Filters** or **Keywords**. Click **Advanced** to filter using Boolean operators.



Server Hosts

View the endpoints that are associated with the server, as shown in the following image.



Note: The Endpoints module All Hosts tab is not displayed when logged into a secondary server.

Respond

The following option are available under **Respond**.

Network isolation

Use this option to separate an endpoint from the network for further investigation.

Use the arrow next to the menu option to click **Enable** or **Disable**. Another way of using this setting is to create a new agent configuration or make changes to an existing one. For more information about making changes to Network Isolation rules, see Isolation Rules.

Endpoint collection actions

The following options are available under **Collect**.

Screenshots

During an investigation, you can capture screenshots as PNG or JPG image files. Every screenshot request requires setting two parameters.

- **Image Format**: Specify the file type, PNG or JPG. A PNG file is a lossless compression which will result in a perfect capture of the pixels rendered on the users' desktops but are larger file sizes. For example, a single 4K display could easily result in a 10MB PNG. A JPG file's quality and size can vary. Typically, JPGs will work for most investigations. The following Image Quality bullet has more details.

- **Image Quality**: If the PNG is specified as the Image Format, the Image Quality parameter is not used. When JPG is specified as the Image Format, you must set the quality in the range from 0 to 100. The recommended default quality is 75 which has a great compression ratio (images for 1920 x 1080 are often only on the order of 100k), and you can clearly see the screen and read the text. A quality of 50, may result in difficulty reading screen text, and the color depth is reduced, but the file size will become so compact (10k) that it could dramatically assist with bandwidth issues.

As part of the screenshot capture functionality, several situations can cause a black or blank capture such as a screen lock or screen saver. A blank screen is captured anytime the screen is not rendered.

There are some specific behaviors to understand when working with an RDP endpoint. Depending on the RDP state on the endpoint, the screenshots may be blank. If the user is not signed into an endpoint RDP session, then the screenshot is blank. If the RDP session is minimized the screenshot is blank.

To collect screenshots on endpoints:

1. Navigate to the **Endpoint module**.
2. Right-click on the **Endpoint** and select Collect Screenshot.
3. Navigate to the **Tasks module** to view the image.

Collect from Host

Create and run collections using the Collection Wizard, see Collections for more details.

Execute Command

Select this option to open the **Execute Command** dialog box, where you can run the command using a Command shell.

The **Execute Command** dialog box relies on the standard Windows Command shell commands and binaries already residing on the endpoint. Enter the command and confirm the selected endpoints, then click **Execute**.

Upload and execute

Select this option to open the specific file to upload and execute on the selected endpoint using the security context of the Nuix Adaptive Security Endpoint Agent.

The agent writes the file to a temporary directory on the endpoint and deletes the file after executing the file. Use any of the following three optional parameters to control how you execute the file on the endpoint:

- **Upload New File**: Select an executable file from the local directory to run on the endpoint.

Warning: Nuix Adaptive Security uploads the selected files directly to the endpoint, writes the files to a temporary path, and deletes the files after execution.

- **Arguments**: Specify the command line arguments to use in running the executable.

Warning: Nuix Adaptive Security does not support executing binaries that interact with UI elements.

- **Run using the Command Shell**: When enabled, this option means that the selected file runs using a Command shell. This is useful if it is necessary to capture the output of the execution by redirecting stdout or stderr to a file and acquiring it after the fact.

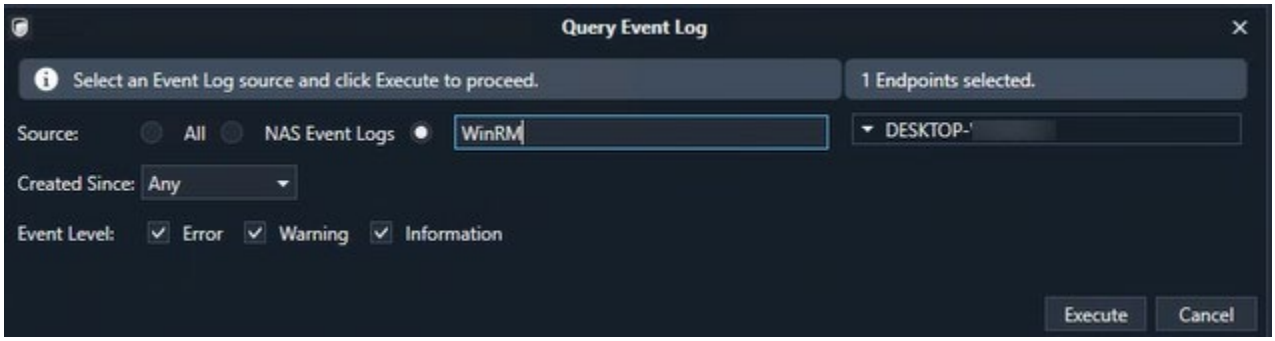
Once you upload the file and confirm the endpoints affected, click **Execute** to run the command.

Query Event Log

Select this option to open the **Query Event Log** dialog box. The options for **Created Since** and **Event Level** are enabled when using a custom source. These options are disabled when using **All** or **NAS Event Logs**.

To query the event log:

4. Select an Event Log source: All, NAS Event Logs, or enter a custom source.
5. If you are using a custom source, select the date range for Created Since.
6. If you are using a custom source, select the Event Level.
7. Click **Execute** to query the event logs.



Survey

Select this option to open the **Get Endpoint Survey** dialog box, where you can perform an endpoint survey, updating the data available on the Endpoint Details tab.

In the window that appears, the application asks for confirmation of this action, as it may take some time. After confirming the selected endpoints, click **Execute** to run the survey.

Microsoft Defender

Nuix Adaptive Security has access to view the Microsoft Defender Antivirus application details if Microsoft Defender is installed on the endpoint. The Microsoft Defender status displays when real-time monitoring is enabled.

Once installed, use the Nuix Adaptive Security application to launch scans, view status reports, and update Microsoft Defender signatures. On endpoints with Windows versions earlier than Windows 10, version 1607, and Windows Server 2016, Microsoft Defender can be enabled and disabled. Newer versions of Windows 10 no longer allow you to disable Microsoft Defender.

The agent queries the Microsoft Defender status on an endpoint at the start of every endpoint session. Each time the endpoint connects, if it has been longer than InitialSessionTaskResendTimeLimitInMinutes, the default 1440 minutes which is 24 hours, then the Microsoft Defender status is re-queried. If the agent reconnects every day, then the Microsoft Defender status is re-queried every day. If the agent stays connected for one year, then the status will never be re-queried unless you request it.

Note: When viewing the Microsoft Defender tab, and real-time protection is enabled and then disabled, the Microsoft Defender information clears when you select to query status. The Microsoft Defender status displays when real-time monitoring is enabled.

Click the Microsoft Defender button on the Investigate or Endpoint tabs to open the list of the following options:

- **Enable/Disable Microsoft Defender**: View whether Microsoft Defender is on and off.
- **Quick Scan**: Launches a Microsoft Defender quick scan that searches all the potential locations for malware, for example, registry keys, Windows startup folders, and mounted removable devices. Quick Scan does not do a complete system scan.

- **Full Scan**: Launches a Microsoft Defender full scan that searches the entire system to identify all components of malware threats.
- **Warning**: Depending on the size of your system, a full scan can take a considerable amount of time. Take this into account when using this scanning option.
- **Query Most Recent Scans**: Returns the results from the last quick or last full scans from the endpoint.
- **Query Status**: Provides the status of Microsoft Defender, including the number of threats discovered, the type of the last scan, the operating status, and the status and versions of the Microsoft Defender components.
- **Query Active Threats**: Displays the list of discovered but not remediated threats. Due to Microsoft Defender's always-on real-time protection capability, the number of active threats is minimal.
- **Query Historic Threats**: Displays the list of discovered and remediated threats on the endpoint.
- **Update Signatures**: Tasks the endpoint's Microsoft Defender to update the malware signatures from Microsoft.

Manage endpoints

The following options are available under **Manage**:

Configure endpoints

The configuration defines the agent settings, logic rule set, namespaces, and hash lists. For more configuration information, see Configuring the agent.

Upgrade endpoints

Select this option to upgrade the Nuix Adaptive Security Endpoint Agent on the selected endpoint. You can also upgrade a group of endpoints, for more information, see Upgrade endpoints in a group.

To perform an upgrade to an endpoint:

1. Select **Upgrade** from the menu. The **Upgrade** dialog box appears.
2. In the dialog box, select the new installer for each platform.
3. Select **Execute**.

The endpoint is upgraded to the selected installer.

Uninstall endpoints

Select this option to uninstall the Nuix Adaptive Security Endpoint Agent on the selected endpoint. You can also uninstall a group of endpoints, for more information, see Uninstall endpoints in a group.

To perform an uninstall on an endpoint:

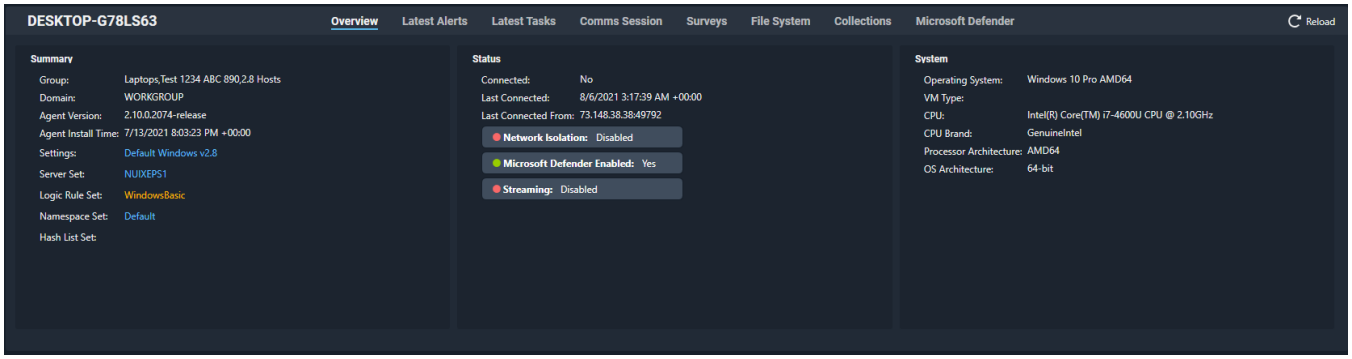
1. Select **Uninstall** from the menu to show a dialog box. This box asks if you are sure you want to remove the agents from the selected endpoints.
2. Confirm the endpoints selected.
3. Click **Execute** to begin the uninstall process.

Add to group

For details on how to add an endpoint to a group, see Assign an endpoint to a group.

Detailed view of an endpoint

When viewing an endpoint in the **Endpoints** module on the **Server Hosts** tab, you can view more detailed information as shown in the following image.



The detail consists of the following tabs:

- Overview
- Latest Alerts
- Latest Tasks
- Comms Session
- Surveys
- File System
- Collections
- Microsoft Defender

Overview

Clicking an endpoint shows the details. The details provided on this tab are related to the host and system information. The Overview tab provides the following information:

Summary: Provides a quick breakdown of information about the endpoint with Nuix Adaptive Security.

- **Groups**: Displays the groups to which the endpoint belongs.
- **Domain**: Displays the domains to which the endpoint belongs.
- **Agent Version**: Displays the version of the Nuix Adaptive Security Agent running on the endpoint.
- **Agent Install Time**: The timestamp when the agent was installed on the endpoint.
- **Settings**: The static configuration settings for the agent.
- **Server Set**: The server for the endpoint.
- **Logic Rule Set:** The logic rule set is assigned to the endpoint.
- **Namespace Set:** The namespace set assigned to the endpoint.
- **Hash List Set:** The hash list assigned to the endpoint.

Status: Shows whether the endpoint has monitoring features enabled or disabled.

- **Connected**: Displays **Yes** or **No** to show whether the endpoint is connected to Nuix Adaptive Security.
- **Last Connected**: If the agent is connected, this displays the date and time the endpoint first connected to Nuix Adaptive Security. If the agent is not connected it displays the last date and time the agent was connected to Nuix Adaptive Security.
- **Last Connected From**: Displays the IP address from where the endpoint is connected.
- **Network Isolation**: Displays **Enabled** (green dot) or **Disabled** (red dot) to show if network isolation is enabled.
- **Microsoft Defender Enabled**: Displays **Yes** (green dot) or **No** (red dot) to show if Microsoft Defender is enabled.

Note: If the endpoint is a Mac or Linux, Network Isolation and Microsoft Defender are not available.

System: Information related to the endpoint.

- **Operating System**: Displays the platform type and software version of the endpoint.
- **VM Type**: Displays the virtual machine type.
- **CPU**: Displays the central processor unit type.
- **CPU Brand**: Displays the central processor unit brand.
- **Processor Architecture**: Displays the endpoint's processor architecture or design of the CPU.
- **OS Architecture**: The core software components of an operating system kernel.

Latest alerts

This section displays the 1,000 most recent alerts and other significant events occurring on the endpoint.

Results List

Refine the results by selecting from one of the following categories:

- **Alert ID**: Displays the alert identification number.
- **Timestamp**: Displays the alerts by timestamp, which can be filtered by ascending or descending order.
- **Status**: Displays alerts by status. Alerts without status are listed first.
- **Assigned User**: Displays alerts by the assigned user. Alerts with no user assigned are listed first.
- **Name**: Displays the rule name.
- **Alert Description**: Displays alerts alphabetically by their description.
- **Rule Group**: Displays alerts alphabetically by their rule group name. Alerts without rule groups are listed first.
- **Process**: Displays alerts by the process that generated the alert, listed alphabetically by the process.
- **Process Id**: Displays alerts by the process Id that generated the alert, listed alphabetically by process ID.
- **Parent Process**: Name of the parent process that generated the alert, listed alphabetically by the parent process.
- **Rule Alert**: Displays alerts by their rule alert, listed alphabetically.
- **Rule Alert Action**: Displays alerts by their rule alert action, listed alphabetically
- **Severity**: Alert severity level as 1, low, medium, and critical.
- **Host Local Timestamp**: Displays alerts by their timestamp.

Latest tasks

Tasks are created when the agent connects to the Nuix Adaptive Security Endpoint Server and if a task was not sent in the last 24 hours. The default value is 1440 minutes, which is one day. You can configure this value by editing the config.txt file and then stopping and starting the NuixEPS service.

Six default tasks are assigned to every new endpoint.

- System Survey
- Network MAC Survey
- Account Survey
- Request DBR entries
- Root directory listing
- Microsoft Defender status (Windows only)

System Survey tasks are run by the application. These tasks do not repeat and will run immediately by default when the agent connects to the server.

Comms session

This tab displays network communication statistics between the Nuix Adaptive Security Endpoint Server and the individual endpoint.

Sort the columns by using the right-click menu. For more information about these functions, see Filtering.

Surveys

This tab displays a more detailed look at the endpoint. The timestamps shown in the list correspond with the times the survey task was performed by the agent.

Additional options appear on this tab, as described in the following table.

Tab	Description
Survey	Various information about the endpoint, including its host-related information and creation date. The survey tasks run immediately when the agent is available. These do not repeat.
System	More detailed information about the endpoint system, including the installation time of the Nuix Adaptive Security Endpoint Agent and the OS type.
Processors	Information about the processors used on the endpoint.
Firmware	Information about the firmware on the endpoint, including the BIOS version and serial number.
Logical Drives	Information about the drives used by the host, including their size, free space, and file system type. Drag any of the column headers to the toolbar to examine the data in more detail. Sort the columns by using the right-click menu. For more information about these functions, see Filtering.
Adapters	Information about the adapters used on the endpoint, including their name, physical address, description, and connection type. Drag any of the column headers to the toolbar to examine the data in more detail. Sort the columns by using the right-click menu. For more information about these functions, see Filtering.

Use the **Previous** and **Next** buttons to move between the tasks that were run on each of the tabs, listed by timestamp, and showing the most recent one completed.

File system

This tab provides data on the file system used by the endpoint, including its size and a look at the directory structure. Times for the following tasks are also available: Create Time, Last Access Time, Last Write Time, Last Change Time, Query Time, Last Seen, Last Seen Task Result Id, Last Query, and Last Query Result IDd.

The following options are available by right-clicking on a volume in the list:

- **Collect**: Collect a file from the file system by entering the number of folder levels, and then click **OK**.

Note: Collecting more than one level at a time potentially increases file size and collection time.

Note: When you select to collect a file or screenshot, the files are saved in a password-protected zip file. The standard Windows 10 unzip tool does not support AES256 encryption used by Nuix Adaptive Security. You will need a third-party tool, such as 7-Zip, to extract the files.

- **Query**: Search for terms in the file system by entering a path. When completed, the search is shown on the Task tab.
- **Delete**: Select a file to remove it. Click **OK** in the confirmation window.
- **Copy**: Copy a file.
-

Collections

This tab provides the active and completed collections for the selected endpoint. You can pivot to the collection module from each collection. For more information about collections, see Collections.

Microsoft Defender

This tab provides status for the Microsoft Defender antivirus software.

Note: This tab does not appear if the endpoint is a Mac or Linux platform.

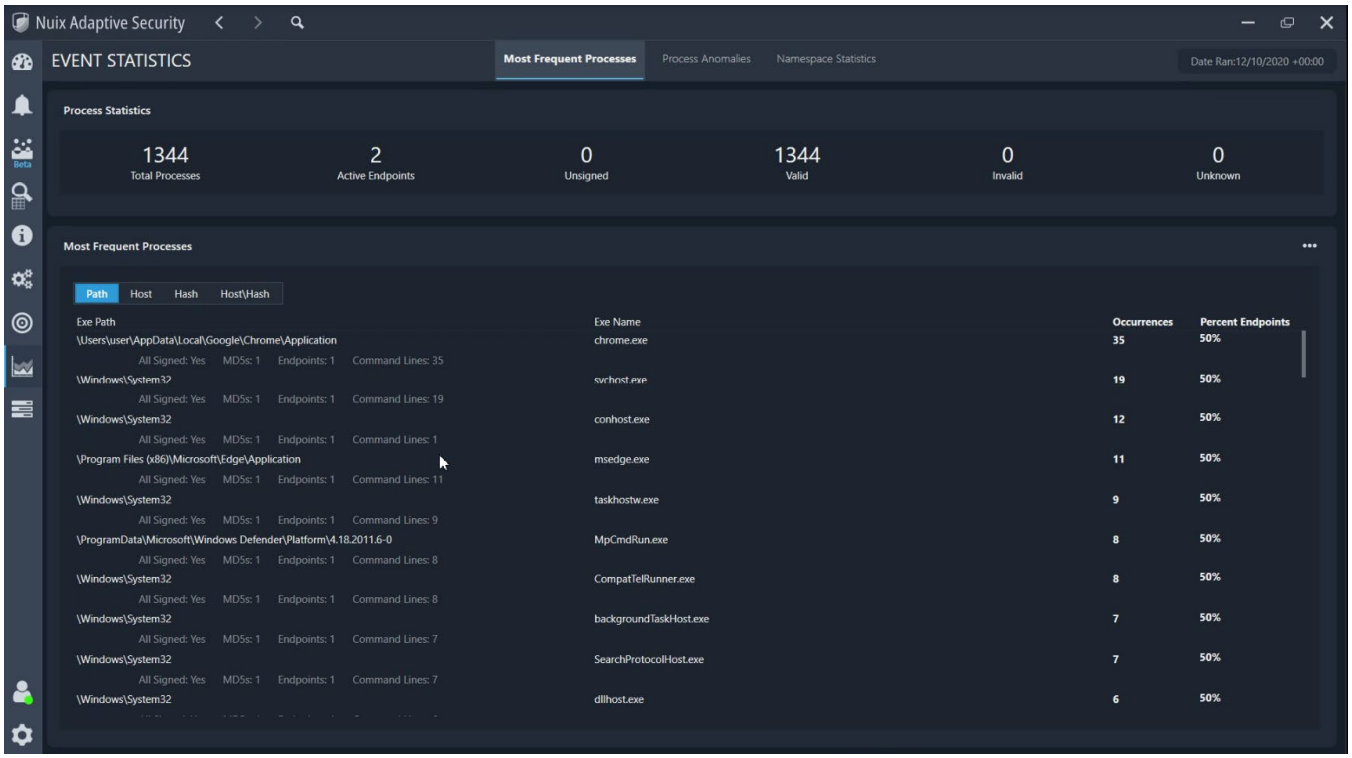
The tab contains the following sections:

- **Status**: Provides information about the most recent report time, whether Microsoft Defender is enabled, the last scan timestamp, the product version, service version, engine version, and file system filter.
- **Component Status**: Provides information about signatures used in detecting threats.
- **Threat Information**: Provides information about any threats yielded by a scan. Sort the columns by using the right-click menu. For more information about these functions, see Filtering.
- **Threat Artifacts**: Subtle traces of a threat that require additional investigation.

Event Statistics

The Event Statistics tab is where you can view daily event details about the endpoints in your environment, as shown in the following image. During an alert triage or investigation, you can look for anomalies or high percentages of certain processes or events. These reports can be used to discover anomalous events that deserve further investigation and provide another way to view and identify threats in your environment.

The statistical analysis shows data across the entire enterprise. Unlike identifying threats and hunting based on specific indicators of compromise, the event statistics allow you to identify anomalies in data without having to know specifically what you are looking for. It can be used a starting point for analysts to have a wide view of the organization versus looking at specific endpoint data.



The statistics are gathered from forwarded process and namespace events from endpoints that were active and connected during the previous day. Use the event statistics to create reports on specific analytics in your environment. For example, you can analyze the frequency a user visits a specific web domain.

By default, the statistics are generated nightly at midnight and cover the previous 24 hours. The time stamp will display the last time the server ran the report to gather the statistics. This report is based on a 24-hour time range from midnight to midnight. The scheduled time and frequency are configurable through the Swagger web access and the appsettings.json configuration file. The frequency can be changed to hourly, daily, weekly, and monthly.

Additionally, the reports can be exported to CSV files using the '...' menu in the top-right corner. You can export data to a CSV file for a specific process. For example, if you select Host and then export CSV, all the host data is exported to the CSV file. You can show or hide details for each item.

A few situations could result in the service not running. The **Date Ran** box in the top-right corner displays the date and time of the most recent run.

There are a few scenarios when the reports will be expected to have no data:

- The initial installation and upgrade of Nuix Adaptive Security. The initial run is scheduled to occur 10 minutes after install. But, depending on the installation process, this may not be enough time to connect active endpoints. The subsequent runs will occur nightly at midnight starting with the current day.

- The Logic Rules were not defined to forward process and namespace events.
- The endpoints were connected but had no activity that generated process or namespace events. It is common to see idle endpoints with no namespace events.
- No endpoints were connected during the previous day.

Process Statistics

The **Process Statistics** header displays the overall process event counts for the connected Adaptive endpoints during the previous day.

- **Total Processes**: The number of summarized process events for all connected endpoints.
- **Active Endpoints**: The number of endpoints that connected to the Nuix Adaptive Security endpoint server.
- **Unsigned**: The number of summarized process events with unsigned signatures in the backing executable.
- **Valid**: The number of summarized process events with valid signatures in the backing executable.
- **Invalid**: The number of summarized process events with invalid signatures in the backing executable.
- **Unknown**: The number of summarized process events with unknown signatures in the backing executable. These typically occur when the Nuix Adaptive Security agent is unable to obtain the signature.

Event reports

The three categories of events are **Most Frequent Processes**, **Process Anomalies** and **Namespace Statistics**. These are accessed using the tabs of the Event Statistics module.

Most Frequent Processes displays four reports describing the frequency of the process event paths. By default, the reports display the most frequent 100 paths and the least frequent 100 paths. The report columns are sortable. View additional row information, such as whether all the executables are signed, by selecting the **Show all details** box from the '...' menu in the top right corner.

Reports:

- **Path**: Occurrences of paths from all connected endpoints.
- **Host**: Occurrences of paths for each endpoint.
- **Hash**: Occurrences of paths grouped by the MD5 hash value of the executable.
- **Host\Hash**: Occurrences of paths grouped by both the endpoint and the MD5 hash value.

Process Anomalies: Displays five reports describing the frequency of the process event command lines. By default, the reports display the most frequent 100 paths and the least frequent 100 paths. The report columns are sortable. View additional row information by selecting **Show all details**.

Reports:

- **Command Line**: Occurrences of command lines from all connected endpoints.
- **Hash**: Occurrences of command lines grouped by the MD5 hash value of the executable.
- **Parent Path**: Occurrences of command lines grouped by both the MD5 hash value of the executable and the full path of the parent executable.
- **Host\Command Line**: Occurrences of command lines per each endpoint.
- **Host\Hash\Command Line**: Occurrences of command lines grouped by both the endpoint and the MD5 Hash value of the executable.

Namespace Statistics: Displays four reports describing the frequency of DNS namespace queries. By default, the reports display the most frequent 100 queries. The columns are sortable. View additional row information by selecting **Show all details**.

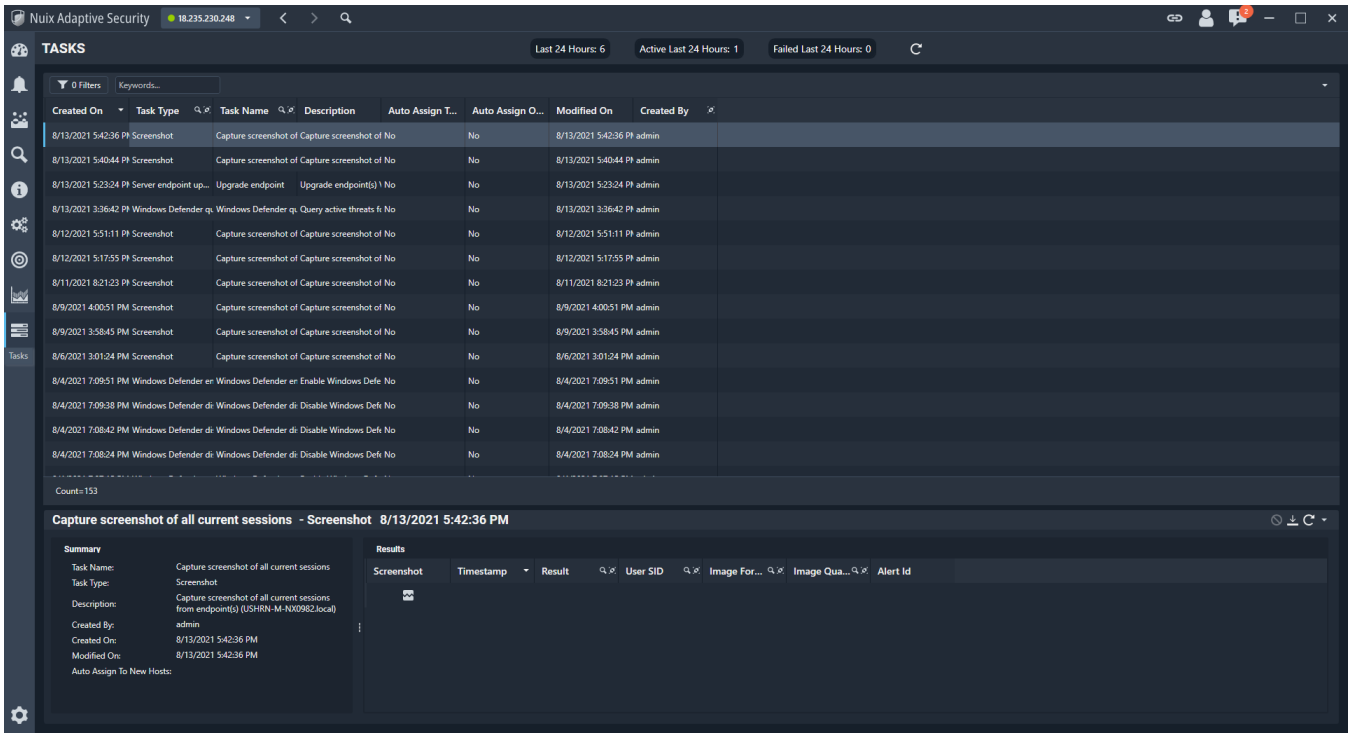
Reports:

- **Query**: Occurrences of DNS queries from all connected endpoints.
- **Host**: Occurrences of DNS queries grouped by endpoint.
- **Process**: Occurrences of DNS queries grouped by process full path.
- **Process\Host**: Occurrences of DNS queries by both endpoint and process full path.

Tasks

Use the Tasks module to view any job that was created on another tab. You can view tasks to see if the tasks are complete or if they failed.

Click on a task and the full detail appears on the bottom. Filter the tasks using the filter list across the top of the window, as shown in the following image.



Filter Tasks

To filter tasks, use the following fields:

- **Group By**: Select how to group tasks by name, type, or created by.
- **Date Range**: Click the boxes to adjust the time period for the data. Use the calendar to adjust the date. Adjust the time manually.
- **Task Type**: Filter by task type.
- **Status**: Filter by the following task status:
  - **Active**: Displays the tasks currently in progress.
  - **Complete**: Displays the tasks that finished.
  - **Failed**: Displays the tasks that finished as failed.
  - **Sent**: Displays the tasks that were sent but have not started.
  - **Canceled**: Displays the tasks that were canceled.

- **Show All Task Types**: Filter to show all tasks.
- **Advanced**: Filter using Boolean operators.
- **Keywords**: Enter a search term and the results will contain just the term. Click **Reset** to clear the search bar. Click **Filter** to narrow the results by search term.

Results list

This list shows all the generated tasks.

- **Created On**: Listed by the date of the task's creation.
- **Task Type**: Listed alphabetically by type.
- **Task Name**: Listed alphabetically by name.
- **Description**: Sorted alphabetically by description.
- **Modified On**: Listed by the date the task was last modified.
- **Auto assign to new hosts**: Select this option to automatically assign the task to new endpoints.
- **Auto assign on new alert**: Select this option to automatically assign the task to a new collected alert.
- **Created By**: Listed by the user creating the task.

The upper-right side of the tab provides the option to reload the data for the current endpoint by clicking the **Reload** button.

Copy 'Text': Select this option to copy the data in the column to the clipboard.

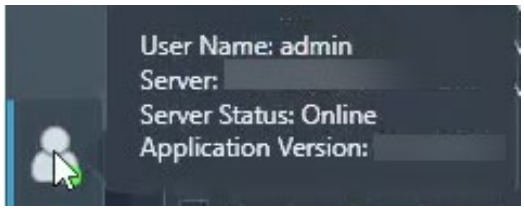
On the right side of the tab, the information that appears has the following format:

- **Top of the tab**: Includes the name, type, and state of the task, who created the task, and at what time, and whether the task is auto assigned on new alerts or to new endpoints.
- **Bottom of the tab**: Includes information about the task. What displays here depends on the type of generated task. For example, if this is a task to change an endpoint configuration, the data includes the host name of the endpoint with the configuration change.

A number appears over the Tasks button when you create a task on another tab.

User Profile

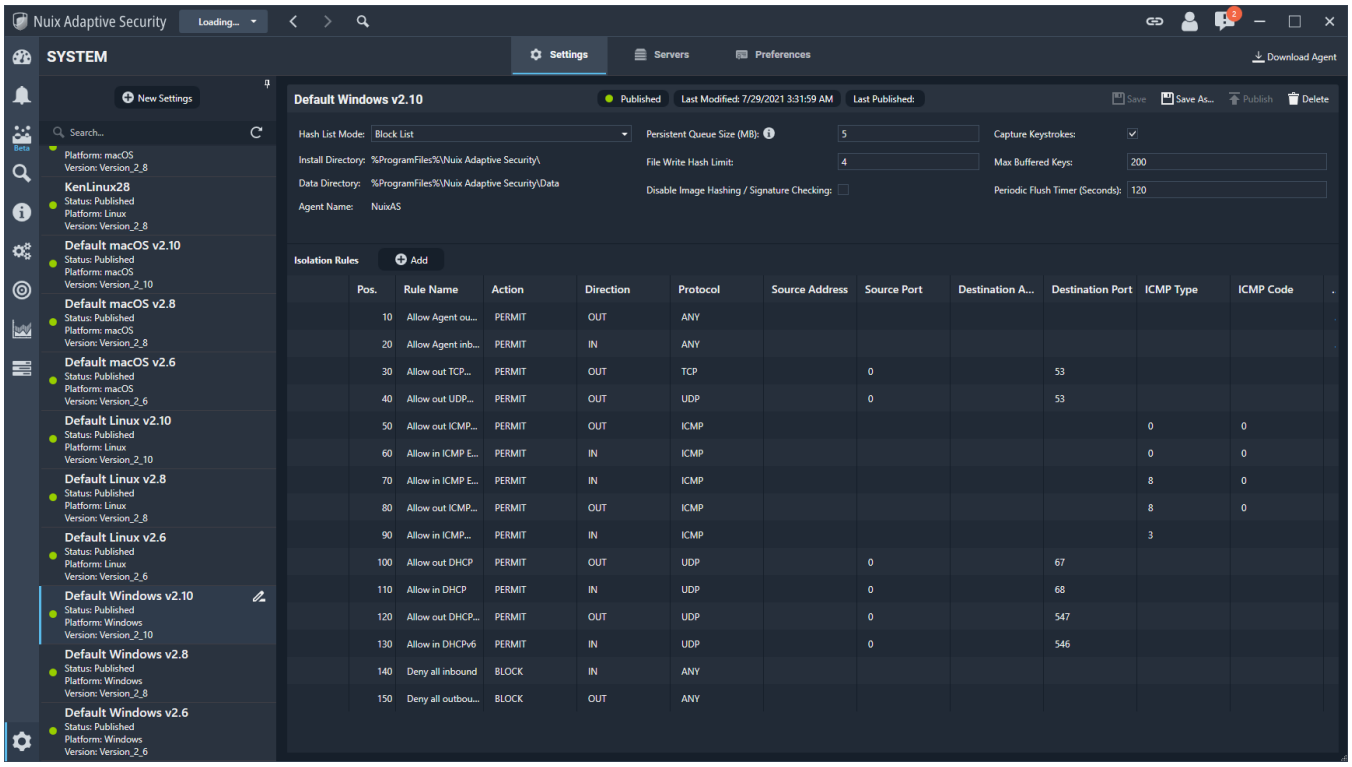
Hover over the **User Profile** button on the left side, as shown in the following image, to see information about your version of Nuix Adaptive Security or to log out of the application.



- **User Name**: Lists the name of the user who is logged in to Nuix Adaptive Security.
- **Server**: Lists the IP address of the Nuix Adaptive Security Server.
- **Server Status**: Lists the status for the Nuix Adaptive Security Endpoint Server. Green means that the server is online. Red means that the server is offline.
- **Application Version**: Lists the version number of Nuix Adaptive Security currently running on the server.

System

The System tab contains the information about settings, servers, and preferences, as shown in the following image.

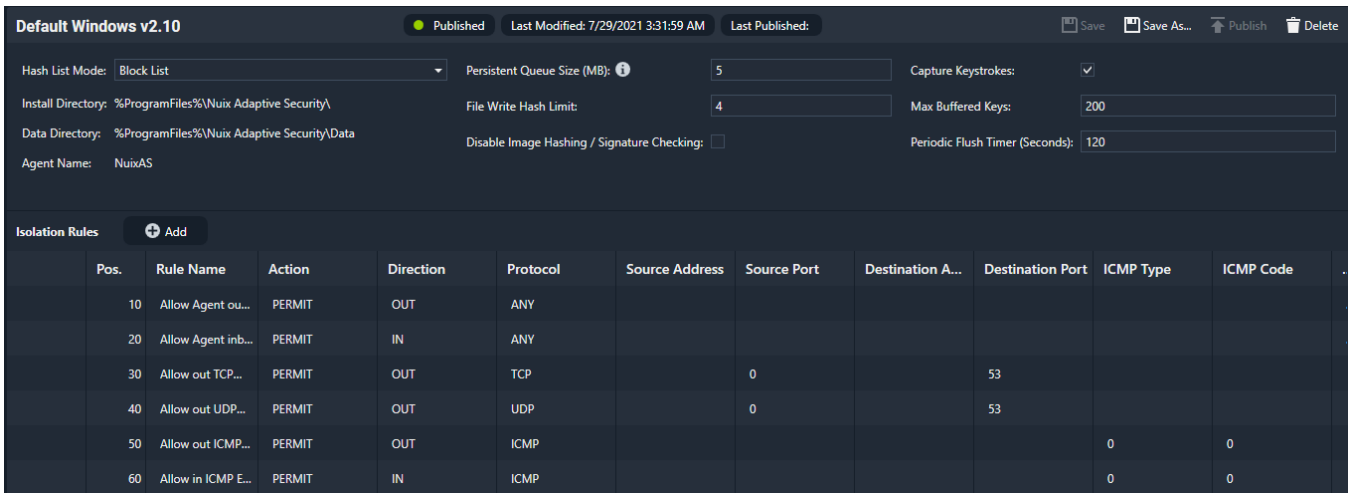


This tab contains the following information:

- Settings
- Servers
- Preferences

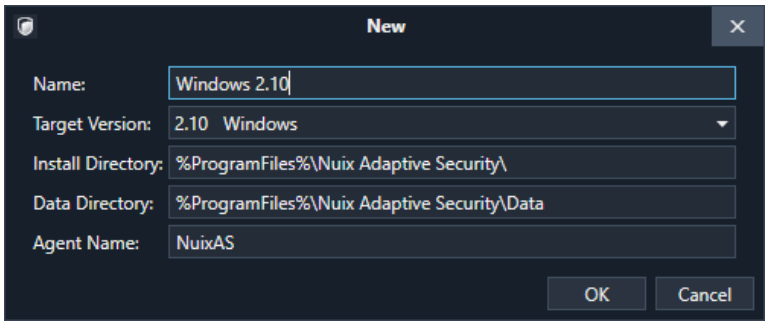
Settings

The settings provide the static configuration settings for the agent, as shown in the following image. This is typically set up during the installation process.



Add new agent settings

Add the new agent name and details. The agent setting fields vary depending on the selected endpoint operating system.



To add new settings:

4. From the **System** > **Settings** tab, select the **+ New Settings** button.
5. Enter the N**ame** for the new settings. The name should explain what the agent settings do or where you are going to deploy the agent settings, for example, to desktops or servers.
6. Select the **Target Version**. The target version includes the Nuix Adaptive Security version and the type of operating system.
7. (*Optional*) Once you provide the name and target version, the other three settings appear. The dialog box lists the default values for the **Install Directory** and **Data Directory** and **Agent Name,** but you can make changes to the values.
8. Once this data is entered, click **OK** to save the data.

Configure settings

The following settings appear on this tab.

Note: You cannot edit the values for Install Directory, Data Directory, and Agent Name on this tab.

- Hash list mode: Select Allow List or Block List from the menu.
- **Install directory**: The directory location where the agent install files are located on the endpoint.

- **Data Directory**: The directory location where the agent data files are located on the endpoint.
- **Agent Name**: The agent name as it appears on the endpoint.
- **Persistent Queue Size (MB):** This is the queue size for the recorded events. It is set to 5 *MB by default*. This size controls the amount of data sent from the endpoint to the endpoint server. This setting caches data if the agent cannot reach the server for any reason and removes the oldest data as the queue fills up. This happens when the size is too small or the agent becomes disconnected from the endpoint server for an extended amount of time.
- **File Write Hash Limit**: Controls the generation of a hash for a closed file after it is open for writing. This setting helps when hashing occurs because hashing requires a lot of resources. If the file is over the hash limit size, the server skips the hashing, and the field is empty in the corresponding file write event. Using this setting can reduce the burden on a system and should be set in a manner that gets the desired hashes. By default, it is set to 4 MB. When selecting an appropriate value, consider the possible existence of large files or databases that are frequently opened for writing, updated, and then closed, because each of these causes rehashing of the files.

Note: Nuix Adaptive Security hashes all files if this limit is set to zero (0) MB. This means you have disabled the limit which will result in an intolerable burden on some systems and should be avoided.

- **Disable Image Hashing / Signature Checking**: Selecting this option disables image hashing and signature checking at runtime. This reduces processing time and CPU consumption for image load threads on the endpoint. This setting is cleared by default.

Note: Logic Rules that reference hash values or signature status of loaded modules will not behave as expected when using this option.

- **Capture Keystrokes**: Selecting this check box captures all keystrokes on an endpoint. Use this setting with caution as it generates a lot of data.
- **Max Buffered Keys**: A section of memory is held to hold keystrokes prior to processing. By default, this is set to 200 MB.
- **Periodic Flush Timer (Seconds)**: Amount of time in seconds to hold a keystroke before flushing the keystroke. By default, this is set to 120 seconds.

Isolation rules

Like firewall rules, isolation rules are network filtering rules applied to endpoints.

Nuix Adaptive Security applies rules when the filter engine matches an isolation rule, or at the direction of a Nuix Adaptive Security administrator.

The default rules allow endpoint agents to communicate with all addresses.

Create a rule from an existing rule

Use the following procedure when creating a new rule from an existing rule. For example, if the existing rule runs on port 500, but also needs to run on port 550.

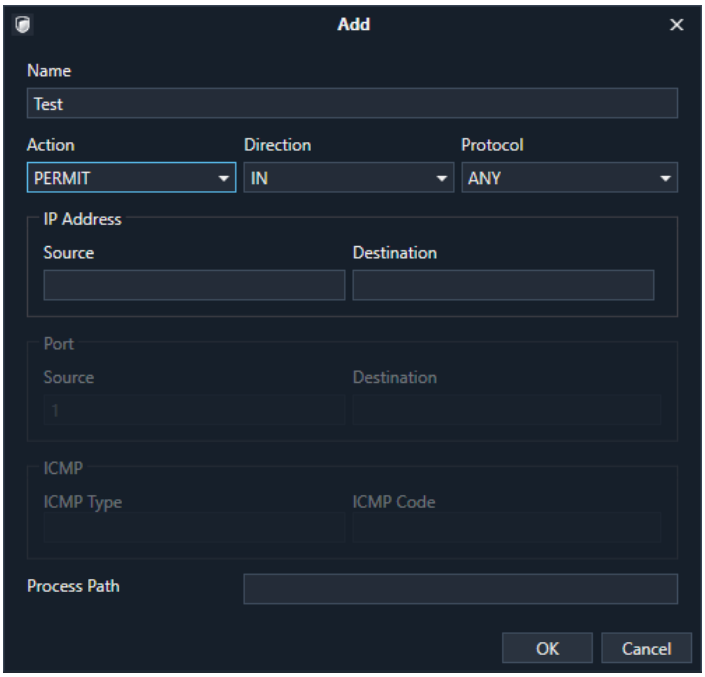
To create a rule from an existing rule:

1. Open the **System > Settings** tab, select an existing rule from the Isolation Rules list. Click the pencil edit symbol to open the isolation rule.
2. Make any necessary changes to the existing rule for the new rule. The new rule is displayed at the bottom of the list.
3. Click **OK**.

Create a new rule

To create a new rule:

1. Open the **System > Settings** tab and select the **+Add** button next to Isolation Rules.
2. This shows the **Network Isolation Rule** dialog box, as shown in the following image.
3. Enter your settings in the box. The settings are described in more detail under the image.



The new rule is displayed at the bottom of the list.

In the Add Isolation Rule dialog box, you can configure the following settings:

- **Name**: Provide a name for the new Rule.
- **Action**: Can be set to **Permit** or **Block**.
- **Direction**: Specifies if the rule applies to inbound traffic (traffic entering the endpoint system from a remote source) or outbound traffic (traffic initiated on the endpoint system). Can be set to **In** or **Out**.
- **Protocol**: Can be set to **Any**, **TCP**, **UDP**, or **ICMP**.
- **IP Address**:
  - **Source**: The source address of the device sending the information.
  - **Destination**: The source address of the device where Nuix Adaptive Security sends the information.
- **Port**: For filters that specify a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), specify the source and destination ports.
- **ICMP**: For filters that specify an Internet Control Message Protocol (ICMP) , specify the ICMP type and ICMP code. For example, a ping request filters by specifying an ICMP type of 8 and an ICMP code of 0.
- **Process Path**: Apply the network filter rules to the data traffic associated with specific processes. To associate a network filter rule with a specific process, enter the executable path of the process here, for example, “c:\windows\system32\svchost.exe”.

4. Click **OK**.

Delete a rule

To delete a rule:

1. Click the **X Delete** button to remove the row.
2. In the dialog box that is displayed, click **Yes** to confirm the action.

Servers

The servers tab is where you can view all the Nuix Adaptive Security endpoint servers in your environment. You can also add, edit, or delete servers on this tab. This is where you add a server for redundancy, as a DMZ or for backup. This is not where you add servers for a multiple server environment which is done during the installation process.

The following settings appear on this tab:

- **Hostname or IP Address**: Specify whether to listen on a specific address or to listen to all IP addresses.

Note: If the server has multiple IP addresses, for example, one for internal use and another for external use, be sure to list the correct IP address when creating a new configuration. Confirm that the IP address entered during the Nuix Adaptive Security installation is the external one to mitigate this issue.

- **Port:** The port number to listen on.

The other two columns contain the following information that cannot be edited:

- **CA Cert**: The digital certificate authority (CA) certification for the server you are adding. When using this with Transport Layer Security/Secure Sockets Layer (TLS/SSL), it may be for an organization or an individual.
- **Subject CN**: The Subject Common Name (CN) is the server name protected by the SSL certificate.

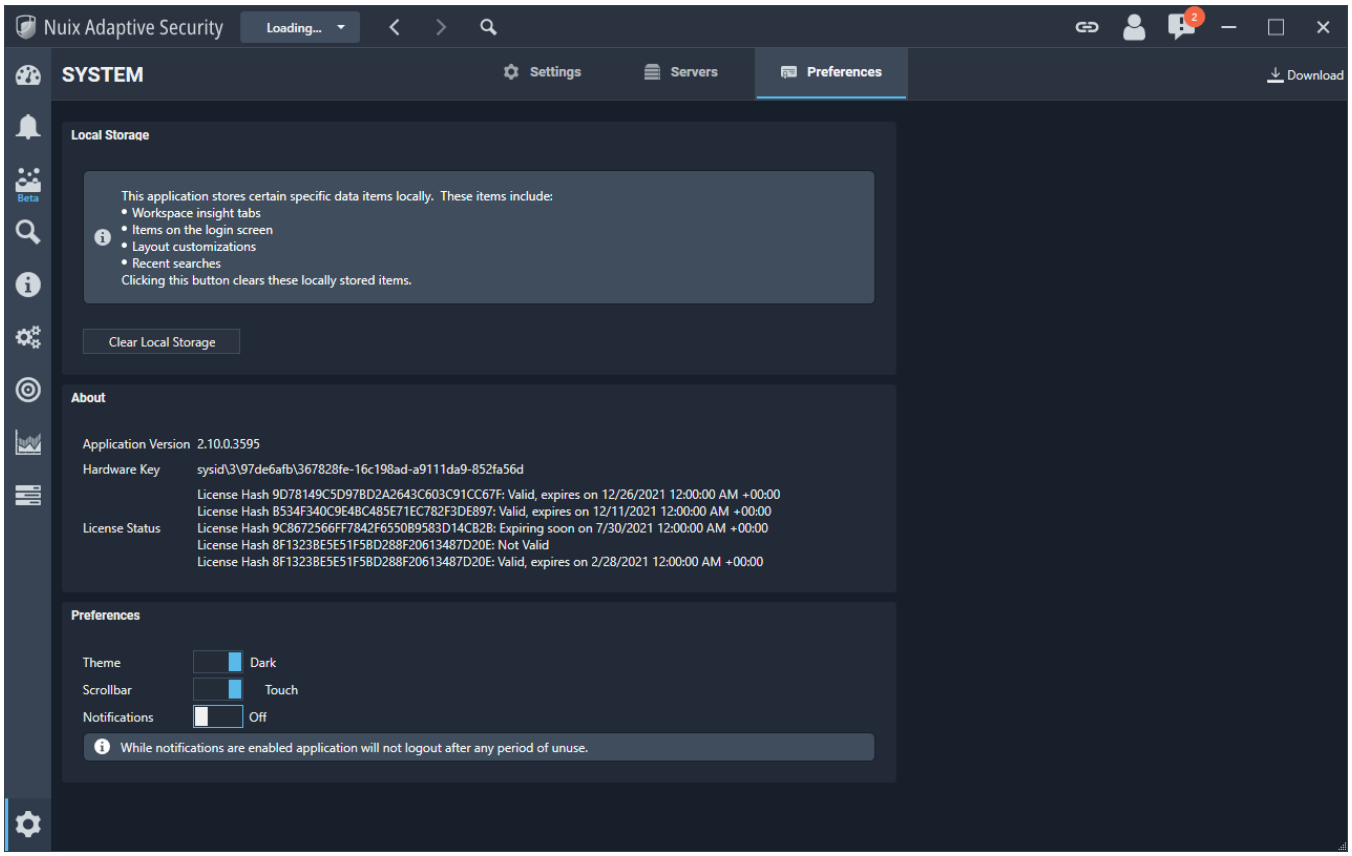
Add a server

To add a server to your environment:

1. From the **System** > **Servers** tab, select the **+Add** button.
2. Add the server's hostname or IP address.
3. Add the server's port, CA certificate, and Subject Common Name (CN).
4. Click **OK**.

Preferences

Preferences contains information on the local storage, about, and preferences, as shown in the following image.



Local Storage

Clear Local Storage: Click this button to delete any locally stored values found at **c:\Users\<current user>\AppData\Local\Temp\Nuix**. These values include the following:

- Workspace insight tabs
- Items on the login screen
- Layout customizations
- Recent searches

To clear your local storage, click **Clear Local Storage**.

About

The **About** provides information about your Nuix Adaptive Security license, including the application version, hardware key, and the expiration date of your license.

For any questions or assistance with licensing, contact your sales representative or contact support at https://nuix.service-now.com/support.

Preferences

In the preferences, you can change the theme from dark to light. Light will change the application pages to a white background. The default is dark theme.

The scrollbar touch option provides the option for a scrollbar that does not take up screen space until it is touched. The standard scrollbar takes up more screen space and is always visible.

You can also turn off notifications. When notifications are enabled, the application will not logout after any period of idle time.

Endpoint agent data flow

The Nuix Adaptive Security endpoint agent provides a deep view of enterprise computers and has powerful capabilities to prevent and react to suspicious activity. The system can collect a massive amount of data. At times, this may be necessary during an investigation. However, collecting excessive data from endpoints across an entire enterprise, taxes the system and impacts performance. By following a few guidelines regarding data collection and rule management, the operator can reduce the volume of data significantly and avoid frivolous alerting.

To effectively collect data and write rules, the operator should understand the basics of data flow within Nuix Adaptive Security.

Logic engine

At the core of the Nuix Adaptive Security endpoint agent is the logic engine. The logic engine receives the events from the agent and executes the logic rules. The types of events that the agent can monitor include the following:

- Process
- File
- Session
- Removable media
- Network
- Registry
- Printing

For more information about this, including a complete list of the events the agent can monitor, see the Event Types.

Agent events

Events are generated in the Nuix Adaptive Security endpoint agent based on endpoint activity. Each event contains pieces of data around the event. The events are sent one by one through the filter engine. The filter engine processes events by executing the rules that are sent to the agent. Each rule consists of an action carried out by a series of Boolean logic. The filter engine evaluates the Boolean logic against the event data. If the expression is true, then the action of that rule is executed. Rules operate on a single event at a time. The rule actions allow you to drill down into specific endpoint processes. Then you can write rules on matching and comparisons of the different event fields.

You can start to correlate activity across multiple events. Then you want to combine data from different types of events into your rules. The process state database allows you to track data across multiple events.

Digital Behavior Recorder

Events are written to the Digital Behavior Recorder log (DBR). The DBR is a circular data buffer on the endpoint agent that caches data for a period of time.

Some events such as registry events will take up more space so you may wish to use the suppress rule, otherwise the DBR log will fill up. The DBR is half of a gigabyte in size by default. As the DBR fills up, the older events are overwritten by newer events. Use the default forward and suppress rules when you want to forward or suppress specific events.

For example, the Windows operating system generates a lot of registry events in normal operations that are generally not interesting. The suppress statement prevents certain types of noisy and uninteresting registry events from storing in the DBR.

```
# Suppress registry key activity for the CRL, CTL, and
```



```
# Certificate registry keys.
    suppress when stristr(registry.keyname, "CRLs");
    suppress when stristr(registry.keyname, "CTLs");
    suppress when stristr(registry.keyname, "Certificate");
```

Nuix Adaptive Security can collect object and thread events, which can be useful but can also generate a massive amount of data. If you create a process handle, that process handle generates an object event. This activity correlates to the use of functions. For example, the Win32 OpenProcess function allows a process to open a handle to another process with varying degrees of permission. Object events can indicate attempts by a process to open a handle to another process for the purpose of reading or writing that other process's address space. Most use cases suppress object and thread events. For example:

```
    suppress when eventtype.object == true;
    suppress when eventtype.thread == true;
```

Note: For a suppressed event not stored in the DBR, the event still passes through the logic engine. Rules will still operate on the events and can generate alerts. Any associated data forwards to the Nuix Adaptive Security server automatically.

For more information about how to suppress events, see the *Nuix Adaptive Security Rule Language Reference Guide*.

Basic filter rules

The Nuix Adaptive Security endpoint agent supports a rule language called Event Filter Language (EFL).

Use this language to write rules to perform various actions in response to events generated by the endpoint agent.

Real-time execution of rules occurs on the endpoint in response to each event generated by the endpoint agent. Each rule specifies values to match against attributes contained in the event data. In addition, the endpoint agent tracks certain state data for each process on the system, which you can reference in rules or use for the setting of user-defined variables at rule run time. This facilitates state tracking across multiple events over time to build more complex rule scenarios.

Note: The *Nuix Adaptive Security Rule Language Reference Guide* provides a more detailed discussion of these and other related topics.

Rule actions

The following table describes the supported rule actions.

Action name	Behavior
Suppress	Suppress writing of this event to the endpoint DBR.
Forward	Forward this event to the Nuix Adaptive Security server.
Alert	Send an alert message to the Nuix Adaptive Security server with this event data.
Block	Block process creation.
Isolate	Enable network isolation on the endpoint.
Set	Set the contents of a user-defined variable in the state engine.
Kill Process	Kill the process associated with this event.

Action name	Behavior
Screenshot (uint32 pid, uint32 interval, uint32 timespan)	Initiate a screenshot task on the endpoint. A screenshot is captured of the desktop for the session containing the process with the process identifier (pid) every (interval) seconds for the next (timespan) seconds.
Memscan (uint32 scanMask, uint32 pid)	Initiate a memory scan task on the endpoint. The scanMask parameter accepts any combination of the following constants: MEMSCAN_INJECTED_MODULES, MEMSCAN_IMAGE_PATCHES. MEMSCAN_INJECTED_MODULES scans only for injected modules, while MEMSCAN_IMAGE_PATCHES scans only for code patches. These can be combined with a bitwise OR to perform both types of scans. The pid parameter can be a specific process ID to scan. It can also specify the constant ALL_PROCESSES, which performs the scan against every active process on the system. Discovery of injected modules during the scan results in the generation of a Memory Scan Injection Event. Discovery of patches during the scan results in the generation of a Memory Scan Patch Event.

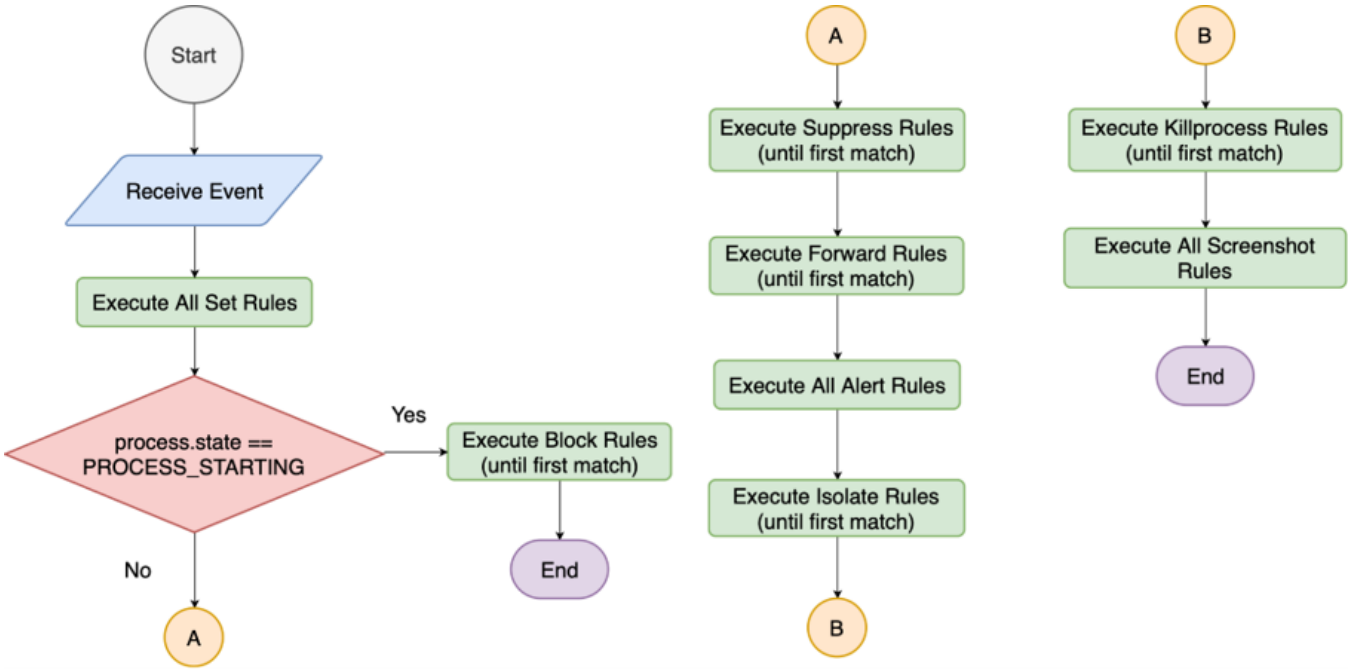
Rule evaluation order

The endpoint agent evaluates filter rules in response to each event generated by the endpoint agent.

The following list is the order of rule evaluation.

1. Any rule that specifies the action of *set* runs.
2. For process creation events, block rules only execute in response to process creation events and evaluate until the first match. If an event occurs, that event prevents process creation, and an alert is sent to the server indicating that the process is blocked from starting. The alert includes information about the process and the rule responsible for blocking the process.

The following diagram depicts the rule evaluation order.



The following table describes the evaluation that occurs for all event types.

Action type	Evaluation
Suppress	Evaluates until the first match. In response to matching a suppression rule, the endpoint declines to write the matching event data to the endpoint DBR.
Forward	Evaluates until the first match. In response to a matching forward rule, the endpoint forwards a copy of that event to the server.
Alert	Evaluates until every alert rule has been evaluated. As a result, multiple alert rules fire for a single event. For each matching alert rule, the endpoint sends an alert message to the server with a copy of the event triggering the match and a copy of the matching rule.
Isolate	Evaluates until the first match. In response to a matching isolate rule, the network isolation firewall rules configured on the endpoint are enabled.
Killprocess	Evaluates until the first match. In response to a matching kill process rule, the associated process terminates. The endpoint never terminates the endpoint agent process in response to a matching rule.
Screenshot	Evaluates until every screenshot rule has been evaluated.
Memscan	Evaluates until every memscan rule has been evaluated.

Forward events

Event data is not sent automatically from the agent to the Nuix Adaptive Security endpoint server. An alert causes the agent to send associated data to send to the server. The forward command also sends data to the server. For example:

```
forward when eventtype.process;
forward when eventtype.session;
forward when eventtype.media;
```

Forwarding all events generates enormous amounts of data, most of which are not useful in typical scenarios. Registry and object events generate high volumes of data that are not useful except in specific use cases.

Actions can cause data to return to the server. For example, the operator can trigger a screenshot on any connected endpoint from the user interface. Rules can trigger screenshots and the Nuix Adaptive Security endpoint server stores the screenshots automatically. It is important to carefully construct rules to avoid triggering many screenshots across the entire endpoint population.

Recording data to the DBR and forwarding data to the Nuix Adaptive Security endpoint server are independent operations. You can suppress events from being stored in the DBR but still forward the events to the server.

Querying the Digital Behavior Recorder

Query and pull event data from the Digital Behavior Recorder (DBR) of an endpoint for a specific date and time to help facilitate an investigation.

In the Nuix Adaptive Security application, right-click on an endpoint or group of endpoints to initiate the action from any insight menu. Right-click an endpoint and select Query DBR to open the dialog box and select the date range and events that you would like the agent to retrieve from the DBR. View the results in the respective event insights and use filtering by date and time to look for specific events.

- **DBR Size**: The amount of event data available in the DBR is a function of the number of events occurring on the endpoint, the number of events being suppressed, and the storage allocated to the DBR. You can allocate storage to the DBR by viewing the endpoint settings and setting the **DBR Size**. The DBR maximum size limit is 1.5 GB and the minimum is 100 MB.
- **DBR Age**: DBR Age tells you how far back the data in an agent's DBR goes. View the **DBR Age** in the Endpoint Insight and the Endpoint detail view in the Endpoint module. The field displays the time and date of the oldest event in the DBR, and the calculated age based on the time and date of that event.

Querying the DBR replaces streaming mode. Streaming mode sends all data stored in the DBR on the agent to the Nuix Adaptive Security server.

Querying the DBR is only available for Windows endpoints.

Test and sample rules

As previously mentioned, improperly considered rules may generate a large amount of data. When an alert triggers, that alert forwards associated data to the Nuix Adaptive Security server. Improperly considered rules can inadvertently cause an extraordinary number of alerts to generate across an enterprise. It is essential that operators test rules on a small subset of systems before deploying across the enterprise.

Examples of scenarios that can cause issues:

- **Network Events**: An improperly written network event rule could trigger an alert for every networking event. Pushed out across an enterprise, this type of rule can lead to hundreds of thousands of alerts and associated data.
- **Endpoint Diversity**: A rule that alerts rarely on one set of endpoints may trigger far more often on a different set of endpoints. For example, a rule watching for use of "cmd" on an endpoint in the finance department may trigger far more often for computers in the engineering department. It is important to test rules on a variety of endpoints before deploying across the enterprise.

Sample rules, included with Nuix Adaptive Security, are meant to serve as examples. Operators should not include every sample rule in a configuration. Operators should consider their objectives and craft rules that best meet their goals. Some parameters of sample rules make it necessary to customize the rules for an individual use case. Test all rules on a small number of endpoints before deploying them across an enterprise.

For detailed information about rules, refer to the *Nuix Adaptive Security Rule Language Reference Guide*.

SIEM-based workflow

Use navigable links to go from your SIEM to the Nuix Adaptive Security application to view artifacts on specific servers.

Use a URI (Uniform Resource Identifier) to open the Nuix Adaptive Security application from the SIEM.

After entering the URI, the Nuix Adaptive Security application will open, and the alert is opened in the Investigate module. If you are not logged in to the Nuix Adaptive Security application, you must sign in and then navigate to the alert or event.

Here is an example of the URI format: `nas://<host>/Investigate/Alerts?id=25`

Where <*host*> is the server's IP address.

Event types

Rules are written around specific events that occur on the endpoint. This section is about the event types. See the *Nuix Adaptive Security Rule Language Reference Guide* for details of the event attributes available for use in rules.

Clipboard paste event (Windows Only)

Clipboard paste events are generated in response to the pasting of data from the clipboard.

Event type (Windows, macOS)

These attributes exist to allow an entire event class to be specified at once. These are appropriate for use in suppress rules to suppress the writing of an entire class of events to the DVR or for use in forwarding rules to forward an entire class of events to the server.

File events (Windows, macOS, and Linux)

File events are generated when a file is closed and had content written to it, was renamed, was deleted on the endpoint, or if a volume was mounted.

Image load event (Windows, macOS, and Linux)

Image load events are generated when an executable image is loaded on the endpoint. This includes the loading of executable images and dynamic link libraries, which takes place when a new process is started. It also includes the loading of dynamic link libraries, which can occur after a process has started through the use of the Win32 LoadLibrary/LoadLibraryEx APIs or the macOS/Linux dlopen API.

Keystroke event (Windows Only)

Keystroke events are generated in response to keystrokes entered on the endpoint machine, but not for each keystroke entered. Instead, keystrokes are collected into a buffer, and then keystroke events are generated at specific tear points, which include when the following occurs:

- The user presses the enter/return key.
- The user presses a control sequence that includes any of the following keys: ALT, CTRL, WIN, F1-F24, ESCAPE, PRINT SCREEN.
- The user shifts focus to another window and enters a keystroke in that window.
- The keystroke log buffer has reached its *maximum buffered keys* limit.
- The timeout keystroke buffer *periodic flush timer* has elapsed.

Media event (Windows, macOS, and Linux)

Media events are generated in response to the insertion or removal of removable media, which includes USB thumb drives as well as external hard drives connected by USB or Firewire.

Memory scan injection event (Windows Only)

Memory scan injection events are generated in response to instances of covertly injected portable executable (PE) modules discovered when executing the memscan rule action on the endpoint.

Memory scan patch event (Windows Only)

Memory scan patch events are generated in response to instances of code patches discovered when executing the memscan rule action on the endpoint.

Microsoft Defender event (Windows Only)

The endpoint agent interacts with Microsoft Defender to identify active threats on the endpoint. When the endpoint agent starts, the endpoint agent polls Microsoft Defender for active threats. After startup, the endpoint agent periodically polls (using a 30-second interval) Microsoft Defender to identify subsequent threats. For each threat reported by Microsoft Defender, the endpoint agent generates an event and sends the event to the filter engine for processing.

Namespace event (Windows Only)

Namespace events are generated in response to Domain Name System queries generated on the endpoint.

Network event (Windows, macOS, and Linux)

Network events are generated when a network connection is established or terminated. Events are also generated periodically during the lifetime of a connection to provide updated statistics on the amount of data transferred to date. Finally, events are generated for certain socket state events of interest such as entering the listening state.

Object event (Windows Only)

Object events are generated when a process handle is created. This activity correlates to the use of functions, for example, the Win32 OpenProcess function that allows a process to open a handle to another process with varying degrees of permission. Object events are interesting because they can indicate attempts by a process to open a handle to other processes for the purpose of reading or writing that other process's address space.

Print event (Windows Only)

Print events are generated in response to the completion of a print job and are generated only for print jobs sent through print queues defined on the system where the agent is running.

Process event (Windows, macOS, and Linux)

Process events are generated in response to processes starting and processes terminating. Also, when the endpoint agent starts up it enumerates all existing processes on the system and generates events.

Registry event (Windows Only)

Registry events are generated in response to creating new registry keys, renaming existing registry keys, and setting values under registry keys.

Removable media event (Windows, macOS, and Linux)

Removable media events are generated in response to the insertion or removal of removable media, which includes USB thumb drives as well as external hard drives connected by USB or Firewire.

Session event (Windows, macOS, and Linux)

Session Events are generated in response to logins such as console logins and RDP logins on Windows, and terminal logins and SSH sessions on macOS.

URL event (Windows, macOS, and Linux)

URL events are generated when a user clicks a link or enters a URL into the browser's address bar when using the Edge, Chrome, Firefox, and Vivaldi web browsers. URL events effectively mirror the entries recorded in the browser's history file. If a user enters a URL that does not resolve, it will not appear in the URL events.

Feature functionality by operating system

The following tables describes the feature functionality and the check boxes indicate whether each feature is supported by the Windows, Mac, and Linux operating systems.

Basic functionalities

Feature	Windows	Mac	Linux
Installation of Endpoint Agent	✓	✓	✓
Deployment Package Generation (server export zip file)	✓	✓	✓
Encrypted Communication	✓	✓	✓

Configuration options

Feature	Windows	Mac	Linux
General Installation Settings	✓	✓	✓
Server Configurations	✓	✓	✓
Logic Rule Sets	✓	✓	✓
Hash lists and Hash list mode	✓	✓	✓
Agent Name Obfuscation	✓	×	×
Isolation Rules	✓	×	×
Keystroke Capture Configuration	✓	×	×

Endpoint details and survey

Feature	Windows	Mac	Linux
Endpoint Details	✓	✓	✓
Endpoint Surveys	✓	✓	✓
Task Assignment	✓	✓	✓
Comm Sessions	✓	✓	✓
File System Browser	✓	✓	✓
Microsoft Defender	✓	×	×

Logic engine capabilities

Feature	Windows	Mac	Linux
Alerts	✓	✓	✓
Suppress	✓	✓	✓
Forward	✓	✓	✓
Set	✓	✓	✓
Namespace Filtering	✓	×	×
Isolate	✓	×	×
Kill Process	✓	✓	✓
Block a Process	✓	✓	✓
Whitelisting	✓	✓	✓
Rules Annotation	✓	✓	✓
Triggering Screenshots	✓	✓	✓

Actions

Feature	Windows	Mac	Linux
Survey	✓	✓	✓
Configuration Assignment	✓	✓	✓
Group Assignment	✓	✓	✓
Network Isolation	✓	×	×
Execute Command	✓	✓	✓
Upload and Execute	✓	✓	✓
File and Folder Acquisition	✓	✓	✓
Screenshot	✓	✓	✓
Upgrade	✓	✓	✓
Uninstall	✓	✓	✓

Real-time monitoring events

Feature	Windows	Mac	Linux
Process Execution	✓	✓	✓
File Writes and Deletes	✓	✓	✓ (Except RH7)
Sessions	✓	✓	✓
Removable Media	✓	✓	✓
Network Activity	✓	✓	✓
DNS Lookup	✓	×	×
Print Activity	✓	×	×
Agent Shutdowns	✓	✓	✓
Shared Library Load	✓	✓	✓
Key Logging	✓	×	×
URL Events	✓	✓	✓
Registry	✓	×	×
Copy and Paste Monitoring (Clipboard)	✓	×	×
Windows Event Logs	✓	×	×
Content Inspection	✓	×	×
Memory Injection	✓	×	×
Memory Patch Scan	✓	×	×

Content and logic rules

Feature	Windows	Mac	Linux
Mitre Attack Behaviors	✓	✓	✓
Insider Threat Behaviors	✓	✓	✓

File collection

Feature	Windows	Mac	Linux
Collect to to File Share	✓	×	×

Feature	Windows	Mac	Linux
Collect to Amazon S3	✓	✓	✓
Collect to Local	✓	✓	✓
Collect to Nuix Adaptive Server	✓	✓	✓

Feature limitations for Windows 7 and 8

Some agent features in Nuix Adaptive Security 2.12 and later may be limited on Windows 7 and 8 due to the inability to get drivers signed by Microsoft for these operating systems.

The following improvements are supported for Windows 10 and later but are not available for Windows 7 and 8.

Feature	Windows 10 or later	Windows 7 and 8

• Object event generation changes
  ○ Open process event
  ○ Remote thread creation event
	Supported	On Windows 7 and 8, the rules that reference these types of events will never be triggered. The rules are compatible with the rules engine and do not need to be changed.

• More accurate user SID population	Supported	Windows 7 and 8 systems will not have the improved user SID reporting, so some expected SIDs will not match.
• Information about process elevation status	Supported	Process elevation information will not be present on Windows 7 and 8. Rules looking for a specific value for elevation status will not match. The rules are compatible with the rules engine and do not need to be changed.
• File open event support	Supported	On Windows 7 and 8, rules that reference the FILE_OPEN type of file event will never be triggered. Rules that reference this value are still compatible with agents running on Windows 7 or 8 and the rules do not need to be changed.