Nuix Adaptive Security

Nuix Adaptive Security 2.16.0

Administration Guide

December 2022

nuix

Version 2

Contents

Introduction

Welcome to the Nuix Adaptive Security Web-Based Administration 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 an impending or ongoing attack, accelerates recovery time, easily adapts to changing environments, regulations, and attack vectors, and ultimately, stops incidents in their tracks.

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 discussed in greater detail in other documents. These include:

- *Nuix Adaptive Security Installation Guide, Version 2.16.0*
- *Nuix Adaptive Security Quick Start Guide, Version 2.16.0*
- *Nuix Adaptive Security Release Notes, Version 2.16.0*
- *Nuix Adaptive Security User Guide, Version 2.16.0*
- *Nuix Adaptive Security Engine Rule Reference Guide, Version 2.16.0*

Nuix Adaptive Security architecture overview

The Nuix Adaptive Security architecture consists of five main components:

- Endpoint server
- Endpoint agent
- Application UI
- API server + SDK
- MySQL database

The Endpoint server communicates with the agent and sends the agent tasks. The Endpoint agent is deployed to endpoints to collect data, perform actions, process rules, and send data back to the Endpoint server. The database can be located on the server or another system or part of a performance cluster database.

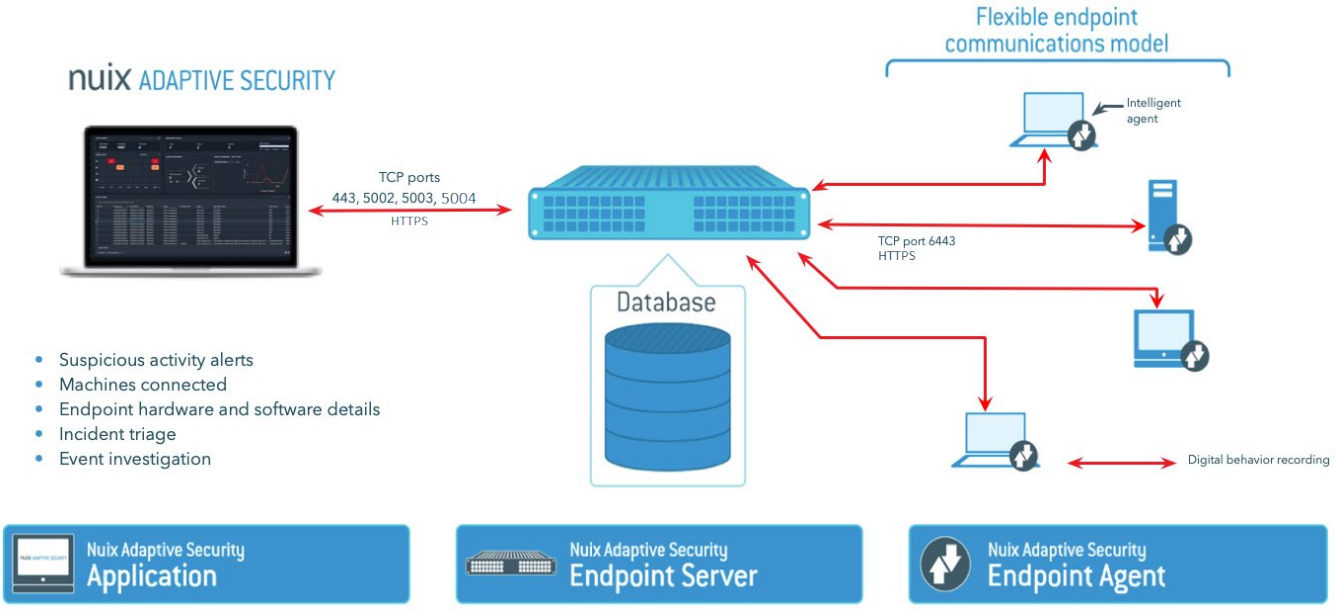
The Nuix Adaptive Security Application is used to view data, manage investigations, and communicate with the server using the API. The application queries the database for the information through the API. The application sends tasks to the database through the API and then the Endpoint server communicates directly with the agent to perform the action.

The database stores the agent information that is collected from endpoints.

The web console is a web-based interface accessed by using the server IP address to perform administration tasks.

Communication channels

The Application UI and API server communicate using the SDK. The API Server and Endpoint server communicate through the MySQL database. The Endpoint server uses protocol buffers to communicate with the Endpoint agents. The typical TCP ports used are 443, 5002, 5003, and 5004, however, the ports are configurable. The communication channels are FIPS compliant.



Access the web-based interface

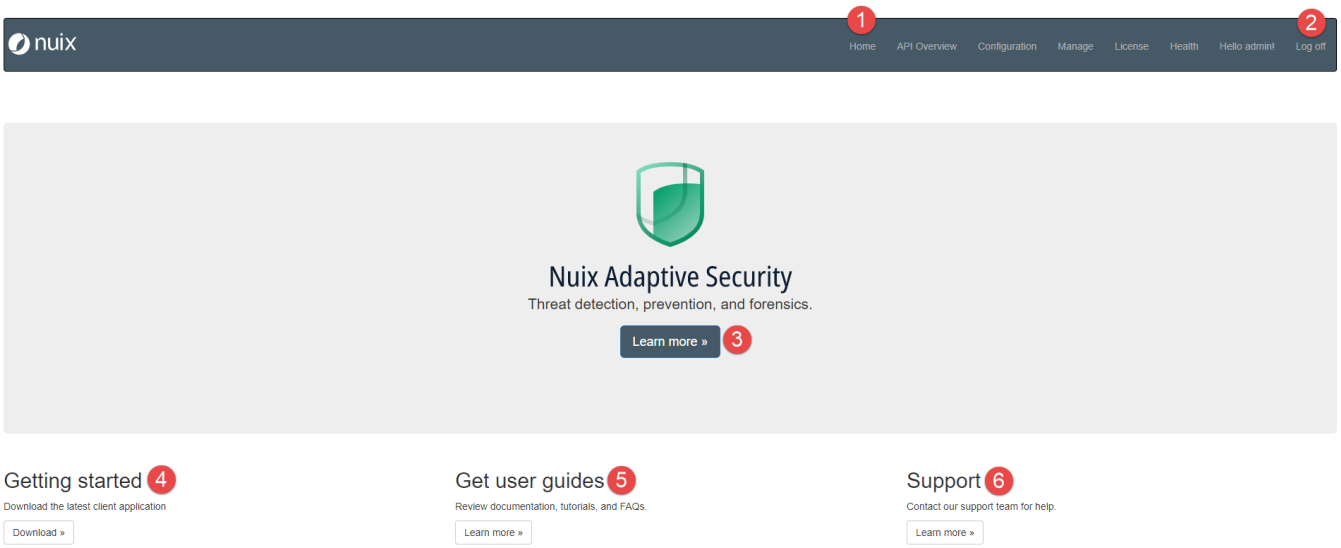
You can access the web-based interface by using its IP address.

To access the web-based interface through the Internet.

1. Open an Internet browser.
2. Enter the IP address of your Nuix Adaptive Security Endpoint Server in the address bar.

Nuix Adaptive Security home page

After you access the web-based interface, the Nuix Adaptive Security home page appears, as shown in the following image.



The functions described in the following table are available on this page:

Number	Function	Description
1	Home	Click **Home** at any point to return to this window.
2	Log in	Click **Log in**, and then enter your user name and password to access the web administration.
3	Learn more	Click **Learn more** to show a page on the Nuix website that provides information about Nuix Adaptive Security.
4	Getting started	Click **Download** to get the latest client application installer. It is displayed as a download at the bottom of your browser.
5	Get more information	Click **Learn more** to open the Nuix Customer Portal where you can access installers and documentation.
6	Support	Click **Learn more** to go to the Nuix Customer Support Portal page. Log in to the page by entering an email address and password. Follow the procedure for entering a ticket.

Log in

To log in to the web-based interface:

1. Enter the IP address for your instance Nuix Adaptive Security in your browser's address bar.
2. On the main navigation bar, click **Login**. The **Login** page appears.
3. Enter the user name provided by your administrator in the **Username** box.
4. Enter the password provided by your administrator in the **Password** box.
5. Once you have entered your credentials, click **Login**.

If you log in and don't see the menu at the top of the page, you may need to add Nuix Adaptive Security as a trusted site.

Configuration

Click **Configuration** to display a menu with the following options:

- Auditing
- Data Retention Policy
- Federated Authentication
- Kafka
- Public IP

Auditing

In the web UI, configure system auditing in **Configuration > Auditing**. The audit configuration is available to administrators or operator roles. Use the audit configuration in the following ways:

- Record user actions on the system.
- Forward user activity to an external system.
- Track changes and view audit logs to ensure no unauthorized changes were made to endpoints in your environment.

Data Retention Policy

The Data Retention Policy is the protocol used for retaining data in your company's Nuix Adaptive Security instance.

In this window, you can make changes to the existing policy.

The following settings are available in this window:

- **Enabled**: Select the check box to enable this setting. If the check box is not selected, the setting is disabled.
- **Number of days of data retention**: Number of days that data is retained. For example, if 10 is set here, then the last 10 days of data are kept.

Click **Save** to commit the changes or **Cancel** to discard the changes.

Federated authentication

Nuix Adaptive Security supports SSO authentication using Microsoft Azure Active Directory. This allows administrators to manage access, define group memberships and roles, enhance security, and monitor user activity.

For more information, see the *Nuix Adaptive Security Installation Guide*.

Kafka forwarding

Kafka is an open-source stream-processing software platform. Nuix Adaptive Security Kafka forwarding is compatible with Nuix Workstation.

If the Kafka option is clicked, a window with the following options appears:

- **Enable forwarding selected data to Kafka**: Select this option to allow Nuix Adaptive Security to forward selected event data to Kafka.
- **Enable Event Storage**: Select this option to store specific selected events to another storage system instead of the local database.
- **Bootstrap Servers (comma delimited)**: List of the servers (and the port) being used by Kafka. If more than one server is being used, the servers are separated by commas.

- **Message send timeout in milliseconds**: Amount of time before a message will stop sending and be considered timed out. This is set to 3000 milliseconds (3 seconds) by default.
- **Number of send retries**: Amount of times Kafka attempts to send a message if it is unsuccessful in getting through during its initial send.
- **Heartbeat interval in minutes**: The heartbeat status is used to detect failures. Set a heartbeat interval in minutes. The default heartbeat is five-minute intervals. A Kafka alert error appears if the heartbeat fails.

Splunk forwarding

Nuix Adaptive Security supports Splunk forwarding by using the API to send alerts and events directly to Splunk. Enable Splunk forwarding in the Nuix Adaptive Security web UI under **Configuration**>**Kafka and Splunk Configuration**.

To set up Splunk forwarding, add a Splunk token and a hostname or IP address. The rest of the configuration settings are under General and are shared with Kafka forwarding.

Create an index in Splunk for every view that you are intending to forward to Splunk. The indexes are the topic base name and the view that is forwarded. See the following index list with the default base name of nuix_adaptive:

- nuix_adaptive_alerts
- nuix_adaptive_clipboard
- nuix_adaptive_file
- nuix_adaptive_keylog
- nuix_adaptive_media
- nuix_adaptive_print
- nuix_adaptive_process
- nuix_adaptive_session
- nuix_adaptive_screenshot
- nuix_adaptive_url

For more information on how to configure Splunk for Nuix Adaptive Security, see **Configure Splunk** in the *Nuix Adaptive Security Installation Guide*.

Kafka and Splunk configuration general settings

The following settings are the general configuration settings for Kafka and Splunk forwarding.

- **Send all events to a single topic:** Select this option to send all events to the same topic when more than one is selected for forwarding.
- **Topic base name**: Name of the category where the records that Kafka is collecting are held.
- **Event polling interval in milliseconds**: Period of time between polling by Kafka. This is set to 30000 milliseconds (30 seconds) by default.
- **The list of views to forward**: Select options from the list of database views. The views include Alerts, Removable Media, File, Session, Print, Process, Keylog, Screenshot, URL, and Clipboard. You can choose multiple views.
- **Alert categories to exclude when forwarding**: Enter the alert category name to be excluded when forwarding to Kafka. Categories must be separated by commas.
- **Don’t forward events earlier than**: Select the date and time stamp to start forwarding events.
- **Force Adaptive to resend all events**: Select this option to resend all event data from Nuix Adaptive Security.

Once these values have been entered, click **Submit** to set up the configuration.

Public IP

In the web UI, you can change the Nuix Adaptive Security endpoint server's public IP address in **Configuration > Public IP**. A reboot is required to activate the new IP address.

Use the following procedure when changing the IP address.

In the web UI, change the IP address.

In the network settings, change the IP address.

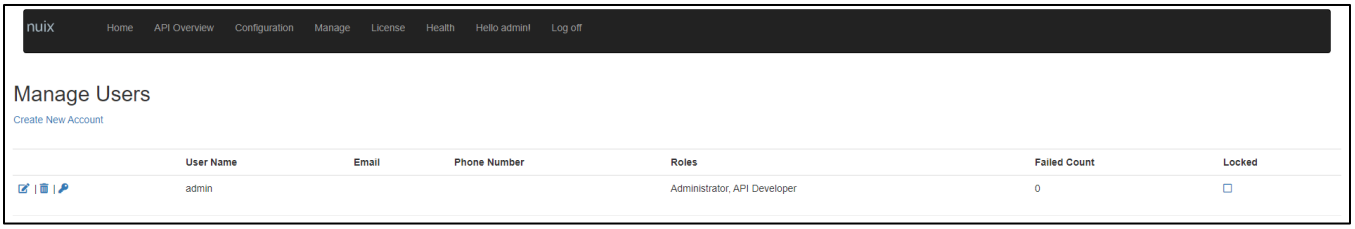
Reboot the Nuix Adaptive Security endpoint server.

Manage

This section provides information about managing users and agents.

User

Click **User** in the **Manage** menu and the following window appears.



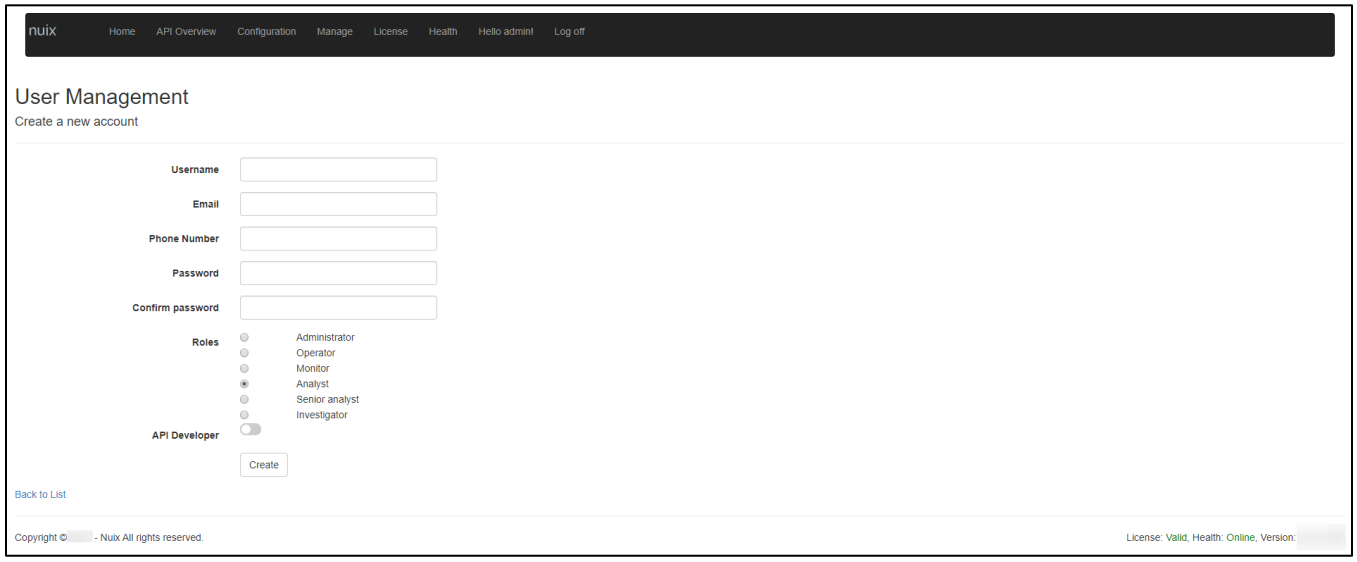
This window lists the created users and includes their user name, email, phone number, roles, and failed login count. If the check box is selected in the **Locked** column, the user is locked. Clear this check box to unlock the user.

The following actions are available for each user. Perform an action using one of the buttons, as described in the following table.

Button	Function
	**Edit**: Shows the **Edit** window for the individual user. Make changes to the User Name, Email, Phone Number, and Roles here. Select the check box to enable a role or clear the check box to disable the role. Once all changes are made, click **Save**.
	**Delete**: Remove the user. A window is displayed asking if the user should be removed. Click **Delete** to perform the action.
	**Reset**: Reset the user's password. Enter a new password in the first box and reenter it in the second to confirm it. Once this is done, click **Reset Password** to complete the action.

To create a new user:

1. On the **Manage Users** page, click **Create New Account**. The following page appears.



2. Enter values for the following settings:
    a. **Username**: Enter a name for the user.
    b. **Email**: Enter the user's email.
    c. **Phone Number**: Enter the user's phone number
    d. **Password:** Enter the user's password.
    e. **Confirm password**: Reenter the user's password to verify the password.
3. **Roles**: Select the check box next to the role to add it to the user's permissions. The roles are explained in more detail in the next section
4. **API Developer**: Move the slider to the right if the user is an API developer.
5. Once the values on this page have been entered, click **Create** to generate the user.

If you are using this page to make changes to a user, **Save** appears instead of **Create**.

To return to the user list, click **Back to List** at the bottom of this window.

Role-Based Access Control

Role-Based Access Control (RBAC) restricts access to Nuix Adaptive Security based on the following roles.

- **Administrator**: The administrator role has access to all capabilities in the Nuix Adaptive Security application. The only role allowed to create other users with similar access controls.
- **Investigator**: The investigator role has the permissions of a senior analyst but can also launch tasks that may impact the operation of an endpoint. Investigators cannot create their own rules.
- **Senior Analyst**: The senior analyst role has the permissions of an analyst but can also perform read-only query actions to pull specific data.
- **Analyst:** The analyst role has access to view and manipulate data collected by the endpoint agents. Users in this role have restricted access to the endpoint agents. The analyst can view additional task data as requested by senior analysts or investigators.
- **Operator**: The operator role has access to endpoints, configuration, user information, and preferences. Users in this role are not able to access behavioral data streamed from the endpoints or perform any non-management or diagnostic-related actions.
- **Monitor**: The monitor role has access to high-level summary information about Nuix Adaptive Security, such as the dashboard. The monitor role cannot pivot or navigate from the dashboards.

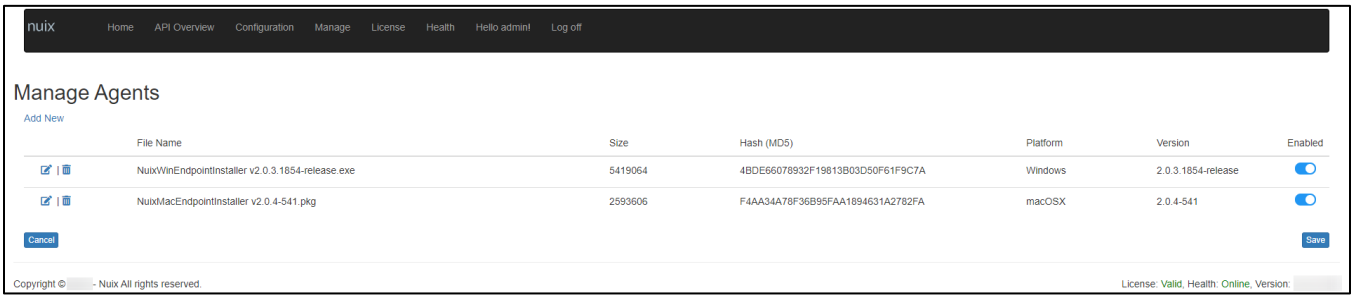
The following table lists what the user can view and the actions they can take in the application for each role.

View	Administrator	Investigator	Senior analyst	Analyst	Operator	Monitor
Dashboard	✓	✓	✓	✓	✗	✓
Alerts	✓	✓	✓	✓	✗	✗
Enterprise Search	✓	✓	✓	✗	✗	✗
Investigations	✓	✓	✓	✓	✗	✗
Endpoints	✓	✓	✓	✓	✓	✗
Tasks	✓	✓	✓	✓	✗	✗
Configuration	✓	✗	✗	✗	✓	✗
User Information	✓	✓	✓	✓	✓	✓
Preferences	✓	✓	✓	✓	✓	✓
Action	**Administrator**	**Investigator**	**Senior analyst**	**Analyst**	**Operator**	**Monitor**
Default	✓	✓	✗	✗	✗	✗
Survey	✓	✓	✓	✓	✓	✗
Upgrade, Uninstall, Assign and Manage Agent settings	✓	✗	✗	✗	✓	✗
New and Assign Groups	✓	✓	✓	✓	✓	✗
Query Microsoft Defender Status and Update Signatures	✓	✓	✓	✓	✓	✗
Open Endpoints	✓	✓	✓	✓	✓	✗

*Default includes all actions except those that are specifically listed in the actions column.

Agents

Click **Agents** on the **Manage** menu to display the **Manage Agents** page, shown in the following image. You may want to use the Manage Agents page when a new agent is available for an existing Nuix Adaptive Security system or you have an agent installer that you wish to upload to the system. You can also delete, enable, and disable agents on this page.



The following settings are displayed on this tab:

- **File Name**: The name of the installer file.
- **Size**: The size of the file (in megabytes).
- **Hash (MD5)**: The hash for the agent.
- **Platform**: The software platform where the agent is installed (Windows, Mac, or Linux).
- **Version**: The Nuix Adaptive Security agent version.
- **Enabled**: Whether the agent is enabled or disabled.

The following actions are available for each agent, as described in the following table.

Action	Function
	**Edit**: This shows the **Edit** window for the individual agent. The agent can be enabled here. Changes can also be made to the File Name, Platform, and the name of the Version. The **Size** and the **Hash (MD5)** settings appear in this window but cannot be edited. To keep changes made in this window, click **Save**. To discard the changes, click **Cancel**.
	**Delete**: Remove the agent. To confirm that the agent can be removed, click **OK** in the box that appears.

Once all the necessary changes are made on this window, click **Save**. To discard the changes, click **Cancel**.

Upload an agent

This section describes how to update an installed release with a new agent. If a new agent is available for an existing Nuix Adaptive Security system, it must be uploaded to the server before it can be deployed for use in the installed base.

To install a new agent into the system:

1. Open the Nuix Adaptive Security web-based administration user interface and log in with an administrator account.
2. Click on the **Manage** menu item at the top and choose Agents.
3. Select **Add New** in the upper left. You will see the following **Add Agent** option.
4. Move the **Enabled** slider to the right to enable the agent.
5. Select the platform.
6. Enter the version name for the agent.

Note: The version nomenclature is Major/Minor/Revision/Build. You must type in the proper version to include at least the revision or the system will reject the upload. For the example below, the version needs to be at least 2.6.1 but it is best to provide the entire version – in this case, 2.6.1.2007.

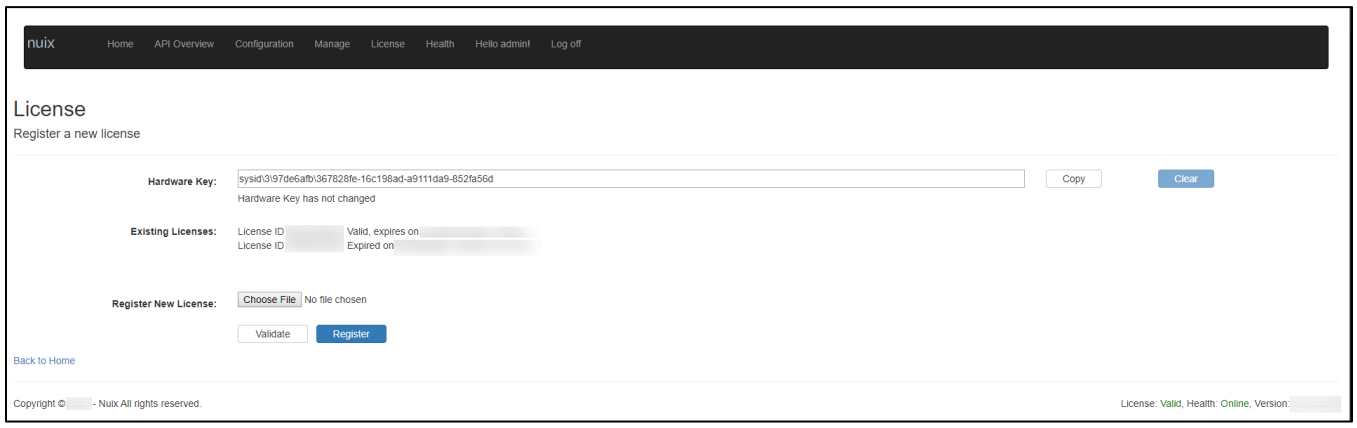
7. Click the **Choose File** button and select the agent executable you wish to add to the system.
8. Select to **Save** the agent executable file.

Once the new agent is in place you can disable the older agent, so it does not appear in the application UI. Alternatively, you can delete the old agent entirely from the system.

The new agent is now available in the application UI and can be used to upgrade existing deployed agents with an existing or newly created configuration. The agent can also be exported with an embedded configuration for deployment via enterprise management tools.

License

This page is where licenses are maintained for Nuix Adaptive Security.



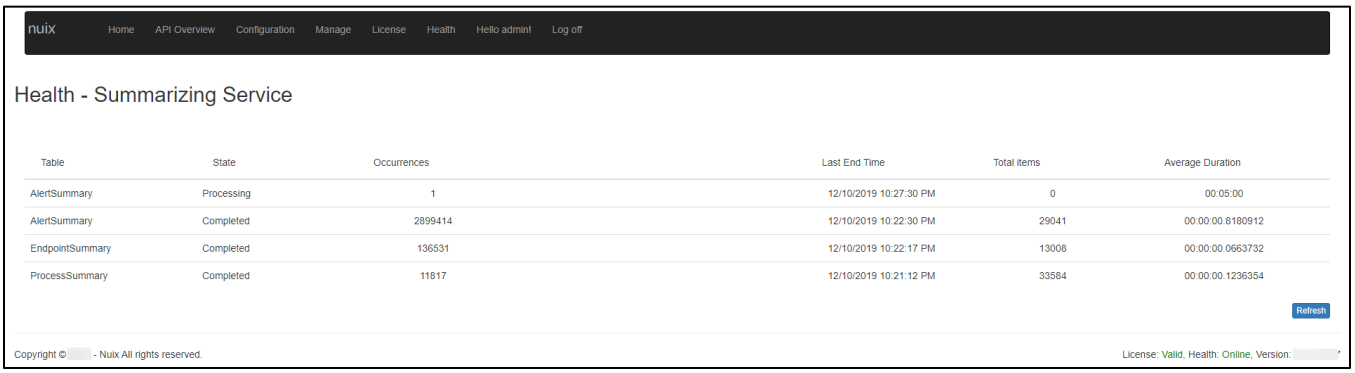
- **Hardware Key**: Key generated when the Nuix Adaptive Security license is created or renewed. Click the **Copy** button to copy your hardware key. To create or renew a license, go to the Nuix Portal, enter your credentials, and click **License.** For any license-related questions, contact Nuix Support at https://nuix.service-now.com/support or your Nuix sales representative.
- **Existing Licenses**: Any licenses related to your instance of Nuix Adaptive Security are listed here, whether the licenses are valid or expired.
- **Register New License**: Click **Choose File** to find the Installer file created for the Agent. The name of the file is displayed once the file is selected. Click **Validate** to test if this is a valid license. Click **Register** to register the selected file.

Health

The section provides information about the services available in the Health tab.

Summarizing Service

On the navigation bar on the **Home** page, click **Health**. On the menu, select **Summarizing Service**. The **Health - Summarizing Service** page appears, as shown in the following image.



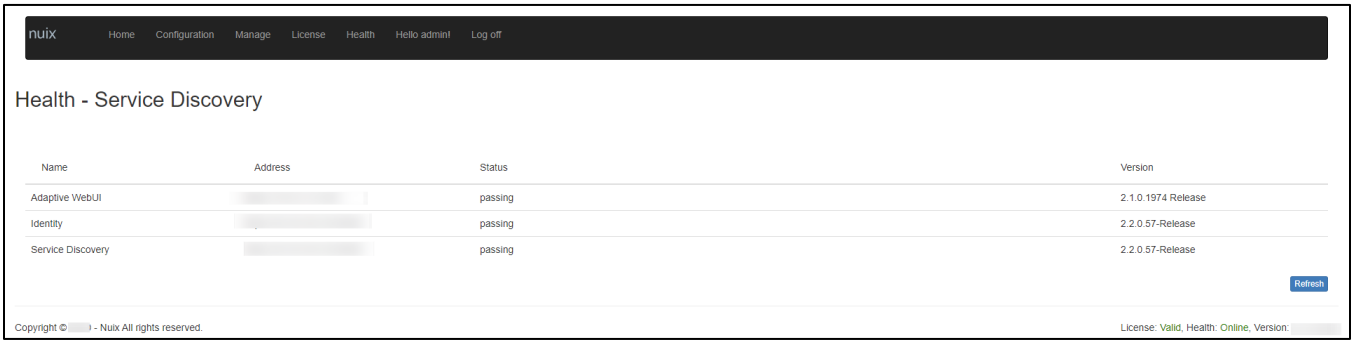
The following columns are displayed on this page:

- **Table**: Name of the summary table in Nuix Adaptive Security.
- **State:** State of the data update for the table listed.
- **Occurrence**: Number of times the table has been updated.
- **Last End Times:** Time the last update of the table finished.
- **Total Items:** Number of items in the table.
- **Average Duration**: Average length of time it takes to update the table.

Click **Refresh** to update the data on this page.

Service Discovery

On the navigation bar on the **Home** page, click **Health**. On the menu, select **Service Discovery**. The **Health - Service Discovery** page appears, as shown in the following image.



The following columns are displayed on this page:

- **Name**: Name of the service.
- **Address:** IP address of the service.

Note: When you change the IP address, you will continue to see the previous IP address and the new IP address if they are both still valid. If the IP address becomes invalid, it will disappear from the Service Discovery page.

- **Status**: Status of the service's connection to the Nuix Adaptive Security Server to send and receive data. The status can be any of the following:

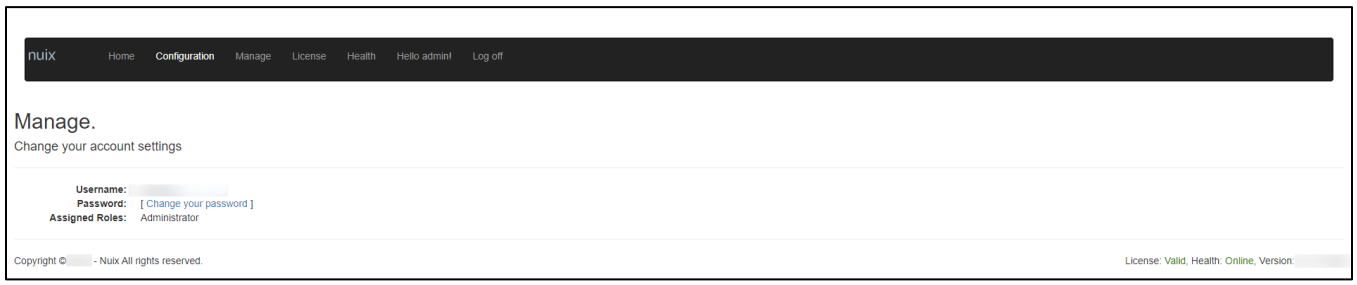
  Passing: The services are functioning properly.
  Known: There is an unknown error, and performance may be degraded as a result.
  Warning: There are multiple instances of the same service running and one or more has a critical error. The service will still be available, but performance will be degraded.
  Maintenance: There is an upgrade in progress.
  Critical: An error exists. As a result, the feature will not work.

- **Version:** Version of Nuix Adaptive Security.

Click **Refresh** to update the data on this page.

Change account password

In this window, you can change your account password, as shown in the following image.



To change the password for your account:

1. Click **Hello (Username)** on the main navigation bar of the home page to display the Manage window
2. Click the Change your password link.
3. In the window that appears, enter the current password for your account.
4. Enter a new password in the second box and confirm the password in the third box.
5. Click **Change Password**.

Your user name is listed above your password, and your assigned roles are listed underneath your password.

Log off

Click **Log off** to exit the web-based Nuix Adaptive Security Interface.

API documentation

Users with API access can view the API documentation from the **API Overview** link in the web UI. Using the REST API documentation, you can query endpoint-related data, update endpoint and configuration settings, and submit task-related operations. Contact Nuix Adaptive Security technical support or your Nuix sales representative for more information.

Server management

This section provides an overview of managing your servers. This section will discuss the following topics:

- Data Retention
- Backing up Data
- Operating System Updates
- Backing Up Agent Certificates
- Log Files Locations

For more information about server backup and recovery information, see https://dev.mysql.com/doc/refman/8.0/en/backup-and-recovery.html.

Data retention

The server will save data based on your data retention settings. Data retention settings will depend on your company standards. Data retention settings will also vary based on whether you are doing an investigation. Typically, most companies will keep data for two to three months maximum. You will also want to consider the amount of data being collected by the rules, the amount of data being stored, and the size of the server(s).

The Nuix Adaptive Security server data retention feature will drop data for the event and summary tables based on the time settings. For example, if you have 60 days of data and you set a 30-day data retention then the files that are 30 days or older are deleted.

The partition data is dropped by date, so it will start dropping partitions that are 30 days old and every day after that. The number of days is configurable.

The more data you store the more disk space and memory it uses and it also slows down the application. There is a balance between the needs of the company regarding how long they need the data and how much disk space they have available.

Monitor the server and if it starts to deteriorate you may want to consider moving to a bigger server or deleting more data.

Backup data

The database is locked during backup. For best results, do a backup from a secondary server, especially if you are running backups daily or weekly. You may want to consider a backup strategy and interval.

If there is a server outage, the agents will collect data locally until they run out of space. Eventually, the agent space will fill up but it depends on the rules and amount of data that is stored.

Once the server is available, the agents will send data as fast as they can to catch up. This may take some time depending on the amount of data.

Generally, each enterprise should refer to their company's requirements for how often their systems are backed up.

Backup the server database from MySQL workbench

You may need to have a secondary database that you use for backups and you may need to ensure that the entire server is backed up at one time.

See the MySQL site for more information on backups, https://dev.mysql.com/doc/refman/8.0/en/backup-and-recovery.html. You may also want to refer to your enterprise backup solution.

Single backup

To perform a single server backup in MySQL Workbench:

Note: Do not use the single server backup procedure as a regular weekly or daily backup on a busy system because the system is locked during the backup process.

1. In MySQL Workbench on the Administration tab, under **Management**, click **Data Export**.
2. Select all schemas except **sys**.
3. Click **Advanced Options** and check the box for "**hex-blob**".
4. Ensure the menu says "Dump structure and data."
5. Under **Objects**, check the following boxes:

   Dump stored procedures and functions
   Dump events
   Dump triggers

6. Select the Export to self-contained file check box.

7. Select the Create dump in a single transaction check box.
8. Select the Include Create Schema check box.

Operating system updates

Refer to your organization's policy when updating your operating system. Consider keeping your Windows operating systems current with the latest Windows updates.

Backup agent certificates

There are two sets of certificates that you will need for the server to communicate with the agents, the agent certificate set and the API/Application certificate set. You need two sets of certificates for the server to communicate with the agents.

The agent certificate set is used to allow the agent to communicate to Nuix Adaptive Security. This is important because if the certificates are lost, the agents are orphaned, and you will have to redeploy the agents.

You can find the agent certificates here:

```
C:\Program Files\Nuix Adaptive Security\Endpoint Server\Data
```

Save the following files:

- ca.key
- ca.cert.pem,
- server.cert.pem
- server.key.pem
- dhparam4096.pem.
- Endpoint Server log files – These are helpful for troubleshooting.

You must copy and paste this folder and store it in a safe place that is backed up regularly.

Backup the configuration file in case it has been customized in any way. This is the config.txt file that is in the same directory as the files above.

The API/Application certificate is used to run the Nuix Adaptive Security API and application. This certificate is not as critical, however, you may see some pop-up notifications in your web browser if it expires or is not available.

You can find the API/Application certificate here:

```
C:\ProgramData\Nuix\Endpoint\Data\Certificates
```

Log files locations

This section describes the server log file locations for Nuix Adaptive Security. There are two main log file locations: the system running the Nuix Adaptive Security Endpoint Server and the system running the Nuix Adaptive Security Application.

To view the latest NUIX EPS, Database Error, and Database Query files:

For a new install, you can find the files here:

```
C:\Program Files\Nuix\Adaptive Security\Endpoint Server\Data\Logs
```

If your system was upgraded from a previous version, the files are located here:

```
C:\Program Files\Nuix Adaptive Security Endpoint Server\Data\Logs
```

This log location is where the Nuix Adaptive Security Endpoint Server logs the interactions with the endpoints and the database.

To view the MySQL log activities, errors, and slow queries:

```
C:\ProgramData\MySQL\MySQL Server 5.7\Data
```

Or

```
C:\ProgramData\MySQL\MySQL Server 8.0\Data
```

To view the Internet Information Services (IIS) log events:

```
C:\inetpub\logs\LogFiles\W3SVC1
```

To view the Web.config file:

```
C:\inetpub\Adaptive\Web.config
```

In the Web.config you can change the maximum number of events that are displayed in some of the grids.

For example, you can increase the number of process events that are viewed at one time in a process grid from 10,000 to 20,000 by changing the value after "ViewLimitProcessEvent" to 20,000.

To view the installer logging:

```
C:\Programdata\Nuix\AdaptiveSecurity/InstallerLog
```

To view the application logs on the system where the application is installed:

```
C:\ProgramData\Nuix\Adaptive Security\Logs
```

You can also find application log data in the database diagnostic table.

To view the Web API logs:

```
C:\ProgramData\Nuix\Adaptive Security\Logs\WebApi
```

You can also view them here:

```
C:\inetpub\logs\LogFiles
```

To view the configuration files for the application:

```
%user%AppData\Local\Temp\Nuix
```

If the application is not responding as expected, you may delete these files and the application will recreate them when it starts.

Use the Windows Event Viewer to see entries in the event log when a service starts or stops.

To view certificates, audit configuration, and consul data store:

```
c:\programdata\nuix\endpoint\data
```


Nuix Adaptive Security endpoint agent management

This section describes the administrative agent management tasks and information.

The agent stores data in the Digital Behavior Recorder (DBR) on disk and collects events and survey information. The Endpoint agent is deployed to endpoints to collect data, perform actions, process rules, and send data back to the Endpoint server.

Uninstall agents

This section describes how to uninstall the agent for Windows, Mac, and Linux operating systems.

Uninstall the windows agent

Uninstalling the Windows agent will delete all files. Use the following command to manually uninstall the agent:

-u <*Name_of_Installer*>

Uninstall the Mac agent

Uninstalling the Mac agent will delete all files. Use the following command to manually uninstall the agent (and KEXT):

```
sudo /Library/Nuix/Endpoint/uninstaller.sh
```

Uninstall the Linux agent

Uninstalling the Linux agent will delete all files. Use the following command to manually uninstall the agent:

```
sudo /opt/nuix/endpoint/uninstaller.sh
```

Agent file locations

This section describes the agent file locations for Windows, Mac, and Linux operating systems.

Windows agent file locations

The installer puts the agent file in the following directories:

Install Directory

```
%ProgramFiles%NuixAdaptiveSecurity\
```

Data Directory

```
%ProgramFiles%NuixAdaptiveSecurity\Data
```

Mac agent file locations

The installer puts the agent file in the following directories:

`/Library/Nuix/Endpoint`

This file location contains the agent executable ("NuixAS"), data files, uninstaller, and the kernel extension ("NuixASDriver.kext").

`/Library/LaunchDaemons`

On a macOS machine, services such as the agent are controlled by a system daemon named “launchd.” This system daemon starts the services as a system startup using the property list file, which the installer places in the following location: `/Library/LaunchDaemons`. This system monitors the agent and restarts it in the event of a crash.

To test launchd, terminate the agent process by entering one of the following in the command line:

```
sudo pkill NuixAS
```

or

```
sudo launchctl kill TERM system/com.nuix.NuixAS
```

If functioning properly, the agent daemon restarts almost immediately. The log file shows the agent terminating and restarting.

`/etc/newsyslog.d`

A log rotation config file ("com.nuix.NuixAS.conf") is placed in this directory. By default, the agent writes a log file to "/var/log/nuix/NuixAS.log", which can be changed by the server. The log is a plain text file. Use a command line text utility, such as cat, tail, or grep to view the log file. A typical log entry looks like the following:

```
2019-03-27_16:09:59.384670 INFO TID:0xb0192 C:00000000 P:16505 [475]:Service
(NuixAS) starting, version: 2.0.0-423
```

Each log entry starts with a timestamp, then a severity (listed as info, warn, or error), a thread ID, an error code (hex), a process ID (PID), and then the message.

The OS rotates the log files to keep their size down, according to the configuration file. The log files are in the installer in the following directory "/etc/newsyslog.d/com.nuix.NuixAS.conf". This file tells the log rotator to create a new log file whenever the old one reaches 6 MB. The old logs are compressed and up to five logs are maintained.

Linux agent file locations

The installer puts the Linux agent file in the following directories. These directories are configurable during installation by modifying the .run script.

`/opt/nuix/endpoint`

This file contains the agent executable (nuixas) and the uninstaller.

`/var/opt/nuix/data`

This file contains the agent data including DBR and comms queues.

`/lib/systemd/system/nuixsas.service`

This file contains the systemd service configuration file. The Linux agent is controlled by a system daemon called “systemd.” Systemd starts the agent at system startup, monitors the agent, and restarts the agent in the event of a system crash.

`Etc/logrotate.d/nuixAS.conf`

This file contains the log rotation configuration file.

Migrate agents to a new server

This section provides an overview and procedure for migrating agents from an existing Nuix Adaptive Security server to another new server. You may need to migrate agents in the following scenarios:

- When building a new Nuix Adaptive Security server on new hardware, for example, to upgrade the operating system or MySQL. In this scenario, you want to migrate agents from the old server to the new one.
- When you want to move a single endpoint agent from a server used for enterprise-wide monitoring to a server only used for active investigations.

This is not an upgrade procedure.

Prerequisites

You need to have both the existing server and the new server up and running.

Agent migration

On the new Nuix Adaptive Security server, take note of the server's IP address and the agent certificate which is the ca.cert.pem file located in Program Files. View the certificate by opening ca.cert.pem file in Notepad or another text reader application. You will need to copy the certificate over to the existing server. There are several ways to copy over the certificate. Use your enterprise's preferred method for copying over the certificate information.

On the existing server, you will add the new server and the certificate using the Nuix Adaptive Security application. This will allow the agents to migrate over to the new server. In the Nuix Adaptive Security application, there are two options on how you can add the new server.

Option 1: Add the server to an existing server set. When using this option, the agents will start to migrate over to the new server once the old server is turned off.

1. Open the application and go to the **System** module.
2. Select the **Servers** tab, then select the server set that you want to modify.
3. Select **+Add**.
4. Add the new server's IP address and certificate.
5. Save and publish the server set.

Note: The agents will try to go to the first server in the server list and then if they can't reach it, they will go to the next server.

Option 2: Create a new server set with both servers. When using this option, the agents will not migrate over until you add the new server set to the agent configuration.

1. Open the application and go to **System** module.
2. Select the **+New Servers** button and name the server set.
3. The default server is added automatically, add the new server's IP address and certificate.
4. Save and publish the new server set.

Important: Wait for the agents to migrate over to the new server before you delete the existing server from the server set. Then you can turn off the existing server.

Agents will continue to alert on logic rules. You can also export logic rules to the new server.

To upgrade the agents, see **Upgrading the agent** in the *Nuix Adaptive Security User Guide*. To configure the agent, see **Configuring the agent** in the *Nuix Adaptive Security User Guide*.

Back up Nuix Adaptive Security

There are two primary items to back up that will allow you to restore to a previous version and continue to have the agent population report into the server.

Step 1: Back up the database

The most important item to back up is the database. Almost everything about the system is stored in the database. To back up MySQL, see **Server Management > Backing up Data** in the *Nuix Adaptive Security Administration Guide*. You should also back up the MySQL my.ini configuration file to make sure you can restore the configuration.

Step 2: Back up the certificates

Next backup the certificates that allow communication between the agent and the server(s), see **Server Management > Backing up Agent Certificates** in the *Nuix Adaptive Security Administration Guide*. For most systems, the certificates are found in **C:\Program Files\Nuix\Adaptive Security\Endpoint Server\Data**, however, if the server was updated from an early version of Nuix Adaptive Security, it may be found in **C:\Program Files\Nuix Adaptive Security Endpoint Server\Data** or elsewhere.

Save the following files:

- ca.key
- ca.cert.pem,
- server.cert.pem
- server.key.pem
- dhparam4096.pem.
- Endpoint Server log files – This is used for troubleshooting.

Backup the configuration file in case it has been customized in any way. This is the config.txt file that is in the same directory as the files above.

You may also want to save the API/Application certificates in **C:\Program Data\Nuix\Endpoint\Data\Certificates**.

Store the license file in a safe place – it can be used for either version of the product.

Roll back to a previous version

First, you must backup Nuix Adaptive Security, see Backing up Nuix Adaptive Security.

Rollback the agent population version

You must rollback the agent version before the server. Newer agent versions may not work with older server versions. Therefore, it is a good idea to rollback the agent population version to the same version as the server. Use the Nuix Adaptive Security application to change the agent population version using profiles. For example, the existing agent population is on version 2.8 with 2.8 profiles, you will want to rollback to 2.6 agents with 2.6 profiles.

Restore a previous version of Nuix Adaptive Security

There are four steps to restoring to a previous version of Nuix Adaptive security.

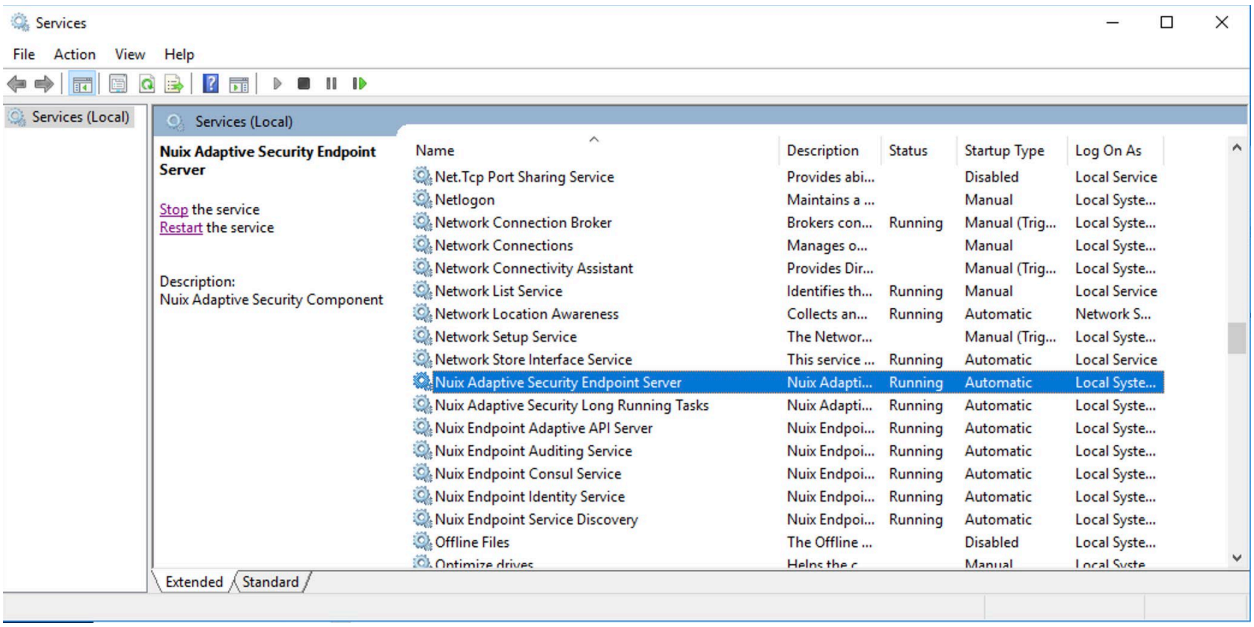
1. Remove the instance of Nuix Adaptive Security on the server.

2. Uninstall the Nuix Adaptive Security application version.
3. Restore the previous version of Nuix Adaptive Security.
4. Install the Nuix Adaptive Security application version that matches the server.

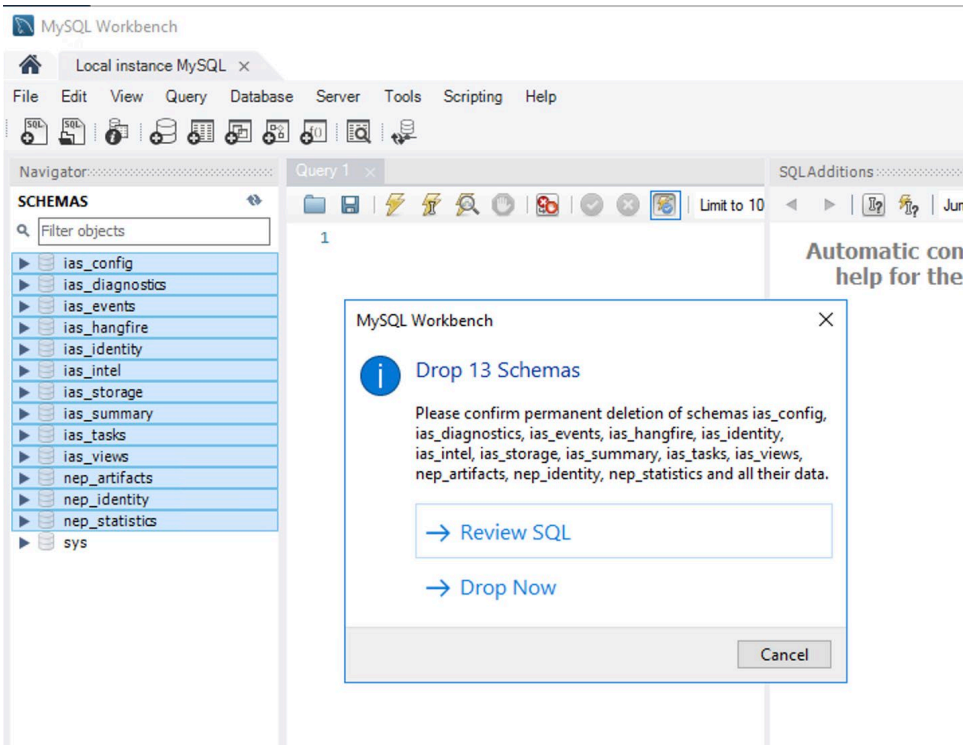
Remove an instance of Nuix Adaptive Security on the server

To remove an instance of Nuix Adaptive Security on the server:

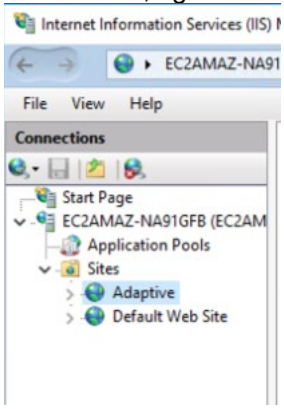
1. Stop the Nuix Adaptive Security Server:
   a. On the Windows server, open the services panel. Find Nuix Adaptive Security Endpoint Server and the Nuix Adaptive Security Microservices which include Long-Running tasks, Adaptive API Server, Auditing Service, Consul Service, Identity Service, and Service Discovery.
   b. Stop all Nuix services.



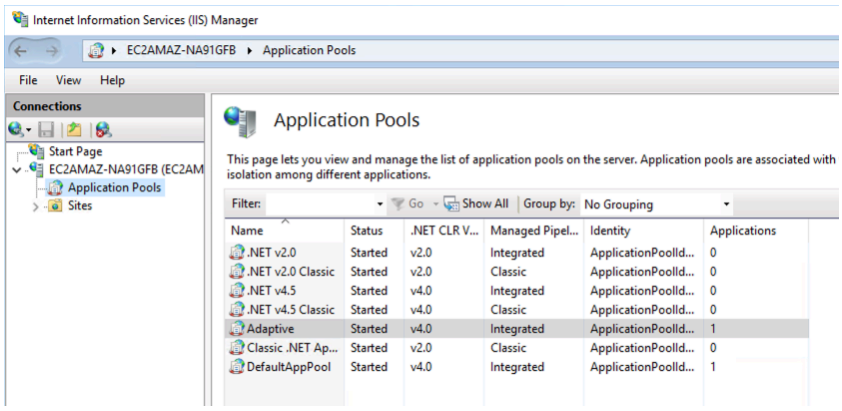
2. Delete the data.
   c. Open MySQL Workbench.
   d. Drop all schemas that begin with "ias_" and "nep_". Do not drop the "sys" schema or any other schema that may be used for other activities.
   e. This will delete all Nuix Adaptive Security data from the previous installation.



3. Uninstall the Nuix Microservices.
   a. Go to the Windows control panel > Programs and Features.
   b. Uninstall the Nuix services associated with Nuix Adaptive Security as listed above in step 1.a.
4. Remove the web services.
   a. Open IIS Manager.
   b. Under Sites, right-click on **Adaptive** and choose remove.



   c. In **Application Pools**, right-click on **Adaptive** and choose **Stop**. Next right-click and choose **Remove**.



d. Go to **C:\inetpub** and delete the Adaptive folder.

5. Delete the Nuix Adaptive Security program.

   a. Delete these folders:

      - C:\Program Files\Nuix\Endpoint\
      - C:\Program Files\Nuix\Adaptive Security\

   Note: If the instance was upgraded from older installs some files may reside in **C:\Program Files\Nuix Adaptive Security\Endpoint Server**. Delete these files.

6. Navigate to the **C:\Program Data\Nuix** folder.

   a. Consider if you want to save any log files before deleting this folder.
   b. Delete the folder.

   Note: If other Nuix products are installed on the server make sure you only delete the folders associated with Nuix Adaptive Security (Adaptive Security and Endpoint).

Uninstall the Nuix Adaptive Security Application

The version of the Nuix Adaptive Security application must match the version of the Nuix Adaptive Security server. On the Windows system running the application go to Control Panel > Add/Remove Programs. Uninstall the Nuix Adaptive Security application.

Restore the previous version of Nuix Adaptive Security

The first step is to restore the database using the backup that was completed at the beginning of this document. To restore the database:

1. In MySQL Workbench, on the Administration tab, under **Management**, click **Data Import/Restore**.
2. Select **Import from Self-Contained File**.
3. Browse and select the backup file.
4. Select Start Import.

If changes were made to the my.ini file during the upgrade, then restore the backup copy.

After the database is restored, run the server installer for the rollback version. If needed, re-apply the license file.

After the install completes, stop the endpoint server. Restore the backed-up endpoint certificates so the existing agents can report to the server. In C:\Program Files\Nuix\Adaptive Security\ Endpoint Server\Data replace the following files with the files you backed up.

- ca.key
- ca.cert.pem
- server.cert.pem
- server.key.pem

- dhparam4096.pem

Also, replace the configuration file with the backed-up version if you customized the configuration in any way.

Replace the API/Application certificates in **C:\Program Data\Nuix\Endpoint\Data\Certificates** with the backup up files if needed.

Once all files are in place, go to the Services pane on the Windows Server and start any Nuix services that are not running including the Nuix Endpoint Server and the Nuix microservices.

Install the Nuix Adaptive Security Application

Install the matching version of the Nuix Adaptive Security application. You should be able to log in and agents should begin reporting into the system.

