Cygna Auditor Web Console

User Guide

Cygna Auditing & Security Suite

For the latest information, visit online documentation at docs.cygnalabs.com

Published 1/11/2022

Version 5.9

Table of Contents

Introduction to Web Console

The Auditor Web Console makes it simple for you to filter through audit data from the Auditor modules.

The Web Console currently supports:

- Cygna Auditor for Active Directory
- Cygna Auditor for SQL Server
- Cygna Auditor for Exchange
- Cygna Auditor for File System

Overview

Users can organize collected audit data and customize how the information is displayed according to their individual needs. The information is stored on a secure site which allows users to retrieve audit data anytime, anywhere.

This guide provides instructions for managing user access, viewing and filtering audit data, customizing the dashboard, and managing agents.

Prerequisites

Auditor Web Console requires a minimum of Internet Explorer 11. Most versions of Firefox, Chrome, and Safari are supported. Microsoft Edge is also supported.

Roles and Access

Two types of access can be assigned to both groups and users in Active Directory:

- Administrator: Administrators can access all sections of the Web Console and can make changes to the User Access page.
- Read Only: Users with Read Only can only access the About and Audit Data pages.

For more information, please see Manage User Access.

Installing Auditor Web Console

The Auditor Web Console is installed using the same installer as Cygna Auditing & Security Suite.

For more information on installing and configuring the Web Console, please see Cygna Auditing & Security Suite Installation Guide.

Manage User Access

Administrators can use the User Access page to perform the following tasks:

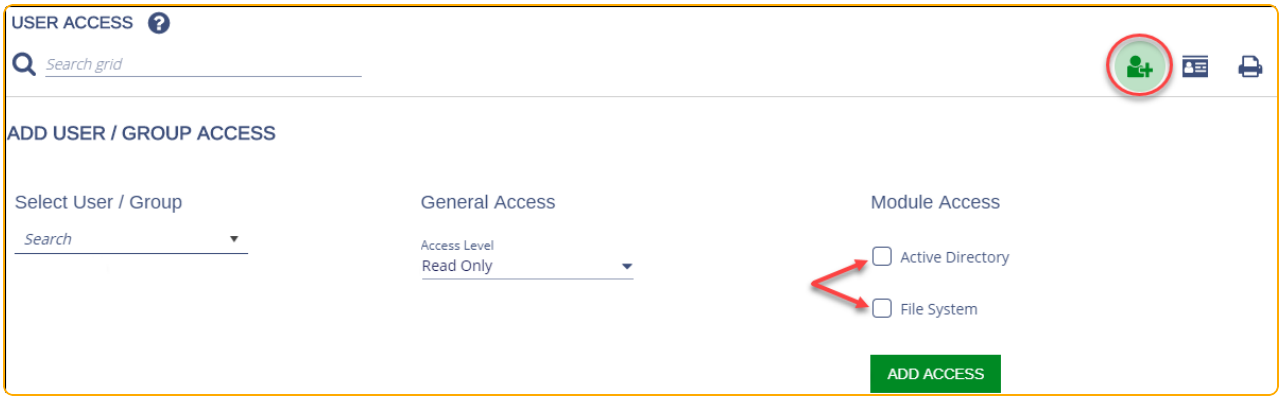
- Add users and groups, granting either Administrator or Read Only access to selected modules
- View the effective access for users based on their group membership
- Edit the access level and the modules a user or group can access
- Remove users and groups from the grid

Once a user or group is added they will be displayed on the User Access Grid. Access can then be edited in the grid.

Adding Users and Groups

You can find users and groups not listed on the first page by typing their name in the Search box above the grid or by clicking the arrows below the grid to move to the next page.

1. Select User Access from the menu.
2. Click the Add User/Group icon above the grid.
3. In the Select User/Group search box, type the name (or part of it) of a user or group you want to add.
4. Select the user or group from the list.
5. Select the access level from the General Access list.



6. Under Module Access, select the modules for the user or group to access.

   Users can view audit data and change the audit view filters for any module they can access.

7. Click Add Access.

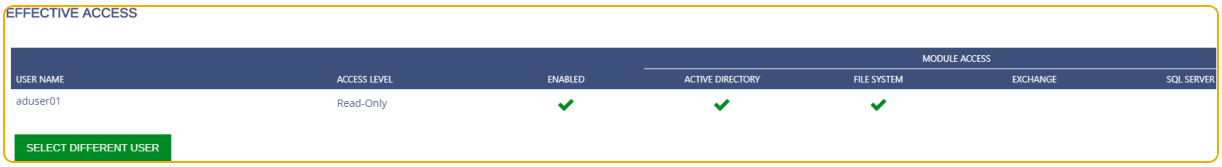
Viewing Effective Access for a User

If a user account is added to the User Access grid, its access overrides all group-based access. Any user in a group has the same access as that group. If a user is in more than one group, access is combined to make up that user's access.

To view effective access for a user:

1. Select User Access from the menu.

2. Click the Effective Access icon (business card) above the grid.
3. In the Select A User search box type a user name (or part of it) and then select the user from the list.
   The user's access level and module access will be shown, as well as whether their account is enabled or not. Only enabled accounts can log on to the web console.



   You can click Select a Different User to search for another user name.

Editing Users and Groups

To edit access for a user or group in the grid:

1. Select User Access from the menu.
2. Select the user or group in the grid.

3. Change the access level, enabled status, and module access accordingly.

Note: Click the information icon (i) to view group membership for the selected user or group.

Removing Users and Groups

To remove a user or group from the grid:

1. Select User Access from the menu.
2. Select the user or group in the grid, and then click the Remove Access icon (trash can).

Navigate the Audit Data Grid

By default, the Audit Data Grid is displayed each time you open the Web Console. You can also access it at any time by selecting it from the menu. The Audit Data grid displays all audit data collected from licensed modules.

You can use the Audit Data grid to do the following:

- Filter the audit data collected based on what action was taken, when it occurred, by who, on what object and from which computer.
- Filtering can be done using built-in Audit Views that contain pre-configured filters or by manually selecting filters and then saving the settings as an audit view.
- View the details of any event listed in the grid by clicking the event.
- Search the data in the grid using key words.
- Export grid data to a Excel file.

Use Audit Views and Filtering

To change the Audit View:

1. From the menu select Audit Data. The Default Audit View is displayed.

2. Click the Audit Views icon (folder) to open the Audit Views panel.
3. Select an audit view from the list. You can scroll through the list or perform a keyword search to find your desired audit view.
4. Review the pre-configured details of the audit view and optionally make this view your default view by selecting the check box.
5. Click Load Audit View. The event data is loaded into the grid.
6. Click the column headers to sort the data.
7. Click Grid Configuration to change how many rows are displayed.
8. Click Grid Columns to choose the columns displayed in the grid.
9. Click Refresh Grid to refresh the data in the grid.
10. Change the refresh rate by selecting a time from the Refresh Rate drop-down list.

11. To further filter the data, click the Filter Audit View icon to open the Filter Audit View panel.
12. Select filter criteria in each of the Who, What, When, and Where sections and click Apply to immediately apply the selected filters to the grid.

You can only select options from one of the filter categories at a time.

To save the filtered data as a new audit view:

1. Click the Save Audit View icon.
2. Provide a name and description and then click Save Audit View.

   Note: To delete customized audit views you saved, select the view from the list and click Delete Audit View on the Review Audit View tab. You cannot delete the built-in audit views.

3. To export the grid data, click the Export to Excel icon above the grid. The excel file is automatically saved in your Downloads folder.

Use the Dashboard

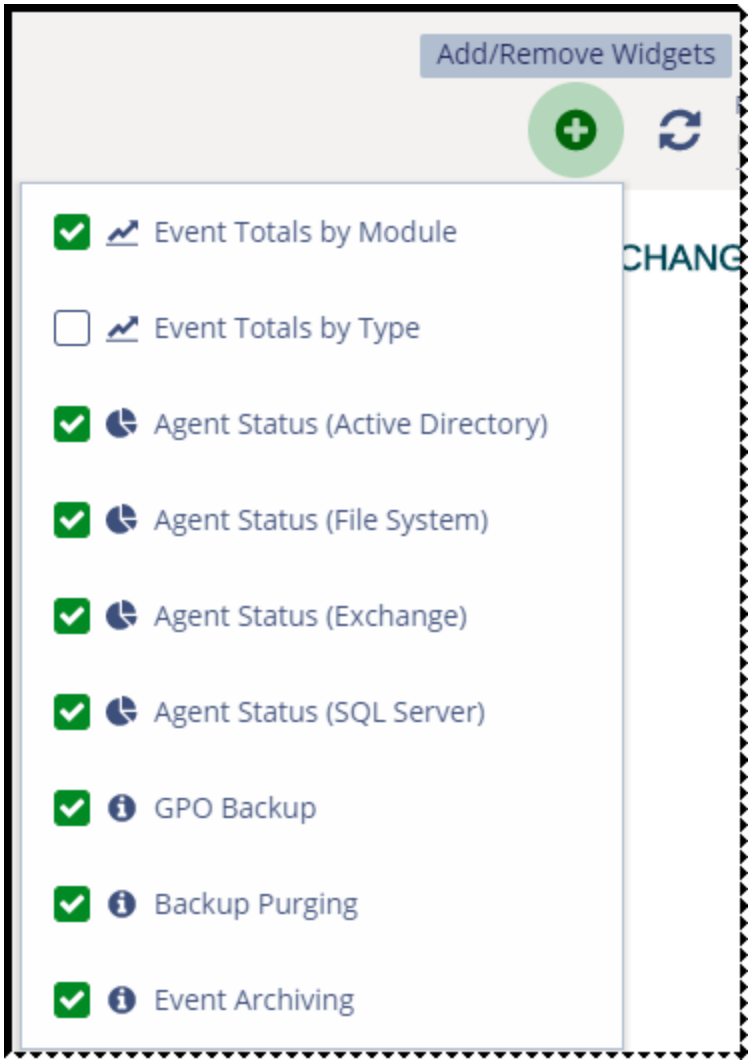
By default, the dashboard displays widgets that provide a visual look at the status of the agents for your Cygna Auditor modules. On the dashboard, you can view:

- Event information
- Backup purging information
- GPO backup information
- Event archiving information

The dashboard can be accessed by selecting it from the menu.

You can customize the dashboard:

- Select and drag the widget to the preferred location on the page



- Click the Add/Remove Widgets icon, and then select / deselect the widget

- Click in the Agent Status widgets to display the Agents page where you can view agent details, as well as deploy, start, stop, restart, update, remove, and refresh settings. Note that not all actions are available for all agent types.

For more information, please see Manage Agents .

Manage Agents

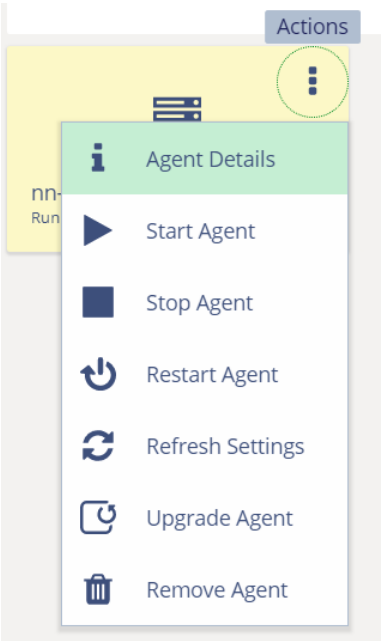
The Agents page can be accessed by selecting Agents from the menu or by clicking an Agent Status widget on the Dashboard page. On the Agents page you can do the following:

- Find out information about your installed agents, such as server name, OS, status, description, heartbeat, last update time, module, and agent version.
- Switch between Card View and Grid View for displaying your agents on the page by clicking their respective icons.
- Refresh the agent data displayed on the page instantly by clicking the Refresh icon or select a Refresh Rate from the drop-down list.
- Deploy Active Directory and File System Agents
- Start, stop, restart, refresh agent settings, upgrade, and remove Active Directory, Files System, and Exchange Agents
- Remove SQL Server Agents

View Agent Details

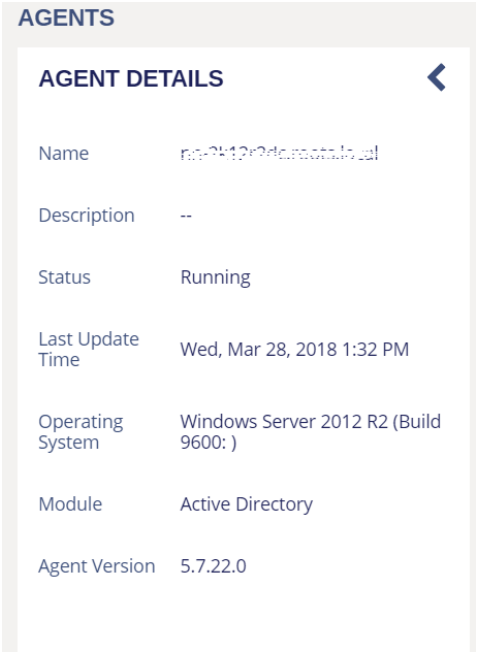
Select the module in the top navigation (Active Directory, File System, Exchange, SQL Server).

1. Click the Actions icon (vertical ellipsis) for the agent.



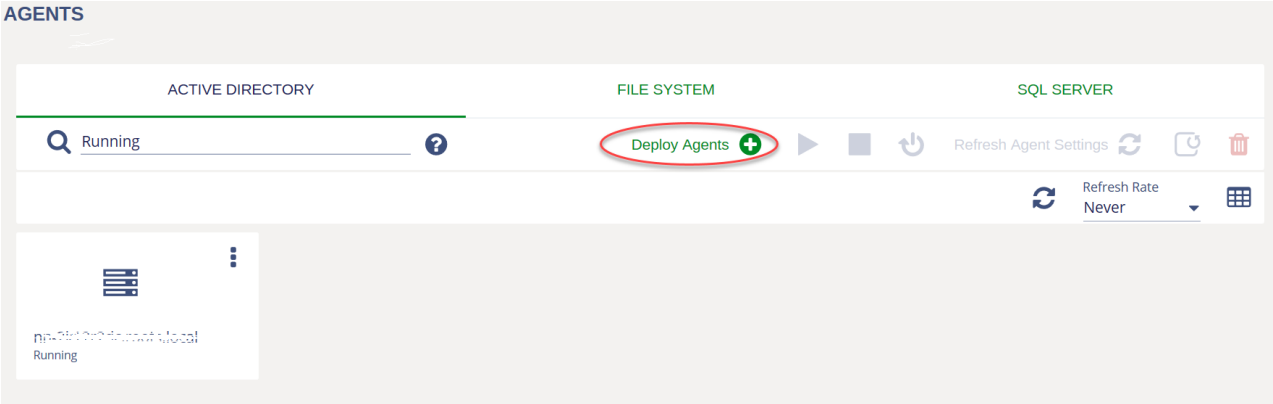
2. Select Agent Details from the menu.

   The Agent Details can be viewed in the left pane.

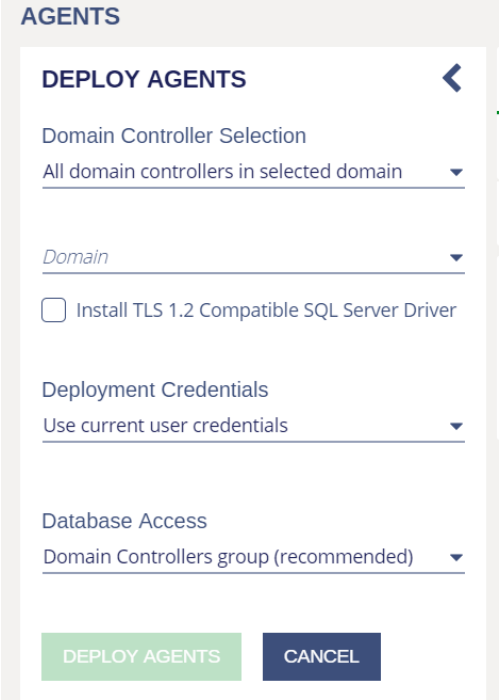


Deploy Agents

1. Select the module in the top navigation (Active Directory or File System).



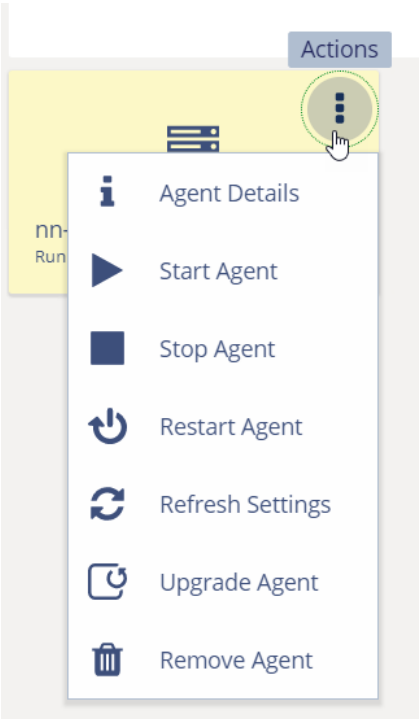
2. Click Deploy Agents.
3. Select details in the Deploy Agents pane on the left. For example, Domain Controller, Deployment Credentials, Database Access, etc.



4. Click Deploy Agents.

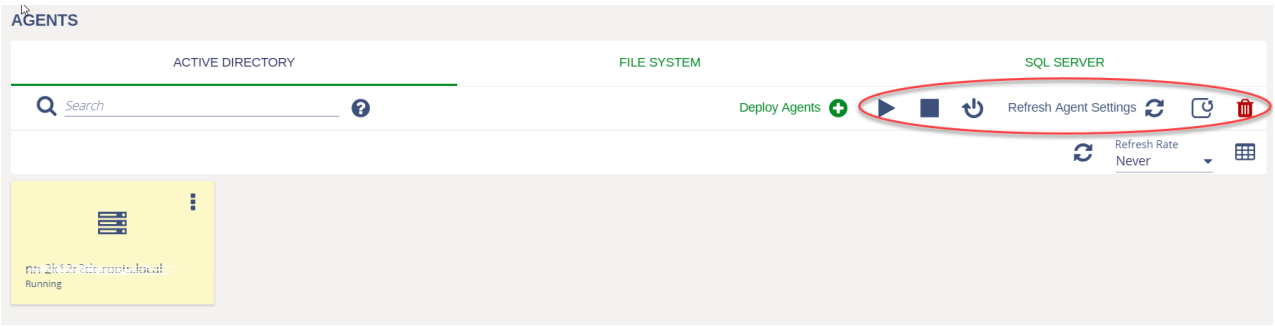
Perform Actions on the Agent

Select the module in the top navigation (Active Directory, File System, Exchange, SQL Server).



1. Click the Actions icon (vertical ellipsis) for the agent.
2. Select an action from the menu.

Note: For SQL Server agents, only Agent Details and Remove Agent are available.



You can also select the agent actions by clicking the icons enabled when you select the agent.

3. After selecting any action, you must provide credentials and click Submit Credentials in the left pane that displays for that action.