



PowerBroker Auditor Web Console

User Guide

Version 5.7 – March 2018

Revision/Update Information: March 2018
Software Version: PowerBroker Auditor Web Console 5.7
Revision Number: 0

CORPORATE HEADQUARTERS
5090 N. 40th Street
Phoenix, AZ 85018
Phone: 1 818-575-4000

COPYRIGHT NOTICE

Copyright © 2018 BeyondTrust Software, Inc. All rights reserved.

The information contained in this document is subject to change without notice.

No part of this document may be photocopied, reproduced or copied or translated in any manner to another language without the prior written consent of BeyondTrust Software.

BeyondTrust Software is not liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages, including lost profit or lost data, whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust Software is not associated with any other vendors or products mentioned in this document.

Contents

- Introduction 2**
 - Contacting Support 2
 - Privileged Account Management Support 2
 - Vulnerability Management Support 2
 - All other Regions 2
- Overview 3**
 - Prerequisites 3
 - Roles & Access 3
 - Installing PowerBroker Auditor Web Console 3
- Managing User Access 4**
 - Adding Users and Groups 4
 - Viewing Effective Access for a User 4
 - Editing Users and Groups 5
 - Removing User and Groups 5
- Navigating the Audit Data Grid 6**
 - Using Audit Views and Filtering 6
- Using the Dashboard 8**
- Managing Agents 9**
 - Viewing Agent Details 9
 - Deploying Agents 10
 - Performing Actions on the Agent 11

Introduction

The PowerBroker Auditor Web Console makes it simple for you to filter through audit data from the PowerBroker Auditing & Security Suite modules.

The Web Console currently supports Auditor for AD, Auditor for SQL Server, Auditor for Exchange and Auditor for File System.

Contacting Support

For support, go to our Customer Portal then follow the link to the product you need assistance with.

The Customer Portal contains information regarding contacting Technical Support by telephone and chat, along with product downloads, product installers, license management, account, latest product releases, product documentation, webcasts and product demos.

Email

PBMS-support@beyondtrust.com

Telephone

Privileged Account Management Support

Within Continental United States: 800.234.9072

Outside Continental United States: 818.575.4040

Vulnerability Management Support

North/South America: 866.529.2201 | 949.333.1997

+ enter access code

All other Regions

Standard Support: 949.333.1995

+ enter access code

Platinum Support: 949.333.1996

+ enter access code

Online

<http://www.beyondtrust.com/Resources/Support/>

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

PowerBroker Auditing & Security Suite Web Console requires a minimum of Internet Explorer 11. Most versions of Firefox, Chrome, and Safari are supported. Microsoft Edge is also supported.

Roles & Access

Two types of access can be assigned to both Groups and Users within Active Directory: Administrator and Read Only. Administrators can access all sections of the web console and can make changes to the User Access page. Users with Read Only can only access the About and Audit Data pages. Refer to [Managing User Access](#) for more details.

Installing PowerBroker Auditor Web Console

The PowerBroker Auditor Web Console is installed from the same wizard as the PowerBroker Auditing & Security Suite. Please refer to the PowerBroker Auditing & Security Suite Installation Guide for information on installing and configuring the Web Console.

Managing User Access

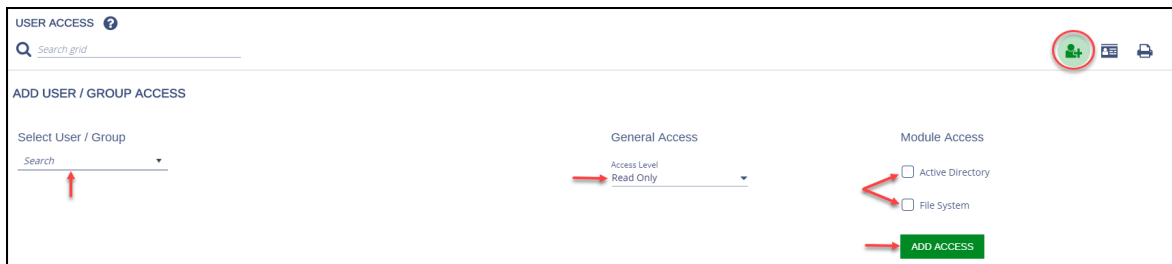
Once a User or Group is added they will be displayed on the User Access Grid. Access can then be edited within the grid. You can find users and groups not listed on the first page by typing their name in the Search grid box above the grid or by clicking the arrows below the grid to move to the next page.

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

- Add users and groups, granting them 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 which modules a user or group can access
- Remove users and groups from the grid

Adding Users and Groups

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 wish 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 have access to.
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 will have the same access as that group. If a user is in multiple groups, that 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 into the web console.
You can click **Select a Different User** to search for another user name.



EFFECTIVE ACCESS						
USER NAME	ACCESS LEVEL	ENABLED	ACTIVE DIRECTORY	MODULE ACCESS		
				FILE SYSTEM	EXCHANGE	SQL SERVER
aduser01	Read-Only	✓	✓	✓		

[SELECT DIFFERENT USER](#)

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 User 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).

Navigating 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.

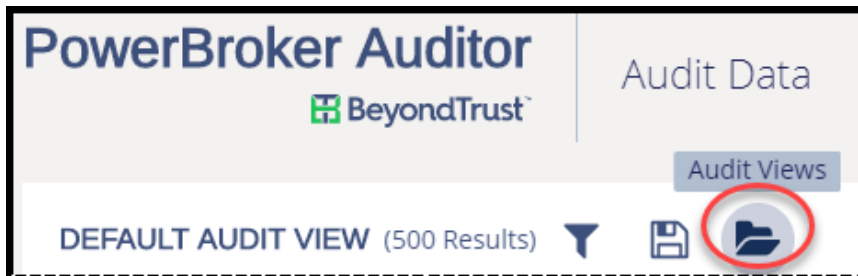
You can use the Audit Data grid to do the following:

- 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.

Using 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.
 - Click the column headers to sort the data.
 - Click **Grid Configuration** to change how many rows are displayed.
 - Click **Grid Columns** to choose which columns are displayed in the grid.
 - Click **Refresh Grid** to refresh the data in the grid.
 - Change the refresh rate by selecting a time from the **Refresh Rate** drop down list.
6. To further filter the data, click the **Filter Audit View** icon to open the Filter Audit View panel.
 - You can select filter criteria in each of the **Who**, **What**, **When**, and **Where** sections and click **Apply** to have the selected filters immediately applied to the grid.
 - You can only select options from one of the filter categories at a time.

7. To save the filtered data as a new audit view:

- Click the **Save Audit View** icon.
- Provide a name and description and then click **Save Audit View**.

Note: You can delete customized audit views that you saved by selecting the view from the list and clicking **Delete Audit View** on the Review Audit View tab. You cannot delete the built-in audit views.

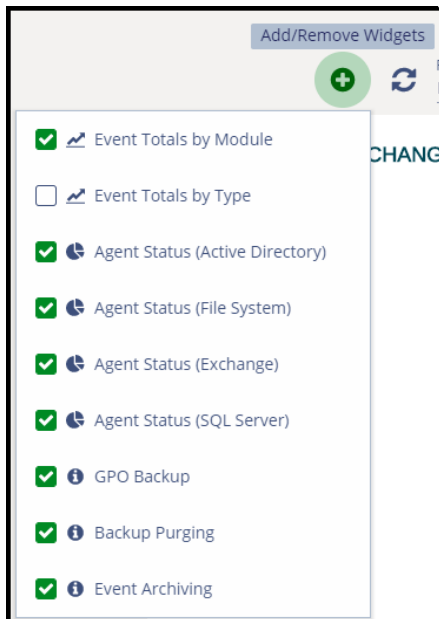
8. To export the grid data, click the **Export to Excel** icon above the grid. The excel file is automatically saved in your Downloads folder.

Using the Dashboard

The dashboard can be accessed by selecting it from the menu. By default the dashboard displays widgets that give you a visual look at the status of the agents for your PowerBroker Auditing & Security Suite modules, as well as event information, backup purging information, GPO backup information, and event archiving information.

You can customize the dashboard by:

- Selecting the widget and dragging and dropping it where desired
- Clicking the **Add/Remove Widgets** icon and then selecting / deselecting the widgets



- You can 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 for an agent. Note that not all actions are available for all agent types. Refer to the Managing Agents section for more information.

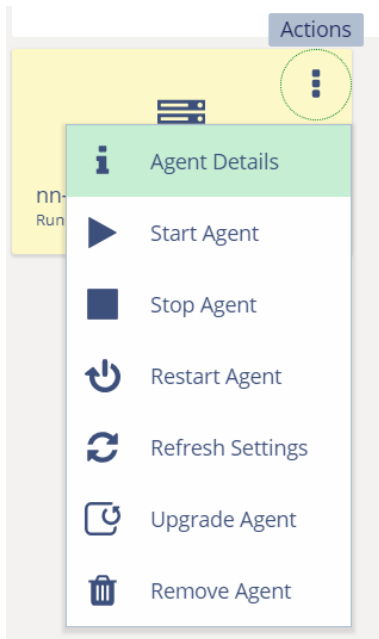
Managing Agents

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:

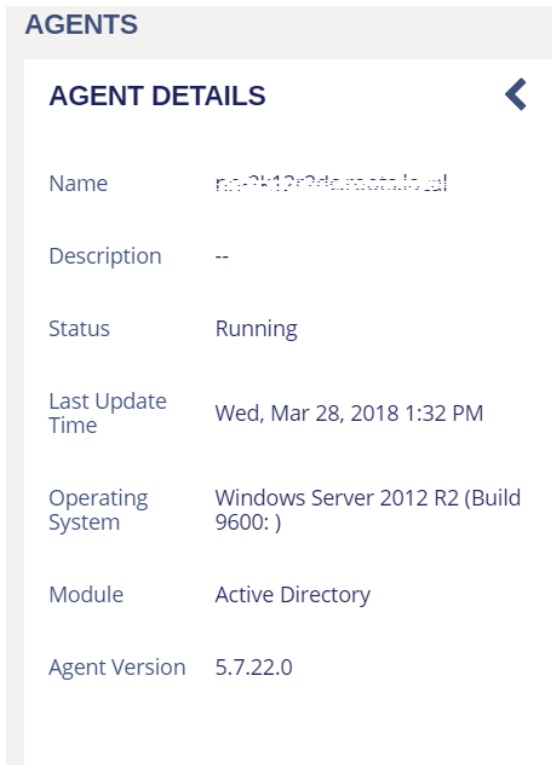
- Find out information about your installed agents, such as server name, OS, status, description, heartbeat, last update time, module, and agent version.
- Switch between **Card View** and **Grid View** for displaying your agents on the page by clicking their respective icons.
- Refresh the agent data displayed on the page instantly by clicking the **Refresh** icon or select a **Refresh Rate** from the drop down.
- 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

Viewing Agent Details

1. Select the module in the top navigation (Active Directory, File System, Exchange, SQL Server).
2. Click the **Actions** icon (vertical ellipsis) for the agent.
3. Select **Agent Details** from the menu.

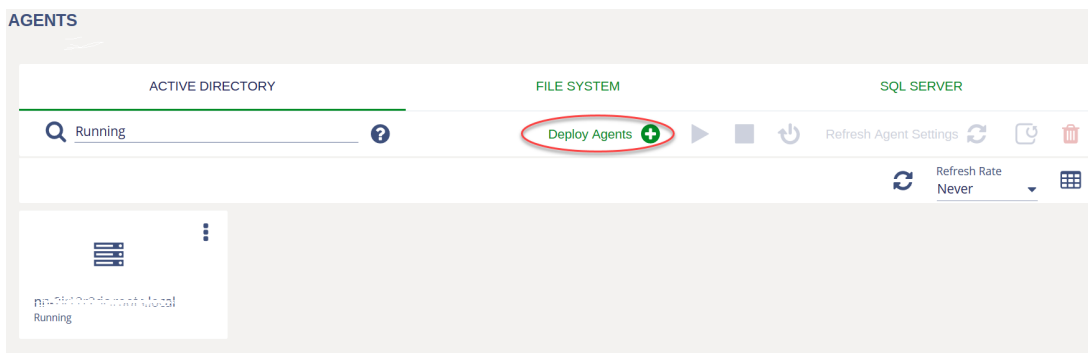


- The Agent Details can be viewed in the left pane.

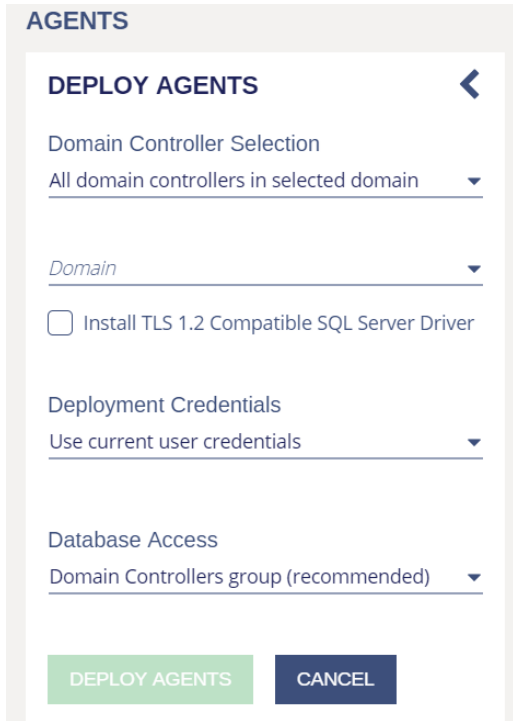


Deploying Agents

- Select the module in the top navigation (Active Directory or File System).
- Click **Deploy Agents**.

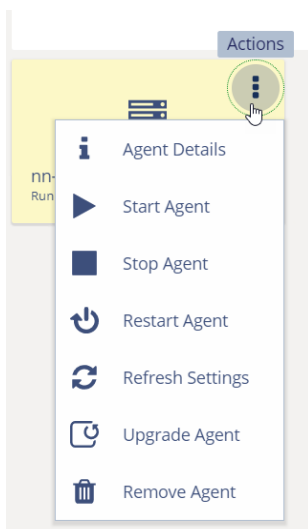


- Select the necessary details, such as Domain Controller, Deployent Credentials, Database Access, etc. in the Deploy Agents pane on the left and then click **Deploy Agents**.

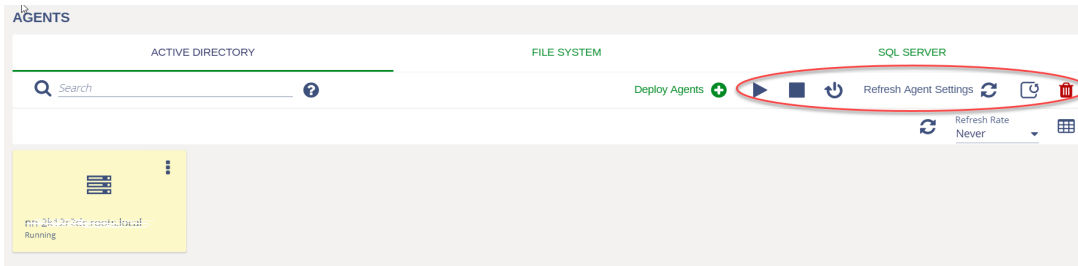


Performing Actions on the Agent

1. Select the module in the top navigation (Active Directory, File System, Exchange, SQL Server).
2. Click the **Actions** icon (vertical ellipsis) for the agent.
3. Select your desired action from the menu. Note that for SQL Server agents, only Agent Details and Remove Agent are available.



Note: You can also select the agent actions by clicking their respective icons that are enabled when you select the agent.



4. After selecting any action, you will need to provide credentials and click **Submit Credentials** in the left pane that displays for that action.