

Cygn Auditor

Getting Started Guide

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

Published 7/13/2022

Copyright

©2022 Cyigna Labs Corp. ALL RIGHTS RESERVED.

Trademarks

Cyigna Labs and the Cyigna Labs logo are trademarks and registered trademarks of Cyigna Labs Corp. in the United States of America and other countries. All other trademarks are property of their respective owners.

Disclaimers

The product documentation is subject to change without notice. For the latest and more detailed documentation, please refer to online documentation at <https://docs.cygnalabs.com>.

The product functionality described in this document shall not be treated as a public offer or commitment.

The information regarding the use and installation of third-party software is provided to assist you but Cyigna Labs Corp. shall not accept any responsibility or liability for any claims or damages caused by incorrect or incomplete information provided about third-party software. For detailed instructions on configuring third-party software components, refer to their respective owners.

Contents

Welcome and Let's Get Started	5
Insight into Architecture and Workflow	6
Workflow	6
Architecture	6
Additional Components	7
Planning Deployment	9
System Requirements	9
Distributed Deployment—Medium and Enterprise Environments	9
Cygna Auditor Application Server	9
Database Server	10
Single Server Deployment—Small Businesses and PoC	11
Account and Permissions Checklist	13
Installation	15
Starting the Product	16
Configuration Wizard	18
Configuring IIS Application Pool	18
Configuring Database	19
Supplying a License	20
Managing System Settings	21
Configuring Data Collection	23
Supported Sources	23
Active Directory	24
Amazon Web Services	27
Windows File System	29
Agent Deployment	30
Configure Monitoring Filters	31
On-Premises Exchange	32
Microsoft 365	34

- VMware 35
- PBMS 35
- Managing Delegation 36
- Auditing & Tools 37
 - Dashboard 38
 - Auditing 39
 - Reading Records in Auditing 40
 - Reviewing All Changes 42
 - Searching for Specific Events 44
 - Excluding Bias 46
 - Distilling Results 47
 - Reports 48
 - Creating a New Report 50
 - Subscribing to Reports 51
 - Alerting 53
- Summary 56
- Index 57

Welcome and Let's Get Started

Welcome to Cygna Auditor, a comprehensive, integrated auditing, alerting, and reporting platform for Active Directory, Windows File System, Microsoft 365, etc. Cygna Auditor is a straightforward and easy-to-use solution that provides clear and affordable overviews of activity in your business critical assets, helps you pass compliance audits and mitigate risks.

Cygna Auditor documentation is designed to assist you any time you have a question about the product or auditing in general. The most up-to-date documentation is always available online at <https://docs.cygnalabs.com>. Do not hesitate to visit the online documentation portal—being the primary source of information about the product it has much more to offer besides general instructions. In [Cygna Auditor documentation portal](#) you can also find detailed tutorials, how-to's, best practices, and articles explaining the auditing basics.

If you prefer to download a printable copy on your desktop, be sure check for newer versions regularly. Note that while fully covering the product functionality, the printable PDF may not include some interactive assistance materials or articles discussing the industry best practices or auditing techniques. Users advised to visit the online portal for this purpose.

After reading the Getting Started guide, you will know everything you need to install, launch, and start using the product.

Without further ado, let's get started. First of all, get some insight into how the product works. Go to [Insight into Architecture and Workflow](#).

Insight into Architecture and Workflow

To get started faster, gain some insights into how Cygna Auditor works and what you'd better have in hand before you install and start using the product.

Workflow

If you take a closer look at your journey with Cygna Auditor, you will discover that it consists of the following simple stages:

1. **Checking prerequisites.** Make sure you have enough resources before you proceed with installation. For more information, see [Planning Deployment](#).
2. **Installation.** For more information, see [Installation](#). If you want to leverage CA&SS (former PowerBroker Management Suite), install it as well.
3. Complete the initial configuration wizard. See [Configuration Wizard](#).
4. **Setting up audit.** Once the product is up and running, start collecting audit data for the systems you are interested in (e.g., Active Directory). Note that for most sources, you have to adjust some settings to enable Cygna Auditor to collect audit events. Check out [Cygna Auditor online documentation portal](#) for more information and detailed instructions.
5. **Administration.** Dive deep into the product administration. Delegate access to your authorized personnel, manage licenses, etc. Check out [Cygna Auditor online documentation portal](#) for more information and detailed instructions.
6. **Basic auditing.** Every so often, review out-of-the-box reports to validate compliance with various standards or use auditing search to investigate potential threats and address risks immediately. For more information, see [Auditing & Tools](#).
7. **Advanced auditing.** As you get to know Cygna Auditor better, configure alerts to be notified if something goes wrong in your environment, start creating reports tailored to your organization's specific needs. For more information, see [Auditing & Tools](#).

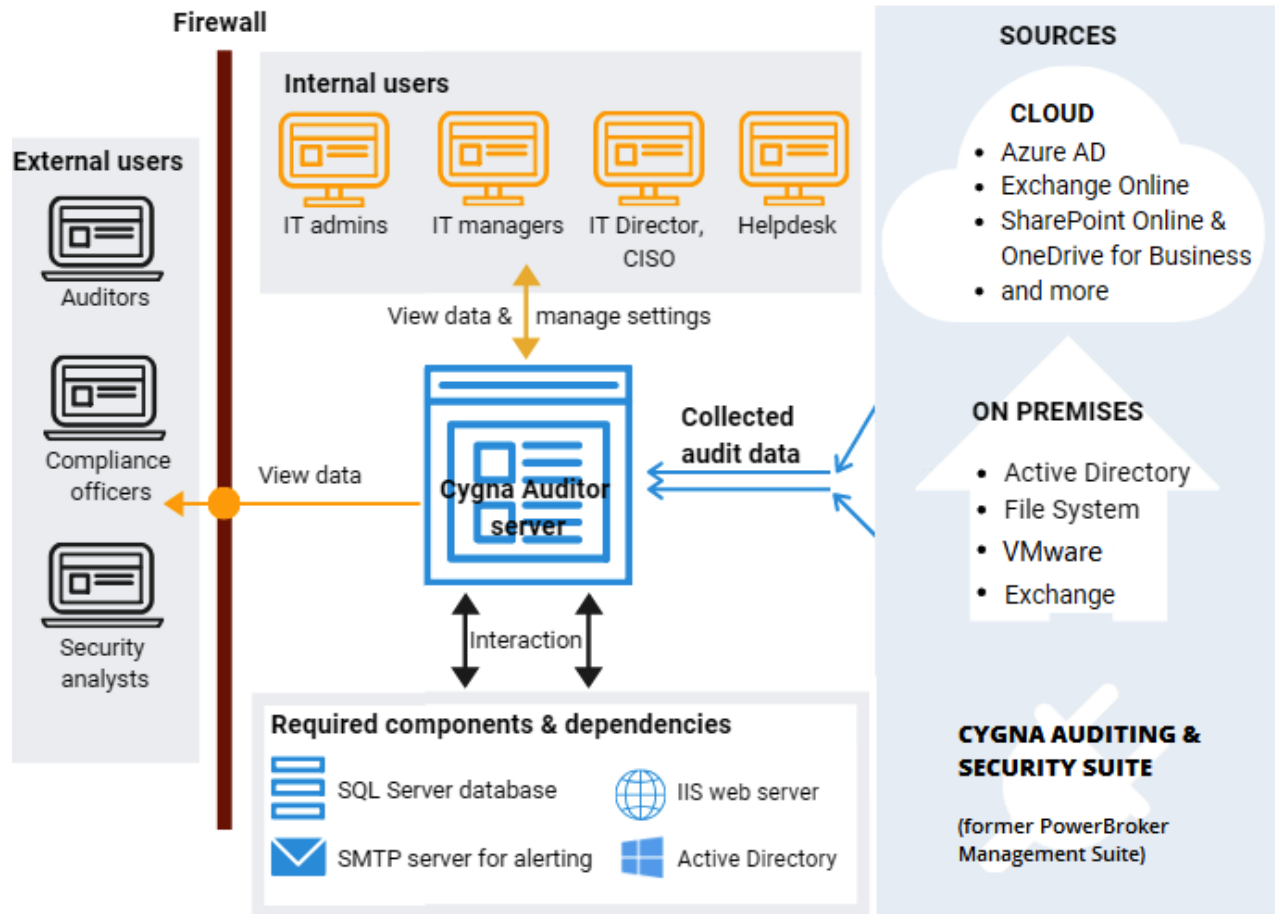
Architecture

Cygna Auditor is designed as a client-server application that supports distributed deployment. Basically, Cygna Auditor consists of the following components:

- Cygna Auditor platform—a server part responsible for data collection and processing.
- Cygna Auditor web-console—a web-based client interface for managing the Cygna Auditor platform and viewing collected audit data. The client website is hosted on the same server where Cygna Auditor platform is installed but all users in your company


can access it through a browser. Depending on the role in the product, users are granted permissions to access certain product functionality.

- Database—SQL Server-based storage of audit data. For better performance, Cygn Labs recommends deploying a SQL Server instance on a separate server.
- Cygn Auditing & Security Suite (former PowerBroker Management Suite)—stand-alone management console products that integrate smoothly with Cygn Auditor and provide extended auditing functionality.




Additional Components

Cygn Auditor relies on the following additional components. While some components are vitally important for the product operability, it is up to you to decide on some others.

COMPONENT	DESCRIPTION	MANDATORY
Active Directory	Ensures that users in your organization—within your corporate domain—can access Cygna Auditor web-console through their browsers.	Yes
	 Note: To ensure data security, users must be delegated appropriate access rights in the product.	
SQL Server	Stores audit data collected by Cygna Auditor.	Yes
IIS web server	Hosts Cygna Auditor web-console.	Yes
SMTP server	Enables email notifications within the product. As an SMTP server, you can use your on-premises mail server or any public SMTP server (e.g., Gmail, etc.).	No

Cygna Labs recommends you to set up all required components before you install Cygna Auditor. Refer to [System Requirements](#) for more information about the additional components and their system requirements.

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.


Planning Deployment

Read this section to learn more about product deployment options, system requirements, essential rights and permissions, etc.

QUICK TIP: Do you want to start right now? Prepare two servers:

1. A clear Windows Server 2019 with preinstalled IIS and .Net Framework 4.8 for Cygna Auditor.
2. The other server with SQL Server 2019 Standard Edition.

Check that both servers are in your corporate Active Directory domain and that you have access to [Cygna customer portal](#).

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.

System Requirements

Read this section to learn more about the Cygna Auditor and its database server system requirements. Depending on your company size and the average number of changes recorded per day, the requirements can vary significantly. Use the metrics below as a general guideline and consider scaling your Cygna Auditor infrastructure if needed:

[Distributed Deployment—Medium and Enterprise Environments](#)


[Single Server Deployment—Small Businesses and PoC](#)

Distributed Deployment—Medium and Enterprise Environments

For medium and enterprise environments, Cygna Labs recommends distributed configuration with two servers.

Cygna Auditor Application Server

Make sure the computer where you plan to install Cygna Auditor (application server) meets the following hardware and software requirements and has all necessary software components and roles enabled.

COMPONENT	REQUIREMENTS
Hardware	<ul style="list-style-type: none">• CPU: Any modern processor with 4 cores• RAM: 4 GB (minimum), 8 GB (recommended)• HDD: 100 MB
Operating system	<ul style="list-style-type: none">• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019• Windows Server 2022
Server roles and features	<ul style="list-style-type: none">• Group Policy Management• Web Server (IIS): Microsoft IIS 8.5 or above, including Windows Authentication, ASP.NET 4.8• .Net Framework: Microsoft .Net Framework 4.8, including ASP.NET 4.8 <p> Note: Depending on the OS, you might need to install ASP.NET manually.</p>
Additional software	Any modern browser, preferably Google Chrome or Microsoft Edge.


Database Server


Review the system requirements for the database server.

COMPONENT	REQUIREMENTS
Hardware	<ul style="list-style-type: none"> • CPU: Any modern processor with 4 cores • RAM: 8 GB (minimum), 16 GB (recommended) • HDD: 2 GB (minimum). <p>For better performance, adjust your hardware configuration based on the number of changes Cygna Auditor collects per day. The more change records are collected and stored in a database, the more impact on your database server. The disk space required for the audit data can grow significantly over time.</p>
Operating system	Any modern OS provided it supports installation of Microsoft SQL Server
Database	<ul style="list-style-type: none"> • SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • SQL Server 2022 <p>Standard and Enterprise editions are supported. Note that Express edition is only suitable for the product evaluation due to database size limitation. Cygna Labs recommends opting for Standard edition.</p>

Single Server Deployment—Small Businesses and PoC

For smaller businesses as well PoC deployments, you can opt for a single server deployment. In this case, both Cygna Auditor application server and database server will reside on the same server.

COMPONENT	REQUIREMENTS
Hardware	<ul style="list-style-type: none"> • CPU: Any modern processor with 4 cores • RAM: 12 GB (minimum), 16 GB (recommended) • HDD: 4 GB <p>For better performance, adjust your hardware configuration based on the number of changes Cygna Auditor collects per day. The more change records are collected and stored in a database, the more impact on your database server. The disk space required for the audit data can grow significantly over time.</p>
Operating system	<ul style="list-style-type: none"> • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Server roles and features	<ul style="list-style-type: none"> • Group Policy Management • Web Server (IIS): Microsoft IIS 8.5 or above, including Windows Authentication, ASP.NET 4.8 • .Net Framework: Microsoft .Net Framework 4.8, including ASP.NET 4.8 <p> Note: Depending on the OS, you might need to install ASP.NET manually.</p>
Database	<ul style="list-style-type: none"> • SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • SQL Server 2022 <p>Standard and Enterprise editions are supported. Note that Express edition is only suitable for the product evaluation due to database size limitation. Cygna Labs recommends opting for Standard edition.</p>
Additional software	Any modern browser, preferably Google Chrome or Microsoft Edge.

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.

Account and Permissions Checklist

During the installation, Cygna Auditor will prompt you to enter account credentials for specific services and applications the product requires access to. Before running the installation, check that these accounts have sufficient rights and permissions.

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
Domain administrator account	<p>Active Directory credentials used to connect to your domain and create an Active Directory object with product configuration.</p> <p>The product stores its configuration in Active Directory forest to ensure the product settings stay in sync across your corporate domain.</p> <p>During the installation, Cygna Auditor will create and start a service.</p>	Domain administrator as it has sufficient permissions to create objects in the Active Directory.
IIS identity account	The account running the IIS can be either LocalSystem or a custom domain account.	A custom domain user account must be a member of the local Administrators group and granted the Log on as a batch job and Log on as a service permissions.
SQL Server account	Account with Windows or SQL Server authentication used to connect to the SQL	<p>New database:</p> <p>The dbcreator server role and the db_datareader and public roles for the master database.</p>

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
	<p>Server instance.</p> <p>During the installation, Cygna Auditor will create a database on a SQL Server instance you specify or reuse the existing database. This database will be used to store audit data.</p>	<p>Existing database:</p> <p>The db_owner and public roles for the audit database.</p>


Installation

QUICK TIP: Have you read the [Planning Deployment](#) chapter? Ensure the computer where you plan to install Cygna Auditor has .NET Framework 4.8 (including ASP.4.8) and Web server (IIS) role enabled.

1. Double-click the Cygna Auditor installer to start the setup wizard – in this case, the product will be installed by the currently logged in user. To install Cygna Auditor as another user, press **Shift** and right-click the installer, and then select "**Run as different user**". Make sure to use **domain administrator** credentials for installation.

Make sure to use domain administrator credentials for installation. For more information, see [Account and Permissions Checklist](#).

2. On the **End User License Agreement** page, carefully read the license text and then accept the license terms if you agree with them.
3. On the **Destination Folder** page, review a default installation path (*C:\Program Files\Cygna Labs*) or click **Change** to specify an alternative installation folder.
4. On the **Ready to install Cygna Auditor** page, click **Install**.

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.

Starting the Product

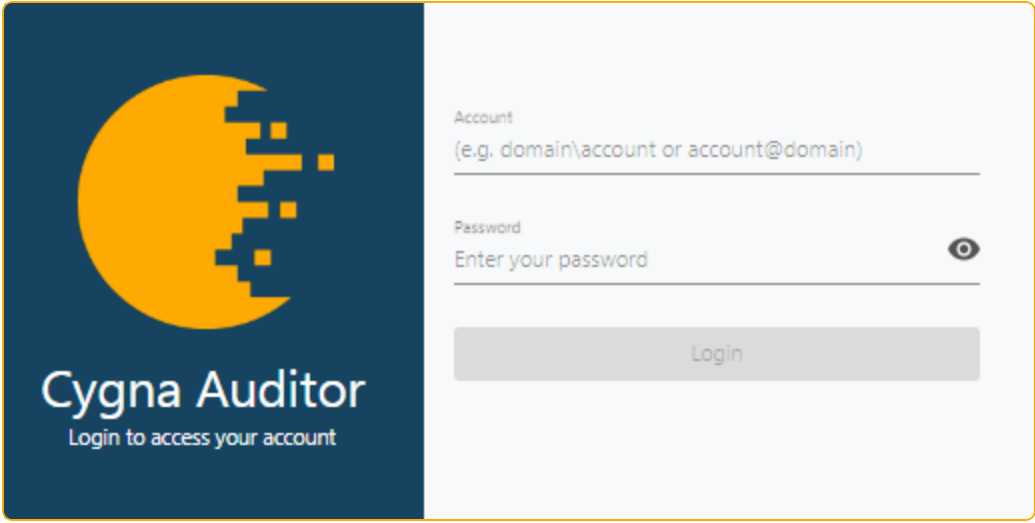
To start Cygna Auditor on a local computer:

- Open a web browser and type "https://localhost/cygna".

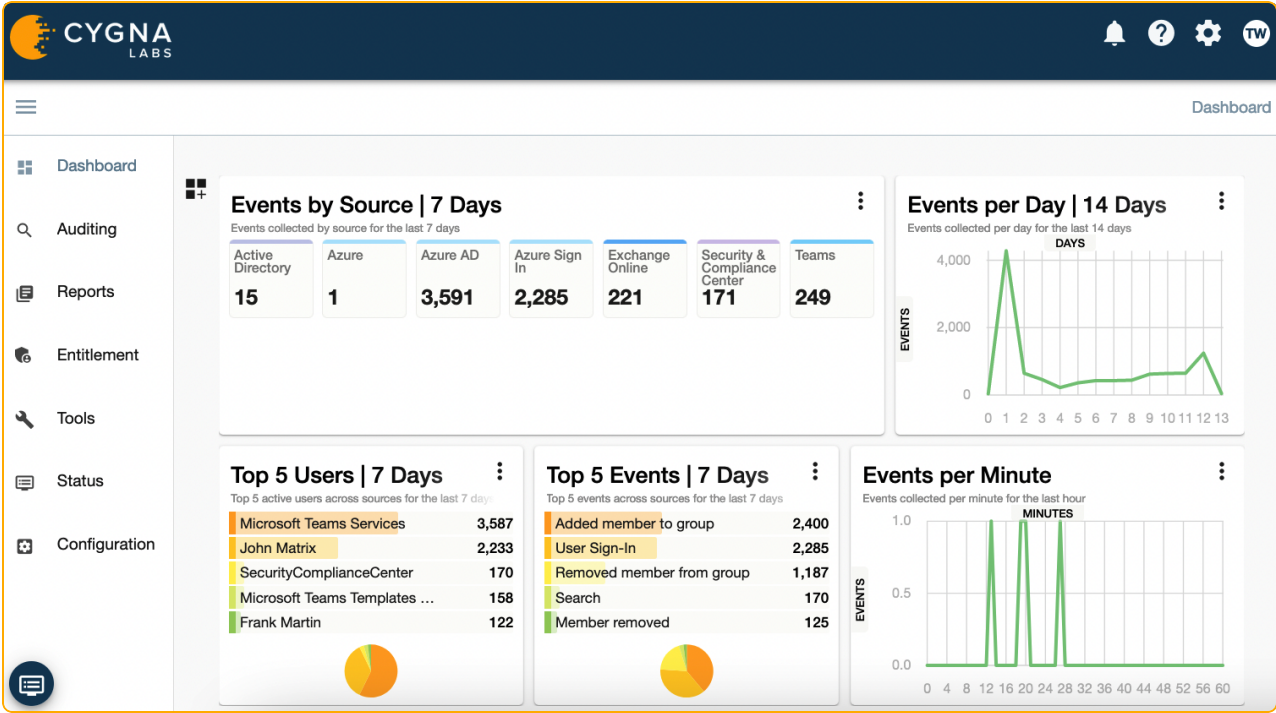
Your current user credentials will be used to log in to the product.

To start Cygna Auditor on any computer in your corporate domain:

1. Open a web browser and type "https://CygnaAuditorMachineName/cygna", where CygnaAuditorMachineName is a name of computer where Cygna Auditor was deployed. For example: *https://cygnaconsole/cygna*.
2. Enter your user credentials.

The image shows the login interface for Cygna Auditor. On the left, there is a dark blue vertical banner with the Cygna Auditor logo, which consists of a yellow circle with a pixelated right edge. Below the logo, the text "Cygna Auditor" is written in white, with the tagline "Login to access your account" underneath. On the right, there is a light gray login form. It contains two input fields: "Account" with a placeholder "(e.g. domain\account or account@domain)" and "Password" with a placeholder "Enter your password" and a toggle icon. Below the fields is a gray "Login" button.

On your first start, you'll be prompted to complete the initial configuration wizard. Later on, after logging in, you will see the dashboard page with the most important auditing metrics as well quick links to product configuration, data collection, and auditing functionality.



QUICK TIP: Cannot log in? Or seeing a message about the lack of permissions?

To protect your audit data, Cygna Auditor restricts access to web-console. By default, only the user who performed installation can operate the product. This user is assigned the Global administrator role and can grant access permissions to others.

Configuration Wizard

Once you install Cygna Auditor, the configuration wizard will start and guide you through the entire setup procedure. Follow the wizard to configure product settings, enable data collection for your audit sources, etc.




Note: You can update these settings later under **Configuration** or by re-running this wizard.

Configuring IIS Application Pool	18
Configuring Database	19
Supplying a License	20
Managing System Settings	21
Configuring Data Collection	23
Managing Delegation	36

Configuring IIS Application Pool


Since Cygna Auditor is a web application, it requires IIS web server to be properly configured. Review and set up the application pool properties.



FIELD	DESCRIPTION
Select Cygna Application Pool	During installation Cygna Auditor creates an application pool called Cygna Labs Web Console but you can select a different pool.
Name	Specify a name and make sure the application pool is started.
.NET CLR version	Ensure you've got the right .NET installed.

FIELD	DESCRIPTION
Managed Pipeline Mode	Set to <i>"Integrated"</i> .
Identity	You can run the application pool as the LocalSystem service account or specify a custom account.
	<p> Note: If you plan to use Windows authentication to connect to the SQL Server, then you have to select this account as the application pool identity.</p> <p>The domain account you specify as a custom account must be a member of the local Administrators group for the computer and granted the Log on as a batch job and Log on as a service permissions.</p>

Configuring Database

Cygna Auditor feeds collected data to the SQL Server database. On this step, configure connection settings and provide access to the database.

FIELD	DESCRIPTION
Enter connection information	
SQL Server instance name	<p>Select the SQL Server instance name from the list or input it in one of the following formats: hostnameinstance (e.g., <i>DemoSQL\SQL 16</i>) or hostname,port (e.g., <i>DemoSQL,1833</i>).</p> <p>Cygna Labs recommends using Standard or Enterprise edition of SQL Server. Express edition is only suitable for evaluation purposes and requires additional configuration steps. For more information, see Cygna Auditor online documentation.</p>
Use Windows authentication	Specify the authentication type and enter credentials.
Use SQL Server authentication	
Account, password	<p> Note: SQL authentication is a recommended method. If you select Windows authentication method, the user</p>

FIELD	DESCRIPTION
	 who runs the installation will be used to access SQL Server. Make sure this Windows account has all the necessary roles on the SQL Server instance and also make sure to check out the Cygna Auditor online documentation.
Connection timeout Connection retry count Connection retry interval	By default, the connection fails if the response time exceeds 15 seconds, Cygna Auditor will attempt to reconnect once after 10 seconds. You can update these settings and set another retry count or timeout time if your network is prone to connectivity issues.
Verify connection information	Click the button to check if the account you specified has sufficient permissions on your SQL Server instance. See Account and Permissions Checklist for more information about server and database roles required.
Configure database	
Database name	Select existing or new database to store audit data.
	 Note: You can leverage an existing database if you used it to store Cygna Auditor data before and want to have access to collected audit data. Since Cygna Auditor will modify the database, specifying the databases employed by other applications is not advised.
Save connection string	
Review database connection settings and save them.	

Supplying a License

On the **Enter product license** step, provide Cygna Auditor license.


Click the key icon and supply the code. Cygna Auditor will verify your license and display its details, including licensed modules, expiration date, number of users, etc.

Managing System Settings

On the **Manage system settings** step, you are advised to configure some of the product's internal properties. You can keep default settings for now and update them later under **Configuration / System**.

Cygna Auditor Service page:

1. Specify the account to run services.
 - Select **Run services as Local System on the computer** to impersonate as the Local System account.
 - Select **Run services as a specified domain user** to utilize any Active Directory account of your choice that has sufficient permissions to log in as a service on a given machine. Make sure to verify credentials.
2. Provide administrative credentials. Making changes to Cygna Auditor platform requires a service restart, Cygna Auditor will use the credentials you specify to automatically update and restart the service. Make sure to verify the credentials.

 **Note:** Make sure the account you specify has sufficient permissions to modify services.

Proxy page:

If your company operates in a regulated industry environment, the proxy server may be required to access resources over Internet. To communicate with Cloud components and collect audit data, Cygna Auditor requires Internet access that can be rerouted through your existing proxy server.

Complete the fields:

OPTION	DESCRIPTION
Use a proxy server for Internet access during data collection	Select the checkbox to enable traffic rerouting.
Server	Specify the proxy server name. To collect Microsoft 365 audit data, allow HTTPS access to the following URLs: cygnacloud.azurewebsites.net (GET and POST) graph.microsoft.com (GET only) login.microsoftonline.com (GET only)

OPTION	DESCRIPTION
	login.windows.net (GET only) *.microsoftonline-p.com (GET only) manage.office.com (GET only) management.azure.com (GET only) To collect AWS audit data, allow access to: *.amazonaws.com (GET and POST) To see online help, you will also need access to: docs.cygnalabs.com. For agent-based Active Directory auditing, allow access to: msdl.microsoft.com/download/symbols msdl.microsoft.com *.core.windows.net (GET)
Port	Specify the port associated with a proxy connection.
Connect to the server as a specific user	Select the checkbox if you want to leverage a specific account when connecting through the proxy server. Provide user credentials.

Notifications page:

To send alert notifications and scheduled reports, Cygna Auditor requires access to SMTP server.

OPTION	DESCRIPTION
Email server	
SMTP server	Specify the SMTP server name—your corporate on-premises or Cloud-based Exchange, or any public SMTP server.
SMTP port	Specify the SMTP port number.
Use SSL	Select the checkbox to connect to your SMTP server over the secured protocol (SSL).
Account name	Provide user credentials for SMTP authentication.
Password	

OPTION	DESCRIPTION
Sender information	
Email	Enter email address as it will appear in the From field.
Name	Enter the name as it will appear in the From field.
Send a test email	Specify a recipient and click Send .

Configuring Data Collection

On the **Configure data collection** step, add sources for auditing. You can update your audit source settings later under **Configuration**.

Supported Sources

SOURCE	VERSIONS
Active Directory	Windows Server 2012 / 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022
Amazon Web Service	n/a
Microsoft Subscriptions	As distributed with Microsoft 365 subscription
On-Premises Exchange	Exchange Server 2016 Exchange Server 2019
VMware	VMware ESXi 6
Windows File System	Windows Server 2012 / 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 8.1 Windows 10 Windows 11

To ensure successful data collection, most sources require some configuration on their side. Check out [Cygna Auditor online documentation portal](#) for more information and detailed instructions.


Did you know? Additionally, by configuring connector to Cygna Auditing & Security Suite (former PowerBroker Management Suite), you can collect enriched audit data from the following data sources: Active Directory, Exchange, File System (including NetApp), and SQL Server.

Active Directory

Active Directory is likely the most critical piece of your IT infrastructure as it keeps your organization together, providing authentication and authorization services, restricting or allowing access to domain resources. Cygna Auditor helps reduce the potential attack surface by keeping the Active Directory activity on radar.

Cygna Auditor tracks activity across your domains and presents it in a user-friendly format. With Cygna Auditor, you will never miss a new group being created in your domain or a user being promoted to administrator.

QUICK TIP: Have you configured your domain for auditing? Check out [Cygna Auditor online documentation portal](#) for more information and detailed instructions. If you want to audit an untrusted domain, make sure you have access to it from the Cygna Auditor application server.

1. Click  to add a new domain.
2. Complete the domain auditing configuration. Generally, Cygna Auditor provides you with two auditing methods, one employing a non-intrusive monitoring service on your domain controllers and the other relying on event logs.

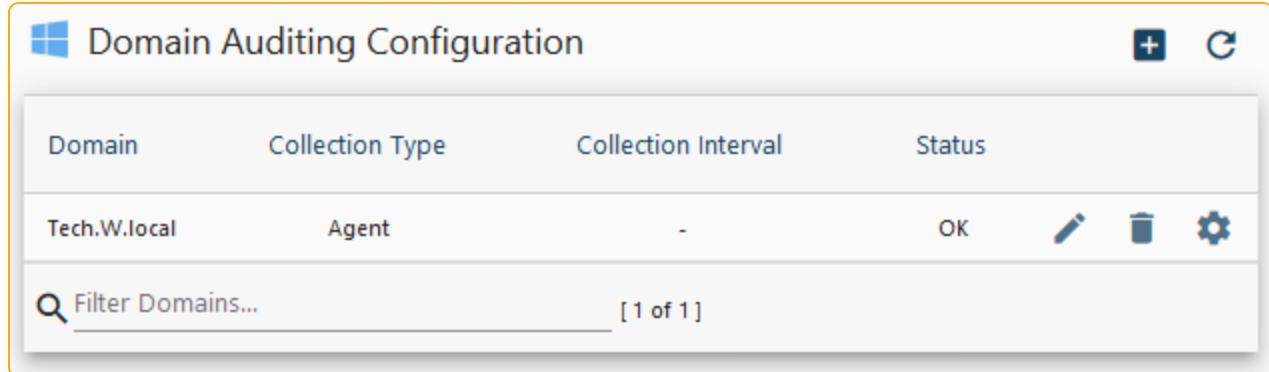
OPTION	DESCRIPTION
Domain Selection tab	
User name	Enter the user credentials. Specify a user name in the following format: domain\username.
Password	Cygna Auditor will use this account to collect audit data from the domains this account has access to. If you specified event log-based auditing, make sure the account has access to domain controllers' event logs.
Domain	By default, the domain where Cygna Auditor is

OPTION	DESCRIPTION
	<p>deployed is specified for auditing. To search for other domains in the forest, enter domain name in the search field and click the loop icon.</p>
Collection Settings tab	
Data collection method	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Cygna Auditor Agent (preferred) • Event log
Combine similar events occurring within the specified interval	<p>Select this option and set the interval (default, 5000 ms) to reduce the number of events written to the database. For example, when the same users performs the same action multiple times within a short period of time, Cygna Auditor will make a single entry in the audit database.</p> <p>If this option is cleared, Cygna Auditor will capture a record for each event.</p>
Attempt to locate workstation information for events	<p>Enable this option to collect originating workstation data—get supplemental information about the workstation from which the action was performed. This information can help troubleshoot security incidents.</p>
Perform reverse name lookup when event only include an IP address for the remote workstation	<p>Select to try identifying a DNS name of a remote workstation.</p>
Ignore login events	<p>Select to skip login events from processing.</p>
Enable nested group alerting and auditing	<p>Select this option to report changes to child groups. For example, when a nested group is removed, you will see a change event for the parent group as well. A user removal from a child group isn't reported for a parent group.</p> <p>Select Manage nested groups and specify groups in the pop-up window. Expand Advanced collector settings to configure</p>

OPTION	DESCRIPTION
Advanced collector settings	<p data-bbox="776 270 1386 302">additional options for nested group auditing.</p> <p data-bbox="776 338 1365 407">Expand this section to configure additional settings if necessary.</p> <ul data-bbox="805 436 1438 1841" style="list-style-type: none"> <li data-bbox="805 436 1386 541">• Exclude attributes from data collection—enter a list of attributes separated by commas. <li data-bbox="805 571 1409 602">• Select the Ignore login events checkbox. <li data-bbox="805 632 1430 663">• Set up GP backup configuration, including: <ul data-bbox="862 688 1438 974" style="list-style-type: none"> <li data-bbox="862 688 1438 835">• Enabling GPO backup for detailed change reporting—with its help you'll be able to see changes in group policy objects over time. <li data-bbox="862 865 1414 974">• Ensuring all GPOs have at least one backup—it gives you ability to see and revert changes at all times. <li data-bbox="805 1003 1365 1150">• If nested group alerting and auditing is enabled, specify details for reporting changes in the Nested group auditing settings section. <ul data-bbox="862 1180 1430 1841" style="list-style-type: none"> <li data-bbox="862 1180 1386 1369">• Process nested changes for non-group objects—e.g., if a user gets removed from a child Group 3, this event will be reported both for child Group 3 and parent Groups 1 and 2. <li data-bbox="862 1398 1409 1587">• Cascade nested group members when adding a group—e.g., if an intermediate Group 2 is removed, the event is recorded both for the parent Group 1 and its nested Group 3. <li data-bbox="862 1617 1430 1841">• Cascade nested non-group object members when adding a group—e.g., if an intermediate Group 2 is removed, the event is recorded both for the parent Group 1 and its nested Group 3. For Group 3 users, an event will be

OPTION	DESCRIPTION
	<p>generated that they were removed from the top level Group 1.</p> <ul style="list-style-type: none"> • Generate backlink events for nested group changes—by default, events are generated for parent objects. Disable to get events only for child changes. • Set the logging level.
Domain Controllers tab	
Show all domain controllers	By default, Cygna Auditor installs its agents on all domain controllers. To customize where to install them, toggle this option and select discovered DCs from the list.

The domains you configured for auditing will appear in the list, with status and data collection frequency for each domain. Click on the domain name to see agent's status for each specific domain controller. Click on the gear icon for quick access to other configuration actions.



Continue reading:

[Dashboard](#)

[Auditing](#)


[Reports](#)

Amazon Web Services

Amazon Web Services is so far the platform of choice for hosting applications and delegating IT administration tasks. It helps save on maintenance costs of on-premises servers and provides cloud computing resources to cater to your company needs.

Cygna Auditor for AWS enables you to track changes to Amazon Identity and Access Management (IAM) configuration, that is an integral part of AWS infrastructure.

By default, Cygna Auditor audits the entire IAM but you can configure it to collect data from a single IAM as several collectors, for example, set up data collection for each AWS region within your IAM separately.

1. Click  to add a new AWS configuration.
2. Complete the auditing configuration:

OPTION	DESCRIPTION
The General step	
Enable this collection	Select the toggle to turn on data collection. You can disable data polling any time without deleting a collector.
Name	Add a name to distinguish one AWS collector from the other. This name will be used internally in Cygna Auditor
Description	(Optional) Add there any further details about current configuration.
The Amazon API Credentials step	
Access key Secret key	Provide your AWS authentication keys, check your AWS account for more information.
Authorized region	Select one or more Amazon regions where your services reside. These regions will be used to provide access to the AWS API and continue with the configuration steps. It must be regions authorized for the Amazon account.
Verify connectivity	<p>Click to check that the AWS API functions for Elastic Cloud Compute (EC2) and Cloud Trail are accessible. These functions are used during configuration and data collection. The connectivity is checked for each region authorized for the account.</p> <p>If you have configured proxy settings, those settings will be used to test connectivity. If a proxy server is used without those proxy settings, access has to be provided outside of Cygna Auditor.</p>
The Collector Settings step	


OPTION	DESCRIPTION
Collection Interval	Specify the duration (in minutes) between event collections.
Initial Collection Interval	Specify the length (in days) of the event backlog to collect the first time the collector runs. Cloud Trail - The name of the cloud trail
Store Interval	Specify the amount of time (in seconds) the collector queues events for storage in the database. The default is recommended.
Cloud Trail	Provide a name of cloud trail in the in Amazon Resource Name (ARN) format. Enter the whole name or start typing and search for trails.
Verify Trail Access	(Optional) Check that the cloud trail and its associated S3 bucket are accessible prior to data collection with the credentials and region provided.
The Ignored Events step	
Ignored Events list	Add the names of events you wish to ignore during event collection. By default, Cygna Auditor suggests to ignore some common “noise” events. These entries can be retained or discarded.
The Summary step	
Summary	Review the data collection details before saving them.

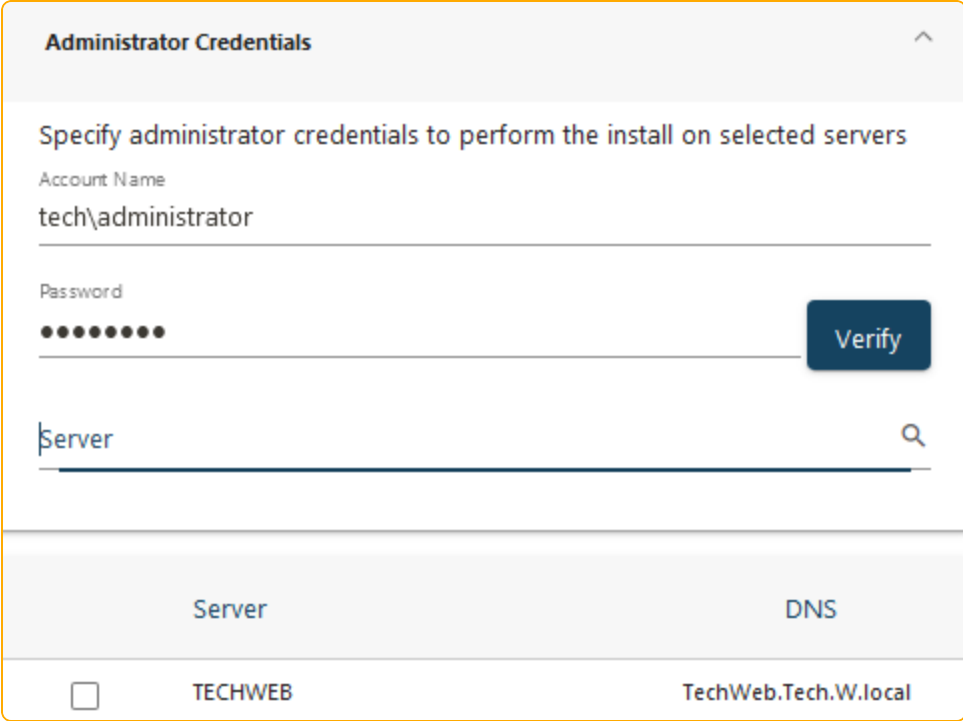
Windows File System

Cygna Auditor helps you secure your business critical assets such as important files and folders stored on your Windows servers and shared resources.

Cygna Auditor notifies you on both successful and failed actions thus allowing you to identify unusual activity peaks or unauthorized access attempts, and mitigate these risks immediately. The reports shipped with the product are designed to help you prove compliance with various security standards and regulations, including PCI and GDPR.


Agent Deployment

1. Click  to add servers for auditing. To collect data, Cyigna Auditor needs to deploy an auditing service on each server you want to audit. The drivers are non-intrusive and will not affect the server operability.
2. In the dialog that opens, provide administrator credentials. Cyigna Auditor will look up for servers and show the list of available servers. Select servers you want to audit and click **Install**.



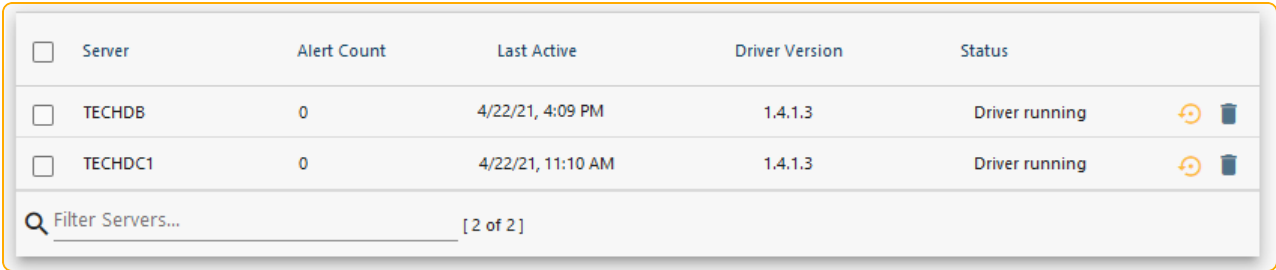
The dialog box titled "Administrator Credentials" contains the following elements:





- Header: Administrator Credentials
- Instruction: Specify administrator credentials to perform the install on selected servers
- Account Name field: tech\administrator
- Password field: masked with 10 dots
- Verify button: A dark blue button labeled "Verify"
- Server search field: A text input field with "Server" and a search icon
- Table with columns: Server, DNS
- Table content: A row with a checkbox, "TECHWEB", and "TechWeb.Tech.W.local"

 **Note:** On these servers, enable the following inbound firewall rules: **Netlogon Service (NP-In)**, **File and Printer Sharing (SMB-In)**, and **File Server Remote Management (SMB-In)**.

3. Cyigna Auditor will suggest you add data collection filters.

Check the data collection status in the audited servers list.



<input type="checkbox"/>	Server	Alert Count	Last Active	Driver Version	Status	
<input type="checkbox"/>	TECHDB	0	4/22/21, 4:09 PM	1.4.1.3	Driver running	 
<input type="checkbox"/>	TECHDC1	0	4/22/21, 11:10 AM	1.4.1.3	Driver running	 

Filter Servers... [2 of 2]


Configure Monitoring Filters

Filters help you narrow down the number of events collected and processed by Cygna Auditor. Typically, file system generates thousands of events, mostly read events, processing all of them may have significant impact on your network bandwidth as well as Cygna Auditor server performance. Create filters to audit and process the events you are interested in (such as create, delete, etc.) and skip others.

1. Provide a name for a filter and description.
2. Add filtering criteria and define exceptions if necessary. For example:

General	Filters	Exclusions
<input checked="" type="checkbox"/> What	Condition is any of	What ▼ Create, Delete, Rename... ▼
<input checked="" type="checkbox"/> Folder	Condition is	Folder ▼ C:\Documents
<input checked="" type="checkbox"/> Servers	Condition is any of	Servers ▼ TECHDB, TECHDC1 ▼

Configuring File System Agent Settings to Allow Access to SQL Server with Windows Authentication

 **Note:** This step is only required if you use Windows authentication on your SQL Server.

To ensure the agent feeds audit data to your Cygna Auditor database, make sure it has sufficient permissions on your SQL Server instance.

For each file server where the agent runs, do the following: On SQL Server, create a login for each computer account (*domain\computeraccount\$*) and assign it the **db_owner** and **public** roles for your Cygna Auditor database.

If you plan on auditing the server where the Cygna Auditor database resides for file changes (it means the File System agent will connect to a local SQL Server instance) and you prefer Windows authentication, then grant database access to **NT_AUTHORITY**.

Continue reading:

[Dashboard](#)

[Auditing](#)


[Reports](#)

On-Premises Exchange

On-premises Exchange remains a critical piece of business infrastructure that provides messaging, task management, and contact management services. Cygna Auditor helps you supervise activity on your on-premises Exchange Server and ensure all security controls are in place and data is protected.

Cygna Auditor tracks activity across your Exchange organization, including changes to mailboxes made by non-owners. The data is presented in a user-friendly format. With Cygna Auditor, you will never miss unauthorized access or changes to mailbox. The product allows auditing up to 2500 mailboxes per Exchange organization with no limits for auditing administrative and configuration events.

QUICK TIP: Have you configured your Exchange Server for auditing? Check out [Cygna Auditor online documentation portal](#) for more information and detailed instructions.

1. Click  to add a new Exchange organization.
2. Complete the Exchange auditing configuration.

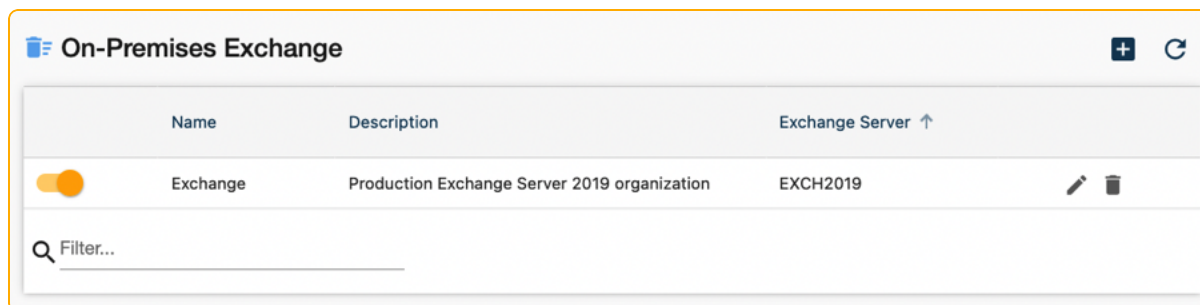
OPTION	DESCRIPTION
General tab	
Enable collector	Switch the toggle to "On".
Name	Provide a name. It can be your Exchange Server name or any title to help it distinguish from other on-premises Exchange collectors.
Description	Provide a description (such as the Exchange version, location, etc.)
Exchange Server tab	
Account name, password	Enter the user credentials. Specify a user name in the following format: domain\username. Cygna Auditor will use this account to collect audit data from the Exchange organization.
Exchange Server	Provide an Exchange Server name.
Authentication mechanism	Specify the auth method and verify connection.
Collection Schedule tab	

OPTION	DESCRIPTION
Create a collection schedule	Select to add a new schedule. You can create several schedules if needed.
Enable scheduled job	Switch the toggle to "On".
Name	Specify a name of the schedule.
Description	Provide a description.
Frequency	Cygna Auditor provides multiple options: one-time, minutes, hours, days, Monday-Friday, weekly, bi-weekly, monthly, quarterly, annually. Select how often to perform data collection depending on your auditing needs.
Start date	Choose when to start collecting data: immediately or specify a date.
End date	Specify an end day for the data collection schedule if necessary or set to "Never".

Summary tab

Review your auditing configuration and save it.

The Exchange organizations you configured for auditing will appear in the list.



Continue reading:


[Dashboard](#)

[Auditing](#)


[Reports](#)

Microsoft 365

Cloud infrastructure requires as much attention as on-premises. With Cygna Auditor, you can secure your data stored in SharePoint Online and OneDrive for Business, trace activity in Teams, and gain transparency in your Azure AD and Exchange Online operations and permissions. Cygna Auditor helps you detect potential threats and mitigate risks of attacks aimed at your Microsoft Subscription and Microsoft 365 apps.

1. Click  to add a Microsoft 365 organization.
2. **Authorize** yourself to deploy the Cygna Labs application in Microsoft 365. The user you specify must have sufficient permissions to deploy applications in Microsoft 365, i.e. be granted the **Global administrator** role in your Azure AD domains.

If you are interested in auditing Azure AD and performing recovery operations, perform additional configuration step. See Online help.

3. Specify the polling interval. By default, 10 minutes. This value controls how often Cygna Auditor will check for updates in your Microsoft 365 apps.
4. Ensure the Enabled column is active .
5. Check connectivity. Click **Verify** to ensure Cygna Auditor has access to these resources:

cygnacloud.azurewebsites.net (GET and POST)

graph.microsoft.com (GET only)



login.microsoftonline.com (GET only)

login.windows.net (GET only)

*.microsoftonline-p.com (GET only)

manage.office.com (GET only)

management.azure.com (GET only)

Name	Last Event	Last Active	Polling Interval	Enabled	Status
Cygna Labs LLC	9/2/20, 7:38 AM	9/2/20, 9:06 AM	3		OK
 Internet connectivity has been verified					

Once you configure Microsoft Subscription settings, data collection will start automatically for Azure AD including sign-in monitoring, Exchange Online, SharePoint Online, etc.

Continue reading:

[Dashboard](#)


[Auditing](#)

[Reports](#)

VMware

Most businesses rely on virtual infrastructure nowadays, it's crucial to monitor virtualization systems in addition to physical workstations. Cygna Auditor helps you stay on top of changes and protect your assets.

Cygna Auditor tracks activity on VMware vCenter Servers and ESXi hosts and presents it in a user-friendly format.

1. Click  to add a server.
2. In the pop-up dialog that opens, complete the fields:

OPTION	DESCRIPTION
Server	Enter the name of the VMware vCenter Server or ESXi host.
Account	Enter the user credentials.
Password	
Interval	Set the data collection frequency.
Ignore certificate	Select the checkbox if you prefer to skip the SSL certificate verification.

Continue reading:[Dashboard](#)[Auditing](#)[Reports](#)

PBMS

Cygna Auditor provides an option to feed data collected by Cygna Auditing & Security Suite (former PowerBroker Management Suite) to Cygna Auditor and make it available for auditing search and reports.

Before you start:


Ensure data collection is configured in Cygna Auditing & Security Suite.

To configure connection:

1. Specify connection details:


OPTION	DESCRIPTION
SQL Server instance name	Provide the name of the instance where Cygna Auditing & Security Suite stores collected data.
Authentication method	Choose Windows or SQL authentication to connect to the database.
Account, password	Provide credentials. The account you specify must have sufficient permissions to access data.
Initial catalog	Specify the PBMS database.
Connection timeout, retry period	Update values if necessary.
Verify connection string	Make sure to verify connection.

Once configured, Cygna Auditor will be able to access data collected by PBMS and show it in Auditing search, reports, etc.

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.

Managing Delegation

To secure collected audit data and ensure that only authorized personnel can review it and update auditing configuration, Cygna Auditor enables you to delegate access within the product. On this step, review built-in roles and then assign them to users.

 **Note:** You can also create custom roles. For more information on how to review current role assignment, delegate access and add more roles, see [online documentation](#).

Auditing & Tools

Cygna Auditor brings you insight and much needed transparency into activity in your organization, no matter how big or small, on-premises or in the Cloud. As simple as it sounds, Cygna Auditor outlines who made the change, when it was made, and what has been changed on a high level and in details.

The screenshot shows the Cygna Auditor interface. The top header features the Cygna Labs logo. A sidebar on the left contains navigation links: Dashboard, Auditing, Reports, Tools, Status, and Configuration. The main content area is titled 'Event Auditing' and shows a notification: 'Event auditing has 1 active filter'. Below this is a table with the following data:

When	Source	What	Who
Aug 19, 2020, 11:26:52 AM		User Sign-In	Roy Batty
Aug 19, 2020, 11:09:00 AM		Collecting	Cygna Auditor
Aug 19, 2020, 8:09:00 AM		Collecting	Cygna Auditor
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart

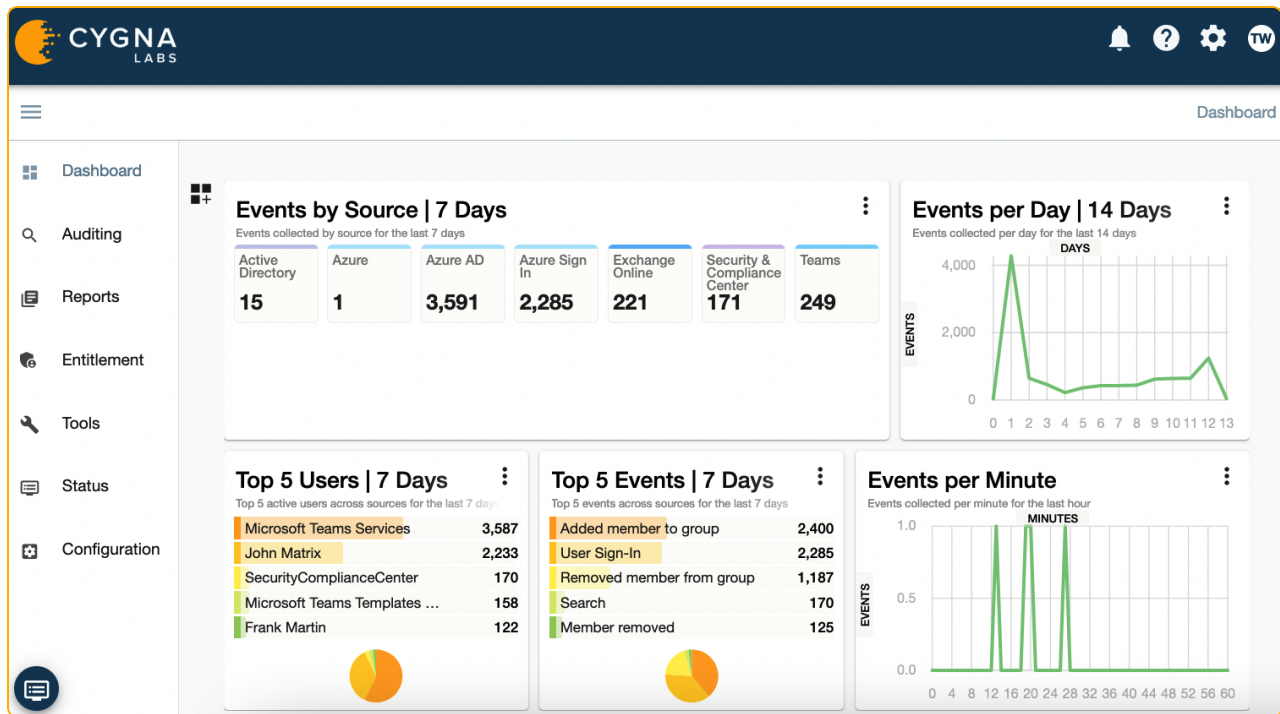
The following features help you keep all changes on your security radar and mitigate risks as they occur:

FEATURE	WHAT IS IT GOOD FOR?
Dashboard	Getting an activity digest. Dashboard widgets provide a visual overview of your audit sources and help you check that everything goes well and no unusual activity was detected.
Auditing	<ul style="list-style-type: none"> • Reviewing activity • Searching for a specific events

FEATURE	WHAT IS IT GOOD FOR?
Reports	<ul style="list-style-type: none">• Digging into security incidents• Investigating user actions from multiple sources• Focusing on event chains—subsequent events leading to a breach or security issue• Identifying potentially harmful users and security breaches in your environment <ul style="list-style-type: none">• Analyzing your environment structure and safe activity patterns across the entire organization• Identifying potential bottlenecks and their impact on your organization• Proving compliance with security standards and regulations (PCI, HIPAA, SOX, etc.)• Passing internal and external audits• Detecting threats as they occur and alerting. Alerts are sent immediately as a potentially harmful action is detected and processed by the product.

Dashboard

The dashboard is the first thing you see in Cygna Auditor. It provides a quick and clear overview of activity for all your audit sources. With live widgets, you can check that everything goes well and activity stays within the safe level. Unlike detailed reports and search queries, widgets give you a bird's eye view of your environment. To drill down to details, click on a chart to open an auditing search with a preset filtering.



On the dashboard, you'll get information:

- How many events occurred per each source
- Who made the most changes
- What is the most common event
- How many event typically occur per hour and day

Auditing

Get the data at your fingertips with Auditing—review activity from all sources in one place, identify rogue users, and detect potential threats throughout your environment. Security analysis is much easier when you are not limited to a certain source and see a bigger picture.

To review activity in your environment and start creating data searches, go to **Auditing**. You will see all changes right away. Switch to the **View summary** tab to get an overview of activity or stay on the **Add/Remove filters** tab and narrow down your search to what bothers you the most. Show or hide data you are interested in by toggling columns in **Add/Remove columns**.

Creating an auditing query is as easy as asking yourself a question. Cygna Auditor will find the matching records in its audit database and show them on the screen on the fly.





Learn about interpreting results here: [Reading Records in Auditing](#).

Auditing search is versatile and in most cases there are multiple ways to get the data you are looking for. Depending on the task you want to accomplish, use one of the following search techniques:

- [Reviewing All Changes](#)
- [Searching for Specific Events](#)
- [Excluding Bias](#)
- [Distilling Results](#)

You can use these techniques interchangeably or supplementing each other. A good idea is to start with all changes on the screen and then drill-down to more specific events.

Additional options are located on the top of the filters:

-  If you like the search you created, you can save it as a report to use it later. See [Reports](#) for more information.
-  Export and download results
-  Change the columns visibility
-  Refresh and re-query

Reading Records in Auditing

Each record includes a date when the activity took place, the source, what was made, the user who made the change, and the item or object that was affected.

CYIGNA LABS

Event Auditing

Event auditing has 1 active filter

When	Source	What	Who
Aug 19, 2020, 11:26:52 AM		User Sign-In	Roy Batty
Aug 19, 2020, 11:09:00 AM		Collecting	Cyigna Auditor
Aug 19, 2020, 8:09:00 AM		Collecting	Cyigna Auditor
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart

And more:

- **Source-specific details:** To get more information, click on the record—the details will expand on the right. Here you will see the data specific to your source. For example, the folder name for File System, AD DN for Active Directory, a tenant name for Azure AD, or identity name for AWS.


Sep 22, 2020, 8:28:08 PM		Created folder	Bradley Cooper	<p>SharePointOnline Event Details</p> <hr/> <p>Who</p> <p>User Address Bradley Cooper (bcooper@cygnacore.onmicrosoft.com) 52.114.168.38</p> <p>When</p> <p>Date Tuesday, September 22, 2020 at 8:28:08 PM GMT+03:00</p> <p>Where</p> <p>Tenant Cyigna Labs LLC</p> <p>What</p> <p>Event Description Path FolderCreated User creates a folder on a site. Shared Documents</p>
Sep 22, 2020, 8:27:19 PM		User Sign-In	Bradley Cooper	
Sep 22, 2020, 8:27:02 PM		User Sign-In	Bradley Cooper	
Sep 22, 2020, 8:27:02 PM		User Sign-In	Bradley Cooper	
Sep 22, 2020, 8:16:16 PM		Sent message using Send As permissions	William Stuart	
Sep 22, 2020, 8:06:11 PM		Sent message using Send As permissions	William Stuart	
Sep 22, 2020, 7:54:10 PM		Sent message using Send As permissions	William Stuart	
Sep 22, 2020, 7:51:49 PM		User Sign-In	Bradley Cooper	
Sep 22, 2020, 7:44:10 PM		Sent message using Send As permissions	William Stuart	
Sep 22, 2020, 7:32:09 PM		Sent message using Send As permissions	William Stuart	


- **Rollback:** Expand details and recover Azure AD changes based on data from the backup snapshot.

The screenshot displays the 'Event Auditing' interface. On the left, a table lists events with columns for 'When', 'Source', and 'What'. The 'What' column for the selected event shows a red triangle icon, indicating a failed attempt. The right pane, titled 'Azure AD Event Details', provides further information:

- Who:** User: Microsoft App Access Panel
- When:** Date: Tuesday, May 17, 2022 at 5:31:57 PM GMT+03:00
- Where:** Tenant: Cygna Labs LLC
- What:**
 - Event: Update user
 - Description: Administrator changes one or more properties of a user account. For a list of the user properties that can be updated, see the "Update user attributes" section in Azure Active Directory Audit Report Events
 - Item: John Matrix
- Changes:** A table with columns 'Attribute Name' and 'Value'.

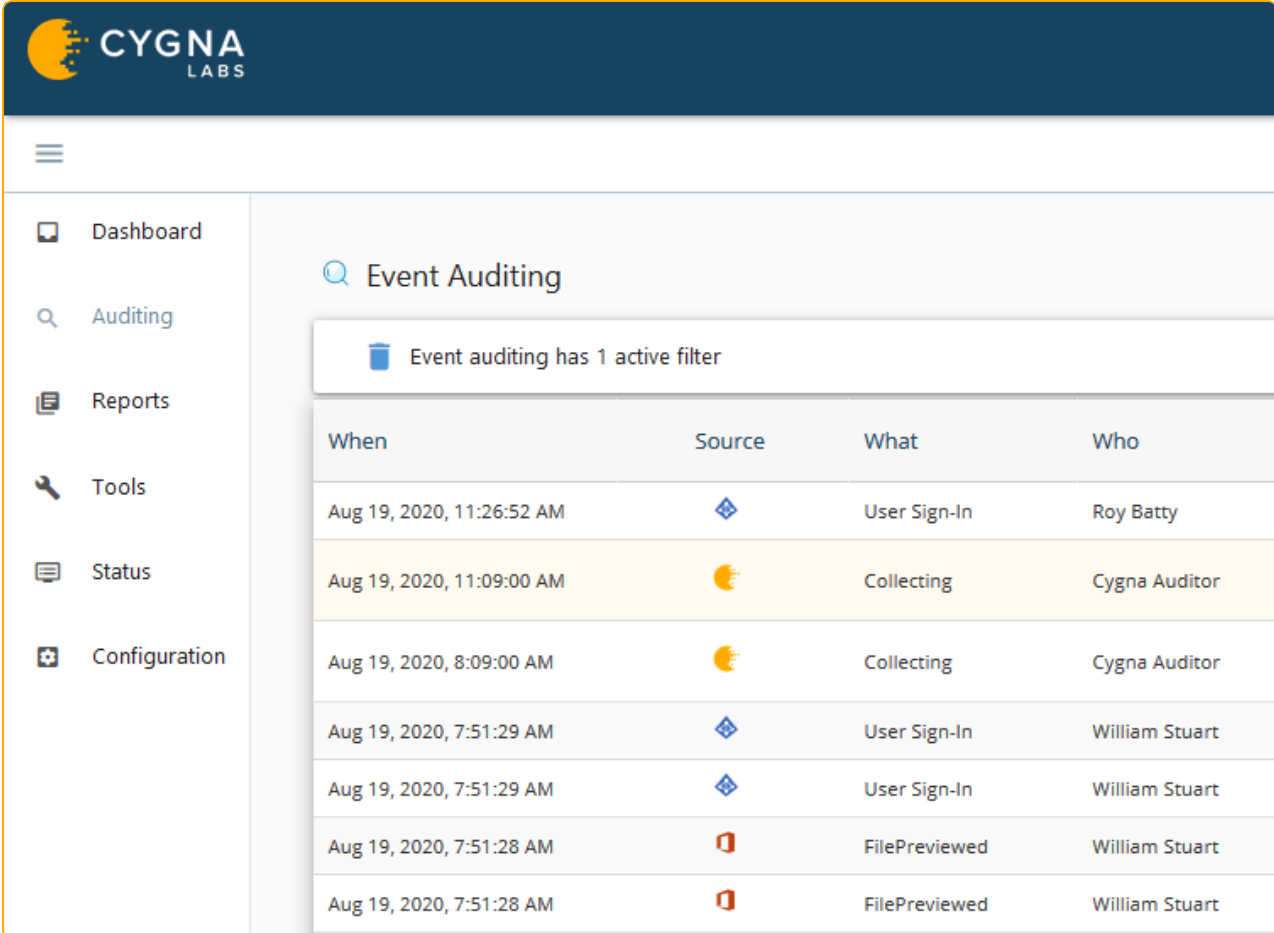
At the bottom right of the interface, there is a 'Rollback' button.

- **Failed attempts:** The sign  next to *What* indicates that the attempt to perform the action has failed. The **Action result** column also notifies you about the outcome.

 **Note:** You might see several records with events that occurred at the same time up to seconds—for example "create user" with subsequent "modify user". Typically they represent a single, one-time action. The reason why Cygna Auditor displays it as several records is that Windows actually generates several events in response to your actions.


Reviewing All Changes

To have a look on whats' going on in your corporate environment, go to **Auditing** and start browsing changes. Reviewing all records is handy if you want to execute control over your data flow.

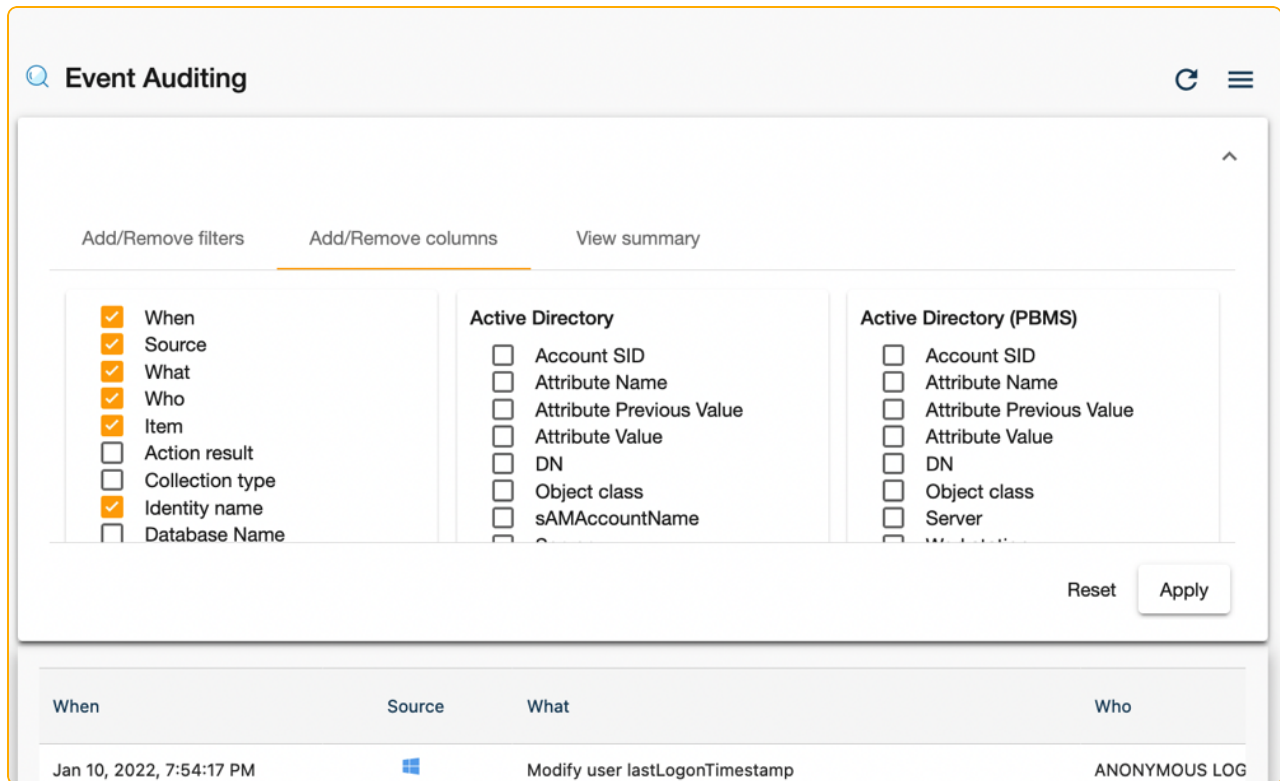


When	Source	What	Who
Aug 19, 2020, 11:26:52 AM		User Sign-In	Roy Batty
Aug 19, 2020, 11:09:00 AM		Collecting	Cygna Auditor
Aug 19, 2020, 8:09:00 AM		Collecting	Cygna Auditor
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:29 AM		User Sign-In	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart
Aug 19, 2020, 7:51:28 AM		FilePreviewed	William Stuart

If you are interested in some particular changes, you can construct a search query by adding search conditions or adjust your search right from the data pane.

By default, Cygna Auditor displays 1,000 newest events to ensure you can review the latest changes across all audit sources you are authorized to work with. To update this setting, go to  **Application Settings** and set the **Audit Event Limit** to a new value.

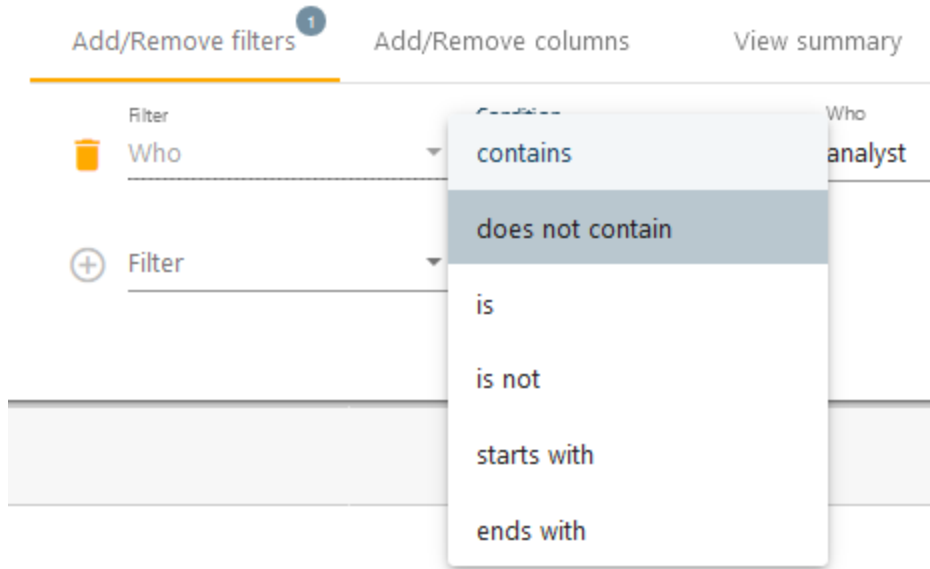
To toggle column (such as Whats, Action result, Source), go to the **Add/Remove columns** tab and check the columns you want to see. I.e., you can hide certain columns from the table view. Note that Cygna Auditor stores all data and you can always review a complete audit record in **Details**. Some of the columns are general and available for all data sources (when, who, etc.) but others are source-specific.



Searching for Specific Events

If you are looking for specific events, e.g., changes to user groups, activity on a certain server performed by a single user, it does not make sense to review all change records. You can jump right to inspecting changes you are interested in. With flexible search parameters, you can construct a search query that fits your auditing needs.

The search conditions describe what you are looking for. Each entry consists of three fields: the filter, the match type, and the value. You can add as many search entries to your search as you want, Cygna Auditor will look for records that match all search conditions at once.



FIELD	DESCRIPTION
Filter	<p>The filter corresponds to the type of information you are searching for. For example, <i>user</i>, <i>server</i>, or <i>when</i>.</p> <p>Some filters are specific to the source, e.g., <i>mailbox folder</i> is for Exchange Online only and <i>region display name</i> is for AWS only. Such filters are grouped under the data source name.</p> <p>If you are paying attention to the activity outcome, if the change action was successful or failed, you can leverage the <i>Action result</i> filter.</p>
Match type (comparison operator)	<p>The match type defines if you are looking for an exact entry (<i>is</i>) or for any entry containing the searched value (<i>contains</i>). You can also search for an entry that <i>starts with</i> or <i>ends with</i> a certain value. The exact and broad search can be negative as well (<i>is not</i> and <i>does not contain</i>).</p> <p>When you are searching for sources, you can leverage the following match types: <i>is any of</i> and <i>is not any of</i>. They enable you to specify several sources from the list and to search for changes in any of these sources or in all sources except selected correspondingly.</p> <p>When filtering events by time (the <i>When</i> filter), you can choose from the following match types: <i>is today</i>, <i>is after</i>, <i>is before</i>, <i>is between</i> for time range, and <i>is in the last X days</i>.</p>
Value	<p>The value field is the area where you specify a value to be searched. For example, the name of a user or a date range.</p>

FIELD DESCRIPTION

Depending on the filter, you can select a value from the drop-down list or enter it manually.

You customize your search query on the go and delete entries you no longer need by clicking the red cross next to the line you'd like to delete.

EXAMPLE :

Add/Remove filters ³ Add/Remove columns View summary

Filter	Condition	
When	is after	Date is after (yyyy-mm-dd): 9/20/2020
Source	is any of	Source Azure AD
Who	is not	Search users Admin

Here, Cyigna Auditor will search for records that match all these conditions at once (i.e., logical AND is applied):

- Any activity (since no specific actions were selected)
- Performed by any user whose name isn't "admin"
- That happened after September 20, 2020
- Coming from the Azure AD source

When	Source	What	Who	Item
Sep 22, 2020, 5:29:41 PM		Added member to group	Bradley Cooper	Darren Hardy
Sep 22, 2020, 5:29:22 PM		Add owner to group	Bradley Cooper	Ellen Ripley
Sep 22, 2020, 2:00:53 AM		Added member to group	Bradley Cooper	Joe Johnson
Sep 21, 2020, 10:54:52 PM		Updated group	Bradley Cooper	







Excluding Bias

As you audit changes, you may want to hide some events that are irrelevant for now. For example, you may want to exclude service accounts from your search. Cyigna Auditor

enables you to adjust your search on the fly, right from the pane that displays data. Cygna Auditor will add search conditions accordingly and update search results immediately.

To exclude data you are no longer interested in seeing, hover a mouse over the cell containing this piece of data and click the red minus icon. Cygna Auditor will hide all entries containing the data you specified.

This technique is handy if you have too much bias in your search results, e.g., activity generated by system accounts or thousands of "open" actions.

When	Source	What	Who
Sep 22, 2020, 2:59:15 PM	Filter  	Open folder	William Stuart
Sep 22, 2020, 2:59:15 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:15 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:13 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:10 PM		Open folder	William Stuart

Distilling Results

As you audit changes, you may want to hide some events that are irrelevant for now and focus on those that matter the most. For example, once you have the general understanding of activity in your environment, you may want to examine some events more closely. Cygna Auditor enables you to adjust your search on the fly, right from the pane that displays data. Cygna Auditor will add search conditions accordingly and update search results immediately.

To narrow down your search results to events of a certain type, e.g., made by a certain user account or specific changes, hover a mouse over this piece of data, and select the green plus icon. In this case, Cygna Auditor will limit the search to entries containing the value you specified.

This technique will be handy for you if you prefer to move from a broad search to individual events or when you discover a potentially harmful activity and want to explore similar events. For example, you found that some non-administrative user modified a group in your Active Directory domain. To facilitate further security investigation, you include this user to your search to see all changes this user made. You can repeat this "narrow down" technique over and over again until you distill the changes you are looking for.

When	Source	What	Who
Sep 22, 2020, 9:44:10 PM		Sent message using Send As permissions	William Stuart
Sep 22, 2020, 9:42:58 PM		User Sign-In	Bradley Cooper
Sep 22, 2020, 9:34:10 PM		Sent message using Send As permissions	William Stuart
Sep 22, 2020, 9:32:13 PM		Sent message using Send As permissions	William Stuart
Sep 22, 2020, 9:32:10 PM		Sent message using Send As permissions	William Stuart

Reports

The expert security team of Cyigna Labs designed and prepacked Cyigna Auditor with a set of auditing reports. With their help, you pass compliance audits (PCI, HIPAA, GDPR, etc.) as well answer most everyday security administration questions such as "were there any changes to security groups?" or "what users got their passwords reset?"

For your convenience, the reports are grouped by data source and by compliance standard. On top of that, Cyigna Auditor reports about its health state with **Infrastructure** and **Security & Compliance Center** reports.



The screenshot shows the Cyigna Auditor web interface. The top navigation bar includes the Cyigna Labs logo and utility icons. A sidebar on the left provides navigation for various system components. The main content area is titled 'Reports' and lists several Active Directory-related reports. A context menu is visible over the reports, offering actions such as Alerts, Clone, Edit, Export, Manage Delegation, Run, and Schedule.

To view a report:

1. Navigate to **Reports**.
2. Select a report. Cygna Auditor will search for events that match report's filters and display them. The builtin reports are read-only but you can apply additional filters to custom reports or clone builtin reports in order to further modify them.

For each report, you can:

- Configure alerts to receive notifications every time the event occurs
- Clone the report
- Schedule a report delivery
- Grant or restrict access to this report through the delegation
- Export results

 **Note:** By default, Cygna Auditor displays 2,500 newest events to ensure you can review the latest changes across all audit sources you are authorized to work with. To update this setting, go to  **Application Settings** and set the **Report Event Limit** to a new value.

Built-In Reports

The built-in reports work out of the box. They do not require any modifications. Just schedule regular reviews with your security response team and keep track of activity and changes in your business critical systems. Browse the list or filter reports by tags. Built-in reports can't be modified but you can add additional filters while browsing the report data.

Custom Reports

Each organization is unique and has specific needs and metrics to track that cannot be covered by build-in reports. Looking beyond the compliance reports specific to the audit source, Cygna Auditor enables you to create custom cross-system reports from scratch or leverage preset reports as customizable templates. To learn more, see [Creating a New Report](#).

Continue reading:


[Creating a New Report](#)


[Subscribing to Reports](#)

[Alerting](#)

Creating a New Report


Flexible filters of Auditing search can be a great tool for internal auditors and security officers who need to analyze activity patterns and detect threats across the entire environment. Unlike one-off searches constructed from scratch every time, custom reports are preserved in Cygna Auditor so that you and your colleagues can use them later.

You can convert your search into a report right on the **Auditing** page or go to **Reports** and click  **Create** to set up a new report. Alternatively, select options next to a report and choose **Clone** to create a copy of a built-in report that you can modify.

- On the **Edit report details** tab, add the report name and description. You can make the report private (available only to you) and specify tags that allow to find it faster.
- On the **Add/Remove filters** tab, specify the search query. For your convenience, reports are featuring the same search techniques and data presentation as **Auditing**. If you are not familiar with these search techniques, refer to [Auditing](#) for more information.
- On the **Add/Remove columns** tab, toggle column and define what columns will be visible in the table view.
- On the **Manage alert settings** tab, specify if you want to monitor such events and get a notification every time is occurs. Provide your email address. Additionally, you can enable Remote Logging and feed collected data to a remote SIEM system.
- On the **View report ownership** tab, see who created or modified the report, the timestamps, and the report privacy settings.
- In the  **Manage resource delegation** pop-up window, grant access to this report to other Active Directory users. You've got an option to choose between read-only and full access.

The screenshot shows the 'Reports' interface in Cygna Auditor. At the top, there are navigation icons for users, reports, refresh, and a menu. Below this is a 'Report Information' section with tabs for 'Edit report details', 'Add/Remove filters' (which is active), 'Add/Remove columns', 'Manage alert settings', and 'View report ownership'. The filter configuration area shows two filters: 'Source' is 'is any of' 'Azure Logins', and 'Action result' is 'is' 'failure'. There is also a 'clear filters' button and a '+ Filter' button to add more filters. Below the filter configuration is a table with the following data:



When	Source	What	Who
May 30, 2022, 5:32:31 PM		User Sign-In	Ellen Ripley
May 30, 2022, 5:32:27 PM		User Sign-In	Ellen Ripley

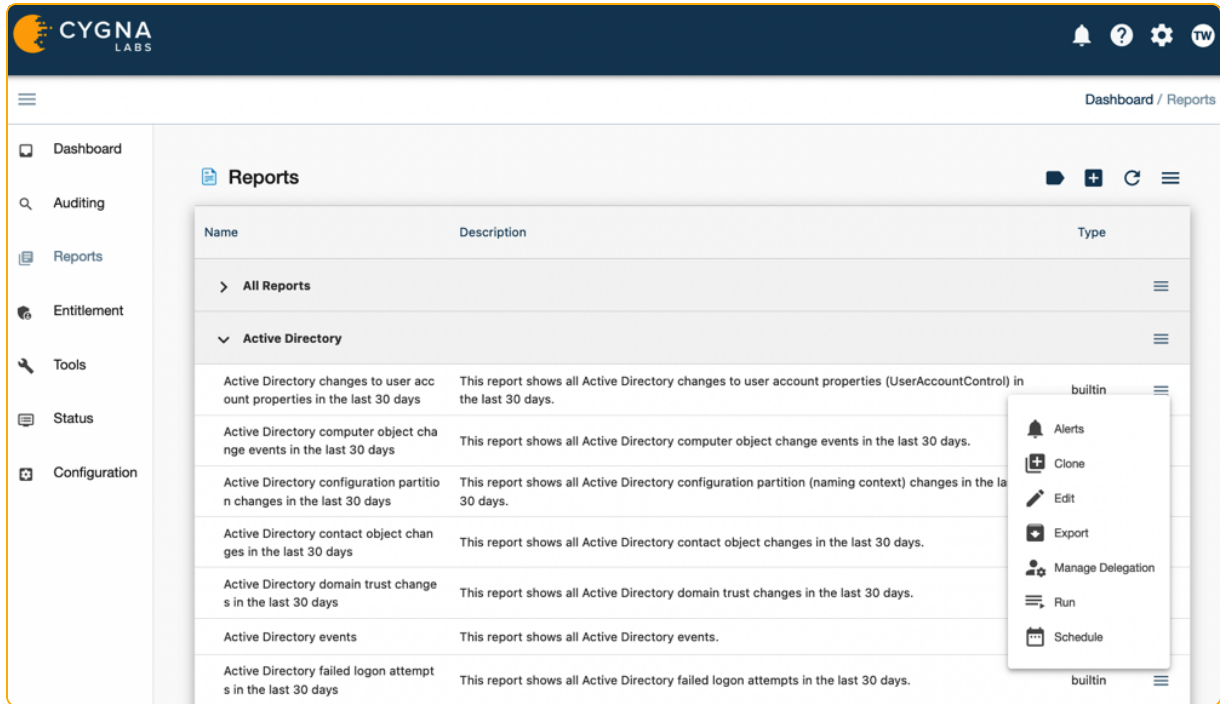
 **Note:** You might see several records with events that occurred at the same time up to seconds—for example "create user" with subsequent "modify user". Typically they represent a single, one-time action. The reason why Cygna Auditor displays it as several records is that Windows actually generates several events in response to your actions.

Subscribing to Reports

You can turn any report into a report subscription – Cygna Auditor will deliver the report to your mailbox according to a specified schedule.

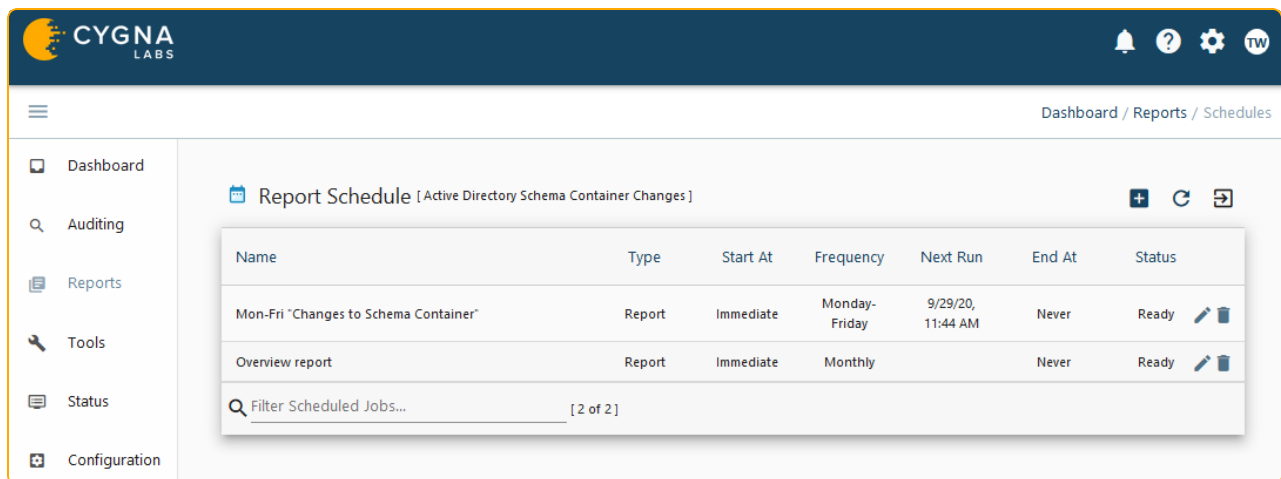
To create a schedule:

1. Navigate to the **Reports**.
2. Expand  options next to a report and select  **Schedule**.



3. On the **Report Schedule** page, select **+ Create**.
4. On the **Settings** tab, define the schedule—provide its name and description, select how often you'd like to receive the report (every day, Mon-Fri, weekly, etc.), the start and the end dates. Make sure the **Enable Scheduled Job** is on.
5. Select **Create New Action**. Here you can define the recipients and provide their email addresses, set up the layout, and decide if you want to receive emails even if the report is empty.

The subscriptions you create for the report, will appear on the **Report Schedule** page. The active subscriptions have **Enabled** status. You can always enable and disable subscriptions, adjust frequency, distribution list, and other settings.




 **Note:** To see all scheduled report, navigate to **Tools / Scheduler**.

Alerting

Are you enjoying reports but want to be notified about some actions immediately? Take advantage of alert notifications to ensure your response team never misses a security incident and keeps tabs on the most critical pieces of your business infrastructure such as changes to Azure AD admin rights or activity in folders containing personal or card payment data.

Depending on your company change control policies and revision routines, it can take days to discover an issue using regular reviews with [Auditing](#) or [Reports](#). Alerts look for the same data as reports but notify you as soon as the action occurs. Sent directly to email, alerts warn your authorized personnel about a possible threat once the triggering action occurs and is processed by the product. Additionally, alert can remotely feed data to SIEM systems such as Splunk and various syslog-compatible solutions, and if Cygna Auditor for Microsoft 365 is configured, to mail-enabled Teams.



Cygna Auditor flexible configuration enables you to tailor alerts to your organization's specific needs and be notified on changes that matter to you the most while reviewing less important changes in due course. You enable alerting for any built-in report or you can create a custom report and set notifications for it.

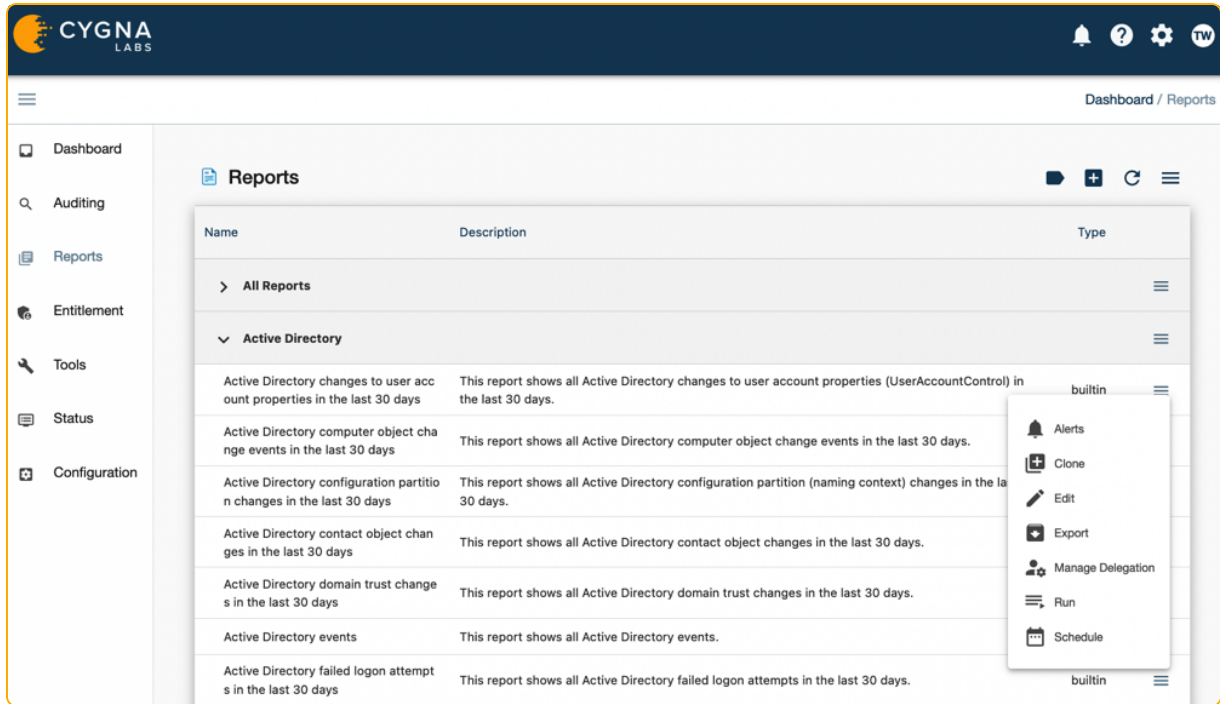
 **Note:** To be able to send alert notifications, configure SMTP settings. On the product home page, navigate to **Configuration / System** and complete the fields.

To enable alerting:

QUICK TIP: Not sure what alerts you need? Try asking yourself, "What is the most important piece of my business environment? What changes have the highest impact both from the security and operability point of view?".

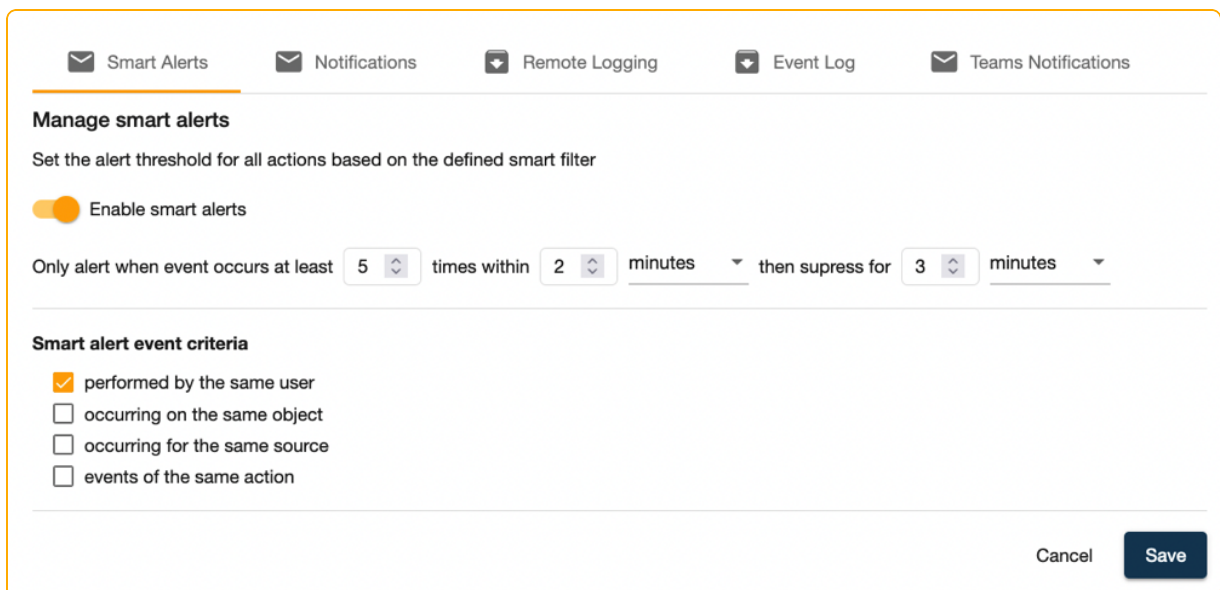
For example, creating a new user in Active Directory is a relatively routine task that does not require supervision or immediate response. On the contrary, adding a user to the Domain Admins group may have a great impact on your domain operability and security. Such changes should be carefully reviewed and approved by authorized personnel as soon as they occur.

1. Navigate to the **Reports**.
2. Expand  options next to a report and select  **Alerts**.



- On the **Smart Alerts** tab, turn on smart alerting if you want to receive alerts only when a certain condition is met. Generally, the alert is sent every time the event occurs. With smart alerts, you can configure rules to trigger an alert notification. For example, when monitoring failed logon attempts, configure Cygna Auditor to send an alert when an event happens five times within two minutes and then suppress notifications for 3 minutes.

Add criteria to send alerts, for example, when push alerts only when the event is performed by the same user or on the same object.



4. On the **Notifications** tab, specify email recipients who should be warned if the action occurs.

The screenshot shows the 'Notifications' tab selected in a navigation bar. Below the navigation bar, the section is titled 'Manage email recipients'. It includes instructions: 'Enter email addresses you wish to receive alert notifications (you may optionally specify multiple emails separated by semicolons)'. There is a toggle switch for 'Enable email alert' which is turned on. A text input field contains the email address 'security@cygnalabs.com'. At the bottom right, there are 'Cancel' and 'Save' buttons.

5. On the **Remote Logging** tab, enable pushing events to a remote logging SIEM system (e.g., Splunk).
6. On the **Event Log** tab, enable writing alert events to Windows Event Log.
7. On the **Teams Notification** tab, enable Teams alerts and specify a channel. Make sure you have an active Microsoft 365 subscription.

The screenshot shows the 'Teams Notifications' tab selected in a navigation bar. Below the navigation bar, the section is titled 'Manage MS Teams recipients'. It includes instructions: 'Select team name - channel pairings you wish to receive email alert notifications Search by partial team name.' There is a toggle switch for 'Enable MS Teams email alert' which is turned on. A text input field contains the team name 'Cygna - Security alerts'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Summary

Congratulations! Now, you have learned the basics and can go explore Cygna Auditor on your own. As a recap, here is the list of topics discussed in this Getting Started guide:

- Cygna Auditor architecture and basic usage workflow
- Deployment planning, including system requirements and account & permissions checklist
- Product installation and configuration
- Audit sources and how to start collecting audit data
- Key features that will help you keep tabs on changes and mitigate risks as they occur

Although your onboarding is complete, we encourage you to have a look at [Cygna Auditor online documentation portal](#). There you can find detailed instructions, how-to's, best practices, and tons of other useful information.

Index

A

- About 5
- Accounts 13
- Active Directory 24
- Activity widgets 38
- Additional components 7
- Alerts 53
- Audit database
 - Requirements 10
- Auditing 37, 39
 - All data 42
 - Conditions 44
 - Distilling results 47
 - Exclude data 46
 - Include data 47
 - Record 40
 - Search specific events 44
- Azure AD 34

C

- Cross-source search 39
- Cygna Auditing & Security Suite
 - Connect 35
 - Data sources 24

D

- Dashboard 38
- Database requirements 9
- Delegation 36

- Deployment, planning 9

E

- Exchange On-Premises 32
- Exchange Online 34

G

- Global reports 48
 - Scheduling 51
 - Subscribe 51

H

- Hardware requirements 9

I

- Installation 15

K

- Key features 37
 - Alerts 53
 - Auditing search 39
 - Reports 48

M

- Microsoft 365 34

O

- On-Premises Exchange 32

P

- PowerBroker Management Suite
 - Connect 35
- Product architecture 6
- Product, launch 16

R

Reports 48

 Create new 50

 Scheduling 51

S

Scheduling reports 51

Search 39

SharePoint Online 34

Software requirements 9

Sources

 Active Directory 24

 Microsoft 365 34

 On-premises Exchange 32

 PBMS 24

 VMware 35

 Windows File System 29

Subscription, reports 51

System requirements 9

T

Tools 37

V

VMware 35

W

Welcome 5

Windows File System 29

Workflow 6