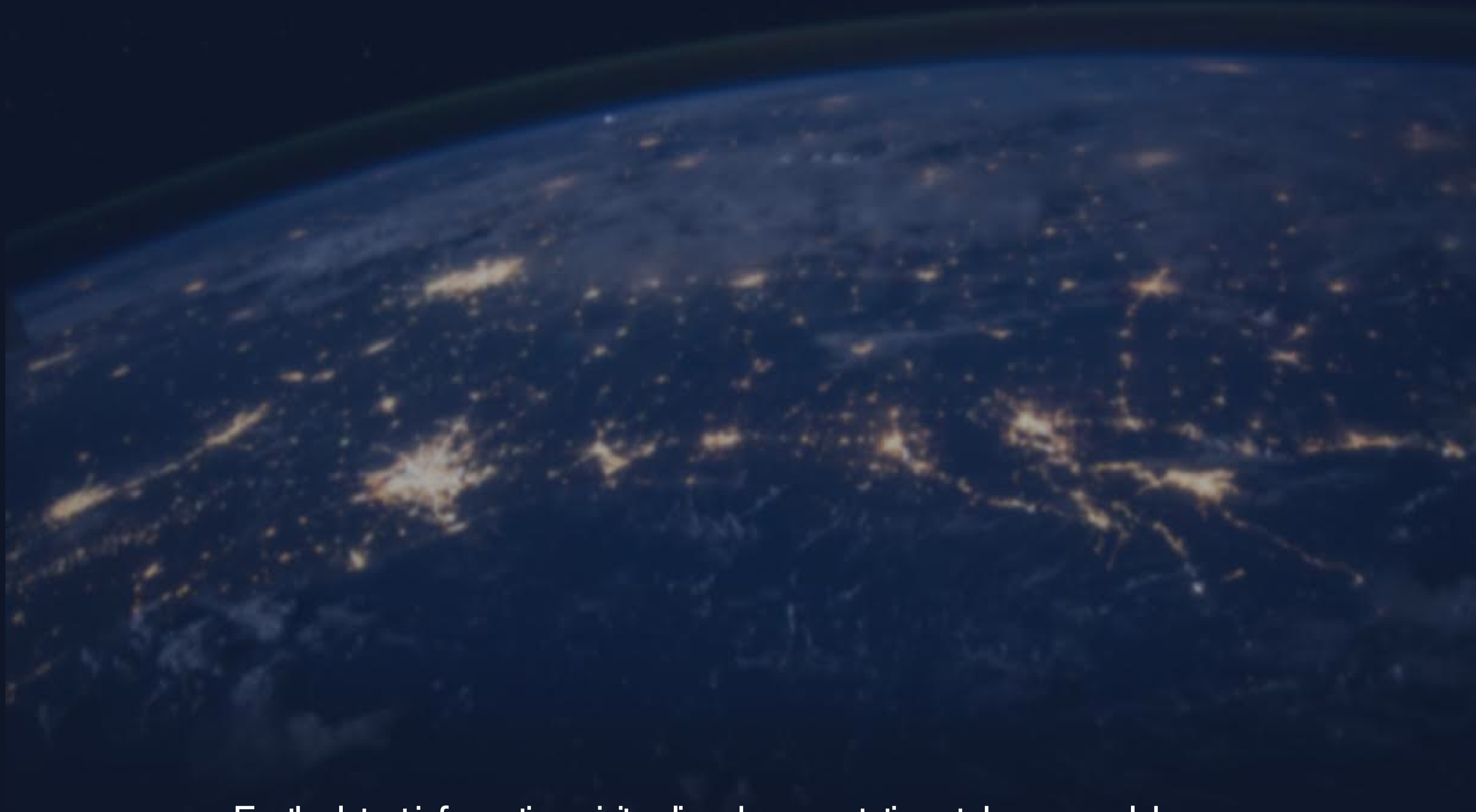
CYGNA LABS

Cygna Auditor

Complete User Guide



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

Published 7/13/2022

Version 2.1

Copyright © 2022

Copyright

©2022 Cygna Labs Corp. ALL RIGHTS RESERVED.

Trademarks

Cygna Labs and the Cygna Labs logo are trademarks and registered trademarks of Cygna 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 Cygna 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

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.

Here are just a few tips on navigating this guide.

- Start by reading a brief overview of Cygna Auditor architecture, followed by the Planning Deployment and Installation chapters.
- Browse the Sources chapter to find more about supported audit sources. Then, navigate to Auditing Settings to check required settings. Refer to source's individual chapters to learn how to enable auditing.
- Go to Auditing & Tools to explore product features and see how Cygna Auditor can help you gain control over your data with Auditing, Reports, etc. In Administration, you can read about fine-tuning the product.
- For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), refer to respective documentation.

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:

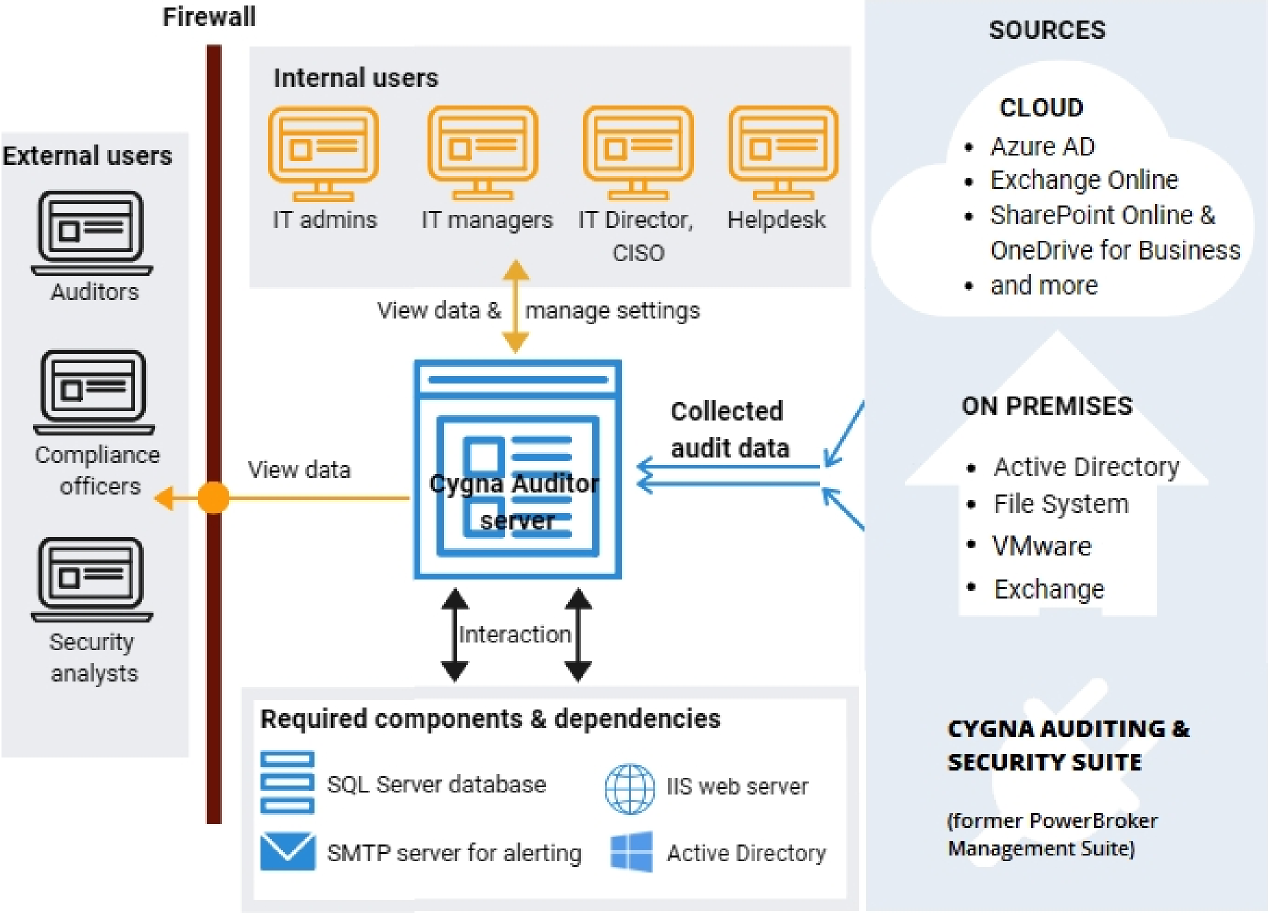
1. **Checking prerequisites.** Make sure you have enough resources before you proceed with installation. For more information, see Planning Deployment.
2. **Installation.** For more information, see Installation. If you want to leverage CA&SS (former PowerBroker Management Suite), install it as well.
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 are 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. For more information, see Auditing Settings.
5. **Administration.** Dive deep into the product administration. Delegate access to your authorized personnel, manage licenses, etc. For more information, see Administration.
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, Cygna Labs recommends deploying a SQL Server instance on a separate server.
- Cygna Auditing & Security Suite (former PowerBroker Management Suite)–stand-alone management console products that integrate smoothly with Cygna Auditor and provide extended auditing functionality.



Additional Components

Cygna 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. **Note:** To ensure data security, users must be delegated appropriate access rights in the product. For more information, see Delegation.	Yes
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 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.

Continue reading:

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.

Deployment Options

Basically, Cygna Labs recommends deploying Cygna Auditor on a clear Windows server. Cygna Auditor supports the following deployment options:

ON-PREMISES	VIRTUAL	CLOUD
On a physical Windows server.	On a Hyper-V or VMware virtual server. Recommended option.	AWS and Azure cloud services.

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	• **CPU**: Any modern processor with 4 cores • **RAM**: 4 GB (minimum), 8 GB (recommended) • **HDD**: 100 MB
Operating system	• Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Server roles and features	• **Group Policy Management** • **Web Server (IIS)**: Microsoft IIS 8.5 or above, including

COMPONENT	REQUIREMENTS
	Windows Authentication, ASP.NET 4.8 • **.Net Framework**: Microsoft .Net Framework 4.8, including ASP.NET 4.8 Note: Depending on the OS, you might need to install ASP.NET manually.
Additional software	Any modern browser, preferably Google Chrome or Microsoft Edge.

Database Server

Review the system requirements for the database server.

COMPONENT	REQUIREMENTS
Hardware	• **CPU**: Any modern processor with 4 cores • **RAM**: 8 GB (minimum), 16 GB (recommended) • **HDD**: 2 GB (minimum). 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.
Operating system	Any modern OS provided it supports installation of Microsoft SQL Server
Database	• SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • SQL Server 2022 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.

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	• **CPU**: Any modern processor with 4 cores • **RAM**: 12 GB (minimum), 16 GB (recommended) • **HDD**: 4 GB 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.
Operating system	• Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Server roles and features	• **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 Note: Depending on the OS, you might need to install ASP.NET manually.
Database	• SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • SQL Server 2022 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

COMPONENT	REQUIREMENTS
	for Standard edition.
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.

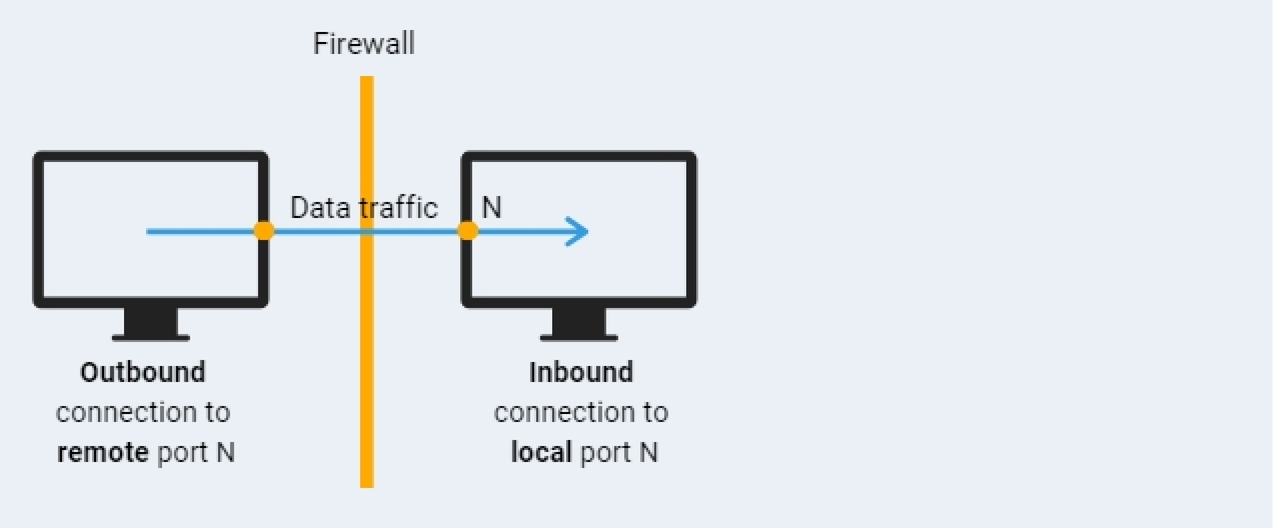
ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
Domain administrator account	Active Directory credentials used to connect to your domain and create an Active Directory object with product configuration. The product stores its configuration in Active Directory forest to ensure the product settings stay in sync across your corporate domain. During the installation, Cygna Auditor will create and start a service.	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	A custom domain user account must be a member of the local **Administrators** group and granted the **Log on as a batch**

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
	account.	**job** and **Log on as a service** permissions.
SQL Server account	Account with Windows or SQL Server authentication used to connect to the SQL Server instance. 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.	**New database:** The **dbcreator** server role and the **db_datareader** and **public** roles for the master database. **Existing database:** The **db_owner** and **public** roles for the audit database.

Ports and Network Resources Reference

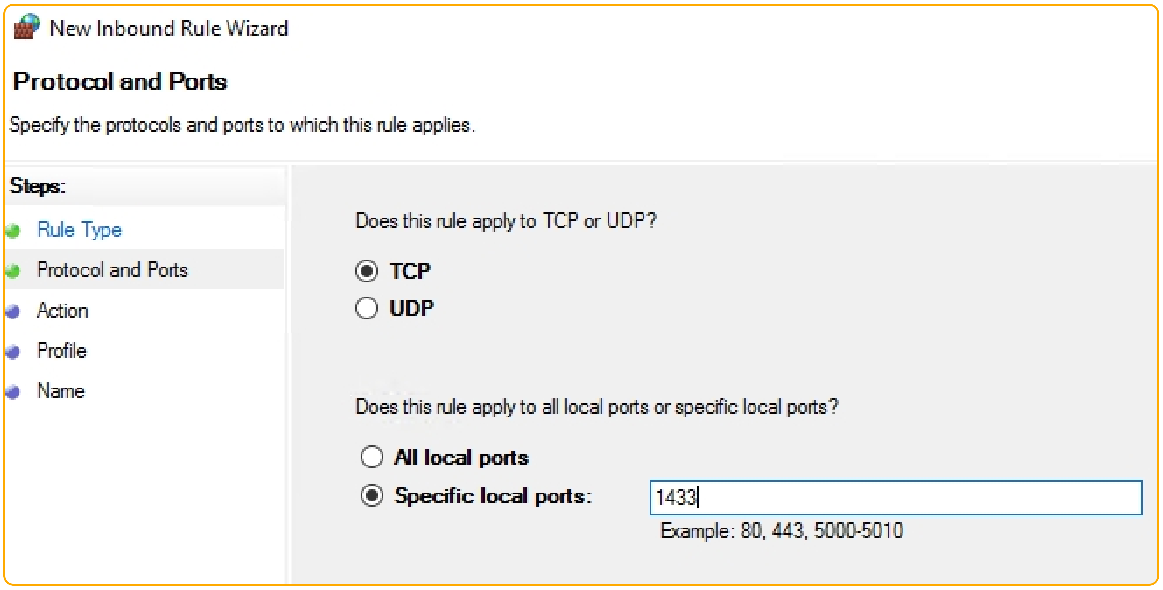
Check this reference and ensure your firewall is configured to allow inbound and outbound connections to the following ports. This port configuration is essential to product operability since facilitates data collection, acquisition, and transmission between the product components and audit sources.

QUICK TIP: Need a quick recap of how the firewall works? For successful data transmission over firewall, the sender computer should be allowed to transfer data (outbound connection) to a specific port on a remote computer. On the other side, the receiver computer should be configured to allow traffic (inbound connection) to the same local port. The best practice is to keep inbound connections all under supervision and not to open ports unless necessary.



Configuring Windows Firewall Rules

1. Start the Windows Firewall with Advanced Security.
2. On the left, specify the type of rule you want to create (inbound or outbound), right-click the section, and select **New Rule**.
3. Complete the wizard as follows:
    a. On the **Rule Type** step, specify **Port**.
    b. On the **Ports and Protocols** step, select the protocol type (TCP or UDP). Depending on the rule you create, specify the port number in the **Specific local ports** or **Specific remote ports** correspondingly.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 1433

Example: 80, 443, 5000-5010

    c. On the **Action** step, select **Allow the connection**.

   d. On the **Profile** step, specify when this rule should be in use (within your corporate domain, private network, or public network).

   e. On the **Name** step, enter the name and description explaining the rule.

4. Ensure the newly created rule is enabled.

Cygna Auditor Platform

The server or workstation where Cygna Auditor platform is deployed should be configured to allow the following connections.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	80 (http) 443 (https)	IIS
Outbound	Remote	TCP	135	RPC

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Outbound	Remote	TCP	1433	Interaction with Cygna Auditor SQL Server-based data storage.
Outbound	Remote	TCP	443 (https)	**Access to Cygna Auditor online help** at docs.cygnalabs.com. **Agent-based Active Directory data collection:** *.core.windows.net (GET) msdl.microsoft.com msdl.microsoft.com/download/symbols **Interactions with Microsoft 365:** 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) **Interactions with AWS:** *.amazonaws.com (GET and POST) If you have a proxy server configured in your environment, it should as well allow connections to these URLs. Also, the computer from which you

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
				configure Microsoft 365 data collection ("authorize") should allow connections to these URLs.

SQL Server-Based Data Storage

The server where SQL Server instance with collected audit data is located should be configured to allow the following connections.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	1433 (default instance) dynamic (named instance)	Interaction with Cygna Auditor platform

Active Directory DCs

Domain controllers in the Active Directory domain you want to audit should be configured to allow the following connections.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	135 and dynamic*	Interaction with Cygna Auditor platform.
	Note: * In Windows Firewall, it is recommended to enable the RPC and RPC-EMAP firewall rules.			
Outbound	Remote	TCP	1433	Interaction with Cygna Auditor SQL Server-based data storage.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	445	Access to the **C$** share for agents.
Inbound	Local	TCP	139	Only required for networks relying on NetBIOS.

File Servers

The servers and workstations you want to audit should be configured to allow the following connections.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Outbound	Remote	TCP	1433	Interaction with Cygna Auditor SQL Server-based data storage.
Inbound	Local	TCP	445	Access to the **C$** share for agents.
Inbound	Local	TCP	139	Only required for networks relying on NetBIOS.

VMware, Microsoft 365

No specific port configuration is required.

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.

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

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 *"Integrated"*.
Identity	You can run the application pool as the **LocalSystem** service account or specify a **custom** account. 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. 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.

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	Select the SQL Server instance name from the list or input it in one of the following formats: **hostname\instance** (e.g., *DemoSQL\SQL16*) or **hostname,port** (e.g., *DemoSQL,1833*). 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 Configuring Additional Steps for SQL Server Express.
Use Windows authentication Use SQL Server authentication Account, password	Specify the authentication type and enter credentials. Note: SQL authentication is a recommended method. If you select Windows authentication method, the user

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 Post-Installation Steps.
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 Password	Provide user credentials for SMTP authentication.

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**.

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? For more information, see Configuring Settings for Active Directory. 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 over relying on event logs.

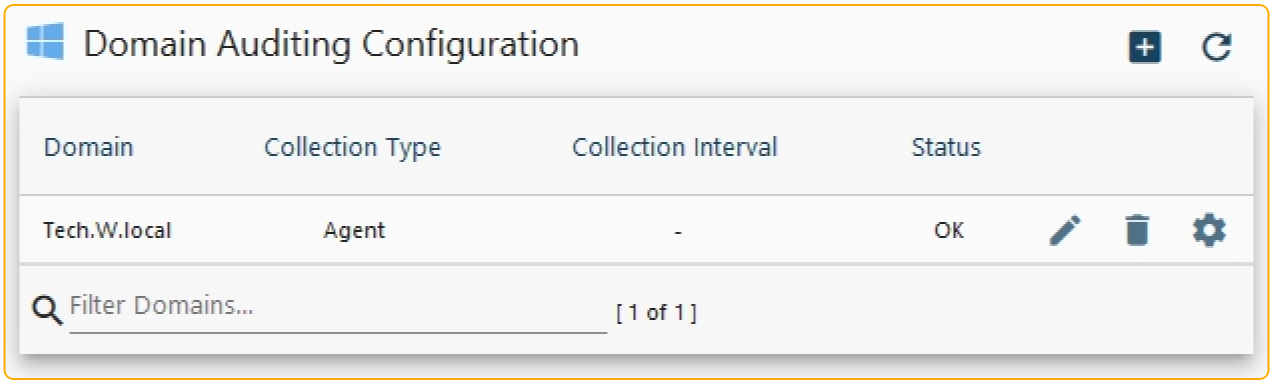
OPTION	DESCRIPTION
	Domain Selection tab
User name Password	Enter the user credentials. Specify a user name in the following format: domain\username. Cygna Auditor will use this account to collect audit data from the domains this account has

OPTION	DESCRIPTION
	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 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.
Collection Settings tab	
Data collection method	Select one of the following: • Cygna Auditor Agent (preferred) • Event log
Combine similar events occurring within the specified interval	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. If this option is cleared, Cygna Auditor will capture a record for each event.
Attempt to locate workstation information for events	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.
Perform reverse name lookup when event only include an IP address for the remote workstation	Select to try identifying a DNS name of a remote workstation.
Ignore login events	Select to skip login events from processing.
Enable nested group alerting and auditing	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

OPTION	DESCRIPTION
	parent group as well. A user removal from a child group isn't reported for a parent group. Select **Manage nested groups** and specify groups in the pop-up window. Expand **Advanced collector settings** to configure additional options for nested group auditing.
Advanced collector settings	Expand this section to configure additional settings if necessary. • Exclude attributes from data collection– enter a list of attributes separated by commas. • Select the **Ignore login events** checkbox. • Set up GP backup configuration, including: • Enabling GPO backup for detailed change reporting–with its help you'll be able to see changes in group policy objects over time. • Ensuring all GPOs have at least one backup–it gives you ability to see and revert changes at all times. • If nested group alerting and auditing is enabled, specify details for reporting changes in the **Nested group auditing settings** section. • **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. • **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. • **Cascade nested non-group object**

OPTION	DESCRIPTION
	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 generated that they were removed from the top level Group 1. • **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.


Domain Auditing Configuration

Domain	Collection Type	Collection Interval	Status
Tech.W.local	Agent	-	OK

Continue reading:

[Dashboard]

[Auditing]

[Reports]

[Rollback for Active Directory]

Recycle Bin for Active Directory

Active Directory Browser

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	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

OPTION	DESCRIPTION
	collection. The connectivity is checked for each region authorized for the account. 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.
	The **Collector Settings** step
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.

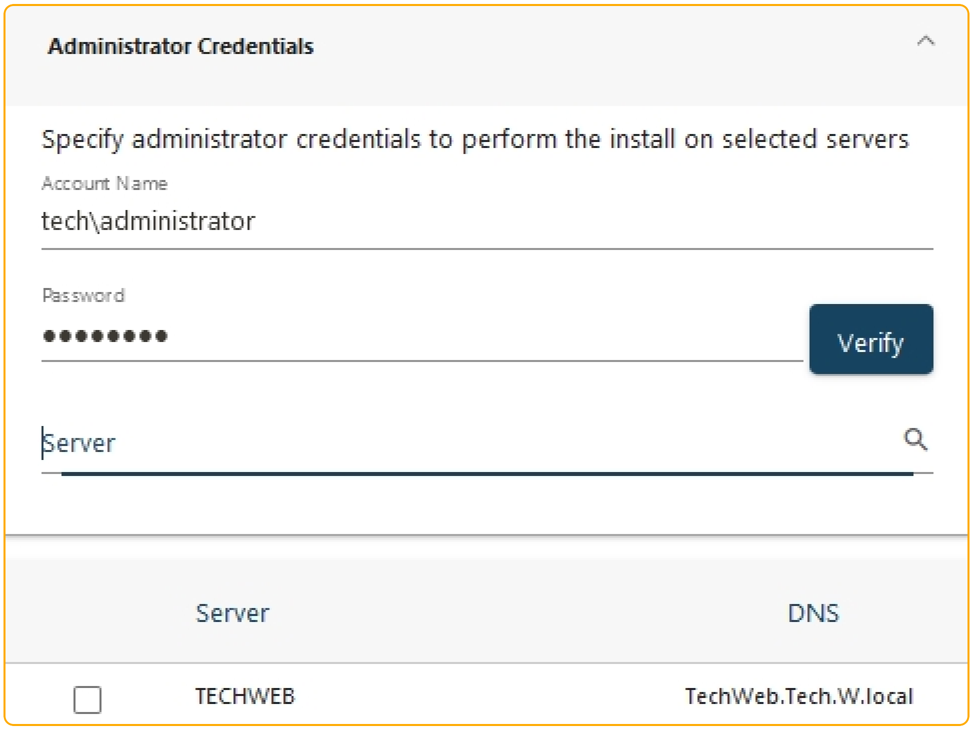
Windows File System

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, Cygna 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. Cygna Auditor will look up for servers and show the list of available servers. Select servers you want to audit and click **Install**.



Administrator Credentials

Specify administrator credentials to perform the install on selected servers

Account Name: tech\administrator

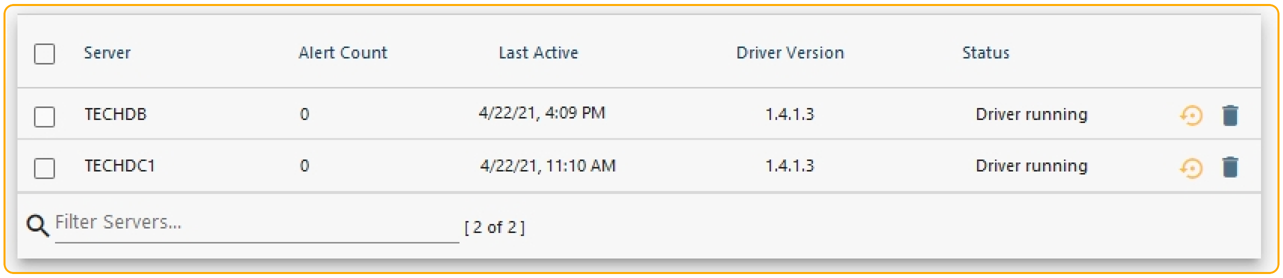
Password: ●●●●●●●●

	Server	DNS
□	TECHWEB	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. Cygna Auditor will suggest you add data collection filters.

Check the data collection status in the audited servers list.



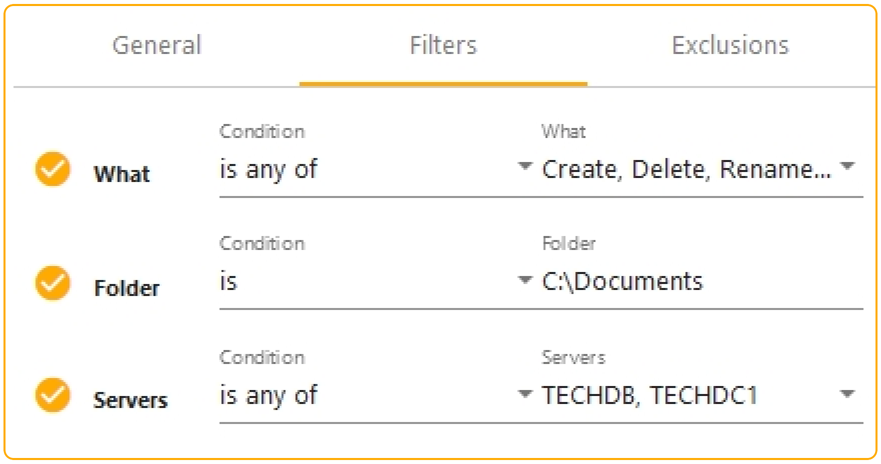
□	Server	Alert Count	Last Active	Driver Version	Status
□	TECHDB	0	4/22/21, 4:09 PM	1.4.1.3	Driver running
□	TECHDC1	0	4/22/21, 11:10 AM	1.4.1.3	Driver running

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:



✓ What — Condition: is any of — What: Create, Delete, Rename...

✓ Folder — Condition: is — Folder: C:\Documents

✓ 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.

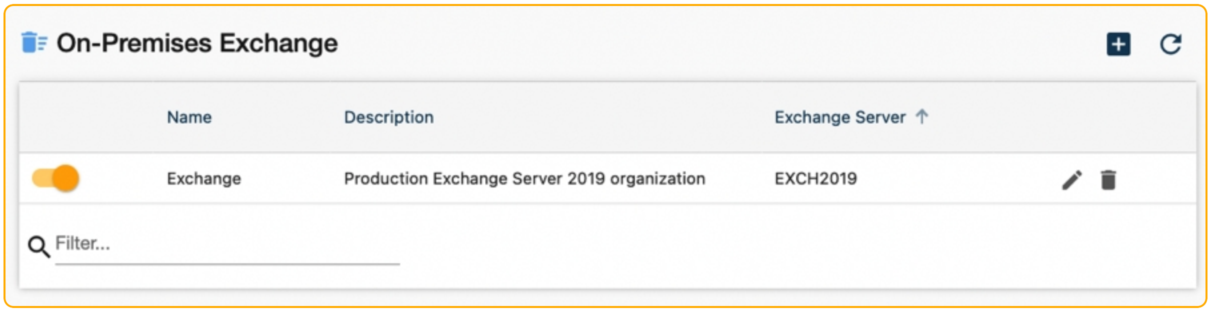
QUICK TIP: Have you configured your Exchange Server for auditing? For more information, see Configuring Settings for On-Premises Exchange.

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	

OPTION	DESCRIPTION
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	
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.



On-Premises Exchange

	Name	Description	Exchange Server ↑	
●	Exchange	Production Exchange Server 2019 organization	EXCH2019	

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 Configuring Settings for Azure.
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)

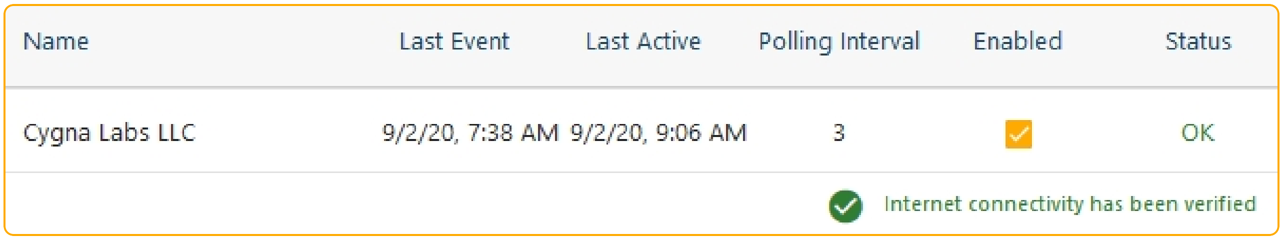
   login.microsoftonline.com (GET only)

   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 Password	Enter the user credentials.
Interval	Set he 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 Delegation.

Post-Installation Steps

These post-installation steps are only required if you

- Use SQL Server Express as a storage for your audit data. Go to Configuring Additional Steps for SQL Server Express.
- Selected Windows authentication method to connect to SQL Server. Go to Allowing Access to Service Accounts.

Configuring Additional Steps for SQL Server Express

Cygna Labs recommends SQL Server Standard edition for storing your audit data. You can opt for SQL Server Express during the product evaluation but note that SQL Server Express requires additional configuration before Cygna Auditor can start writing your data in the audit storage.

To update protocol preferences:

1. On the server that hosts your SQL Server Express, start **SQL Server Configuration Manager**.
2. Go to **SQL Server Network Configuration / Protocols for SQLEXPRESS** and set **TCP/IP** to *"Enabled"*.

To update service properties:

1. On the server that hosts your SQL Server Express, start **Services**.
2. Locate the **SQL Server Browser** service and set its **Startup type** to *"Automatic"*, and then start the service.
3. Locate the **SQL Server (SQLEXPRESS)** service and restart it.

Allowing Access to Service Accounts

If you choose the Windows authentication on your SQL Server, you have to enable Cygna Auditor components and services to connect to and access the audit database.

Create login for	Assign roles	Explanation
	SQL Server installed locally	
Local IIS users group (*computername\IIS_IUSRS*	**db_owner** and	Cygna web console uses the

Create login for	Assign roles	Explanation
	public roles for the audit database	account running the Cygna Labs Web Console application pool to access the database (ApplicationPoolIdentity by default, it belongs to *computername*\IIS_IUSRS group).
NT_AUTHORITY\SYSTEM	**db_owner** and **public** roles for the audit database	Other Cygna components and services connect to the SQL Server as NT_AUTHORITY\SYSTEM account.
SQL Server installed remotely		
Computer account of Cygna Auditor host (*domain\computeraccount$*)	**db_owner** and **public** roles for the audit database	Cygna Auditor components and services connect to a remote SQL Server as the AD computer account of the Cygna Auditor host.

With Windows authentication, you'll have to allow access to computer accounts of file servers and domain controllers where the Cygna Auditor agents will run once you enable auditing. See Configuring File System Agent Settings to Allow Access to SQL Server with Windows Authentication and Configuring Active Directory Agent Settings to Allow Access to SQL Server with Windows Authentication.

Security Considerations

As a security concern, Cygna Labs recommends switching to encrypted HTTP (HTTPS) on your IIS web server. Acquire the SSL certificate from a reliable source to ensure you audit data is protected from external threats.

After installing the product:

- You can configure Cygna Auditor to utilize a proxy server you typically use to reroute traffic outside your network. See Proxy for more information.
- You can opt to run Cygna Auditor platform service by a specific domain account instead of the Local System account. See Service for more information.

QUICK TIP: To learn more how to secure your data from unauthorized access within your organization, refer to Delegation.

Starting the Product

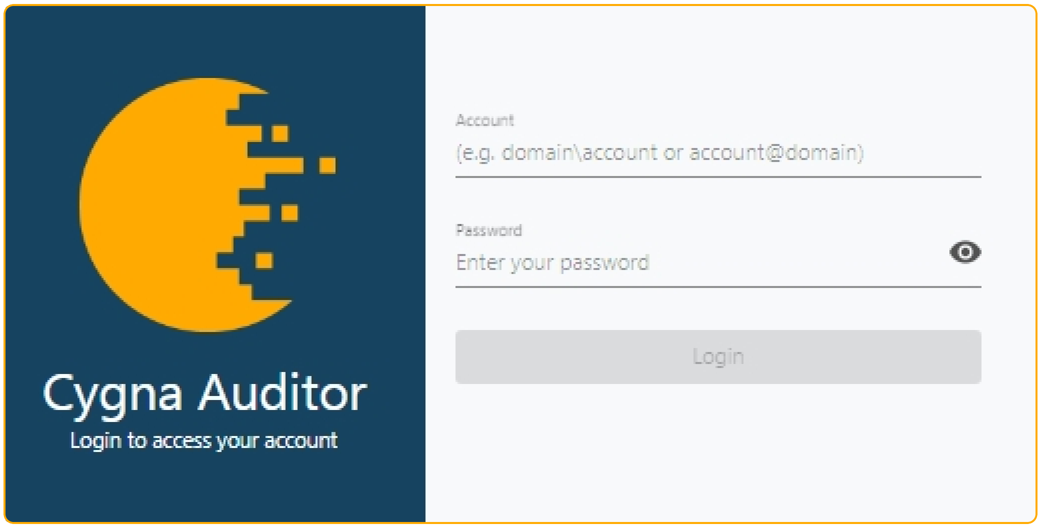
To start Cygna Auditor on a local computer:

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

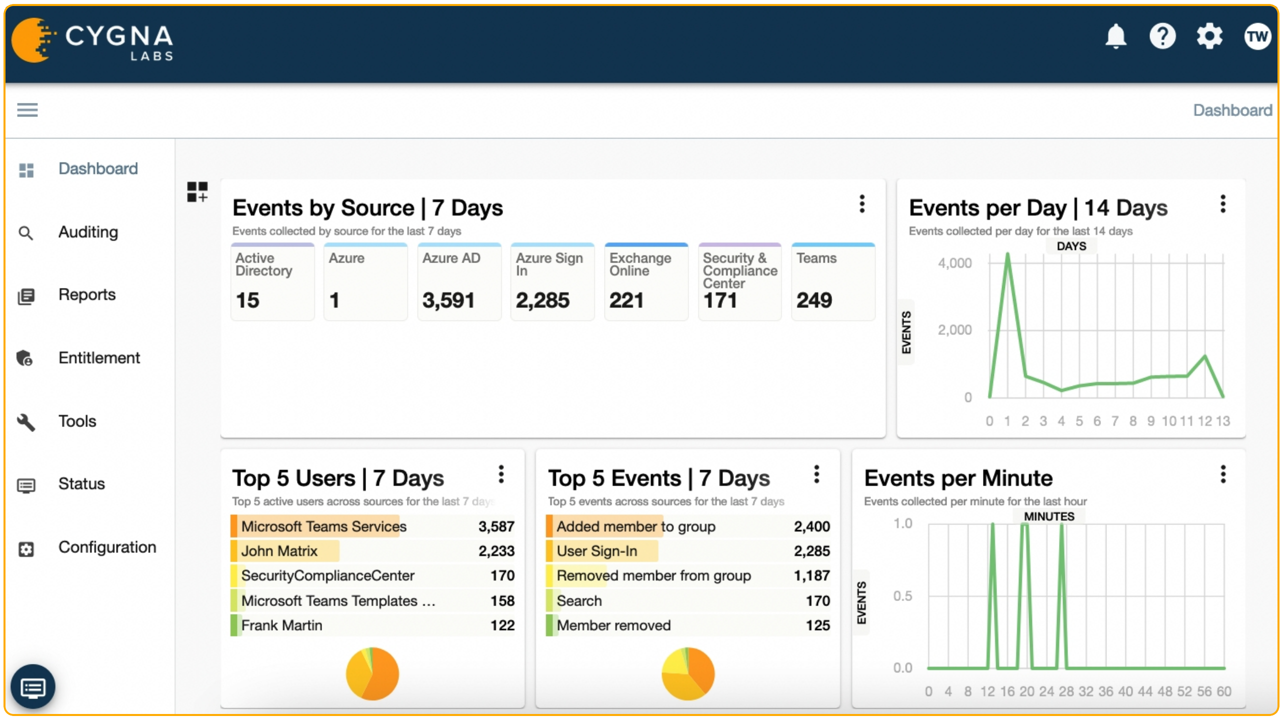
Your current user credentials will be used to log in to the product.

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.


Cygna Auditor
Login to access your account
Account
(e.g. domain\account or account@domain)
Password
Enter your password
Login

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.



Events by Source | 7 Days

Events collected by source for the last 7 days

Active Directory	Azure	Azure AD	Azure Sign In	Exchange Online	Security & Compliance Center	Teams
15	1	3,591	2,285	221	171	249

Events per Day | 14 Days

Events collected per day for the last 14 days

Top 5 Users | 7 Days

Top 5 active users across sources for the last 7 days

Microsoft Teams Services	3,587
John Matrix	2,233
SecurityComplianceCenter	170
Microsoft Teams Templates ...	158
Frank Martin	122

Top 5 Events | 7 Days

Top 5 events across sources for the last 7 days

Added member to group	2,400
User Sign-In	2,285
Removed member from group	1,187
Search	170
Member removed	125

Events per Minute

Events collected per minute for the last hour

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. For more information, see Delegation.

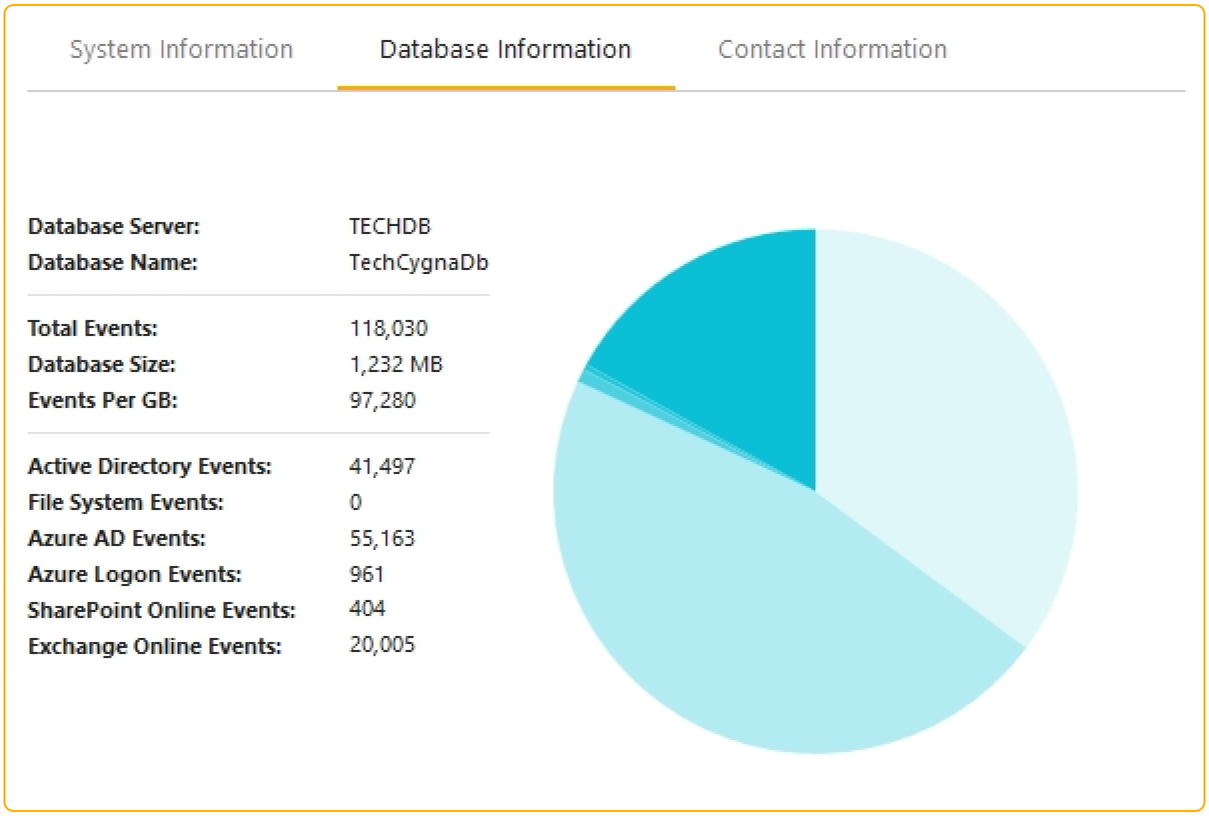
Product Information and Statistics

To learn about the product and see usage statistics, select ? on top of the Cygna Auditor page and then click **About** link.

In the **About** page, you'll find tabs with product details:

- Cygna Auditor version
- License expiration date
- The name of the application server where Cygna Auditor is deployed and its characteristics
- Database statistics with the total number of events stored in the database, the number events per each source, and the total database size in MB
- etc.

Use the statistics and the information about the product to plan maintenance and allocate additional resources when necessary.



Database Server:	TECHDB
Database Name:	TechCygnaDb
Total Events:	118,030
Database Size:	1,232 MB
Events Per GB:	97,280
Active Directory Events:	41,497
File System Events:	0
Azure AD Events:	55,163
Azure Logon Events:	961
SharePoint Online Events:	404
Exchange Online Events:	20,005

Configuration

Read this section to prepare your infrastructure for auditing and set up Cygna Auditor configuration.

- Refer to Sources for a complete list of supported audit sources
- Refer to Auditing Settings for instructions on how to prepare your infrastructure for auditing
- See articles about each audit source to learn how to enable auditing and reporting
- Find out more about Administration, including data purging, delegation, and connecting to Cygna Auditing & Security Suite (former PowerBroker Management Suite).

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.

Sources

SOURCE	VERSIONS
Active Directory	Windows Server 2012 / 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022
Amazon Web Services	n/a
Microsoft Subscriptions: Azure AD and Azure Logins Exchange Online SharePoint Online Teams	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. For more information, see Auditing Settings.

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. See CA&SS documentation for more information.

Auditing Settings

Before you can start auditing your systems, check that all required audit settings are configured on your **target systems**. These settings are essential for Cygna Auditor as they enable the product collect complete and reliable audit data. The settings may vary depending on the source.

Continue reading:

QUICK TIP: If the audit source is missing in the list, it means no prior configuration is required and you can enable audit data collection right away.

Configuring Settings for Active Directory

To ensure Cygna Auditor collects complete and reliable audit data, configure the following settings in your Active Directory environment.

- Make sure Group Policy Management feature is enabled on the Cygna Auditor host (required for GPO backup and restore operations)
- Update group policy for your domain controllers. Refer to Updating Group Policies for more information.
- Allow remote access to DC's event logs. Refer to Enabling Remote Event Log Management for more information.
- Update ACL auditing settings with ADSI Edit tool. Refer to Updating ACL Settings for more information.

Continue reading:

Active Directory

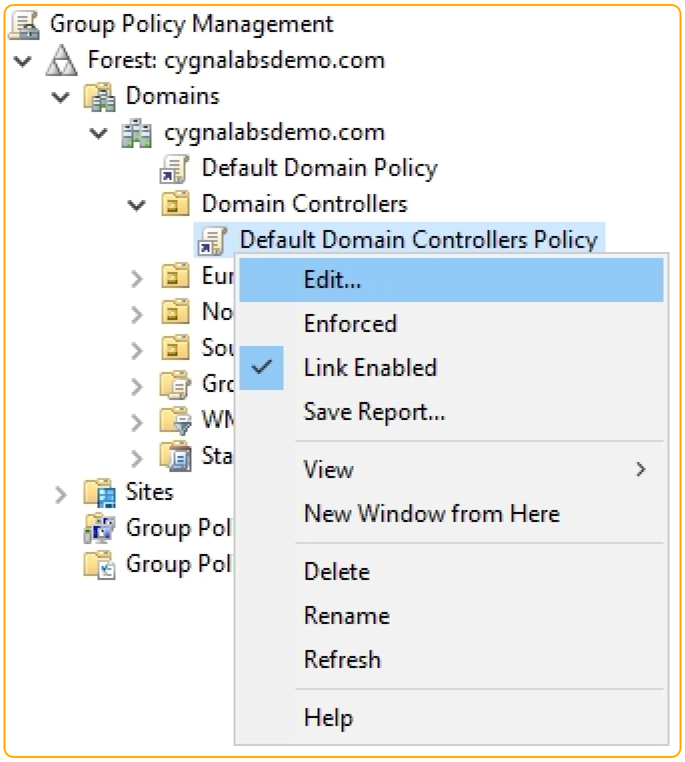
Configuring Settings for Recovery for Active Directory

Updating Group Policies

First, make sure Group Policy Management feature is enabled on the Cygna Auditor host. To enable it, navigate to **Server Manager**, in the upper-right corner select **Manage / Add roles and features** and then specify **Group Policy Management** option on the **Features** tab in the dialog.

To enable Cygna Auditor to collect audit data, configure the following settings in the Group Policy Management console.

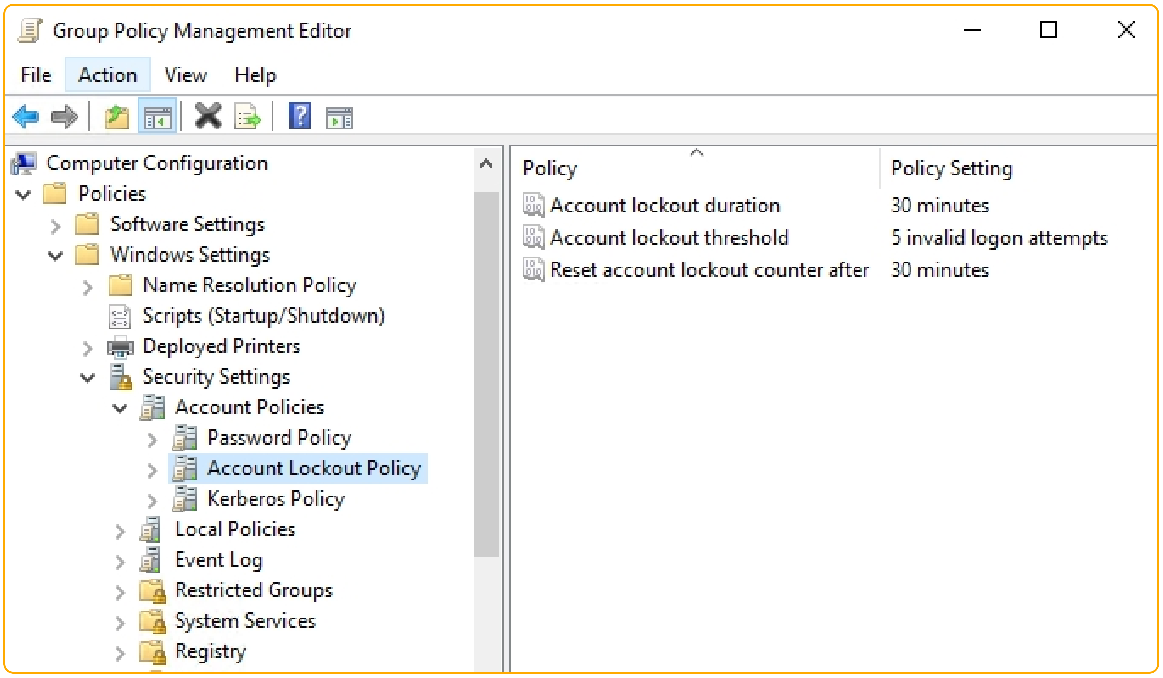
1. In the Group Policy Management console, locate the **Default Domain Controllers** policy, right-click it and select **Edit**.



2. Update the policies as described below:

   a. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Account Policies/ Account Lockout Policy**

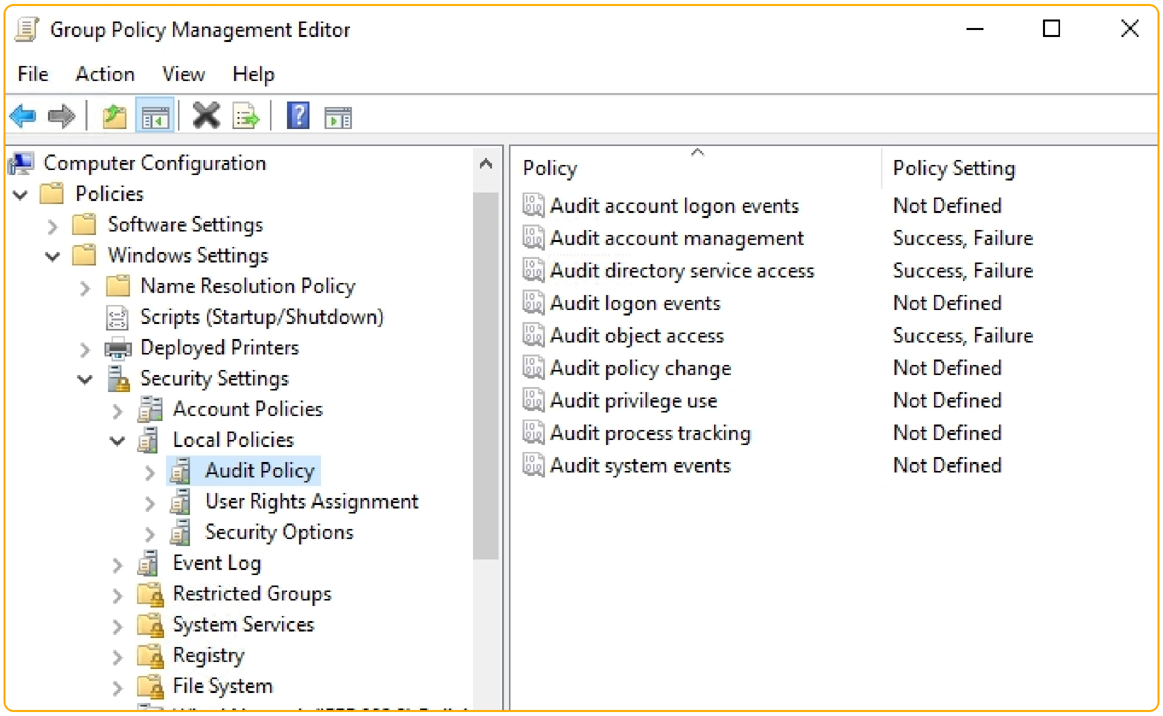
GROUP POLICY	POLICY SETTINGS
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes



Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

b. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Audit Policy**

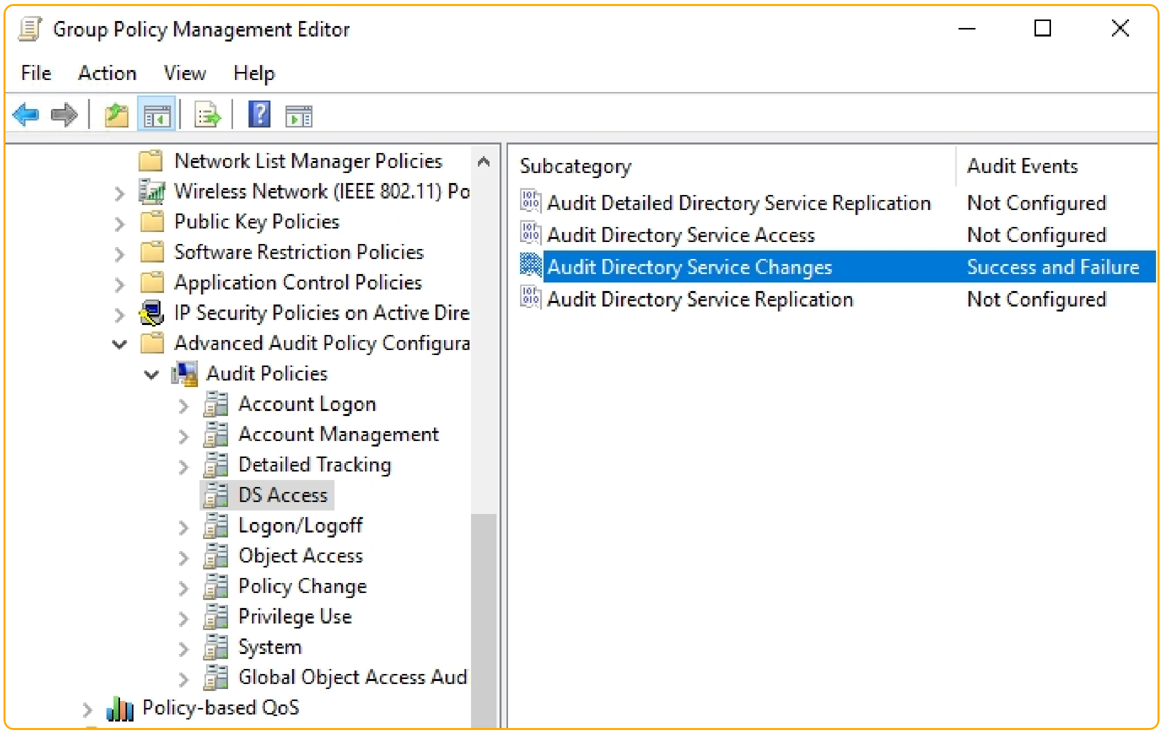
GROUP POLICY	POLICY SETTINGS
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit object access	Success, Failure



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Not Defined
Audit object access	Success, Failure
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

c. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / DS Access**

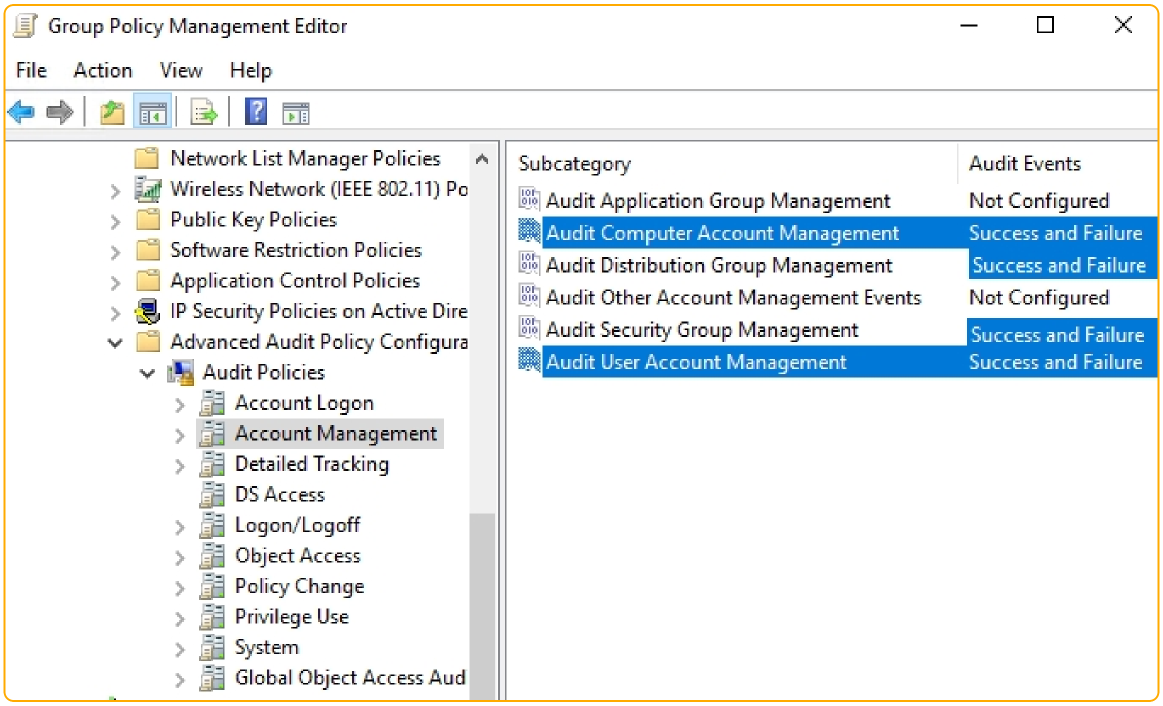
GROUP POLICY	AUDIT EVENTS
Audit Directory Service Changes	Success, Failure


Group Policy Management Editor
File
Action
View
Help
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dire
Advanced Audit Policy Configura
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Aud
Policy-based QoS

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured

d. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Account Management**

GROUP POLICY	AUDIT EVENTS
Audit Computer Account Management	Success, Failure
Audit User Account Management	Success, Failure
Audit Distribution Group Management	Success, Failure
Audit Security Group Management	Success, Failure

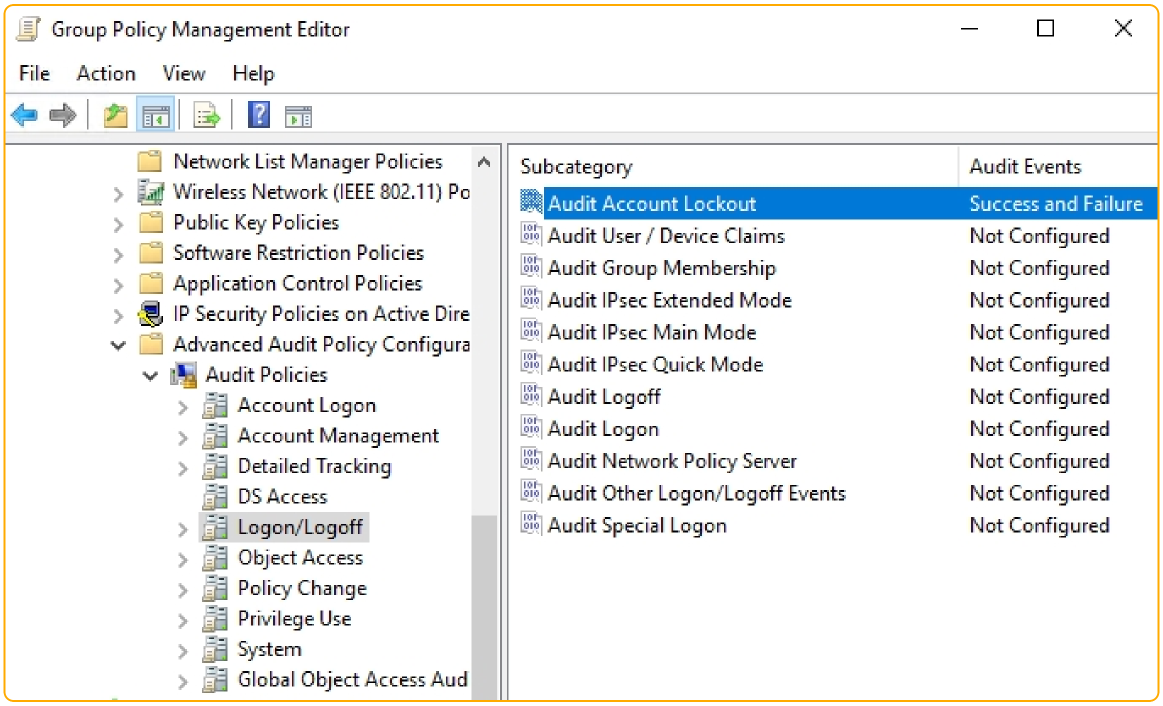


- Network List Manager Policies
- Wireless Network (IEEE 802.11) Po
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Active Dire
- Advanced Audit Policy Configura
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Aud

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

e. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Logon/Logoff**

GROUP POLICY	AUDIT EVENTS
Audit Account Lockout	Success, Failure

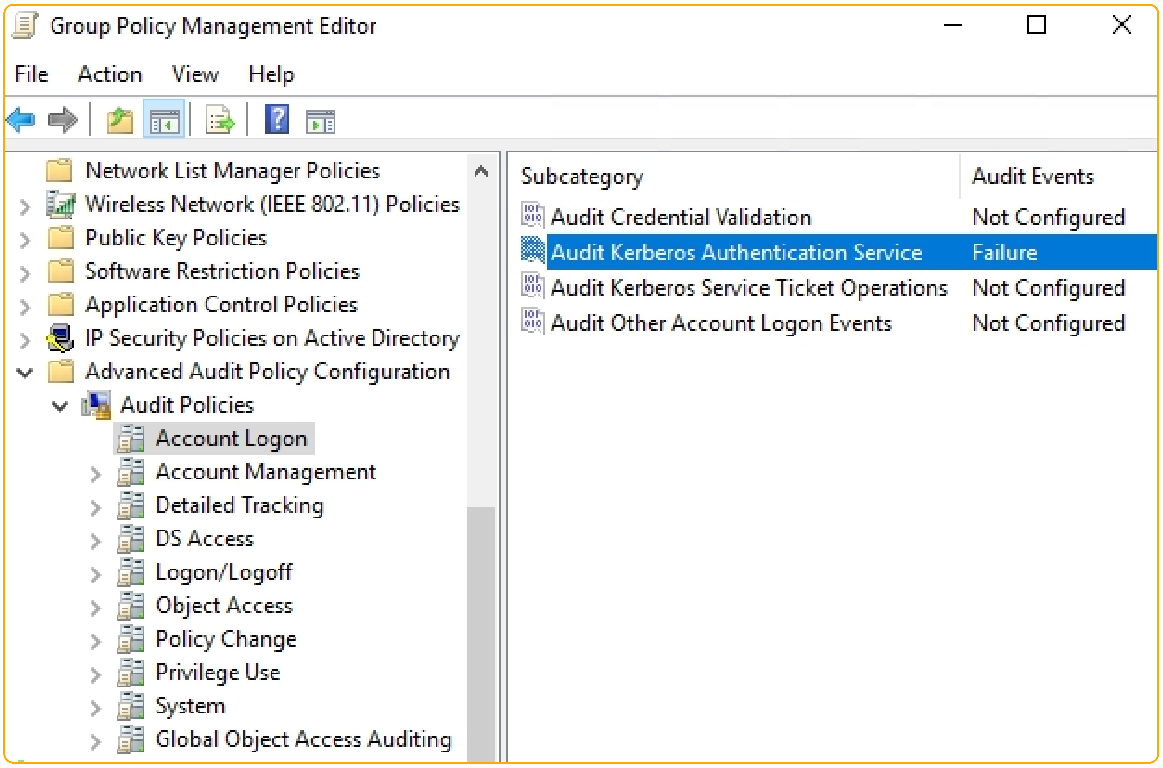


Group Policy Management Editor
File Action View Help
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dire
Advanced Audit Policy Configura
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Aud

Subcategory	Audit Events
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Not Configured
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

f. Path: **Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Account Logon**

GROUP POLICY	AUDIT EVENTS
Audit Kerberos Authentication Service	Failure


Group Policy Management Editor
File
Action
View
Help
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

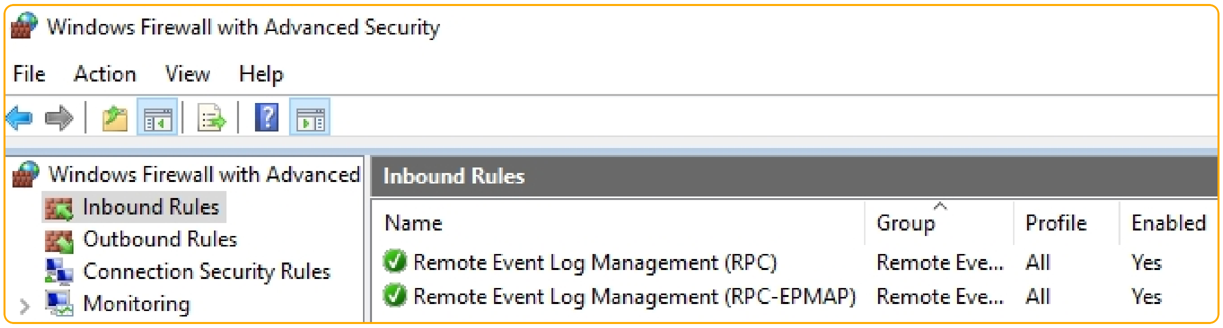
Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Failure
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

3. Run `gpupdate /force` in the command prompt.

Enabling Remote Event Log Management

To collect audit events, Cygna Auditor needs access to event logs on the domains controllers. Perform this operation on each domain controller in your domain.

1. Start the Windows Firewall with Advanced Security.
2. In **Inbound rules**, locate the following rules and enable them:
    - Remote event log management (RPC)
    - Remote event log management (RPC-EPMAP)

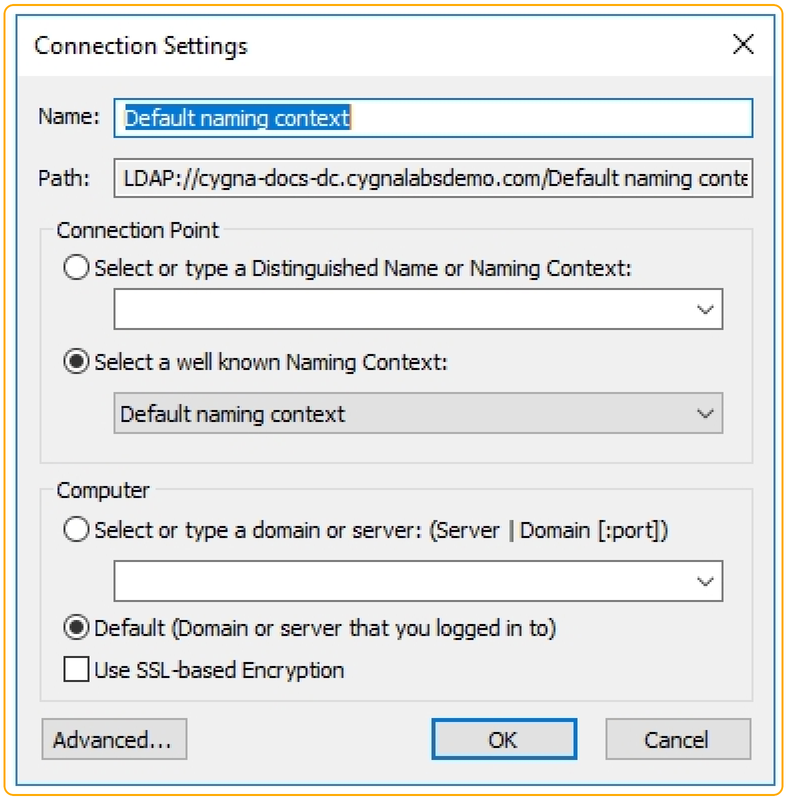

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled
Remote Event Log Management (RPC)	Remote Eve...	All	Yes
Remote Event Log Management (RPC-EPMAP)	Remote Eve...	All	Yes

Updating ACL Settings

To enable logging of actions performed in your domain, you need to update ACL auditing settings applied to the following naming contexts: Default naming context and Configuration.

1. Start **ADSI Edit** tool.
2. In **ADSI Edit** window, right-click the root node and select **Connect to**.
3. In the **Connection Settings** dialog, expand the drop-down list under **Select a well known Naming Context** and specify **Default naming context**.



Connection Settings

Name: Default naming context

Path: LDAP://cygna-docs-dc.cygnalabsdemo.com/Default naming conte

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context:

Default naming context

Computer

○ Select or type a domain or server: (Server | Domain [:port])

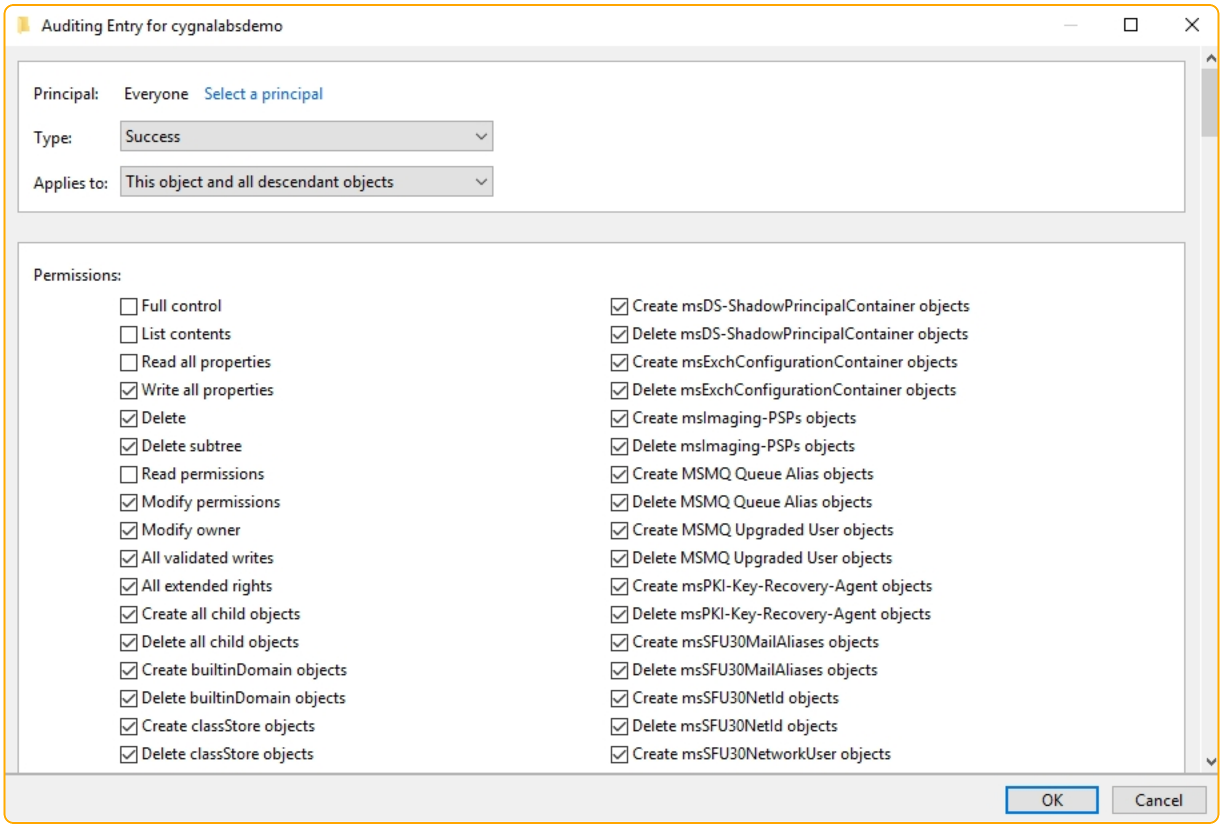
● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

4. Expand the context node, right-click your domain node, and then click **Properties**.
5. In the dialog that opens, select the **Security** tab and click **Advanced**.
6. In the **Advanced Security Settings** dialog, select the **Auditing** tab and click **Add**.
7. In the **Auditing Entry** dialog, complete the following fields:

OPTION	SET TO
Select a principal	Everyone
Type	Success

OPTION	SET TO
Applies to	This object and all descendant objects
Permissions	All checkboxes except **Full control**, **List contents**, **Read permissions**, and **Read all properties**.



Auditing Entry for cygnalabsdemo

Principal: Everyone Select a principal

Type: Success

Applies to: This object and all descendant objects

Permissions:

- □ Full control
- □ List contents
- □ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☑ Delete subtree
- □ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes
- ☑ All extended rights
- ☑ Create all child objects
- ☑ Delete all child objects
- ☑ Create builtinDomain objects
- ☑ Delete builtinDomain objects
- ☑ Create classStore objects
- ☑ Delete classStore objects
- ☑ Create msDS-ShadowPrincipalContainer objects
- ☑ Delete msDS-ShadowPrincipalContainer objects
- ☑ Create msExchConfigurationContainer objects
- ☑ Delete msExchConfigurationContainer objects
- ☑ Create msImaging-PSPs objects
- ☑ Delete msImaging-PSPs objects
- ☑ Create MSMQ Queue Alias objects
- ☑ Delete MSMQ Queue Alias objects
- ☑ Create MSMQ Upgraded User objects
- ☑ Delete MSMQ Upgraded User objects
- ☑ Create msPKI-Key-Recovery-Agent objects
- ☑ Delete msPKI-Key-Recovery-Agent objects
- ☑ Create msSFU30MailAliases objects
- ☑ Delete msSFU30MailAliases objects
- ☑ Create msSFU30NetId objects
- ☑ Delete msSFU30NetId objects
- ☑ Create msSFU30NetworkUser objects

8. Close the dialogs.
9. In the ADSI Edit window, right-click the root node and connect to the **Configuration** naming context. Create the same auditing entry for the **Configuration** partition. Go back to step 4.

Configuring Settings for Recovery for Active Directory

To recover system attributes and restore deleted AD users and passwords, you've got to update your Active Directory schema to store attributes in the recycle bin. Perform the following configuration steps in your Active Directory infrastructure.

Note: Make sure to use the account that is a member of the **Schema Admins** and that the changes to the schema are authorized.

1. Start **ADSI Edit** tool.
2. In **ADSI Edit** window, right-click the root node and select **Connect to**.
3. In the **Connection Settings** dialog,
   - expand the drop-down list under **Select a well known Naming Context** and specify *Schema*,
   - In **Select or type a domain controller or server**, provide a name of a DC that holds the **Schema Master FSMO** role.
4. Expand the **Schema** container, locate objects to update. Select objects, one by one. For each object, specify **Properties**, locate the **searchFlags** attribute, and provide a new value (equals to old value + 8).

OBJECT	ATTRIBUTE	VALUE
	SID History	
SID-History (sIDHistory)	searchFlags	Current + 8
	Passwords	
Unicode-Pwd (unicodePwd)	searchFlags	Current + 8
DBCS-Pwd (dBCSPwd)	searchFlags	Current + 8
Supplemental-Credentials (supplementalCredentials)	searchFlags	Current + 8
Lm-Pwd-History (lmPwdHistory)	searchFlags	Current + 8
Nt-Pwd-History (nTPwdHistory)	searchFlags	Current + 8

Configuring Settings for Windows File System

To enable Cygna Auditor to automatically install a data collecting service on the servers you want to audit, enable the following firewall rules.

1. On each server you want to audit, start the Windows Firewall with Advanced Security.
2. In **Inbound rules**, locate the following rules and enable them:

- Netlogon Service (NP-In)
- File and Printer Sharing (SMB-In)
- File Server Remote Management (SMB-In)

Note: You can skip this settings and opt to install the Cygna Auditor File Monitor service manually. If you plan to audit Cygna Auditor application server for file system changes, you must deploy the service manually.

Continue reading:

Windows File System

Configuring Settings for Azure

In most cases, you don't have to configure anything specifically to start auditing Azure AD, app authorization is enough.

To start collecting and auditing Azure Subscription information, then perform the following configuration steps even if you authorized the app before.

1. Start **Windows Powershell**.
2. Run command:

```
New-AzRoleAssignment -Scope "/" -RoleDefinitionName  "Monitoring Reader" -ApplicationId
'97bdeda3-63b1-480c-a013-3431aed2667a'
```

Continue reading:

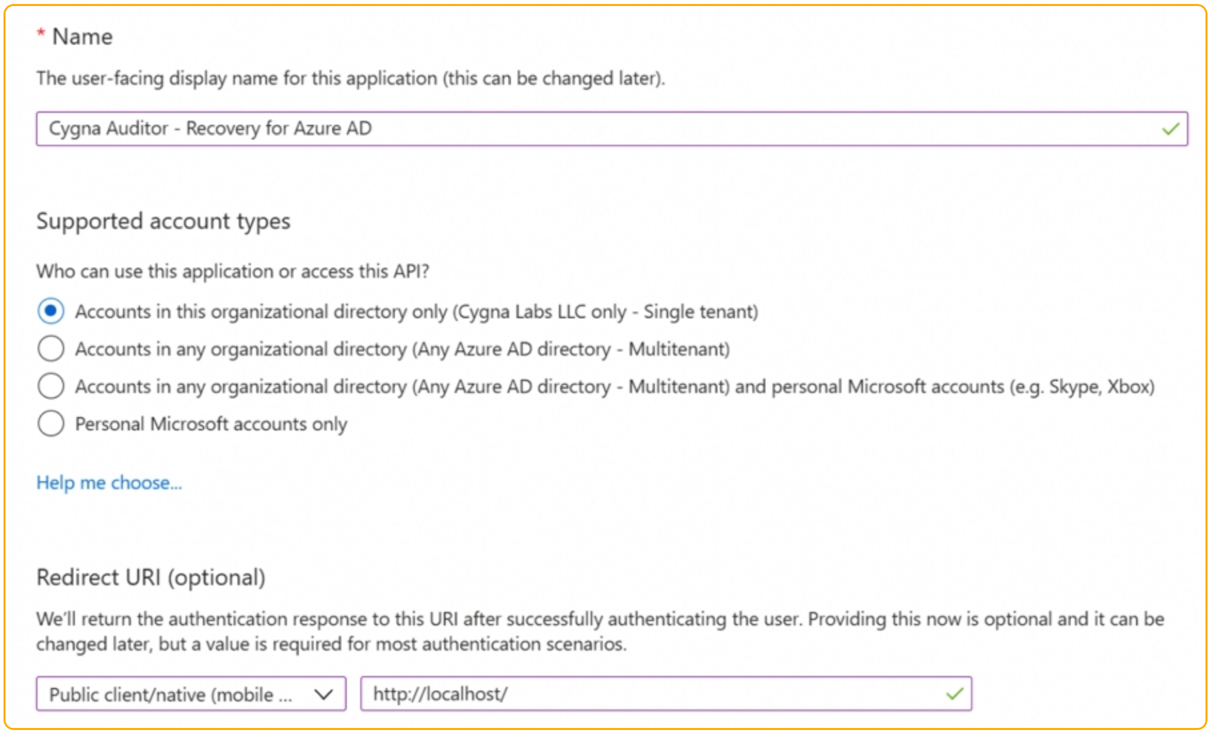
Microsoft Subscriptions

Configuring Settings for Recovery for Azure AD

To collect backup snapshots of your Azure AD and recover unwanted changes, perform the following configuration steps in your Azure infrastructure.

1. Log in to the Azure Portal. The account you use must be granted at least **Cloud Application Administrator** and **Privileged Role Administrator** roles.
2. Select **Azure Active Directory** and then specify **App registrations**.
3. Select **New registration** to create a new Azure AD application.
4. Provide an application **name** (e.g., *Cygna Auditor - Recovery for Azure AD*), specify the **supported account types**, and add a **Redirect URI**. Then select **Register** to create

the new application.



* Name

The user-facing display name for this application (this can be changed later).

Cygna Auditor - Recovery for Azure AD

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (Cygna Labs LLC only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | http://localhost/

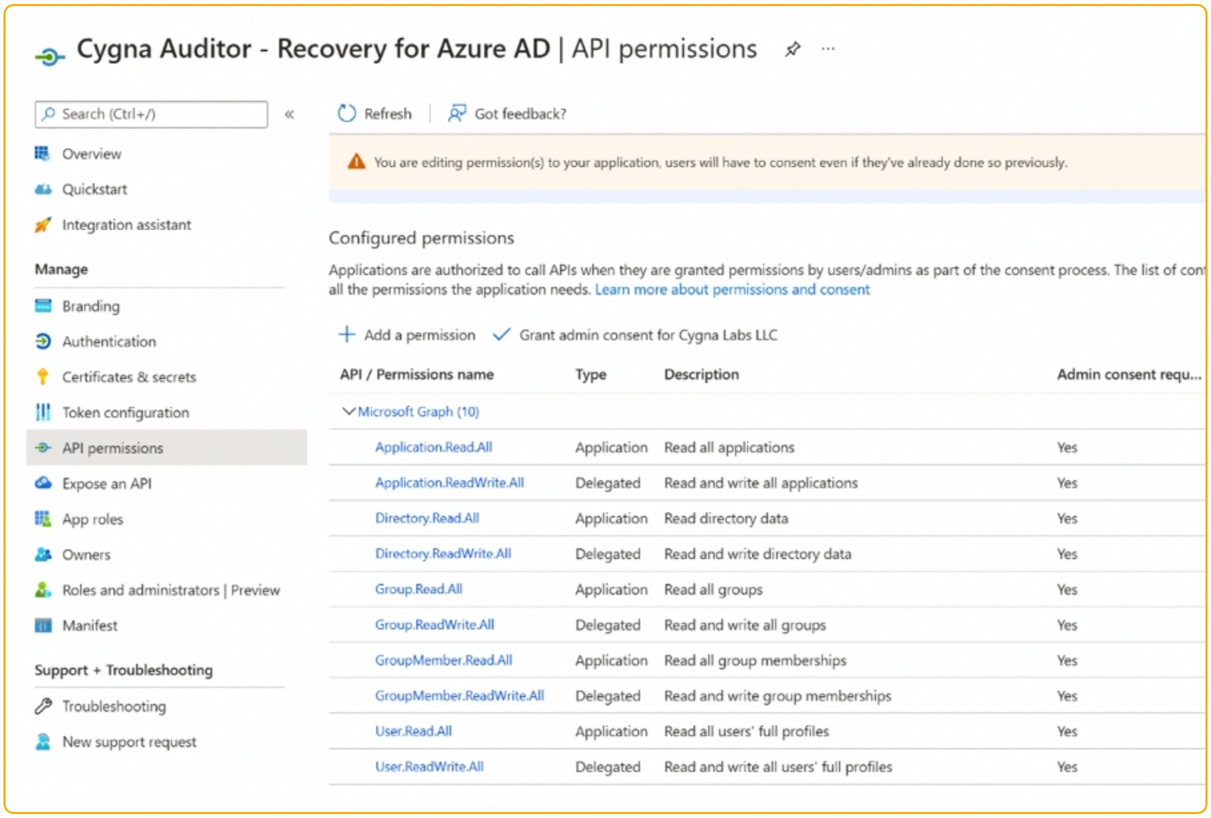
5. Copy the **Application ID** and **Directory (tenant) ID**.
6. In the new app, proceed to **Authentication / Advanced Settings** and set **Enable the following mobile and desktop flows** to *"Yes"*. Save.
7. In the left navigation bar, select **API permissions**, select **Microsoft Graph**, and add the following permissions:

Permission	Type
Application.ReadWrite.All	Delegated
Directory.ReadWrite.All	Delegated
Group.ReadWrite.All	Delegated
GroupMember.ReadWrite.All	Delegated
User.ReadWrite.All	Delegated
Application.Read.All	Application
Directory.Read.All	Application
GroupMember.Read.All	Application

Permission	Type
GroupMember.Read.All	Application
User.Read.All	Application

Note: If your tenant has MFA enabled, the "Recover As" functionality will not work as the underlying Graph API does not support MFA for these operations. In this case, either the local AD account must have permission to perform Recovery operations, or you may grant ReadWrite (instead of Read) access to the Application. For the second option, Recovery will work from within Cygna Auditor, but all operations will be performed by the Application instead of the User.

8. Select **Grant admin consent to** to confirm these permissions for the newly-created application.



Cygna Auditor - Recovery for Azure AD | API permissions

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of con all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...
Microsoft Graph (10)			
Application.Read.All	Application	Read all applications	Yes
Application.ReadWrite.All	Delegated	Read and write all applications	Yes
Directory.Read.All	Application	Read directory data	Yes
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes
Group.Read.All	Application	Read all groups	Yes
Group.ReadWrite.All	Delegated	Read and write all groups	Yes
GroupMember.Read.All	Application	Read all group memberships	Yes
GroupMember.ReadWrite.All	Delegated	Read and write group memberships	Yes
User.Read.All	Application	Read all users' full profiles	Yes
User.ReadWrite.All	Delegated	Read and write all users' full profiles	Yes

9. Navigate to **Certificates & secrets** and create a secret for the application. For security purposes, use this secret only for collection and recovery operations made by Cygna Auditor.

   - Select **New client secret**, provide a description and expiry, then select **Add**. Note that recovery collections will stop after the expiry and you will need to generate a new secret at that time.

- Copy the value to use later. These values will be inaccessible after you leave this screen.

Configuring Settings for Exchange Online

Enabling Mailbox Auditing

To enable Cygna Auditor to collect audit data, configure the following settings through the Windows PowerShell.

1. Start the **Windows PowerShell**.
2. Connect to your Exchange Online organization. Subsequently run the following commands:

   ```
   $UserCredential = Get-Credential
   ```

   Upon request, enter the **Microsoft 365 global admin** credentials.

   ```
   $Session = New-PSSession –ConfigurationName Microsoft.Exchange –ConnectionUri
   https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential –Authentication
   Basic -AllowRedirection
   ```

   ```
   Import-PSSession $Session
   ```

3. Enable mailbox logging and configure auditing of all actions for all user mailboxes in your Exchange Online organization.

   ```
   Get-mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | ForEach {Set-Mailbox
   $_.Identity -AuditEnabled $true -AuditAdmin
   Copy,Create,FolderBind,HardDelete,MessageBind,Move,MoveToDeletedItems,SendAs,Send
   OnBehalf,SoftDelete,Update -AuditDelegate
   Create,FolderBind,HardDelete,Move,MoveToDeletedItems,SendAs,SendOnBehalf,SoftDelete,
   Update -AuditOwner
   Create,HardDelete,MailboxLogin,Move,MoveToDeletedItems,SoftDelete,Update }
   ```

Continue reading:

Microsoft Subscriptions

Configuring Settings for On-Premises Exchange

Enabling Mailbox Auditing for Exchange Server 2016

1. Start the **Windows PowerShell**.
2. Enable mailbox logging and configure auditing of user mailboxes for your on-premises Exchange organization by running the following commands:

   ```
   Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditLogAgeLimit 365 -AuditEnabled $true
   ```

   ```
   Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets * -
   AdminAuditLogParameters * -AdminAuditLogExcludedCmdlets $null -Force -LogLevel Verbose
   -TestCmdletLoggingEnabled $true -AdminAuditLogAgeLimit 365
   ```

3. Specify activity to be audited. Run commands:

   ```
   Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditOwner Update, Move,
   MoveToDeletedItems, SoftDelete, HardDelete, Create, MailboxLogin
   ```

   ```
   Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditDelegate
   Update,Move,Create,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendO
   nBehalf
   ```

   ```
   Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditAdmin Update, Move,
   MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs, SendOnBehalf,
   Create,Copy,MessageBind
   ```

Enabling Mailbox Auditing for Exchange Server 2019

1. Start the **Windows PowerShell**.
2. Enable mailbox logging and configure auditing of user mailboxes for your on-premises Exchange organization by running the following commands:

   ```
   Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditLogAgeLimit 365 -AuditEnabled $true
   ```

   ```
   Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets * -
   AdminAuditLogParameters * -AdminAuditLogExcludedCmdlets $null -Force -LogLevel Verbose
   -TestCmdletLoggingEnabled $true -AdminAuditLogAgeLimit 365
   ```

3. Specify activity to be audited. Run commands:

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditOwner Update, Move, MoveToDeletedItems, SoftDelete, HardDelete, Create, UpdateFolderPermissions, UpdateInboxRules, UpdateCalendarDelegation, MailboxLogin
```

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditDelegate Update,Move,Create,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf
```

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditAdmin Update, Move, MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs, SendOnBehalf, Create, UpdateFolderPermissions, UpdateInboxRules, UpdateCalendarDelegation,Copy,MessageBind
```

Granting Permissions

1. Navigate to **Exchange admin center / Permissions**.
2. Assign the **Compliance Management** and **Organization Management** admin role groups to the collector account (the one Cygna Auditor can use to collect data from Exchange).

Enabling PowerShell Authentication

1. Navigate to **Exchange admin center / Servers** and select **Virtual directories**.
2. Configure as follows:
    - **Select servers**: All servers
    - **Select type**: PowerShell
3. Select **PowerShell (Default Web Site)**, proceed to the **Authentication** tab, and enable **Basic authentication**.

Continue reading:

On-Premises Exchange

Configuring Settings for VMware

To enable Cygna Auditor to collect audit data, configure the following settings on your VMware station:

- Assign the Cygna user account a role with the Global.Health privilege to view the system events and health.

Continue reading:

VMware

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.

Start Collecting Data

> **QUICK TIP**: Have you configured your domain for auditing? If you want to audit an untrusted domain, make sure you have access to it from the Cygna Auditor application server.

1. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **Active Directory / Domains**.
2. Click ⊞ to add a new domain.
3. 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 over relying on event logs.

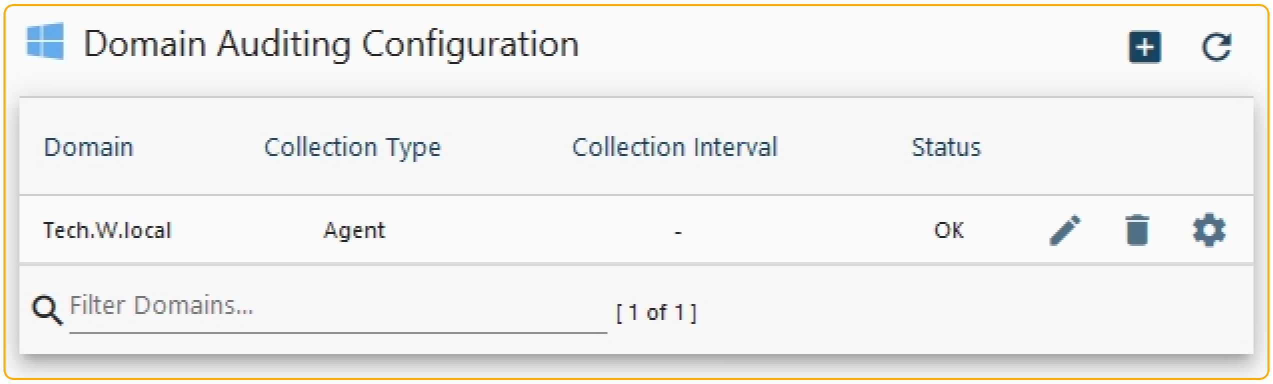
OPTION	DESCRIPTION
Domain Selection tab	
User name Password	Enter the user credentials. Specify a user name in the following format: domain\username. Cygna Auditor will use this account to collect audit data from the domains this account has access to. If you specified event log-based auditing, make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

OPTION	DESCRIPTION
Collection Settings tab	
Data collection method	Select one of the following: • Cygna Auditor Agent (preferred) • Event log
Combine similar events occurring within the specified interval	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. If this option is cleared, Cygna Auditor will capture a record for each event.
Attempt to locate workstation information for events	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.
Perform reverse name lookup when event only include an IP address for the remote workstation	Select to try identifying a DNS name of a remote workstation.
Ignore login events	Select to skip login events from processing.
Enable nested group alerting and auditing	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. Select **Manage nested groups** and specify groups in the pop-up window. Expand **Advanced collector settings** to configure additional options for nested group auditing.
Advanced collector settings	Expand this section to configure additional settings if necessary.

OPTION	DESCRIPTION
	• Exclude attributes from data collection–enter a list of attributes separated by commas. • Select the **Ignore login events** checkbox. • Set up GP backup configuration, including: • Enabling GPO backup for detailed change reporting–with its help you'll be able to see changes in group policy objects over time. • Ensuring all GPOs have at least one backup–it gives you ability to see and revert changes at all times. • If nested group alerting and auditing is enabled, specify details for reporting changes in the **Nested group auditing settings** section. • **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. • **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. • **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 generated that they were removed from the top level Group 1. • **Generate backlink events for nested group changes**–by default, events are

OPTION	DESCRIPTION
	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.



Domain Auditing Configuration

Domain	Collection Type	Collection Interval	Status
Tech.W.local	Agent	-	OK

Filter Domains... [1 of 1]

Configuring Active Directory 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 domain controller 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.

Continue reading:

Configuring Auditing Policies

Configuring Collector Settings

Configuring Password Expiry Alerts

Dashboard

Auditing

Reports

Rollback for Active Directory

Recycle Bin for Active Directory

Active Directory Browser

Configuring Auditing Policies

Cygna Auditor enables you to fine-tune Active Directory agent-based auditing and pre-filter events on the data collection stage with a help of auditing policies. You can pick the events you want to track and write only the most important ones to the audit database. On top of that, you can allow or forbid certain AD actions within your domain based on these auditing policies.

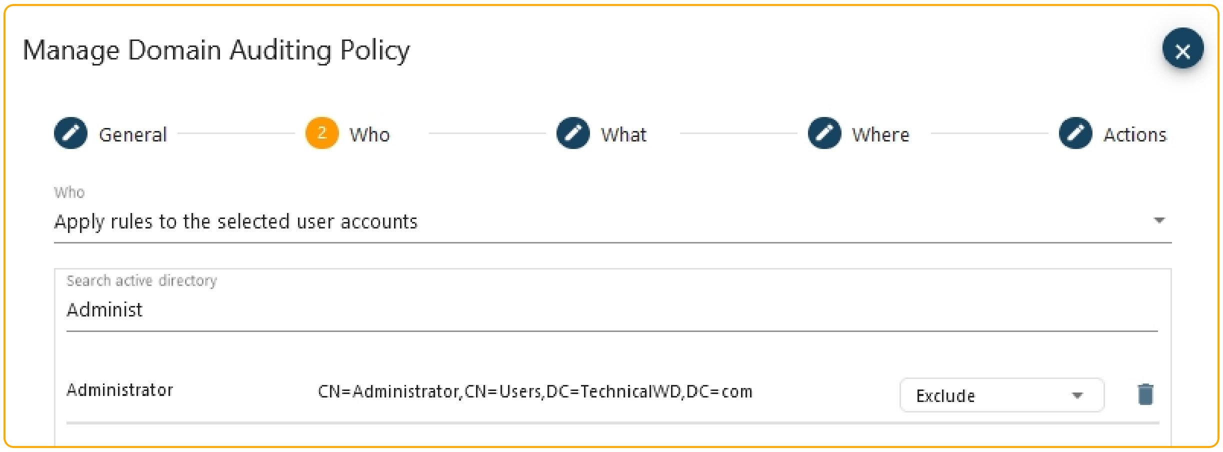
Example 1: configure an auditing policy to skip all service account activity.

Example 2: configure a protective auditing policy that will restrict modifications of domain-critical OUs and groups (e.g., Domain Admins) for all users except one or two system administrators.

Configuring auditing policies is optional. To collect all AD events without pre-processing, skip the steps below.

Note: Applies to agent-based data collection only.

1. Navigate to **Configuration / Active Directory / Auditing Policies** and select ⊞ to add a new policy.
2. On the **General** step, select a domain and provide a policy name and description. You can create the policy without enforcing it (for example, create a pull of policies for the future) or enable it right away.
3. On the **Who** step, assign the policy to all users or pick specific users from the list, include or exclude them. Tips:
   - **Including** a user means the policy you configure will only apply to this user, all users will be excluded.
   - **Excluding** a user means the policy you configure will apply to all users except those who are excluded.
   - Don't include and exclude users in the same policy to avoid collisions.



Manage Domain Auditing Policy

Who: Apply rules to the selected user accounts

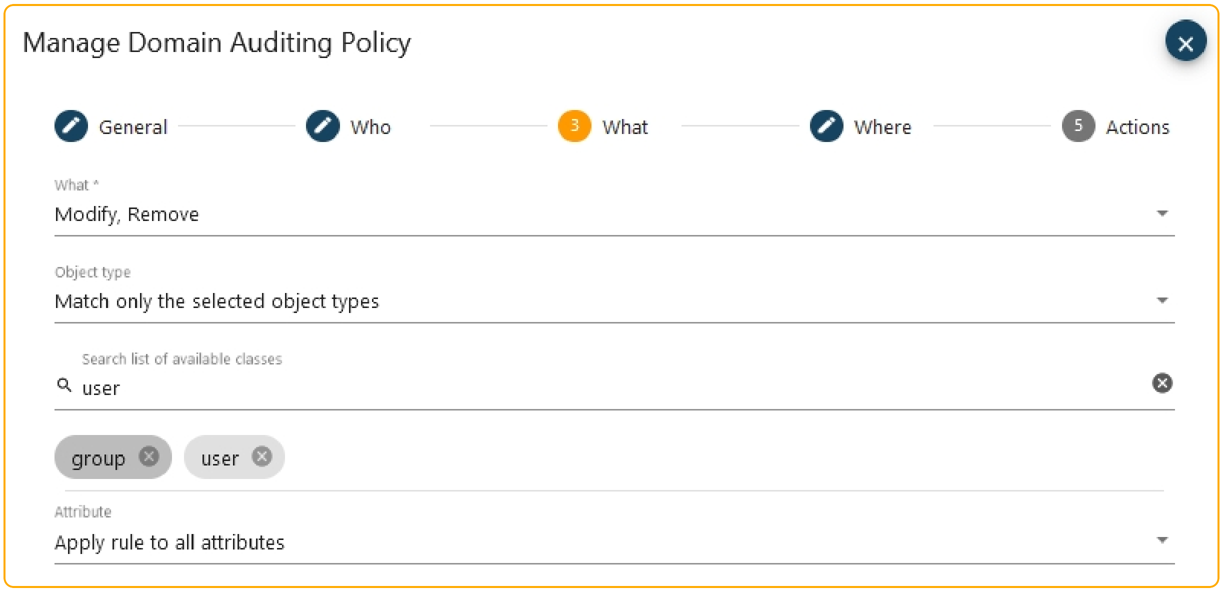
Search active directory: Administ

Administrator CN=Administrator,CN=Users,DC=TechnicalWD,DC=com Exclude

4. On the **What** step, pick actions such as Create, Modify, etc. You can restrict actions to specific objects and attributes.

   If you create a protection policy, you'll typically want to restrict:

   - All deletes
   - All modify events for GPO
   - All modify or other events for group, contact, printQueue, volume, organizationalUnit, and container object types.



Manage Domain Auditing Policy

What *: Modify, Remove

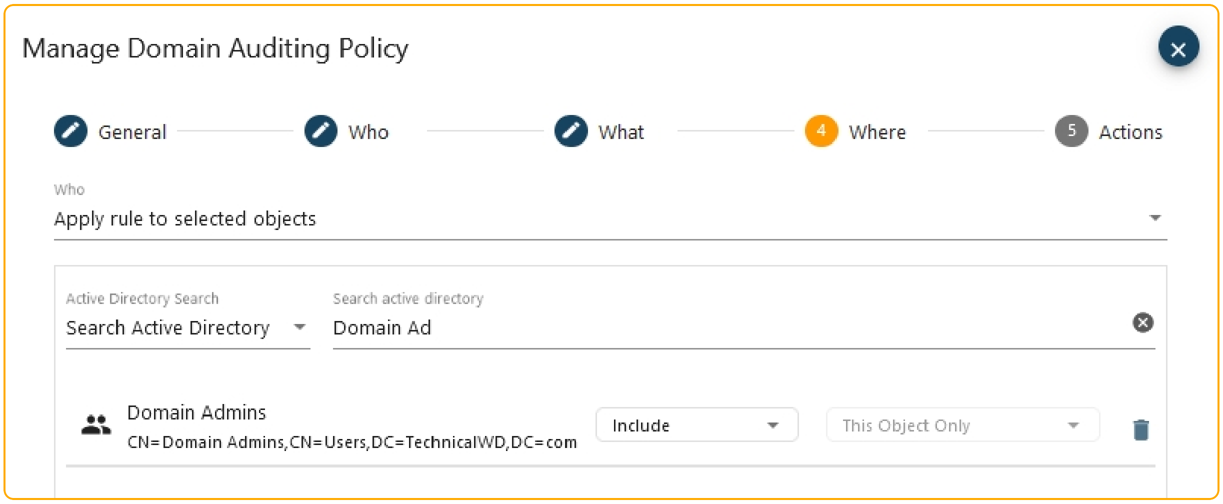
Object type: Match only the selected object types

Search list of available classes: user

group user

Attribute: Apply rule to all attributes

5. On the **Where** step, decide if the policy applies to the entire domain or specific AD objects or containers. Include or exclude them if necessary.



Manage Domain Auditing Policy

Who: Apply rule to selected objects

Active Directory Search: Search Active Directory

Search active directory: Domain Ad

Domain Admins
CN=Domain Admins,CN=Users,DC=TechnicalWD,DC=com

Include

This Object Only

6. On the **Actions** step, enable options for the auditing policy. It can affect auditing and events collection as well as protect your AD domain from unauthorized actions.

Option	Description
Enable auditing	• **Enable** auditing to start collecting events matching the criteria you specified. • **Disabling** auditing means any event matching the policy will skipped by Cygna Auditor and won't be written to the audit database. For example, you can create a policy and disable auditing to exclude changes by service accounts, or changes to attributes.
Enable protection	Enabling protection restricts events matching the policy from occurring. Users will typically get "Object not found" error as they try to perform restricted actions. • Select **Write a Protection Policy Event to the Microsoft Event Log** to capture such failed events and add them to the event log on the Domain Controller that prevented the change. • Select **Write a Protection Policy Event to Cygna Auditor for AD audit log** to capture such failed attempts and add them to Cygna Auditor database.

Continue reading:

Configuring Collector Settings

Dashboard

Auditing

Reports

Rollback for Active Directory

Recycle Bin for Active Directory

Active Directory Browser

Configuring Collector Settings

The collector captures your Active Directory state and performs backup collections of AD objects.

Note: Active Directory collector is independent from data collection and Cygna Auditor agents.

1. Navigate to **Configuration / Active Directory / Collector** and select ⊞ to add a new collector.
2. On the **General** step, select a domain and provide a description if necessary. You can create the collector configuration without enforcing it or turn it on right away.
3. On the **Domain** step, enter administrator's credentials and look up for DCs.
4. On the **Options** step, define collector configuration:

Option	Description
Collection interval	Specify the frequency of AD state collection.
Select a naming context	Choose a domain partition to collect data for: default, configuration, schema, or custom.
Select the collector scope	Specify the nesting level for data collection: this object only, this object and all child objects, or child objects only.
Perform a full backup on every collection interval	Enable to create full backups.

5. Check the **Summary** page and save configuration.

Continue reading:

Dashboard

Auditing

Reports

Rollback for Active Directory

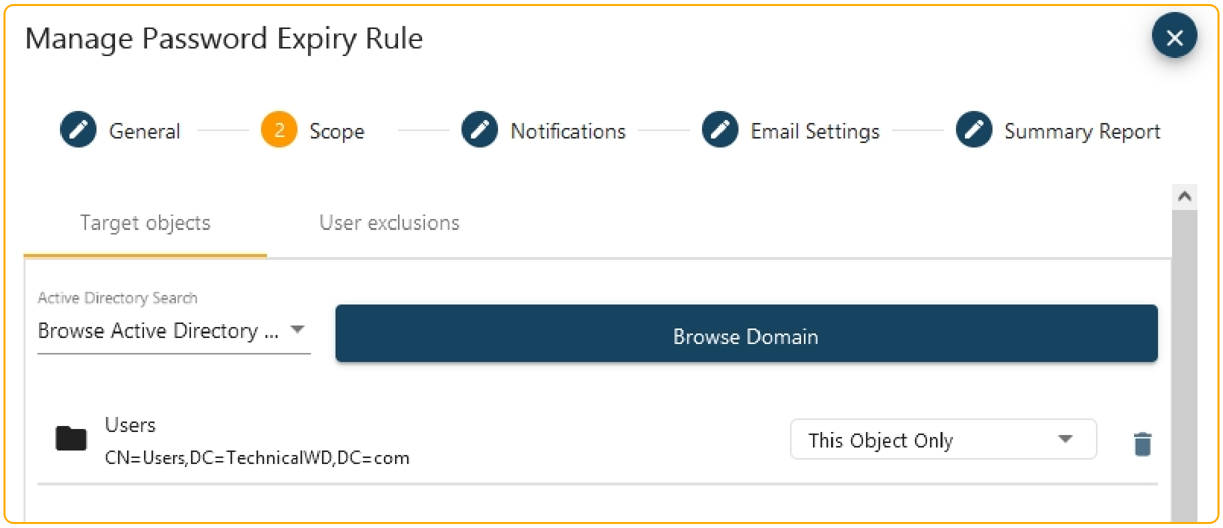
Recycle Bin for Active Directory

Active Directory Browser

Configuring Password Expiry Alerts

Protect your AD accounts by enforcing a strong password policy that includes both complexity requirements and password expiration period. Cygna Auditor can send alerts about passwords that are about to expire.

1. Navigate to **Configuration / Active Directory / Password Expiry Alerts** and select ⊞ to add a new password expiry rule.
2. On the **General** step, select a domain, provide a rule and description for a rule. You can create a rule without enforcing it or turn it on right away.
3. On the **Scope** step:
    1. First proceed to the **Target objects** tab and define the AD containers and groups that should be monitored for password expiration. You can search for a specific group (e.g., *CA admins*) or browse Active Directory and pick an object (e.g., *Users*). For a selected object, specify the nesting level: this object only, this object and all child objects, or child objects only.
    2. Proceed to the **User exclusions** tab to specify users that shouldn't be tracked for expiring passwords.

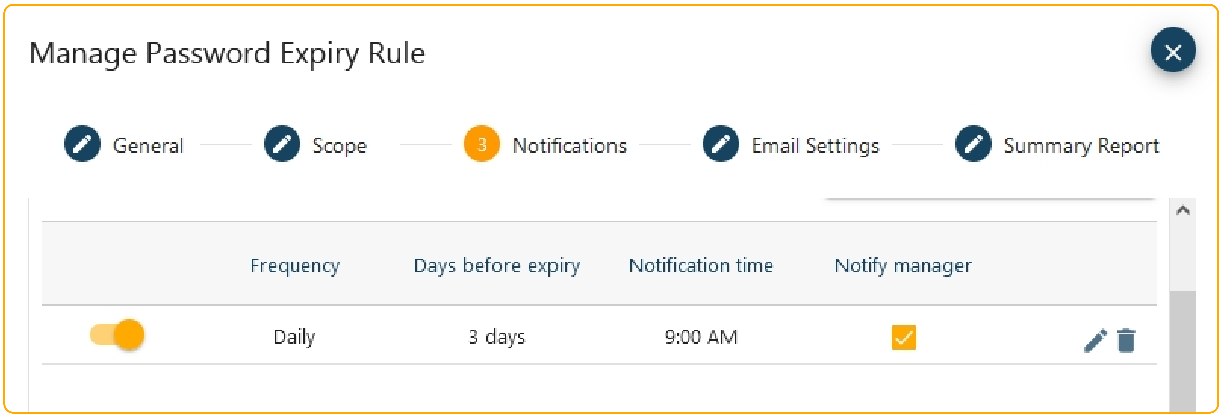


Manage Password Expiry Rule

Active Directory Search: Browse Active Directory ...

Users
CN=Users,DC=TechnicalWD,DC=com
This Object Only

4. On the **Notifications** step, create one or more scheduled notifications. Enable notification, specify its frequency (one time or daily), set how many days in advance the users should be notified, at what time. You've got an option to inform user's manager as well.



Manage Password Expiry Rule

	Frequency	Days before expiry	Notification time	Notify manager	
●	Daily	3 days	9:00 AM	☑	

5. On the **Email Settings** step, enter the email address to send notifications from and the subject.
6. On the **Summary Report** step, configure overview emails. Specify how often you want to send emails, recipients, etc.

Continue reading:

Dashboard

Auditing

Reports

Rollback for Active Directory

Recycle Bin for Active Directory

Active Directory Browser

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.

Start Collecting Data

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. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **Amazon Web Services Configuration**.
2. Click ⊞ to add a new AWS configuration.
3. 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.

OPTION	DESCRIPTION
Verify connectivity	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. 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.
	The **Collector Settings** step
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.

Note: Make sure Cygna Auditor has access to ***.amazonaws.com (GET and POST)**.

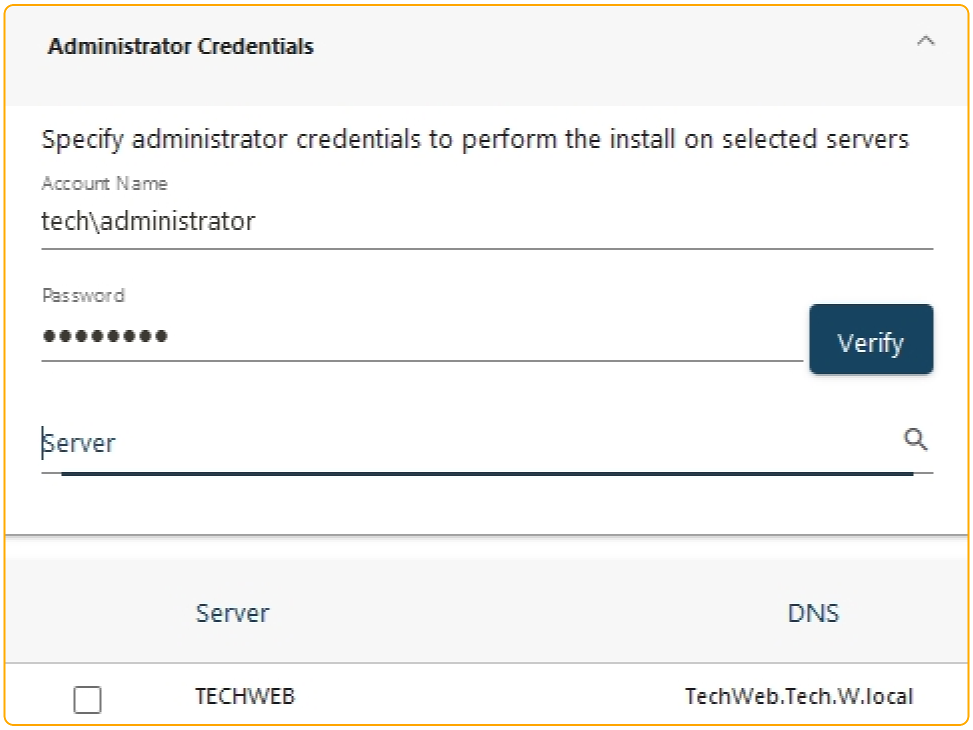
Windows File System

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.

Start Collecting Data

1. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **File System / Servers**.
2. Click + to add servers for auditing. To collect data, Cygna 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.
3. In the dialog that opens, provide administrator credentials. Cygna Auditor will look up for servers and show the list of available servers. Select servers you want to audit and click **Install**.



Administrator Credentials

Specify administrator credentials to perform the install on selected servers

Account Name: tech\administrator

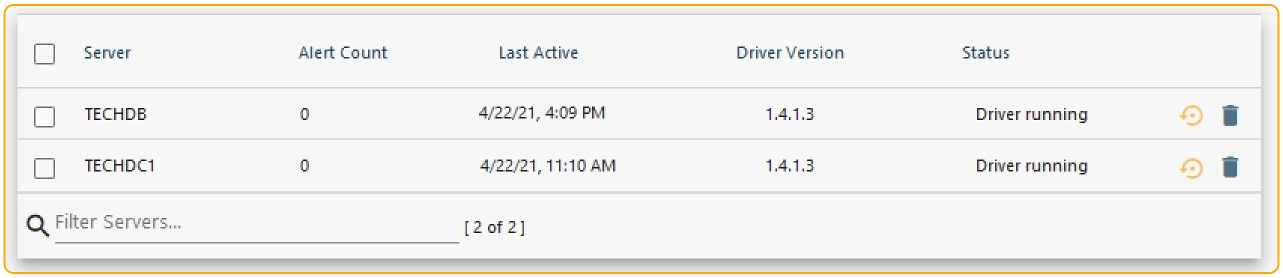
Password: ••••••••

	Server	DNS
□	TECHWEB	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)**.

4. Cygna Auditor will suggest you add data collection filters.

Check the data collection status in the audited servers list.

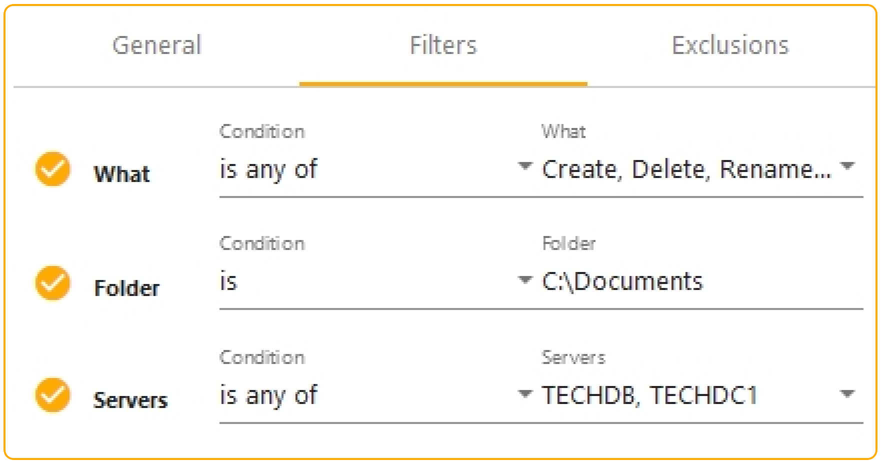


□	Server	Alert Count	Last Active	Driver Version	Status
□	TECHDB	0	4/22/21, 4:09 PM	1.4.1.3	Driver running
□	TECHDC1	0	4/22/21, 11:10 AM	1.4.1.3	Driver running

Configure Monitoring Filters

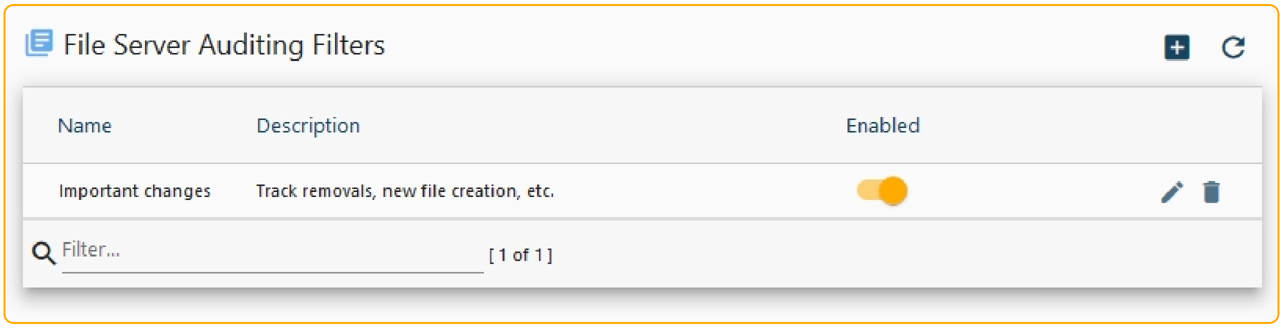
Filters help you narrow down the number of events collected and processed by Cygna Auditor. Typically, file system generates thousands of events, mostly read events, processing all of them may have significant impact on your network bandwidth as well as Cygna Auditor server performance. Create filters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

1. Navigate to **Configuration / File System / Filters** and click ⊞.
2. Provide a name for a filter and description.
3. Add filtering criteria and define exceptions if necessary. For example:



	Condition	
✓ What	is any of	What: Create, Delete, Rename...
✓ Folder	is	Folder: C:\Documents
✓ Servers	is any of	Servers: TECHDB, TECHDC1

You'll see all filters in the list. Disable or update filters if necessary.



File Server Auditing Filters

Name	Description	Enabled
Important changes	Track removals, new file creation, etc.	●

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.

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.

Start Collecting Data

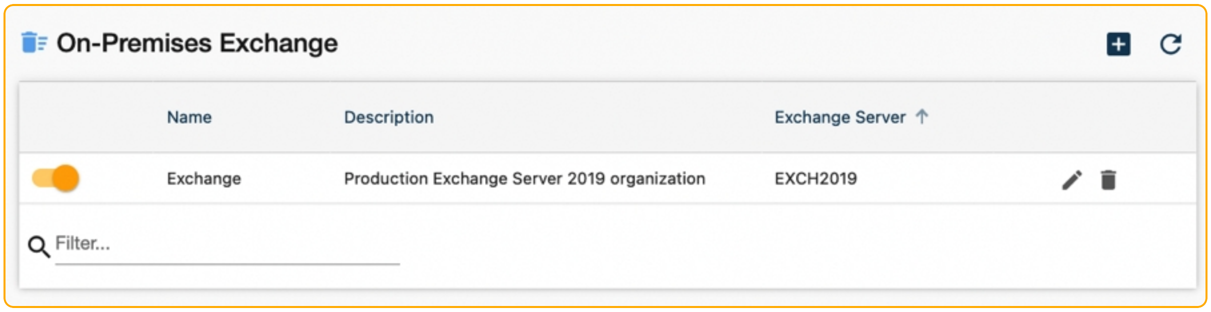
QUICK TIP: Have you configured your Exchange Server for auditing? For more information, see Configuring Settings for On-Premises Exchange.

1. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **On-Premises Exchange / Servers**.
2. Click + to add a new Exchange organization.
3. 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.

OPTION	DESCRIPTION
Exchange Server	Provide an Exchange Server name.
Authentication mechanism	Specify the auth method and verify connection.
Collection Schedule tab	
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.



On-Premises Exchange

	Name	Description	Exchange Server ↑
●	Exchange	Production Exchange Server 2019 organization	EXCH2019

Configuring Filters for Data Collection

Filters help you narrow down the number of events collected and processed by Cygna Auditor. Typically, the Exchange Server generates thousands of events, mostly read events, such events are regarded as noise. Create filters to audit and process the events you are interested in and skip others.

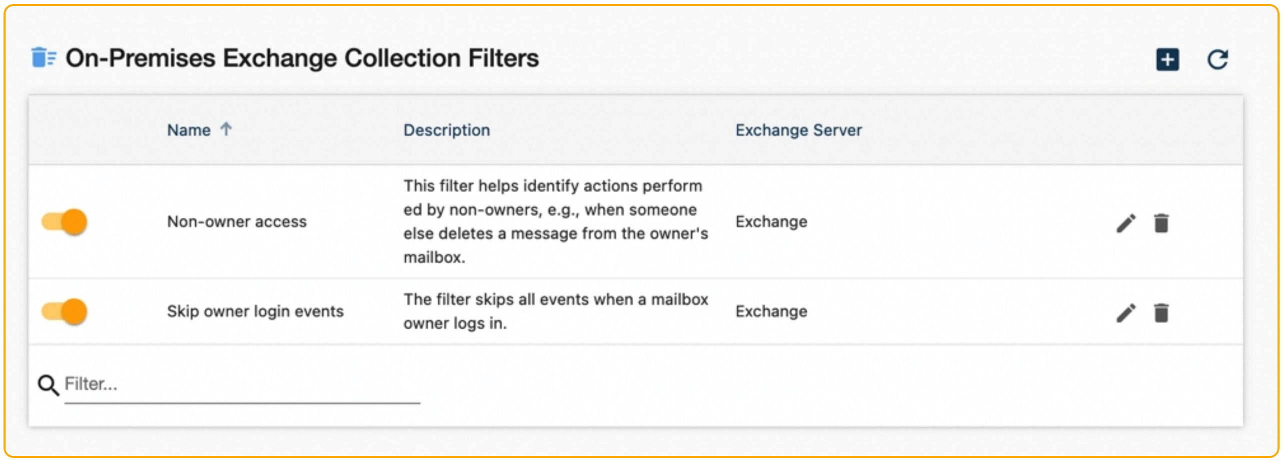
Note: The filters are optional.

1. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **On-Premises Exchange / Filters**.
2. Click + to add a new data collection filter.
3. Complete the filter configuration.

OPTION	DESCRIPTION
The **General** tab	
Enable this collection filter	Set to "on" to activate the filter.
Select an Exchange Server	Pick an Exchange Server from the list.
Name	Provide a name for a filter
Description	Add an explanation what this filter is used for.
The **Who** tab	
Who	Specify users or groups to be affected by this filter. Set to one of the following: • **Apply filter to all mailboxes and groups** • **Apply filter to the selected mailboxes and groups**–search for AD users or groups and decide whether to include or exclude them. For example, exclude the Domain Admins group to skip all changes made by your system administrators.
The **What** tab	
What	Specify events to be filtered. Set to one of the following: • **Apply filter to all events** • **Apply filter to the selected events**–specify events from the list and decide whether to include or exclude them. For example, include only events

OPTION	DESCRIPTION
	made by non-owners.
	The **Where** tab
Where	Specify target users or groups for this filter. Set to one of the following: • **Apply filter to all mailboxes and groups** • **Apply filter to the selected mailboxes and groups**–search for AD users or groups and decide whether to include or exclude them. For example, include the Domain Users group.

The filters you create will appear in the list.



On-Premises Exchange Collection Filters

	Name ↑	Description	Exchange Server
●	Non-owner access	This filter helps identify actions performed by non-owners, e.g., when someone else deletes a message from the owner's mailbox.	Exchange
●	Skip owner login events	The filter skips all events when a mailbox owner logs in.	Exchange

Continue reading:

[Dashboard]

[Auditing]

[Reports]

Microsoft Subscriptions

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.

Start Collecting Data

1. On the Cygna Auditor home page, select **Configuration** and then drill down to **Microsoft Subscriptions**.
2. Click + to add a Microsoft 365 organization.
3. **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 Configuring Settings for Azure.
4. Specify the polling interval. By default, 10 minutes. This value controls how often Cygna Auditor will check for updates in your Microsoft 365 apps.
5. Ensure the Enabled column is active ☑ .
6. Check connectivity. Click **Verify** to ensure Cygna Auditor has access to these resources:

   cygnacloud.azurewebsites.net (GET and POST)

   graph.microsoft.com (GET only)

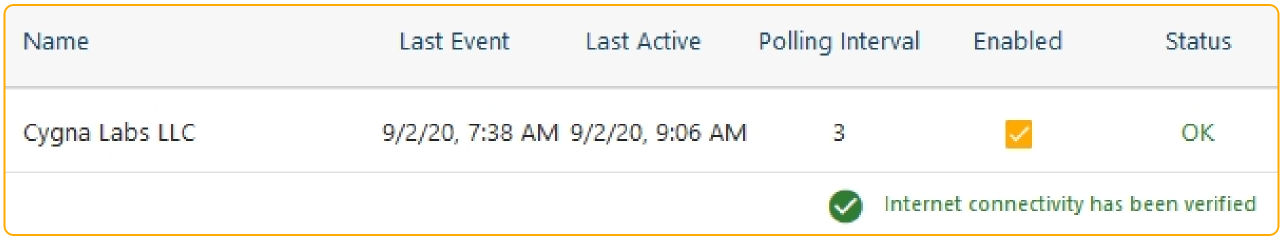
   login.microsoftonline.com (GET only)

   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.

Start Collecting Data

1. On the Cygna Auditor home page, click the **Configuration** tile and then drill-down to **VMware vCenter**.
2. Click ⊞ to add a server.
3. 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 Password	Enter the user credentials.
Interval	Set he data collection frequency.
Ignore certificate	Select the checkbox if you prefer to skip the SSL certificate verification.

The servers you specified will appear in the list.

Continue reading:

Dashboard

Auditing

Reports

Administration

Cygna Auditor does not require a lot of administration or maintenance, here are just a few administrative tasks you should take care of:

TASK	GO TO	IN THE PRODUCT
Assigning roles within the product	Delegation	Configuration / Delegation
Configure connection to PowerBroker Management Suite	PowerBroker Management Suite Connection	Configuration / PowerBroker Management Suite
Configuring email notification settings	Notifications	Configuration / System Configuration / Email
Configuring Cygna Auditor service settings	Service	Configuration / System Configuration / Service
Adding a proxy gateway	Proxy	Configuration / System Configuration / Proxy
Configure logging for Syslog and Splunk	Remote Logging	Configuration / System Configuration / Remote Logging
Managing licenses	Licenses	Configuration / Licenses
Clearing stale data	Data Purging	Configuration / Data Purging
Checking data collecting status	Status	Status or 🔔
Managing database connections	Database Connections	Configuration / Database Connections
Configuring product look&feel	Application Settings	⚙
Re-running a configuration wizard	Configuration Wizard	? or Configuration / Configuration Wizard
Downloading Cygna RSAT for Active Directory Users and Computers	Cygna RSAT	🔔 / About

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.

Delegation

Cygna Auditor collects activity data in your organization so that you can be sure that no breach can occur. If distributed freely, the audit data can be a huge security issue of its own since internal attackers can use it to their own advantage. 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.

As a security rule of thumb, the most strict model is enforced by default–only the user who installed Cygna Auditor can operate the web-console. This user is assigned the Global administrator role in the product and can grant and revoke permissions. Unauthorized users as they log in will only see a product home page without any configuration details or data.

Looking for more examples? Check out this Cygna blog post.

Built-in Roles

Cygna Auditor comes with a set of built-in roles. These roles cannot be removed or modified. To view available roles, navigate to **Configuration / Delegation / Roles**.

- The most powerful role is **Global administrator**. It provides access to all product functionality including role delegation. The first user to install Cygna Auditor is granted the **Global administrator** role.
- For each audit source, three roles are available:
  - Owner–provides extensive permissions to view data and manage configuration
  - Contributor–provides permissions to partially manage configuration and view data
  - Reader–provides permissions to view data

  For example "Active Directory Owner", "Microsoft 365 Reader".

Creating Custom Roles

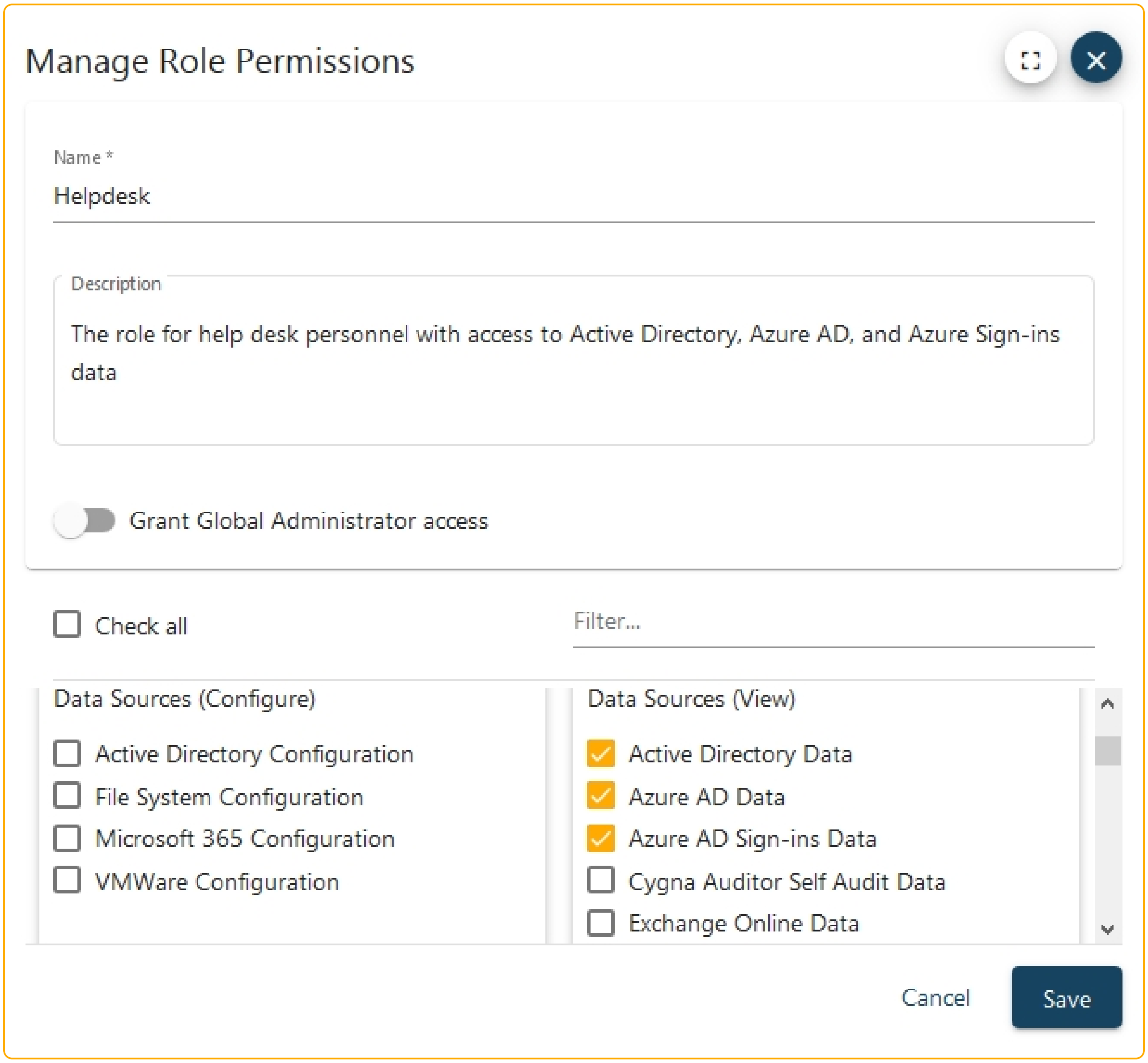
As an administrator, you can create custom roles with atomic permissions to ensure that users are given access to the exact amount of data they need based on your company's security guidelines and policies.

Cygna Auditor enables you to create new roles from scratch or clone an existing role and modify it.

To create a new role:

1. Navigate to **Configuration / Delegation / Roles**.
2. Do one of the following:
   - To create a new role: click ⊞ .
   - To copy and then modify an existing role: click ≡ next to a role and select **Clone**.
3. In the **Manage Role Permissions** window:

FIELD	DESCRIPTION
Name, description	Add the role name and a short explanation, for example: "Helpdesk – The role for helpdesk personnel with access to Active Directory, Microsoft 365, and Azure Sign-ins data".
Grant Global Administrator access	Enable with option if you want to create a duplicate for the global administrator role. If you enable this option, you won't be able to pick permissions individually, all permissions will be enabled for this role.
Permissions section	Check permissions you want to grant. Note: If you create a powerful role, you may opt-in to **Check all** permissions and then clear those you don't need.



Manage Role Permissions

Name *
Helpdesk

Description
The role for help desk personnel with access to Active Directory, Azure AD, and Azure Sign-ins data

○ Grant Global Administrator access

□ Check all

Filter...

Data Sources (Configure)

- □ Active Directory Configuration
- □ File System Configuration
- □ Microsoft 365 Configuration
- □ VMWare Configuration

Data Sources (View)

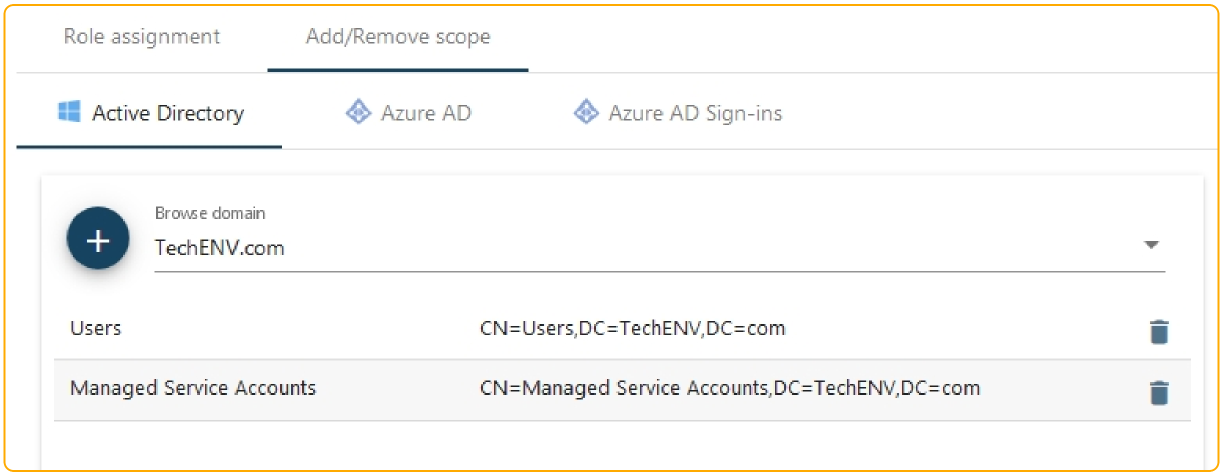
- ☑ Active Directory Data
- ☑ Azure AD Data
- ☑ Azure AD Sign-ins Data
- □ Cygna Auditor Self Audit Data
- □ Exchange Online Data

Assigning Roles to Users

1. Navigate to **Configuration / Delegation / Role Assignment**.
2. Select ⊞.
3. On the **Role Assignment** tab:
   - Select a role from the list.
   - Specify if you want to assign this role to a user or a group.
   - Provide a name.

4. On the **Add/Remove Scope** tab, you can limit role access to specific objects within the data source module (AD domain, tenant, etc.). The scope can be as discrete as Azure AD tenant or a certain AD container (e.g., Users, Managed Service Accounts).

   Note: To provide access to all objects, configure a scope and leave it blank.

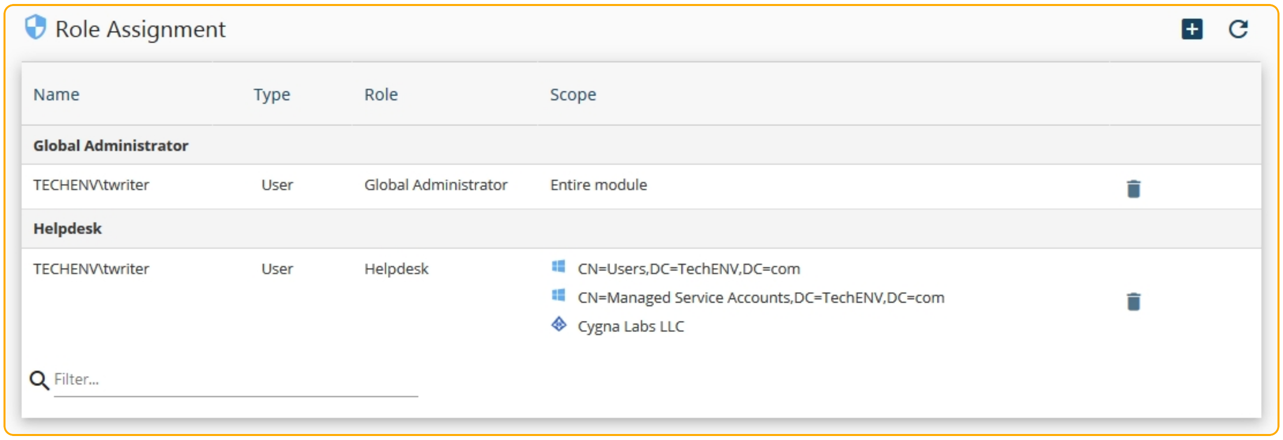


Browse domain: TechENV.com

Users	CN=Users,DC=TechENV,DC=com
Managed Service Accounts	CN=Managed Service Accounts,DC=TechENV,DC=com

5. Select **Save**.

You can always review users with their assigned roles and rearrange them if necessary.


Role Assignment

Name	Type	Role	Scope
Global Administrator			
TECHENV\twriter	User	Global Administrator	Entire module
Helpdesk			

TECHENV\twriter	User	Helpdesk	CN=Users,DC=TechENV,DC=com
			CN=Managed Service Accounts,DC=TechENV,DC=com
			Cygna Labs LLC

PowerBroker Management Suite Connection

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. Navigate to **Configuration / PowerBroker Management Suite**.
2. 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.

Data Purging

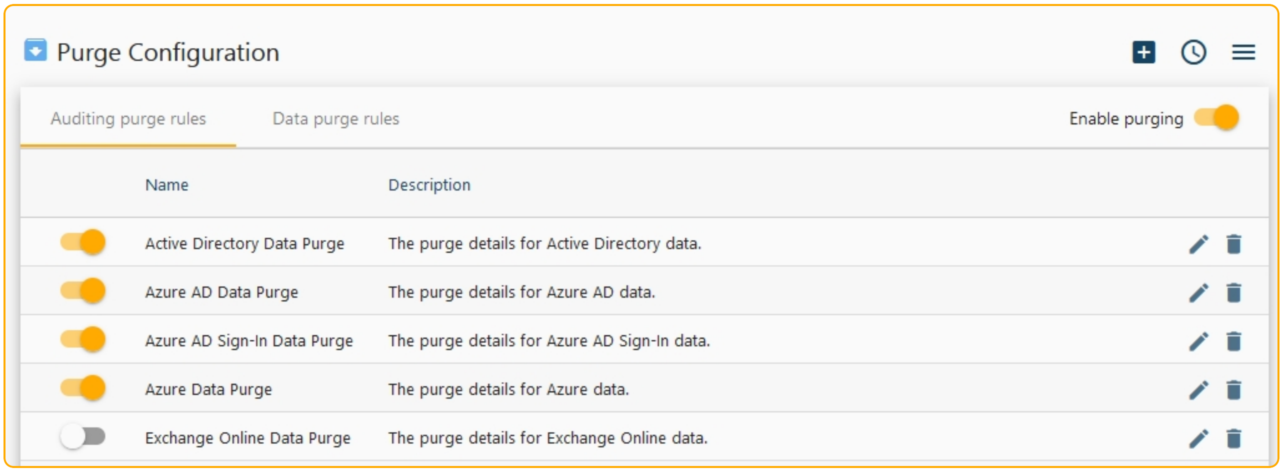
Cygna Auditor enables you to clear stale data and free up space in the Audit Database. By default, Cygna Auditor comes with preset data purging rules. The retention is set to 365 days for each data source–it means events and data older than 365 days are removed from the database.

Enable ready-to-use rules or configure custom data purging. For example, you can keep Active Directory events longer but remove Azure AD Sign-Ins after 60 days to save up space.

To configure data purging:

1. Navigate to **Configuration / Data Purging**.
2. Toggle **Enable purging**.

3. On the **Auditing purge rules** tab, toggle the rules. The auditing purge rules apply to change events. Drill down to a rule to change data purging period and set up filtering for a specific data source. Alternatively, create a new rule by clicking the plus icon. Provide its name and create an auditing query (see Auditing)–events matching the search criteria will be purged.
4. On the **Data purge rules** tab, toggle rules for backups. Here you can update the maximum days value for clearing up the backup data.



Purge Configuration

	Name	Description
●	Active Directory Data Purge	The purge details for Active Directory data.
●	Azure AD Data Purge	The purge details for Azure AD data.
●	Azure AD Sign-In Data Purge	The purge details for Azure AD Sign-In data.
●	Azure Data Purge	The purge details for Azure data.
○	Exchange Online Data Purge	The purge details for Exchange Online data.

Notifications

To send alert notifications and scheduled reports, Cygna Auditor requires access to SMTP server. To manage your notification settings, on the product home page, navigate to **Configuration / System Configuration** and select the **Email** tab.

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 Password	Provide user credentials for SMTP authentication.
Sender information	

OPTION	DESCRIPTION
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**.

Service

Cygna Auditor platform employs Windows services to collect data from your sources. By default, the Local System account is used to run services but you can opt to specify any other Active Directory account.

The service account settings are configured under **Configuration / System Configuration / Service**.

To update your preferences:

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

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.

To add a proxy and configure routing:

1. On the product home page, navigate to **Configuration / System Configuration**, and select the **Proxy** tab.

2. 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) 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.

3. Verify the proxy configuration.

4. Provide administrator credentials that will be used to restart Cygna Auditor platform service. Make sure to verify these credentials.

5. Click **Save**.

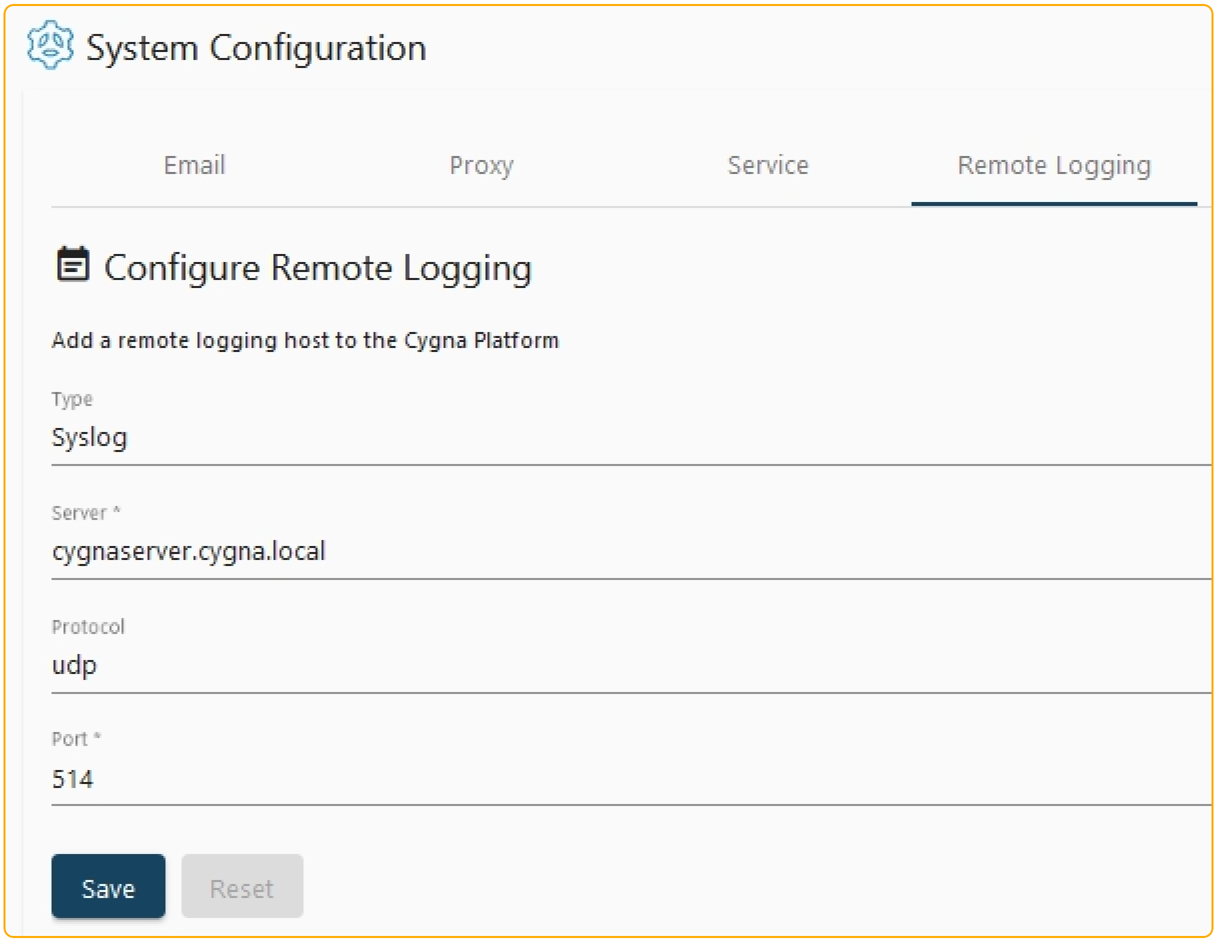
Remote Logging

Enrich and compliment data collected by other SIEM systems with Cygna auditing records. Cygna Auditor enables you to configure integration with Splunk and any Syslog-compatible solution and feed collected data to your audit threads in native format.

Configuring Remote Logging

To set up remote logging, navigate to **Configuration / System / Remote Logging**.

For Syslog:



System Configuration

Configure Remote Logging

Add a remote logging host to the Cygna Platform

Type
Syslog

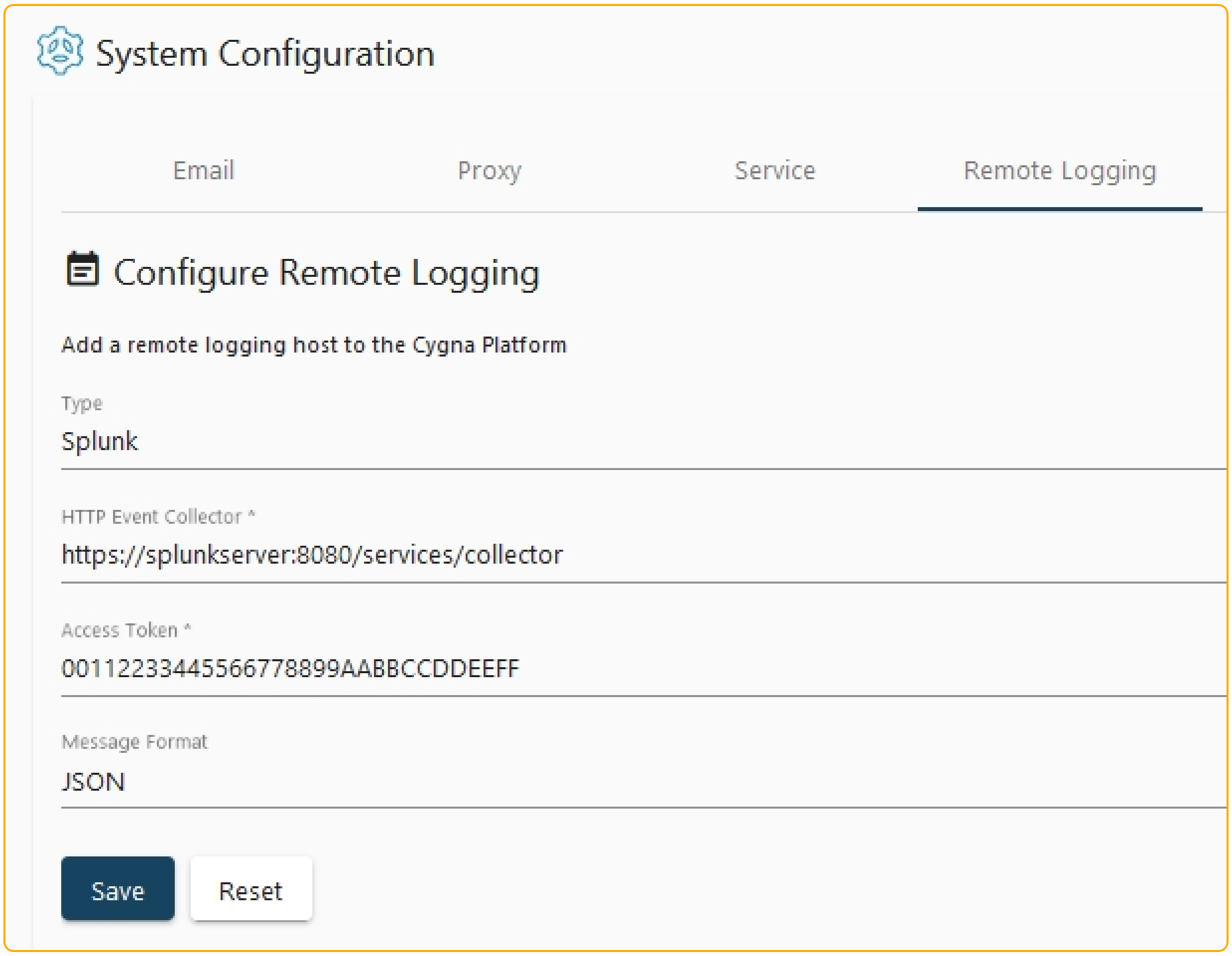
Server *
cygnaserver.cygna.local

Protocol
udp

Port *
514

Specify the Syslog type, the remote server, as well as the port and protocol for connection.

For Splunk:



Configure Remote Logging

Add a remote logging host to the Cygna Platform

Type
Splunk

HTTP Event Collector *
https://splunkserver:8080/services/collector

Access Token *
00112233445566778899AABBCCDDEEFF

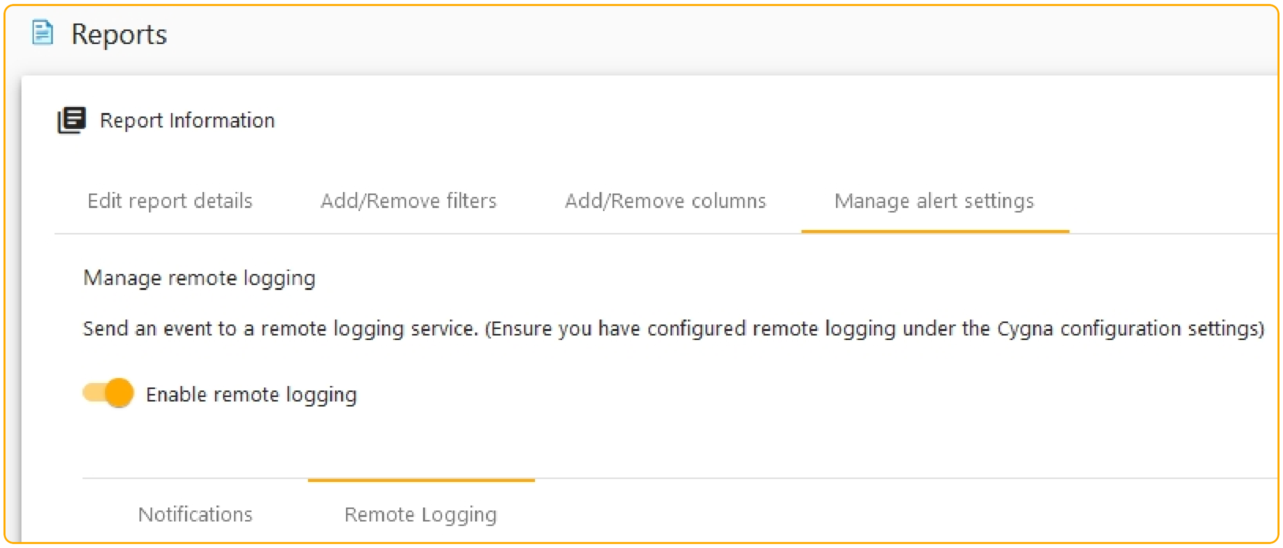
Message Format
JSON

Specify the Splunk type, the Splunk URL, and access token. The data can be provided in JSON or rich text format.

Enabling Remote Logging for Reports

After you specified remote servers to feed data to, go to **Reports** and enable remote logging for each report you want to collect data for.

To do it, go to Reports, specify a report from the list, and then proceed to the **Manage alert settings** tab. Pick Remote logging and make sure to enable it. In this Cygna Auditor will be sending notifications to remote systems within two minutes after processing an event.



Reports

Report Information

Edit report details | Add/Remove filters | Add/Remove columns | Manage alert settings

Manage remote logging

Send an event to a remote logging service. (Ensure you have configured remote logging under the Cygna configuration settings)

● Enable remote logging

Notifications | Remote Logging

Licenses

License management center within Cygna Auditor enables you to verify your license status, manage your Cygna customer portal credentials, and submit licenses manually.

To manage your licenses, on the product home page, navigate to **Configuration / License**. On this page you can review the license status for each module, expiration date, your count quota.

To upload a new license, select 🔑 and submit a new key.

Database Connections

Cygna Auditor enables you to leverage multiple audit databases. The **Database Connections** page provides an insight into what databases are in use with Cygna Auditor and PBMS (CA&AS) products and enables you to add more connections if necessary.

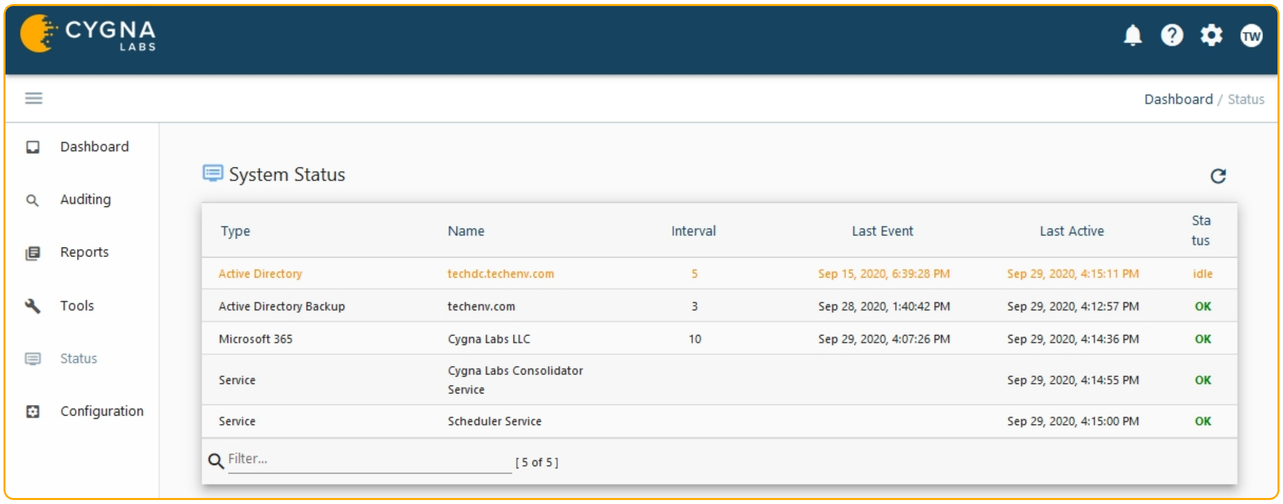
To add a new database connection:

1. Navigate to **Configuration /Database Connections**.
2. Review the list of connections.
3. Click ⊞ to add a new connection.
4. On the **General Information** tab, select the connection type (what product it uses - Cygna Auditor or PBMS), name, and description. Enable the database connection.
5. On **Connection Information** tab, provide details about the SQL Server instance, credentials, select a database. Make sure to verify connection.
6. On the **Summary** tab, review the connection details and save it.

Status

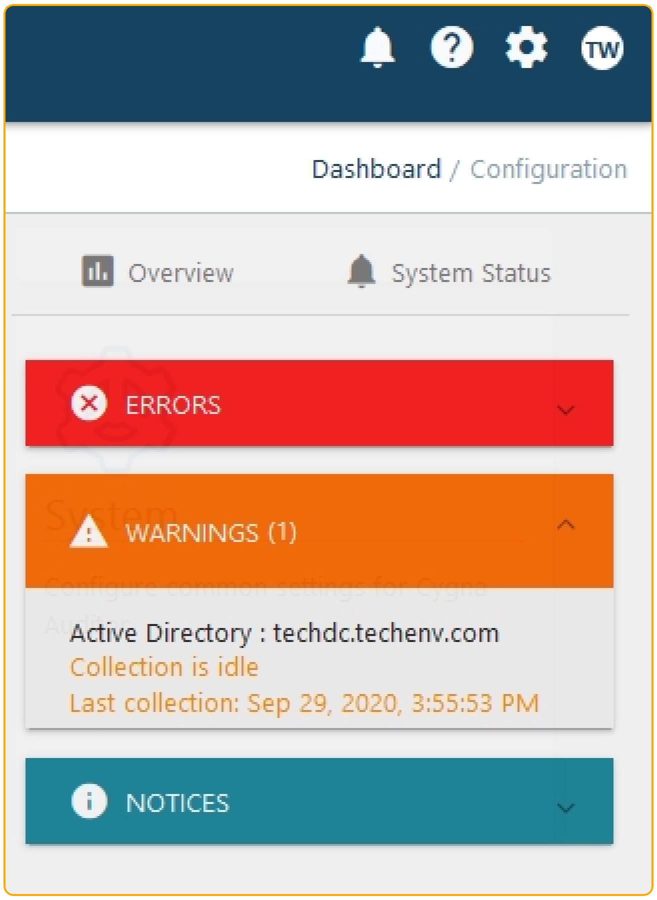
To verify that data collections run on time and the product operates normally, go to **Status**. The page outlines servers and other entities you are auditing, with data collection status and time since the last data collection for each of them.

With this dashboard, you can identify systems that need your special attention and control overall data collection health.



Type	Name	Interval	Last Event	Last Active	Status
Active Directory	techdc.techenv.com	5	Sep 15, 2020, 6:39:28 PM	Sep 29, 2020, 4:15:11 PM	idle
Active Directory Backup	techenv.com	3	Sep 28, 2020, 1:40:42 PM	Sep 29, 2020, 4:12:57 PM	OK
Microsoft 365	Cygna Labs LLC	10	Sep 29, 2020, 4:07:26 PM	Sep 29, 2020, 4:14:36 PM	OK
Service	Cygna Labs Consolidator Service			Sep 29, 2020, 4:14:55 PM	OK
Service	Scheduler Service			Sep 29, 2020, 4:15:00 PM	OK

For quick overview, you can always select 🔔 on top of the page. You'll see all errors, warnings, and notices.



Active Directory : techdc.techenv.com
Collection is idle
Last collection: Sep 29, 2020, 3:55:53 PM

Application Settings

Customize Cygna Auditor look&feel and tailor application to your preferences. Click ⚙ icon on top of the page.

- Change color theme
- Change the side bar menu appereance
- etc.

Cygna RSAT

Cygna Remote System Administration Tools seamlessly integrate with Active Directory Users and Computers (ADUC) snap-in and provide diverse user management capabilities such as the ability to view audit trails for an object, account activity, group membership changes. On top of that, you'll be able to perform rollbacks and recover items from the recycle bin. All these actions are available through the context menu right in ADUC.

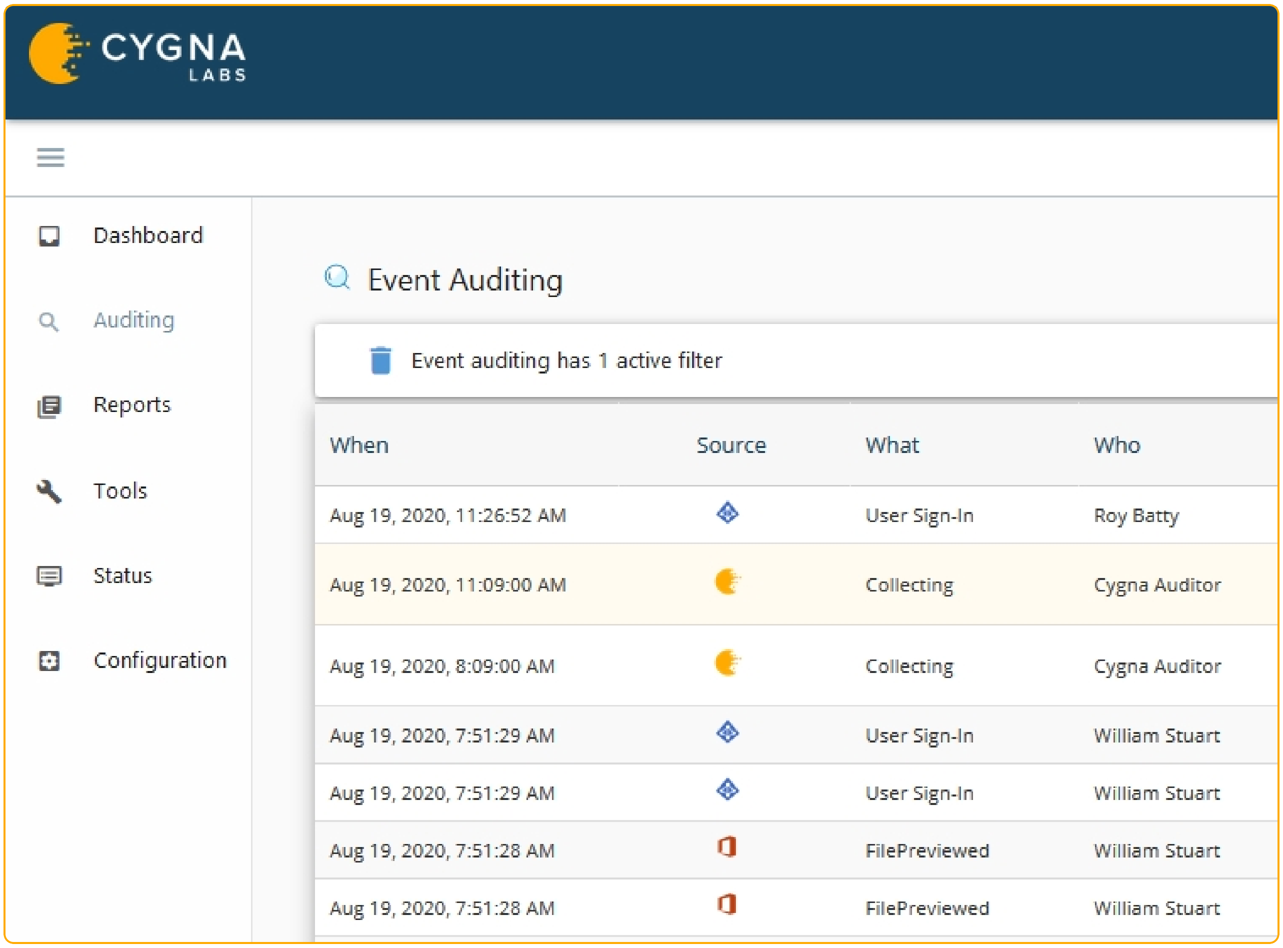
To set up Cygna RSAT for ADUC:

1. Navigate to 🔔 **/ About**.
2. Download and run the installer.

Now, you can instantly manage accounts in Active Directory Users and Computers.

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.



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	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	• Reviewing activity • Searching for a specific events

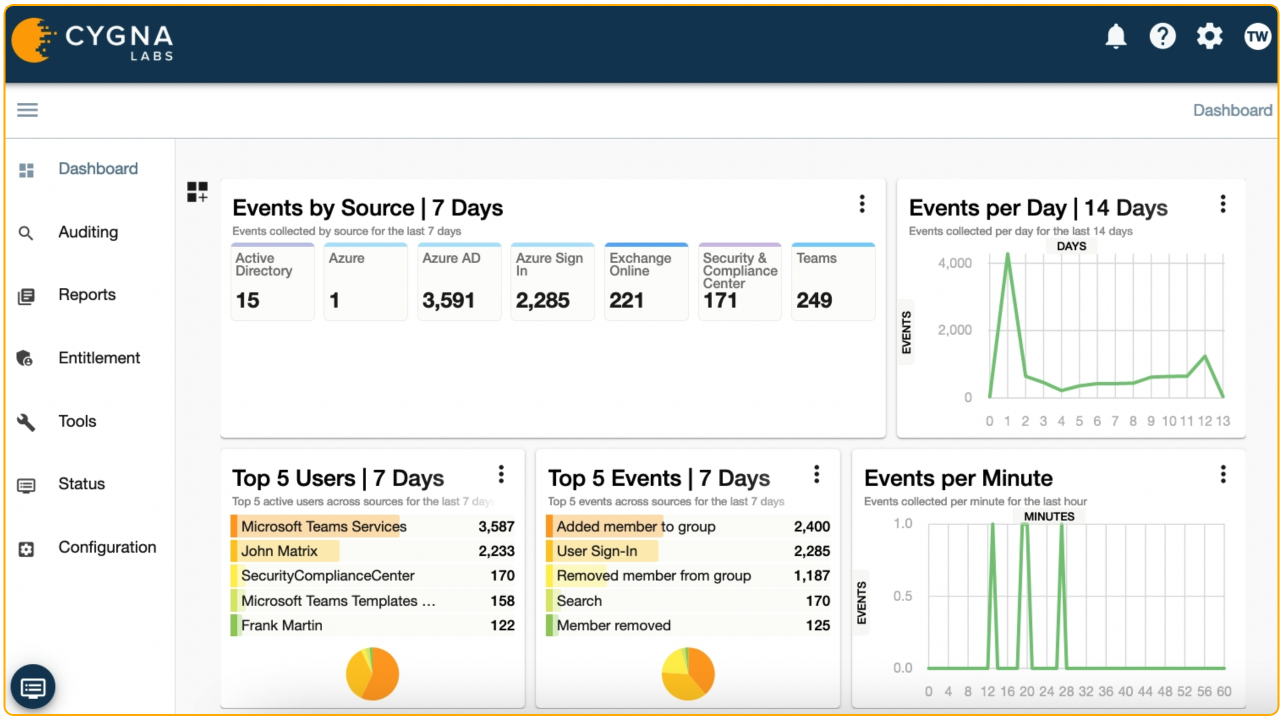
FEATURE	WHAT IS IT GOOD FOR?
	• Digging into security incidents • Investigating user actions from multiple sources • Focusing on event chains–subsequent events leading to a breach or security issue • Identifying potentially harmful users and security breaches in your environment
Reports	• Analyzing your 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.

In the **Tools** section, you'll find utilities that will help you secure and manage Active Directory efficiently.

TOOLS	WHAT IS IT GOOD FOR?
Recycle Bin for Active Directory	Restoring deleted AD object such as groups and users. With Recycle Bin, you can address security risks faster than ever before.
Rollback for Active Directory	Rolling back changes and reverting AD attributes back to their original values. With Rollback, you can address issues and fix them granularly.
Active Directory Browser	Reviewing your Active Directory domains to ensure its operability and security.
Scheduler	Creating subscriptions to reports.

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.



Events by Source | 7 Days

Events collected by source for the last 7 days

Active Directory	Azure	Azure AD	Azure Sign In	Exchange Online	Security & Compliance Center	Teams
15	1	3,591	2,285	221	171	249

Top 5 Users | 7 Days

Top 5 active users across sources for the last 7 days

Microsoft Teams Services	3,587
John Matrix	2,233
SecurityComplianceCenter	170
Microsoft Teams Templates ...	158
Frank Martin	122

Top 5 Events | 7 Days

Top 5 events across sources for the last 7 days

Added member to group	2,400
User Sign-In	2,285
Removed member from group	1,187
Search	170
Member removed	125

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.

> **QUICK TIP**: Seeing results just for one source or no search results at all? You are missing required permissions. Discuss your role with Cygna Auditor's global administrator.

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

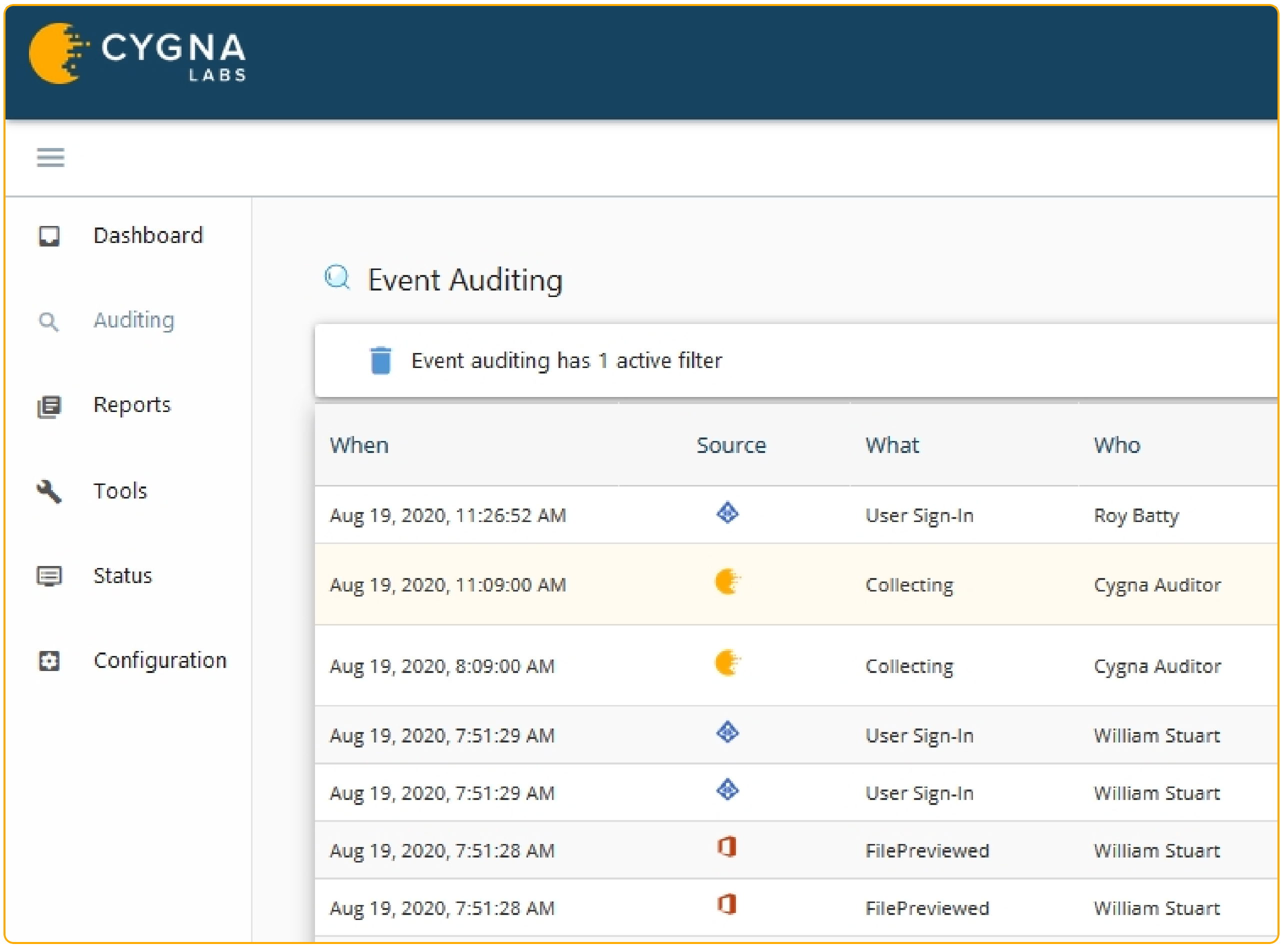
You can use these techniques interchangeably or supplementing each other. A good idea is to start with all changes on the screen and then drill-down to more specific events.

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.



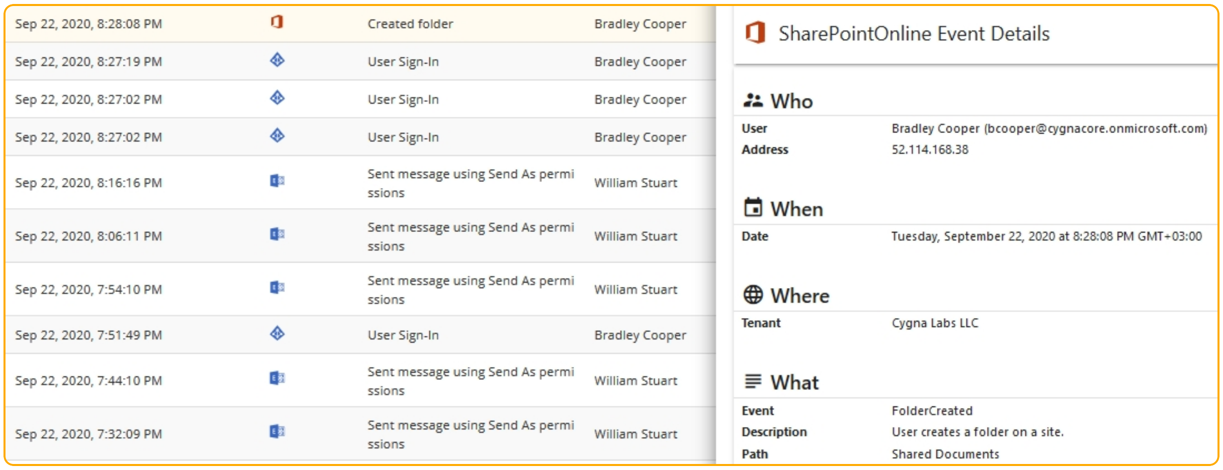
Event Auditing

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	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

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
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 permi ssions	William Stuart
Sep 22, 2020, 8:06:11 PM	▣	Sent message using Send As permi ssions	William Stuart
Sep 22, 2020, 7:54:10 PM	▣	Sent message using Send As permi ssions	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 permi ssions	William Stuart
Sep 22, 2020, 7:32:09 PM	▣	Sent message using Send As permi ssions	William Stuart

SharePointOnline Event Details

Who

User	Bradley Cooper (bcooper@cygnacore.onmicrosoft.com)
Address	52.114.168.38

When

Date	Tuesday, September 22, 2020 at 8:28:08 PM GMT+03:00

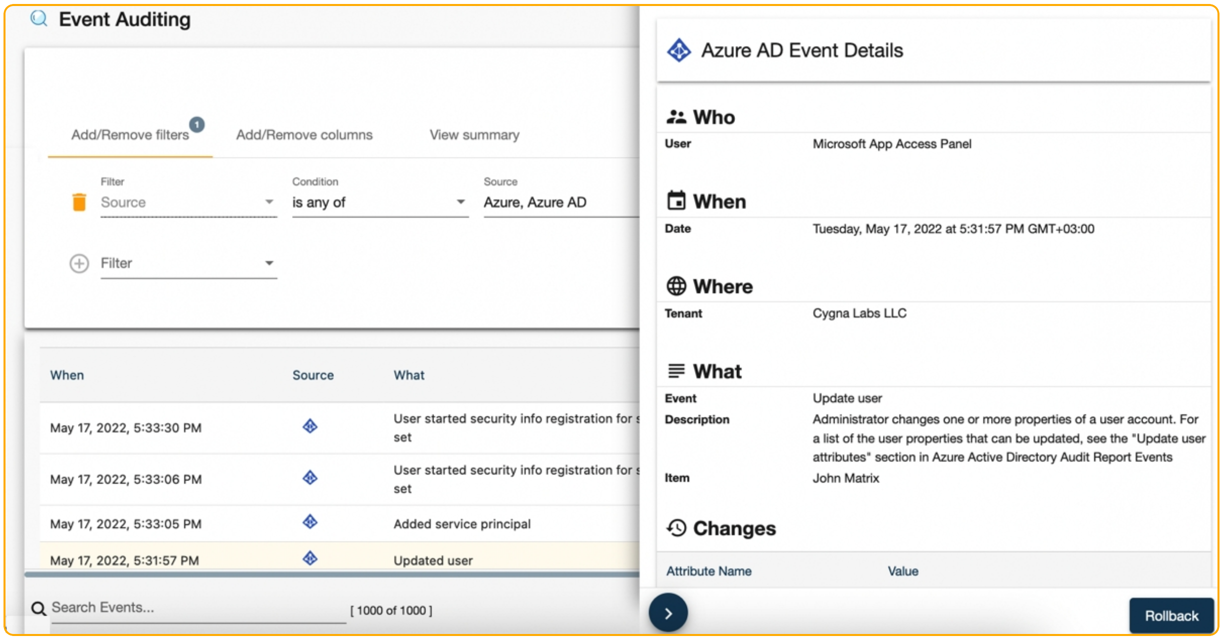
Where

Tenant	Cygna Labs LLC

What

Event	FolderCreated
Description	User creates a folder on a site.
Path	Shared Documents

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



Event Auditing

Filter	Condition	Source
Source	is any of	Azure, Azure AD

When	Source	What
May 17, 2022, 5:33:30 PM		User started security info registration for s set
May 17, 2022, 5:33:06 PM		User started security info registration for s set
May 17, 2022, 5:33:05 PM		Added service principal
May 17, 2022, 5:31:57 PM		Updated user

Search Events... [1000 of 1000]

Azure AD Event Details

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

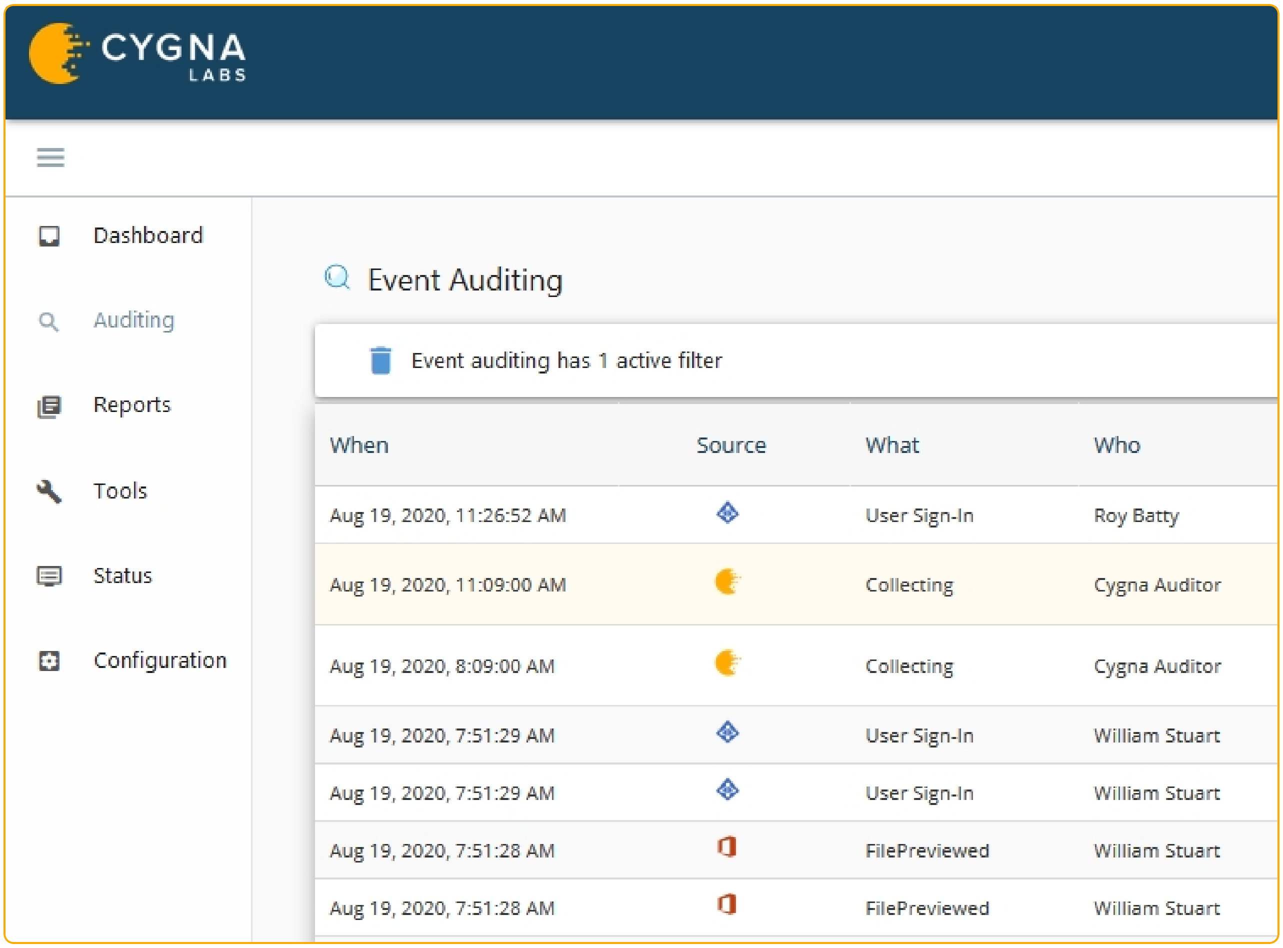
Attribute Name	Value

- **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.



Event Auditing

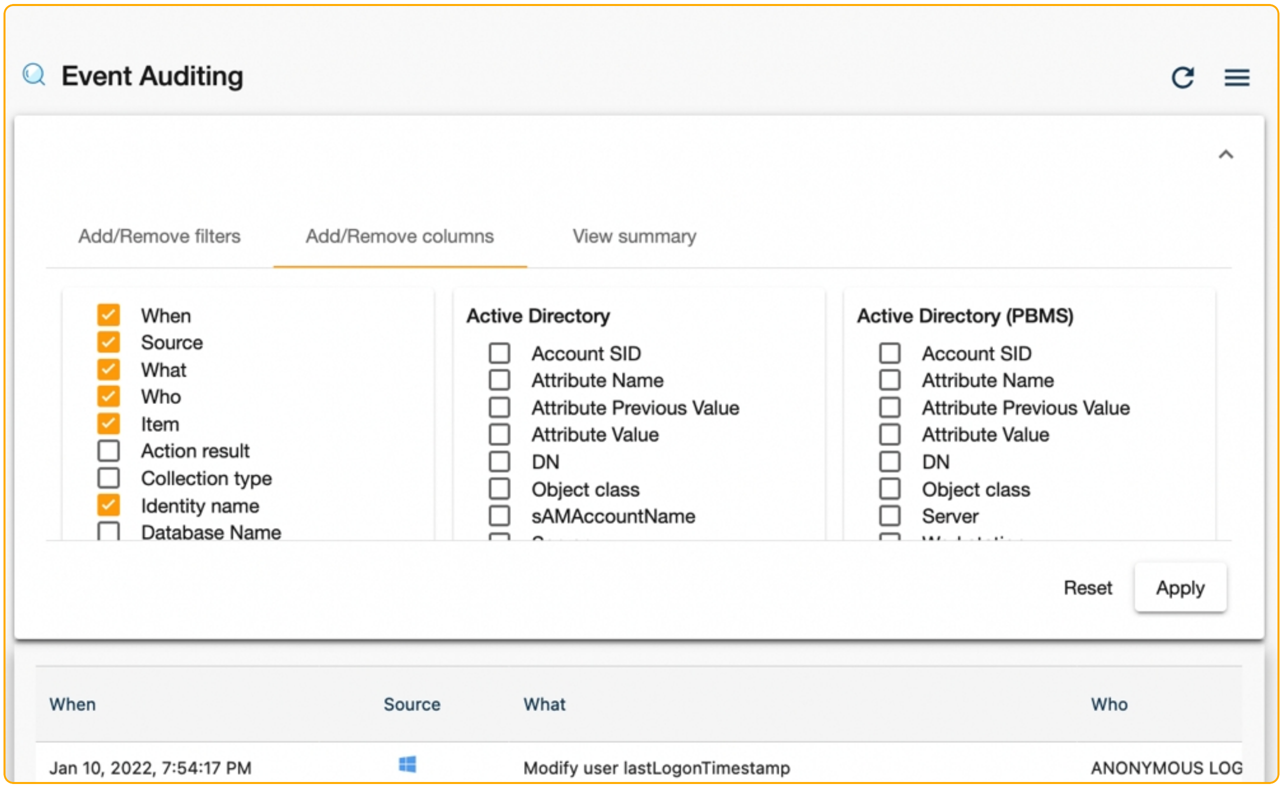
Event auditing has 1 active filter

When	Source	What	Who
Aug 19, 2020, 11:26:52 AM	◆	User Sign-In	Roy Batty
Aug 19, 2020, 11:09:00 AM	●	Collecting	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.



Event Auditing

Add/Remove filters | Add/Remove columns | View summary

☑ When
☑ Source
☑ What
☑ Who
☑ Item
□ Action result
□ Collection type
☑ Identity name
□ Database Name

Active Directory

□ Account SID
□ Attribute Name
□ Attribute Previous Value
□ Attribute Value
□ DN
□ Object class
□ sAMAccountName

Active Directory (PBMS)

□ Account SID
□ Attribute Name
□ Attribute Previous Value
□ Attribute Value
□ DN
□ Object class
□ Server

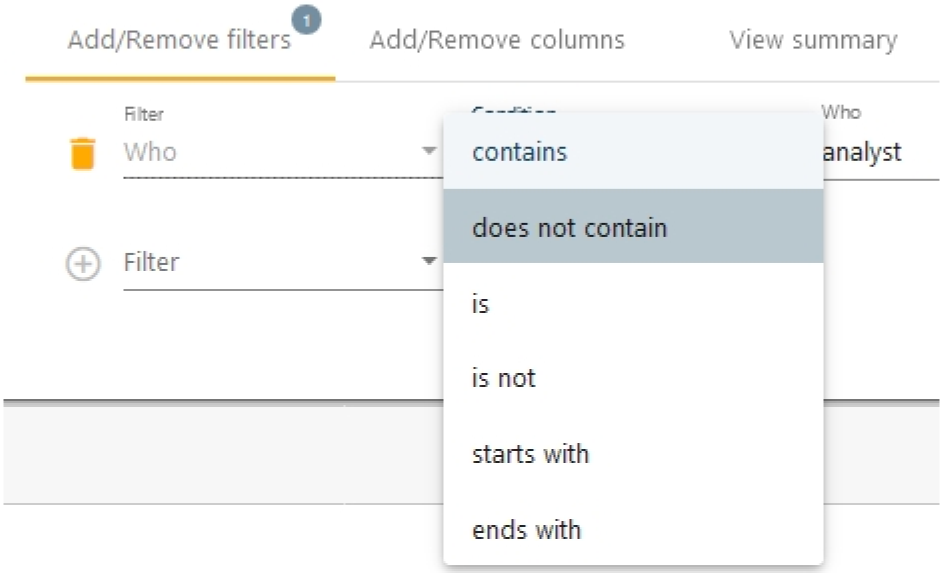
Reset | Apply

When	Source	What	Who
Jan 10, 2022, 7:54:17 PM	⊞	Modify user lastLogonTimestamp	ANONYMOUS LOG

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.



Filter: Who

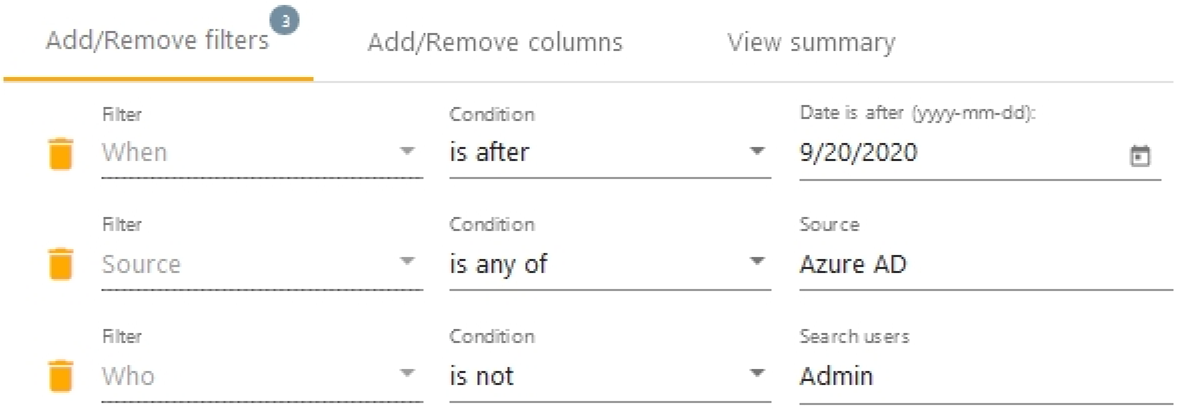
Who: analyst

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

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:



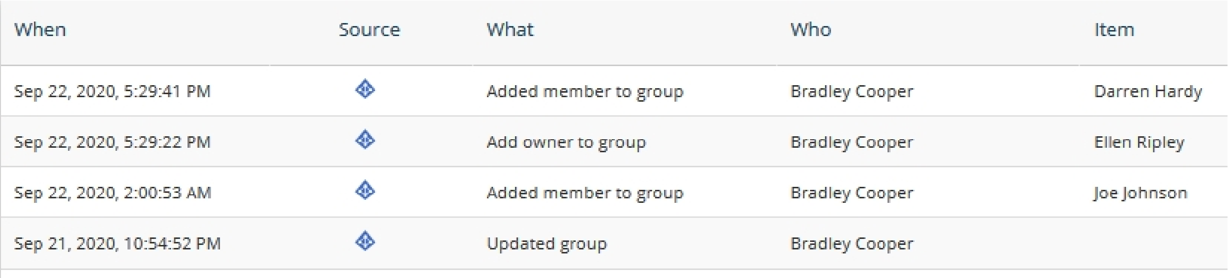
Filter: When — Condition: is after — Date is after (yyyy-mm-dd): 9/20/2020

Filter: Source — Condition: is any of — Source: Azure AD

Filter: Who — Condition: is not — Search users: Admin

Here, Cygna 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



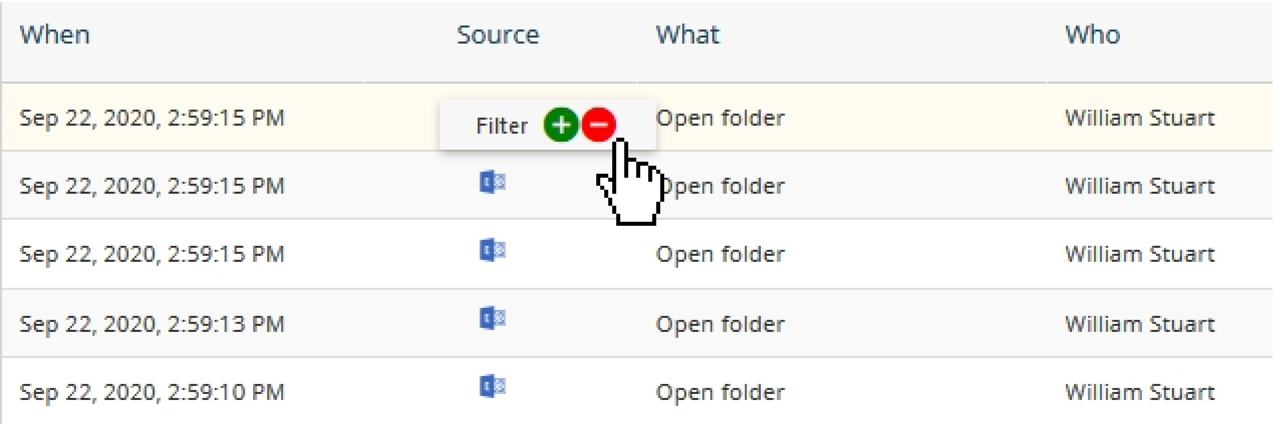
When	Source	What	Who	Item
Sep 22, 2020, 5:29:41 PM	◈	Added member to group	Bradley Cooper	Darren Hardy
Sep 22, 2020, 5:29:22 PM	◈	Add owner to group	Bradley Cooper	Ellen Ripley
Sep 22, 2020, 2:00:53 AM	◈	Added member to group	Bradley Cooper	Joe Johnson
Sep 21, 2020, 10:54:52 PM	◈	Updated group	Bradley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



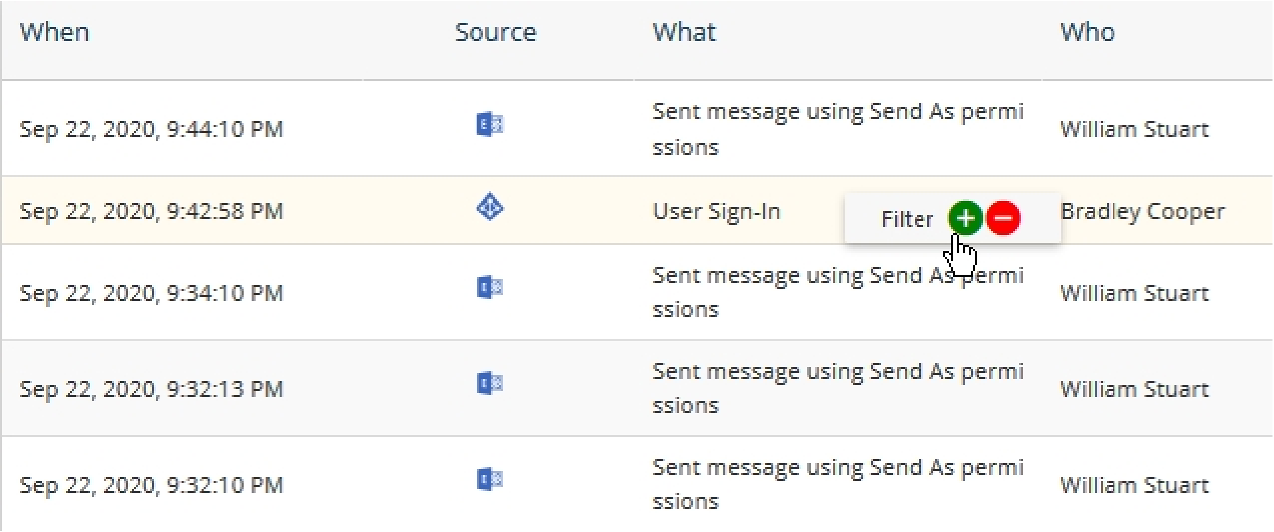
When	Source	What	Who
Sep 22, 2020, 2:59:15 PM	Filter ⊕ ⊖	Open folder	William Stuart
Sep 22, 2020, 2:59:15 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:15 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:13 PM		Open folder	William Stuart
Sep 22, 2020, 2:59:10 PM		Open folder	William Stuart

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.

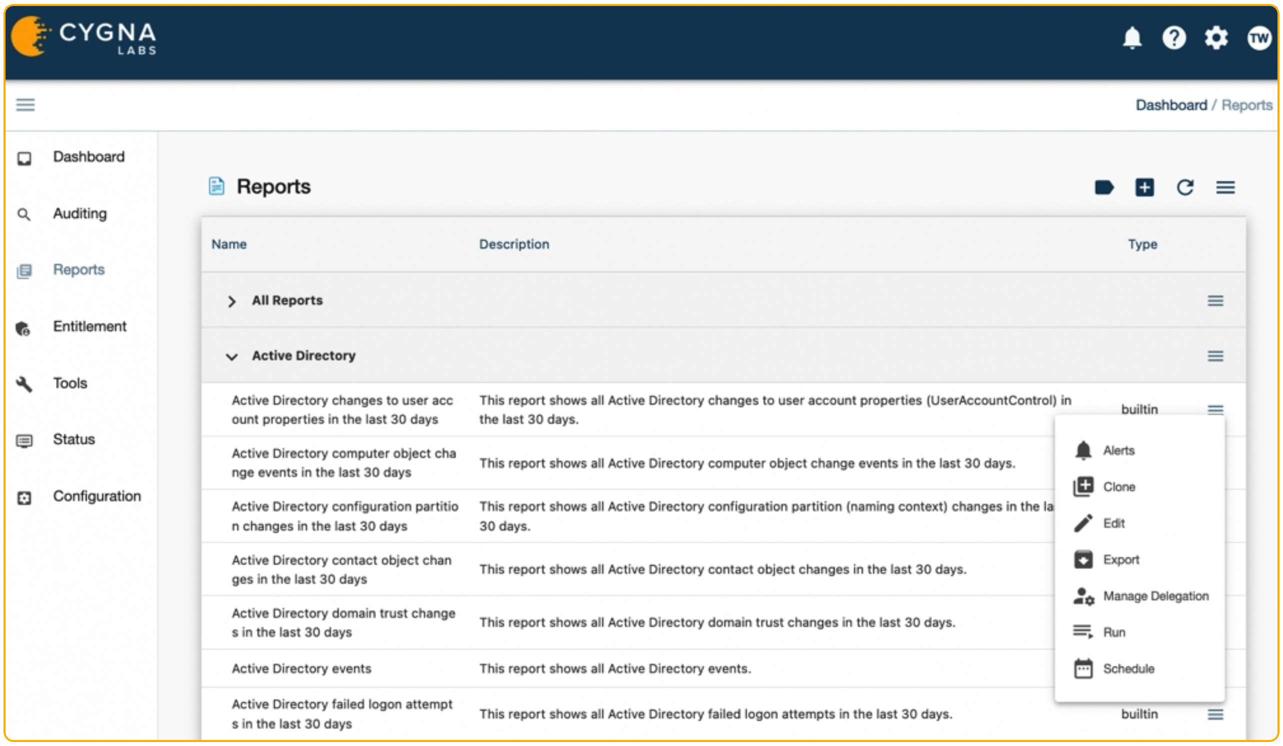


When	Source	What	Who
Sep 22, 2020, 9:44:10 PM		Sent message using Send As permissions	William Stuart
Sep 22, 2020, 9:42:58 PM		User Sign-In	Bradley Cooper
Sep 22, 2020, 9:34:10 PM		Sent message using Send As permissions	William Stuart
Sep 22, 2020, 9:32:13 PM		Sent message using Send As permissions	William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

Reports

The expert security team of Cygna Labs designed and prepacked Cygna 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, Cygna Auditor reports about its health state with **Infrastructure** and **Security & Compliance Center** reports.



Name	Description	Type
All Reports		
Active Directory		
Active Directory changes to user account properties in the last 30 days	This report shows all Active Directory changes to user account properties (UserAccountControl) in the last 30 days.	builtin
Active Directory computer object change events in the last 30 days	This report shows all Active Directory computer object change events in the last 30 days.	
Active Directory configuration partition changes in the last 30 days	This report shows all Active Directory configuration partition (naming context) changes in the la 30 days.	
Active Directory contact object changes in the last 30 days	This report shows all Active Directory contact object changes in the last 30 days.	
Active Directory domain trust changes in the last 30 days	This report shows all Active Directory domain trust changes in the last 30 days.	
Active Directory events	This report shows all Active Directory events.	
Active Directory failed logon attempts in the last 30 days	This report shows all Active Directory failed logon attempts in the last 30 days.	builtin

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 retrict 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

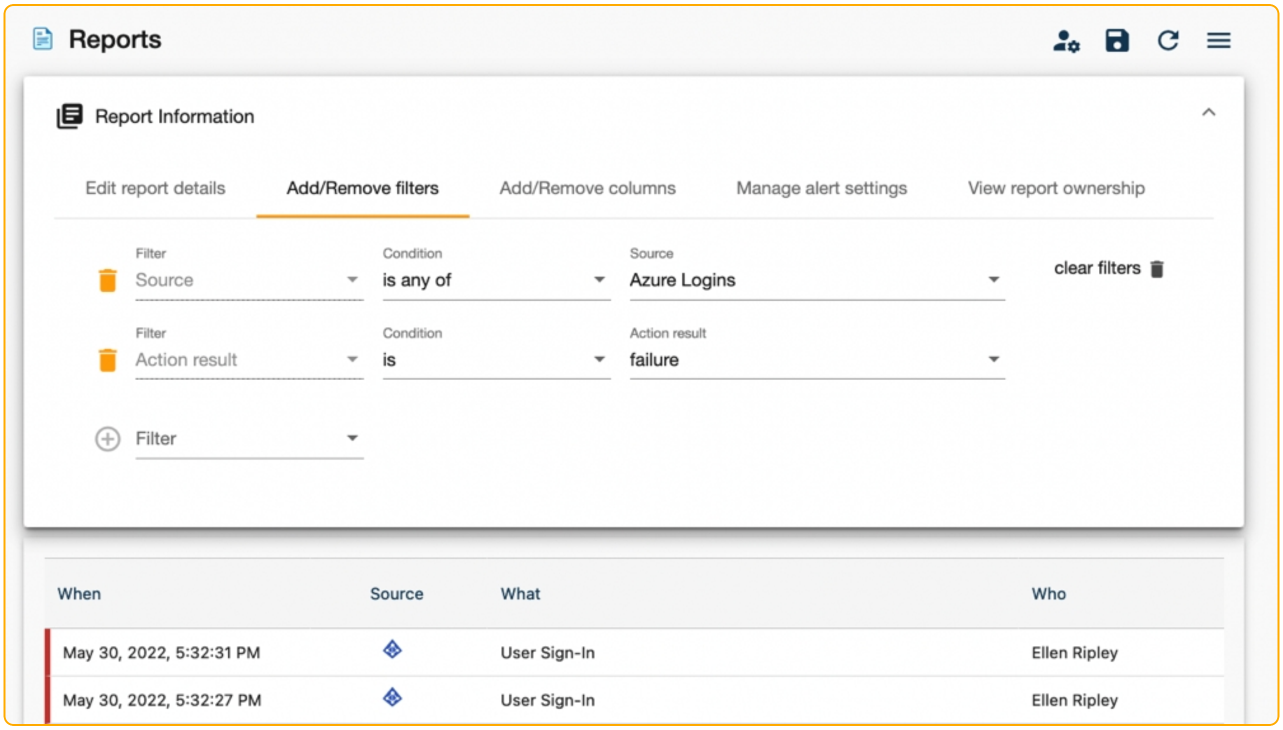
Alerting

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.



Filter	Condition	Source
Source	is any of	Azure Logins

Filter	Condition	Action result
Action result	is	failure

Filter

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

QUICK TIP: Seeing results just for one source or no search results at all? You are missing required permissions. Discuss your permission set with Cygna Auditor's global administrator.

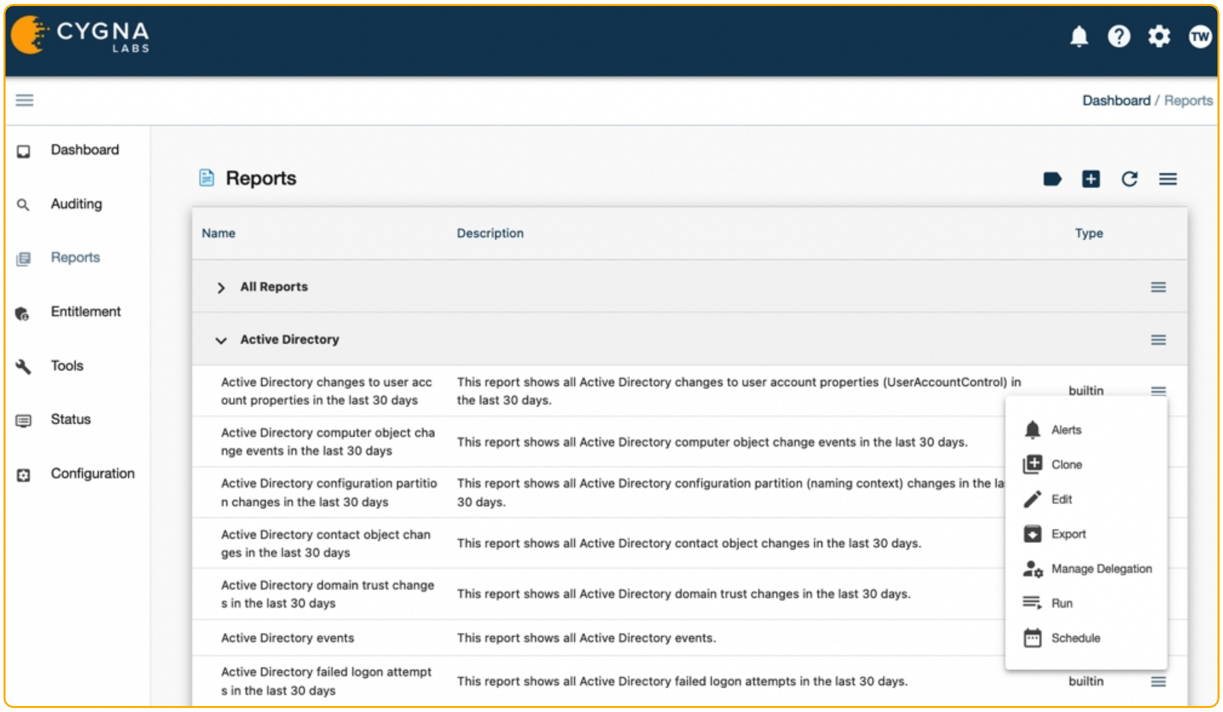
Note: You might see several records with events that occurred at the same time up to seconds–for example "create user" with subsequent "modify user". Typically they represent a single, one-time action. The reason why Cygna Auditor displays it as several records is that Windows actually generates several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

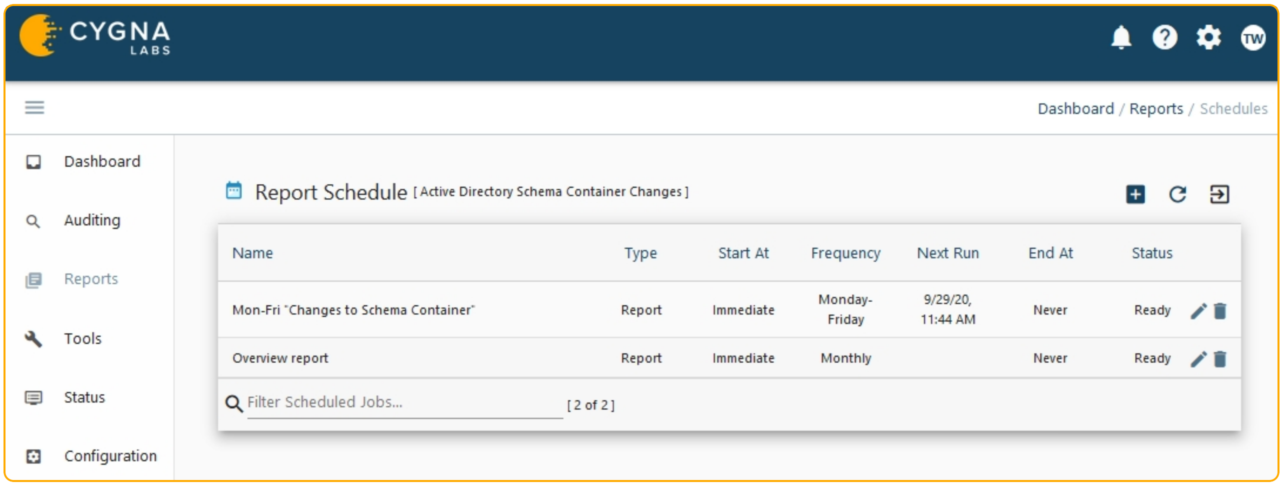


Reports

Name	Description	Type
All Reports		
Active Directory		
Active Directory changes to user account properties in the last 30 days	This report shows all Active Directory changes to user account properties (UserAccountControl) in the last 30 days.	builtin
Active Directory computer object change events in the last 30 days	This report shows all Active Directory computer object change events in the last 30 days.	
Active Directory configuration partition changes in the last 30 days	This report shows all Active Directory configuration partition (naming context) changes in the la 30 days.	
Active Directory contact object changes in the last 30 days	This report shows all Active Directory contact object changes in the last 30 days.	
Active Directory domain trust changes in the last 30 days	This report shows all Active Directory domain trust changes in the last 30 days.	
Active Directory events	This report shows all Active Directory events.	
Active Directory failed logon attempts in the last 30 days	This report shows all Active Directory failed logon attempts in the last 30 days.	builtin

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.



Report Schedule [Active Directory Schema Container Changes]

Name	Type	Start At	Frequency	Next Run	End At	Status
Mon-Fri "Changes to Schema Container"	Report	Immediate	Monday-Friday	9/29/20, 11:44 AM	Never	Ready
Overview report	Report	Immediate	Monthly		Never	Ready

Filter Scheduled Jobs... [2 of 2]

Note: To see all scheduled report, navigate to **Tools / Scheduler**. See Scheduler for more information.

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 (see Remote Logging), 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.

QUICK TIP: Don't have access to alerts? You are missing required permissions. Discuss your permission set with Cygna Auditor's global administrator.

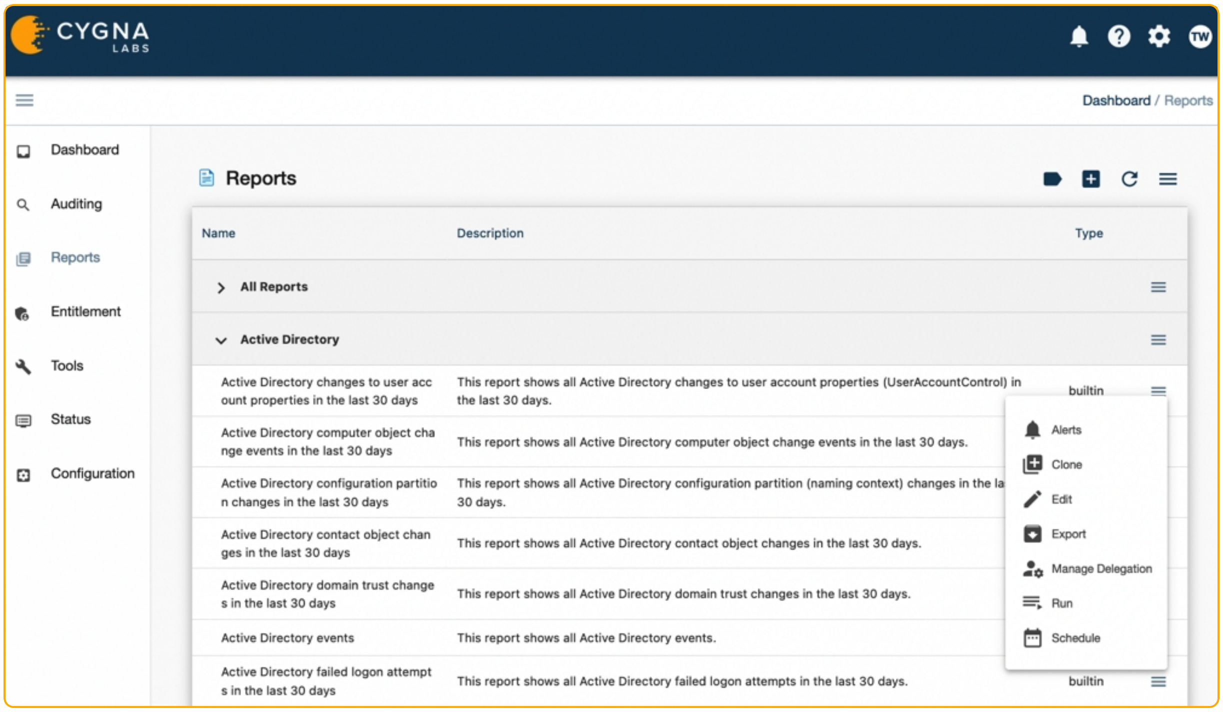
Note: To be able to send alert notifications, configure SMTP settings. On the product home page, navigate to **Configuration / System** and complete the fields. For more information, see Notifications.

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.

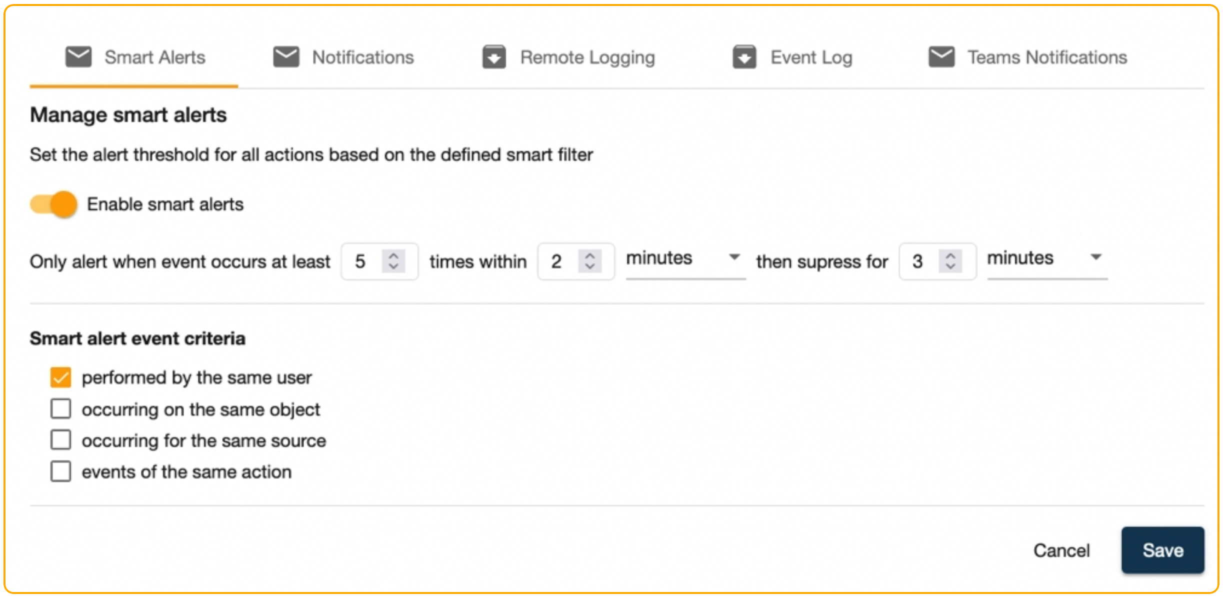
1. Navigate to the **Reports**.
2. Expand ≡ options next to a report and select 🔔 **Alerts**.



Name	Description	Type
All Reports		
Active Directory		
Active Directory changes to user account properties in the last 30 days	This report shows all Active Directory changes to user account properties (UserAccountControl) in the last 30 days.	builtin
Active Directory computer object change events in the last 30 days	This report shows all Active Directory computer object change events in the last 30 days.	
Active Directory configuration partition changes in the last 30 days	This report shows all Active Directory configuration partition (naming context) changes in the la 30 days.	
Active Directory contact object changes in the last 30 days	This report shows all Active Directory contact object changes in the last 30 days.	
Active Directory domain trust changes in the last 30 days	This report shows all Active Directory domain trust changes in the last 30 days.	
Active Directory events	This report shows all Active Directory events.	
Active Directory failed logon attempts in the last 30 days	This report shows all Active Directory failed logon attempts in the last 30 days.	builtin

3. 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 cofigure rules to trigger an alert notification. For example, when monitoring faield logon attempts, configure Cygna Auditor to send an alert when an event happens five times within two minutes and then surpress notifications for 3 minutes.

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



Manage smart alerts

Set the alert threshold for all actions based on the defined smart filter

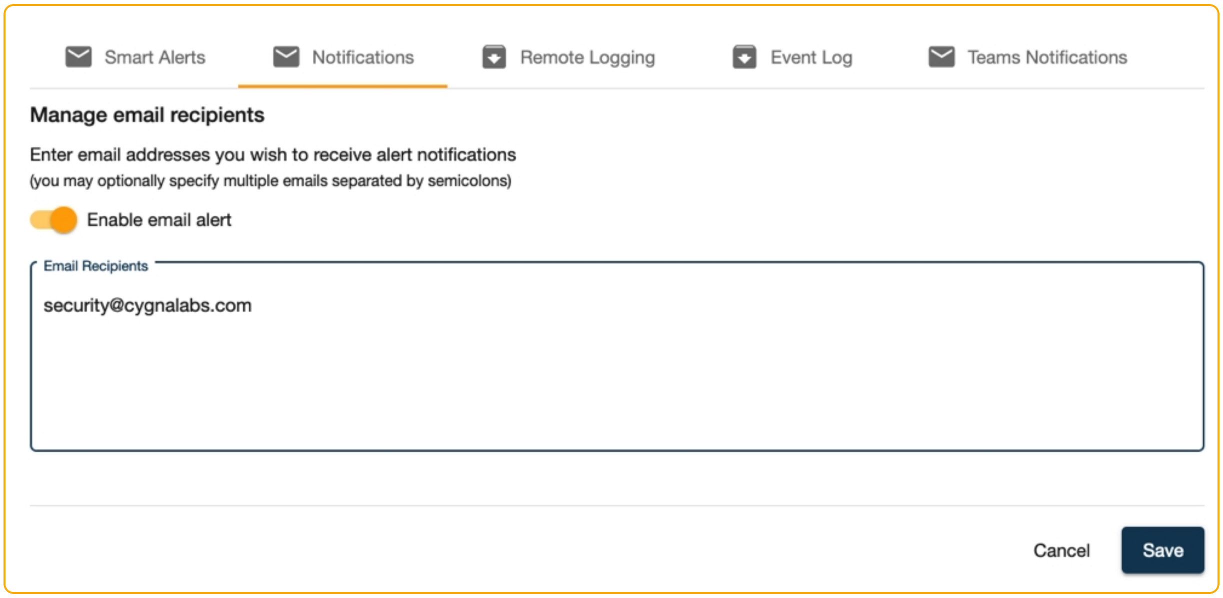
● Enable smart alerts

Only alert when event occurs at least 5 times within 2 minutes then supress for 3 minutes

Smart alert event criteria

☑ performed by the same user
☐ occurring on the same object
☐ occurring for the same source
☐ events of the same action

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



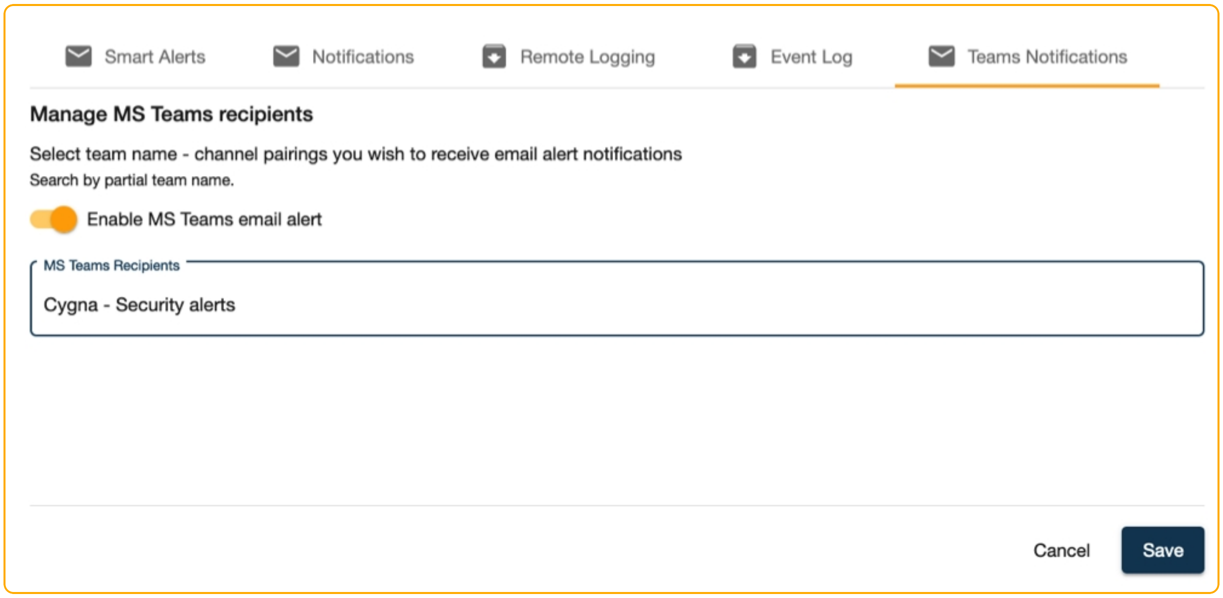
Manage email recipients

Enter email addresses you wish to receive alert notifications
(you may optionally specify multiple emails separated by semicolons)

● Enable email alert

Email Recipients
security@cygnalabs.com

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.



Manage MS Teams recipients

Select team name - channel pairings you wish to receive email alert notifications

Search by partial team name.

Enable MS Teams email alert

MS Teams Recipients: Cygna - Security alerts

Tools

Besides reporting and auditing, Cygna Auditor enables you to manage your audit sources and do some basic administration chores right in the app.

Navigate to the **Tools** section and then select a tile:

- Rollback for Active Directory
- Recycle Bin for Active Directory
- Active Directory Browser
- Recovery for Azure AD
- Scheduler
- Cygna Identities

Rollback for Active Directory

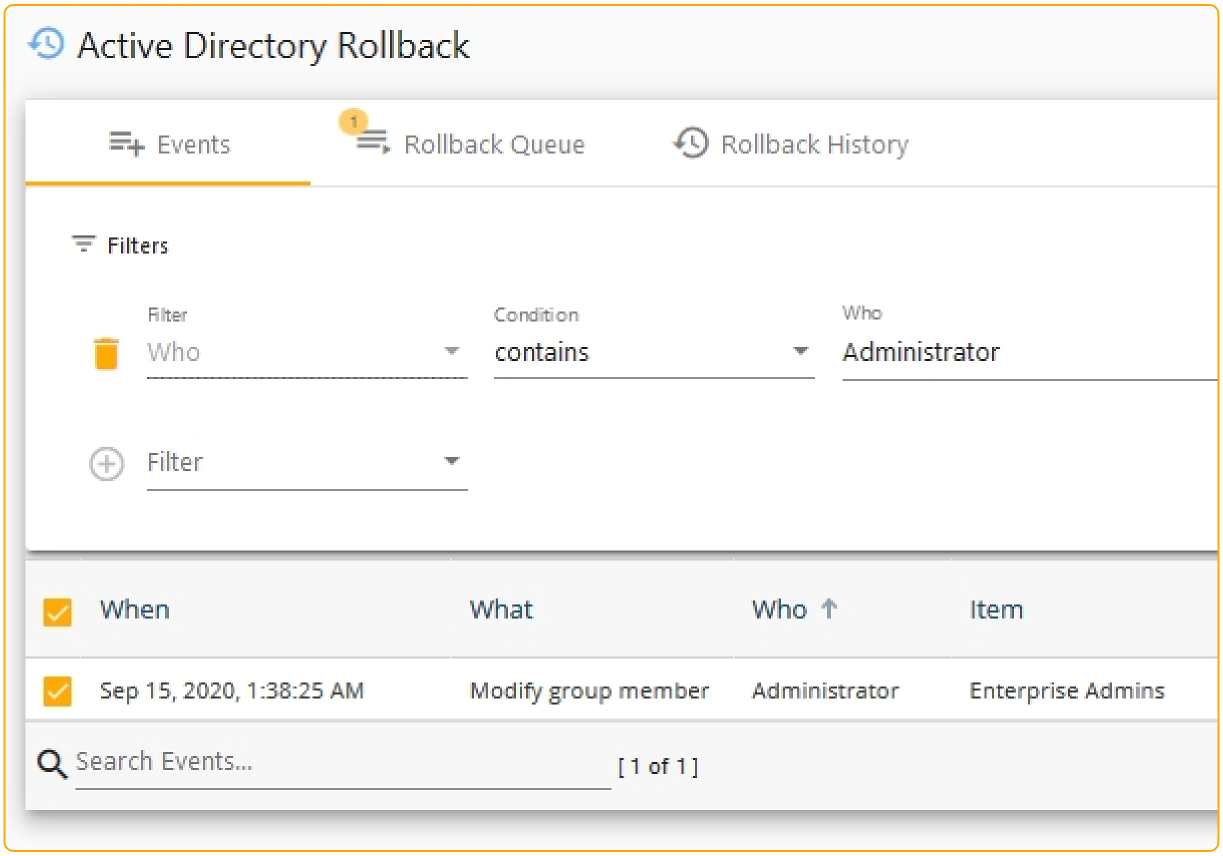
Cygna Auditor enables you to rollback unwanted Active Directory changes, such as changes to group membership, user properties, and other AD attributes. Empowered with this feature, you can not only detect security issues but also fix them in a fraction of second and with a highest precision (up to individual attributes!).

If you are looking for a way to recover deleted AD objects, see Recycle Bin for Active Directory.

Note: If the object was deleted, you cannot roll back changes to its attributes. You have to restore the object with Recovery.

To add events to rollback queue:

1. Navigate to **Tools / Active Directory Rollback**.
2. On the **Events** tab, review recent changes. Apply filters to search for specific changes.
3. Select changes you want to rollback and then select checkboxes next to these entries–these changes will be added to a queue.



Filter: Who
Condition: contains
Who: Administrator

☑	When	What	Who ↑	Item
☑	Sep 15, 2020, 1:38:25 AM	Modify group member	Administrator	Enterprise Admins

Search Events... [1 of 1]

4. On the **Rollback Queue** tab, review the items you are about to rollback to their previous values.

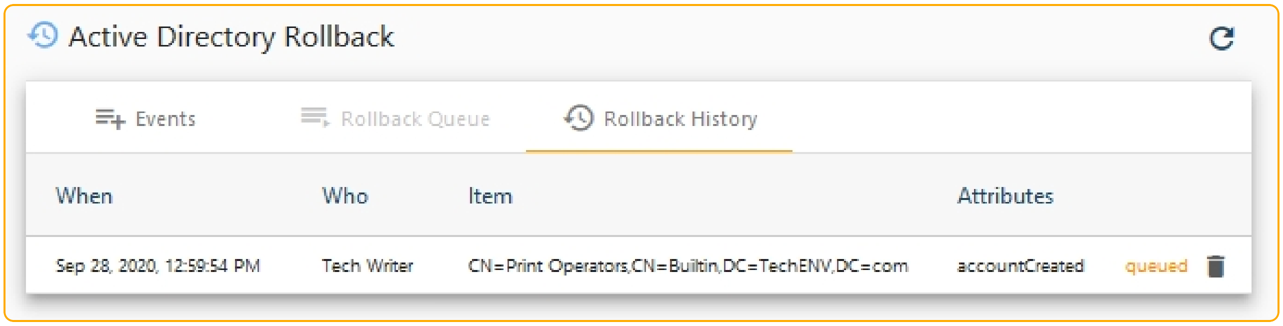
   To rollback specific attributes or to a certain snapshot, select ☰. Cygna Auditor rolls back changes and reverts objects to the state they were at the moment of the snapshot creation. You can use the most recent snapshot or a snapshot taken on a certain date. Follow the wizard to review attribute values that are going to be reverted.

5. Click **Process Queue**.
6. On the next step, select timing, provide administrator credentials, and provide an email address if you want to send a rollback status email.
7. Select **Process Queue Entries**.

To see pending rollbacks and status:

It may take a while to roll back changes.

- Go to the **Pending Rollbacks** tab to see the rollback queue, with details and status for each change. To remove a change from a queue and cancel its rollback, click on the recycle bin icon next to it.



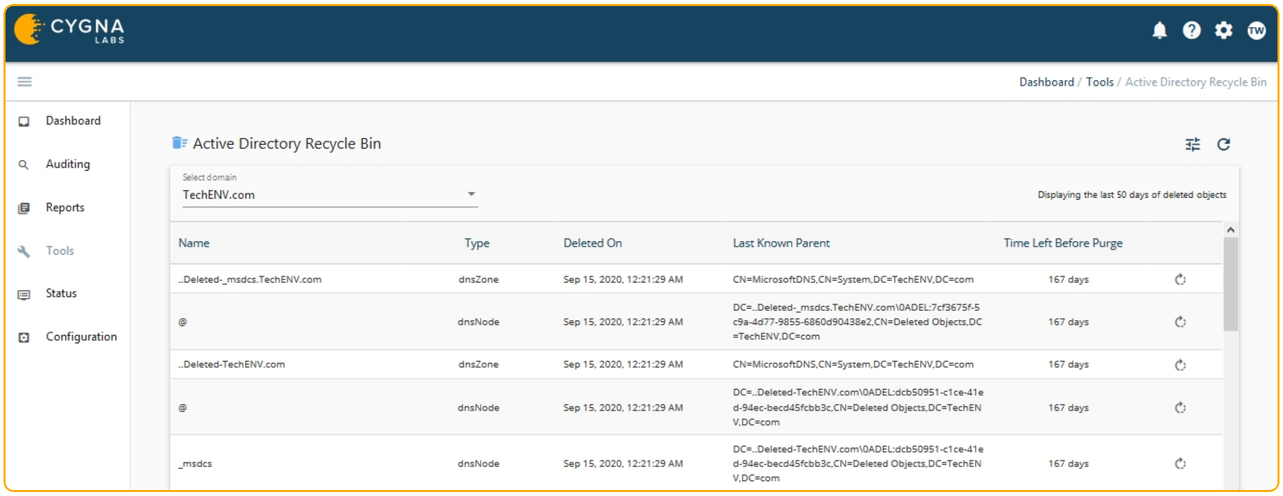
Active Directory Rollback

When	Who	Item	Attributes		
Sep 28, 2020, 12:59:54 PM	Tech Writer	CN=Print Operators,CN=Builtin,DC=TechENV,DC=com	accountCreated	queued	🗑

Recycle Bin for Active Directory

Cygna Auditor enables you to restore Active Directory objects such as deleted AD users or groups. Empowered with this feature, you can not only detect security issues but also fix them in a fraction of second.

If you are looking for a way to roll back changes, see Rollback for Active Directory.



Active Directory Recycle Bin

Select domain
TechENV.com

Displaying the last 50 days of deleted objects

Name	Type	Deleted On	Last Known Parent	Time Left Before Purge	
..Deleted-_msdcs.TechENV.com	dnsZone	Sep 15, 2020, 12:21:29 AM	CN=MicrosoftDNS,CN=System,DC=TechENV,DC=com	167 days	↻
@	dnsNode	Sep 15, 2020, 12:21:29 AM	DC=..Deleted-_msdcs.TechENV.com\0ADEL:7cf3675f-5c9a-4d77-9855-6860d90438e2,CN=Deleted Objects,DC=TechENV,DC=com	167 days	↻
..Deleted-TechENV.com	dnsZone	Sep 15, 2020, 12:21:29 AM	CN=MicrosoftDNS,CN=System,DC=TechENV,DC=com	167 days	↻
@	dnsNode	Sep 15, 2020, 12:21:29 AM	DC=..Deleted-TechENV.com\0ADEL:dcb50951-c1ce-41ed-94ec-becd45fcbb3c,CN=Deleted Objects,DC=TechENV,DC=com	167 days	↻
_msdcs	dnsNode	Sep 15, 2020, 12:21:29 AM	DC=..Deleted-TechENV.com\0ADEL:dcb50951-c1ce-41ed-94ec-becd45fcbb3c,CN=Deleted Objects,DC=TechENV,DC=com	167 days	↻

To add events to rollback queue:

1. Navigate to **Tools / Recycle Bin for Active Directory**, select a domain.
2. Review deleted objects. By default, Cygna Auditor lists objects for the last 7 days. Update this value if necessary.
3. Select a entry you want to recover.
4. On the **Recovery Target** step, review changes, old and new values, etc.

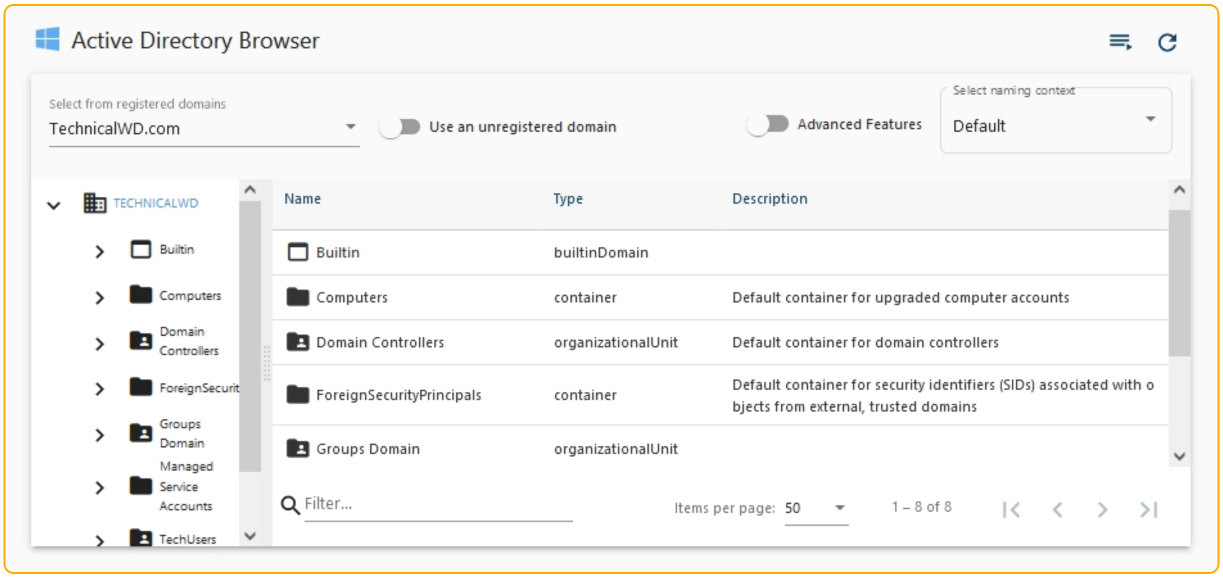
5. On the **Snapshot Selection** step, pick a snapshot. Cygna Auditor will restore the object to the state it was at the moment of the snapshot creation. You can use the most recent snapshot or a snapshot taken on a certain date.
6. Review **Summary** and click **Recover**. You've got an option to recover an object as a currently logged in user or impersonate as administrator. In this case, you'll be prompted to provide administrative credentials.

Active Directory Browser

Cygna Auditor enables you to browse your AD domain right in the application. Review groups, users and confirm changes and rollbacks. There is no need to install Remote Administration Tools or connect to your domain controllers via RDP. Your domain structure is listed in the Cygna Auditor.

To browse your AD domain:

1. Navigate to **Tools / Active Directory Browser**, select a domain, naming context, etc. Check **Use an unregistered domain** to browse a domain that's not connected to Cygna Auditor.
2. Expand folders.



Select from registered domains: TechnicalWD.com

Use an unregistered domain

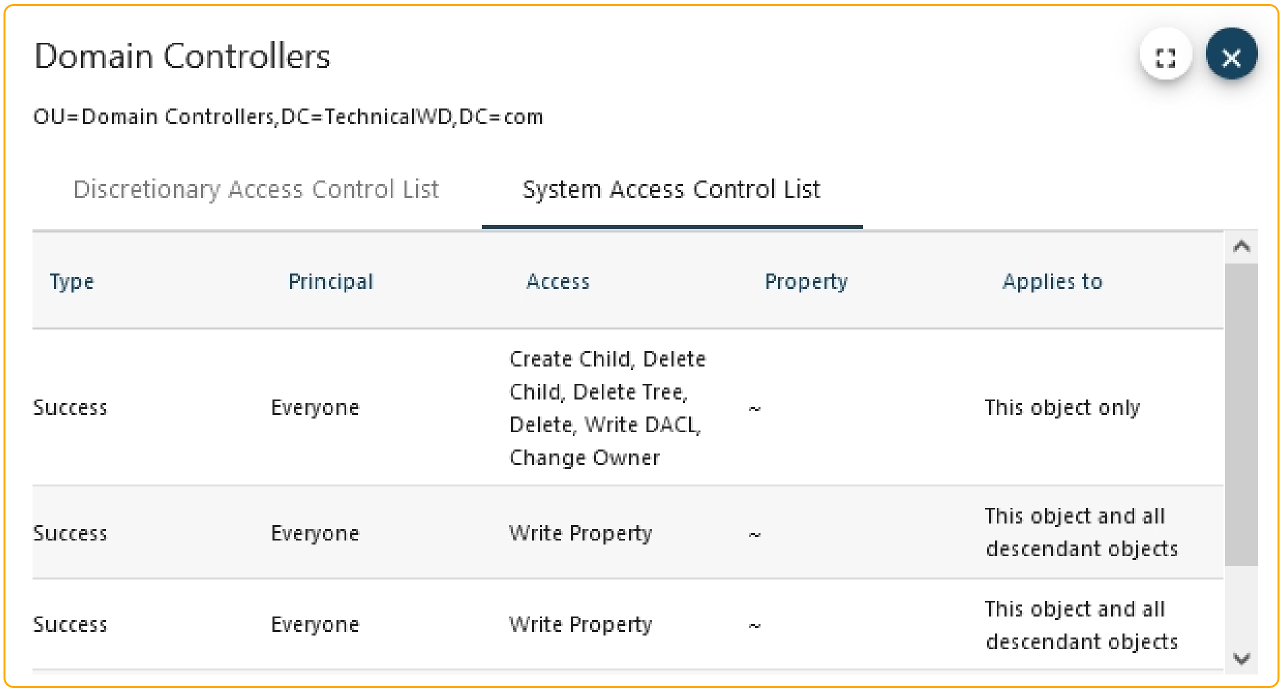
Advanced Features

Select naming context: Default

Name	Type	Description
Builtin	builtinDomain	
Computers	container	Default container for upgraded computer accounts
Domain Controllers	organizationalUnit	Default container for domain controllers
ForeignSecurityPrincipals	container	Default container for security identifiers (SIDs) associated with o bjects from external, trusted domains
Groups Domain	organizationalUnit	

Items per page: 50 1 – 8 of 8

3. Right-click an object to **add to a rollback queue**, inspect **security** permissions or **attributes**.



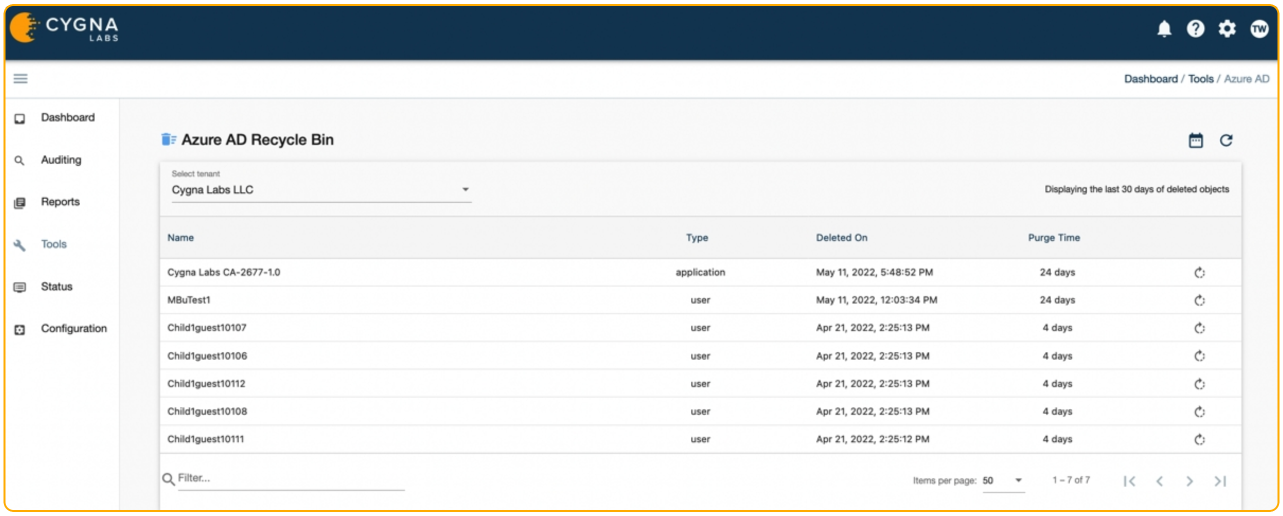
Domain Controllers

OU=Domain Controllers,DC=TechnicalWD,DC=com

Type	Principal	Access	Property	Applies to
Success	Everyone	Create Child, Delete Child, Delete Tree, Delete, Write DACL, Change Owner	~	This object only
Success	Everyone	Write Property	~	This object and all descendant objects
Success	Everyone	Write Property	~	This object and all descendant objects

Recovery for Azure AD

Cygna Auditor enables you to recover Azure AD objects such as deleted users as well as revert changes to various object attributes. With Recovery feature, you can manage your Azure AD and switch between its current state and previous snapshots.



Azure AD Recycle Bin

Select tenant: Cygna Labs LLC

Displaying the last 30 days of deleted objects

Name	Type	Deleted On	Purge Time
Cygna Labs CA-2677-1.0	application	May 11, 2022, 5:48:52 PM	24 days
MBuTest1	user	May 11, 2022, 12:03:34 PM	24 days
Child1guest10107	user	Apr 21, 2022, 2:25:13 PM	4 days
Child1guest10106	user	Apr 21, 2022, 2:25:13 PM	4 days
Child1guest10112	user	Apr 21, 2022, 2:25:13 PM	4 days
Child1guest10108	user	Apr 21, 2022, 2:25:13 PM	4 days
Child1guest10111	user	Apr 21, 2022, 2:25:12 PM	4 days

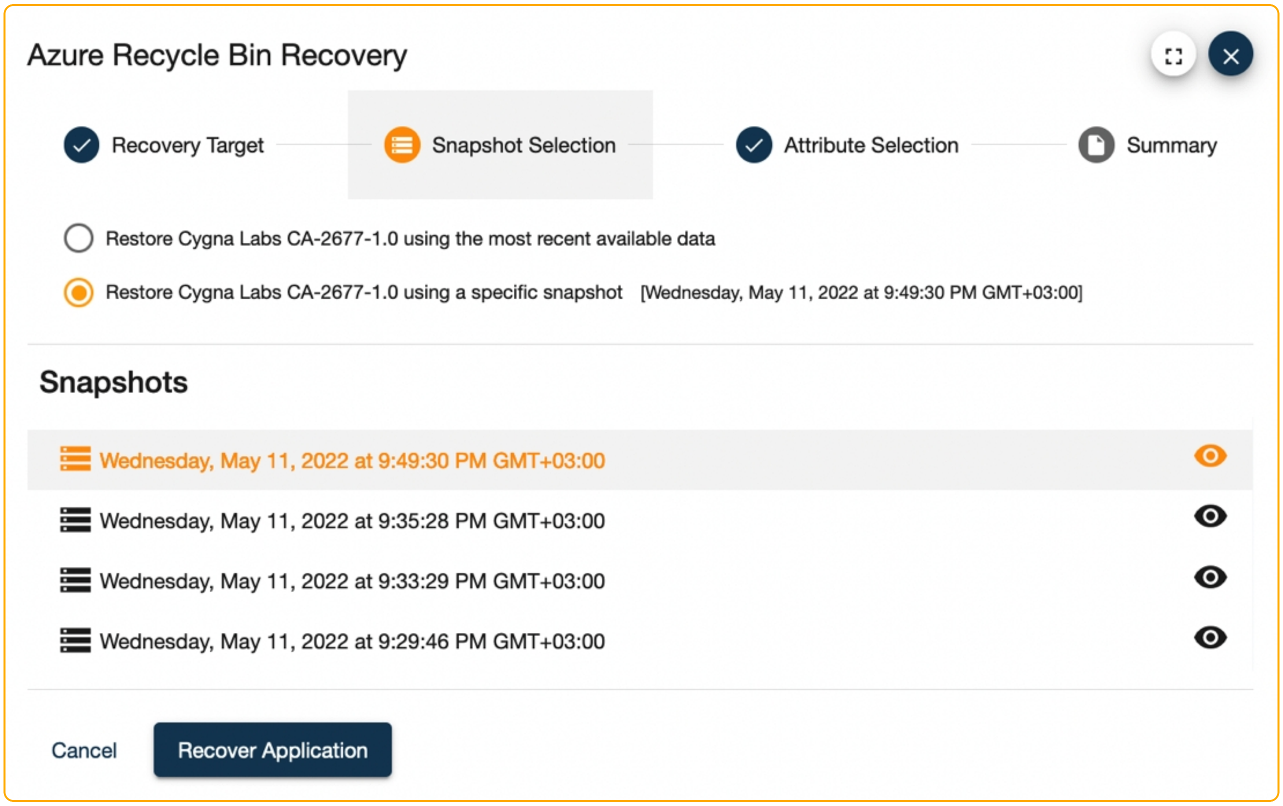
To recover changes:

1. Navigate to **Tools / Azure AD Recovery** to see the **Azure AD Recycle Bin**.

   Alternatively, to recover Azure AD changes right from the Auditing search, select an entry, expand its properties and select **Rollback**.

2. Select the Microsoft Subscriptions tenant account from the list.

3. Review recent changes. By default, Cygna Auditor lists objects were placed in the Azure Recycle Bin within last 30 days. Click on the calendar icon 📅 to update these settings.
4. Select a entry you want to recover.
5. In the wizard, on the **Recovery Target** step, review information about the object you are about to recover.
6. On the **Snapshot Selection** step, pick a snapshot. Cygna Auditor will restore the object to the state it was at the moment of the snapshot creation. You can use the most recent snapshot or any snapshot of your choice.
7. If you selected a specific snapshot, proceed to the **Attribute Selection** step. On this step, you can review object attributes that has been updated and pick the attributes to roll back their changes. By default, Cygna Recovery roll back all attributes to a selected snapshot state but you can fine-tune this process and pick the attributes manually.
8. Review the **Summary** page and click **Recover**. You've got an option to recover an object as a currently logged in user or impersonate as administrator. In this case, you'll be prompted to provide administrative credentials.



○ Restore Cygna Labs CA-2677-1.0 using the most recent available data

● Restore Cygna Labs CA-2677-1.0 using a specific snapshot [Wednesday, May 11, 2022 at 9:49:30 PM GMT+03:00]

Snapshots

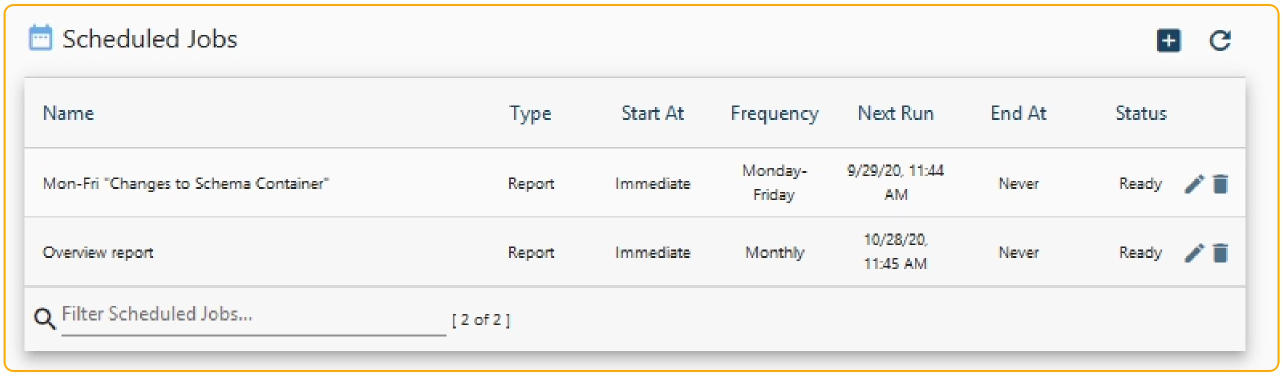
- Wednesday, May 11, 2022 at 9:49:30 PM GMT+03:00
- Wednesday, May 11, 2022 at 9:35:28 PM GMT+03:00
- Wednesday, May 11, 2022 at 9:33:29 PM GMT+03:00
- Wednesday, May 11, 2022 at 9:29:46 PM GMT+03:00

Scheduler

Cygna Auditor Scheduler enables you to review all active subscriptions on the same page as well as add new report subscriptions.

To review subscriptions:

1. Navigate to **Tools / Scheduler**.
2. Review currently scheduled reports and update jobs if necessary.



Scheduled Jobs

Name	Type	Start At	Frequency	Next Run	End At	Status
Mon-Fri "Changes to Schema Container"	Report	Immediate	Monday-Friday	9/29/20, 11:44 AM	Never	Ready
Overview report	Report	Immediate	Monthly	10/28/20, 11:45 AM	Never	Ready

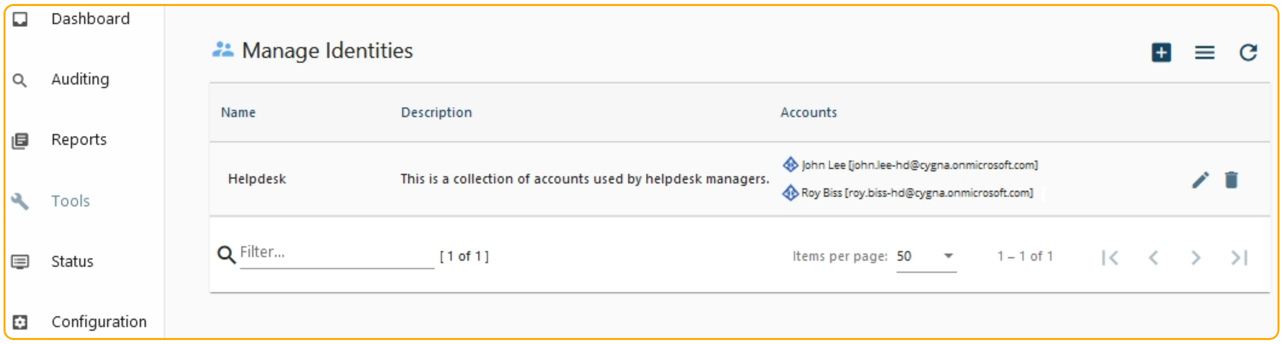
Cygna Identities

Cygna Auditor helps you manage user accounts in a smart way. It automatically detects accounts that likely belong to the same person and groups activity by this identity. This features comes handy if you have multiple authentication systems that provide access to interconnected corporate resources.

For example, Anna Smith is a tier-2 helpdesk specialist, she has her Active Directory credentials, SQL Server credentials, and VMware administration credentials. By default, the activity recorded by different data sources is regarded as independent. It means you'll see three different Anna accounts in the Who column. For your convenience, Cygna Auditor creates a higher Cygna identity Anna Smith and ties all Anna's activity coming from Active Directory, SQL Server, and other sources to a single identity.

Cygna Auditor analyzes all auditing events and creates new identities based on this data. Alternatively, you can always create Cygna identities yourself. For example, you can create a super-identity for the entire Helpdesk department in order to have better understanding of their chores and daily activity.

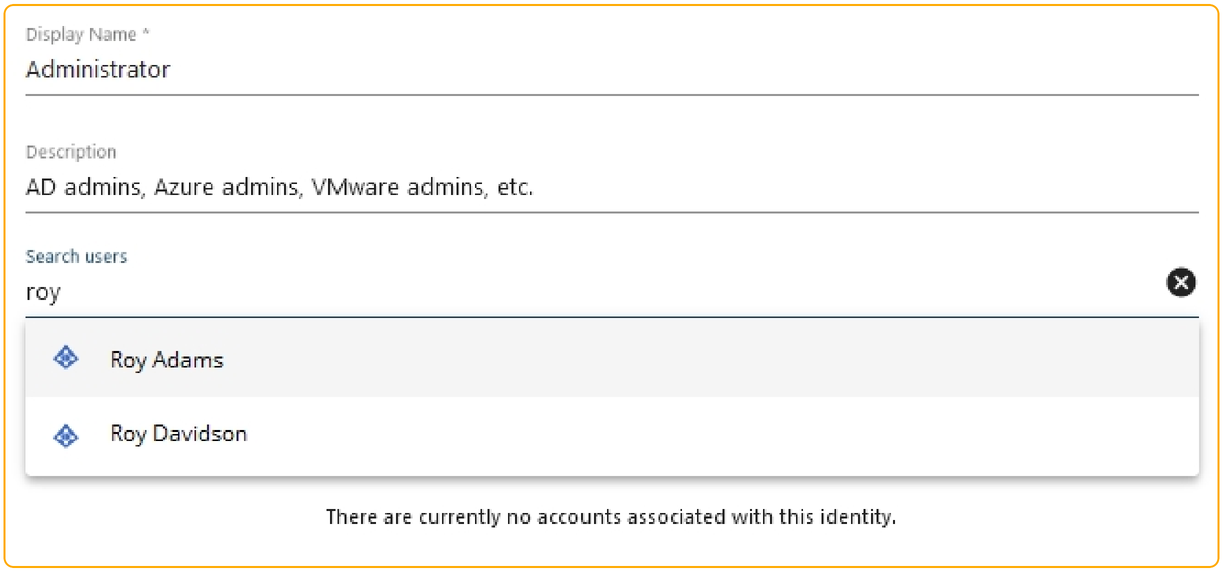
Creating an Identity



Name	Description	Accounts
Helpdesk	This is a collection of accounts used by helpdesk managers.	John Lee [john.lee-hd@cygna.onmicrosoft.com] Roy Biss [roy.biss-hd@cygna.onmicrosoft.com]

To create a custom identity and review those suggested by Cygna Auditor:

1. Navigate to **Tools / Cygna Identities**.
2. Select ⊞ to add a new identity.
3. Provide a name for a new identity, description, and search for users.



Display Name *
Administrator

Description
AD admins, Azure admins, VMware admins, etc.

Search users
roy

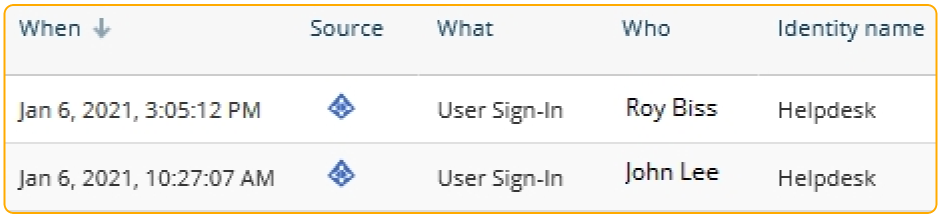
Roy Adams

Roy Davidson

There are currently no accounts associated with this identity.

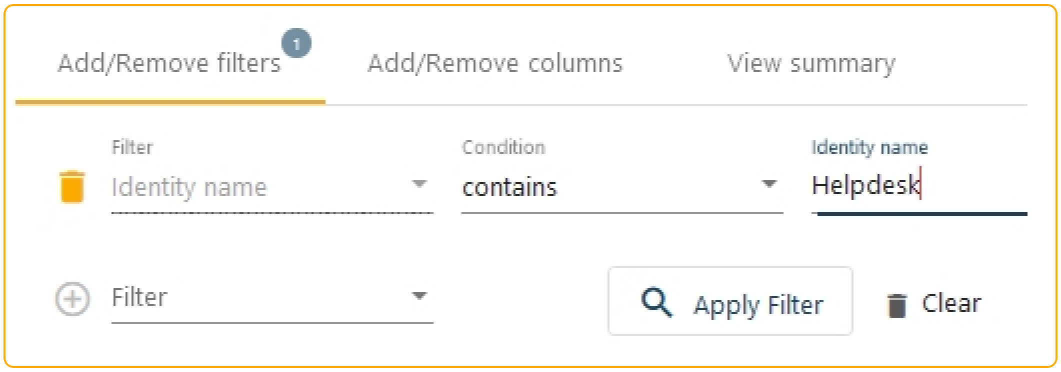
Searching for Identity

Identities appear in **Reports** and **Auditing** search.



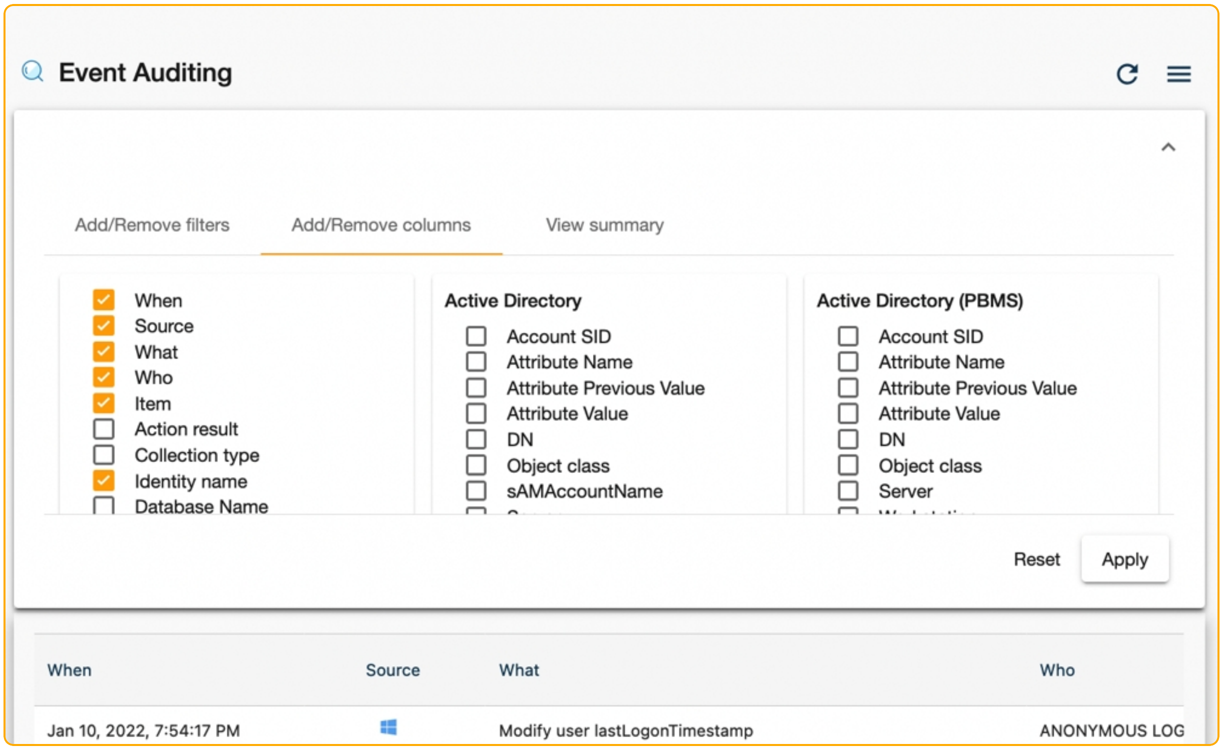
When ↓	Source	What	Who	Identity name
Jan 6, 2021, 3:05:12 PM	◈	User Sign-In	Roy Biss	Helpdesk
Jan 6, 2021, 10:27:07 AM	◈	User Sign-In	John Lee	Helpdesk

- Search by **Identity**. Add the identity filter and provide a value.



Filter: Identity name
Condition: contains
Identity name: Helpdesk

- Add the **Identity** column to your search results. On the **Add/Remove columns**, select the **Identity name** to display this column in the Auditing search results.



☑ When
☑ Source
☑ What
☑ Who
☑ Item
☐ Action result
☐ Collection type
☑ Identity name
☐ Database Name

Active Directory

☐ Account SID
☐ Attribute Name
☐ Attribute Previous Value
☐ Attribute Value
☐ DN
☐ Object class
☐ sAMAccountName

Active Directory (PBMS)

☐ Account SID
☐ Attribute Name
☐ Attribute Previous Value
☐ Attribute Value
☐ DN
☐ Object class
☐ Server

When	Source	What	Who
Jan 10, 2022, 7:54:17 PM		Modify user lastLogonTimestamp	ANONYMOUS LOG

Index