CYGNA LABS

Cygna Auditor

Getting Started Guide

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

Published 1/9/2019

Version 1.2

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, Office 365, etc. Cygna Auditor is a straightforward and easy-to-use solution that provides clear and affordable overviews of activity in your business critical assets, helps you pass compliance audits and mitigate risks.

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

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

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

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

Insight into Architecture and Workflow

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

Workflow

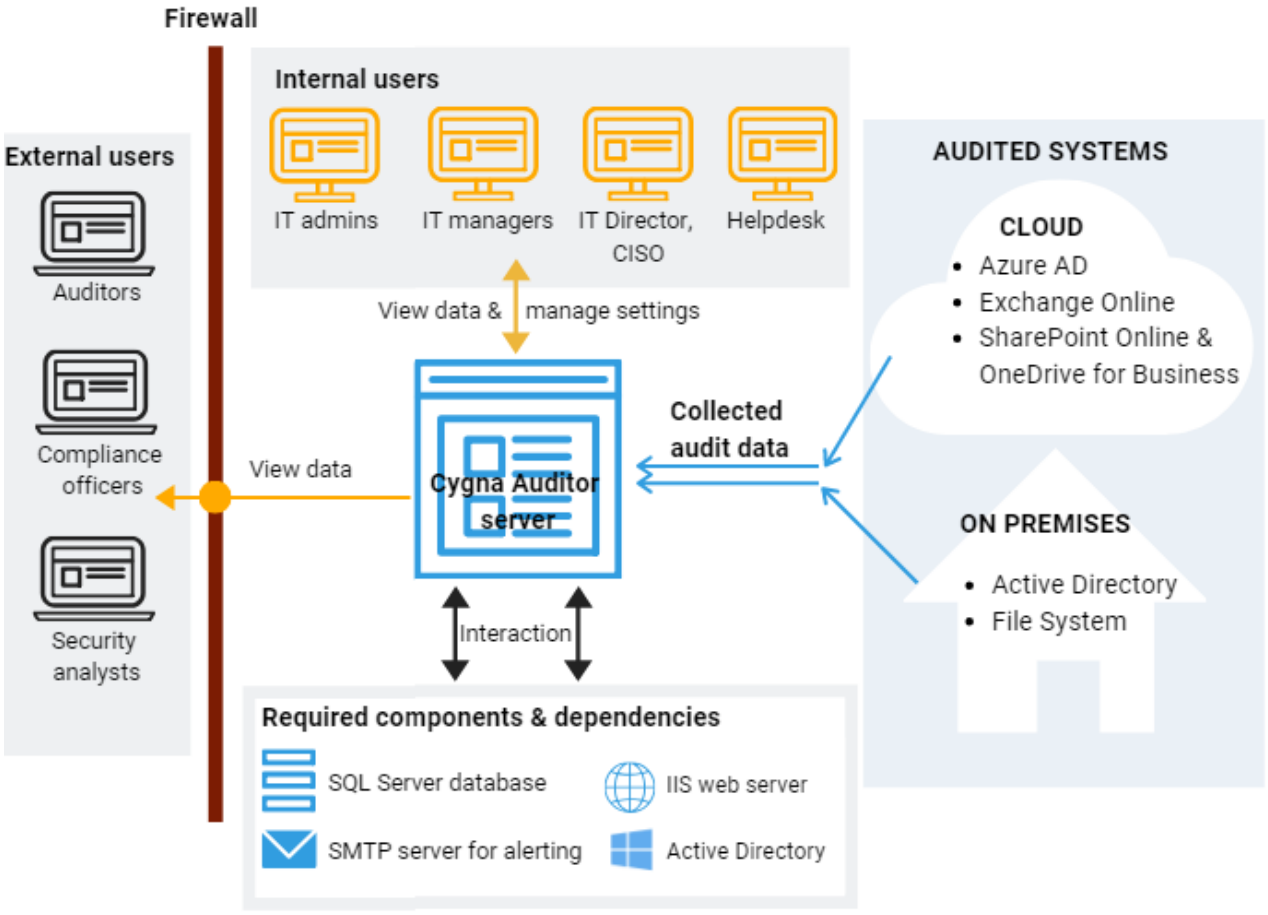
If you take a closer look at your journey with Cygna Auditor, you will discover that it consists of the following simple stages:

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 Installing the Product.
3. **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 audited systems, you have to adjust some settings to enable Cygna Auditor to collect audit events. Check out Cygna Auditor online documentation portal for more information and detailed instructions.
4. **Administration.** Dive deep into the product administration. Delegate access to your authorized personnel, manage licenses, etc. Check out Cygna Auditor online documentation portal for more information and detailed instructions.
5. **Basic auditing.** Every so often, review out-of-the-box reports to validate compliance with various standards or use search to investigate potential threats and address risks immediately. For more information, see Key Features.
6. **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, or construct global all modules-wide searches. For more information, see Key Features.

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.



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.	Yes
SQL Server	Stores audit data collected by Cygna Auditor.	Yes
IIS web server	Hosts Cygna Auditor web-console.	Yes
SMTP server	Enables email and SMS 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.

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 2016 with preinstalled IIS and .Net Framework 4.6 for Cygna Auditor.
2. The other server with SQL Server 2016 Standard Edition.

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

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 • Windows Server 2012 R2 • Windows Server 2016
Server roles and features	• **Web Server (IIS)**: Microsoft IIS 8.0 or above, including Windows Authentication, ASP.NET 4.6 • **.Net Framework**: Microsoft .Net Framework 4.6, including ASP.NET 4.6 Note: Depending on the OS, you might need to install ASP.NET 4.6 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 2012 • SQL Server 2014 • SQL Server 2016 (Recommended) • SQL Server 2017 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 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
Server roles and features	• **Web Server (IIS)**: Microsoft IIS 8.0 or above, including Windows Authentication, ASP.NET 4.6 • **.Net Framework**: Microsoft .Net Framework 4.6, including ASP.NET 4.6 Note: Depending on the OS, you might need to install ASP.NET 4.6 manually.
Database	• SQL Server 2012 • SQL Server 2014 • SQL Server 2016 (Recommended) • SQL Server 2017 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.
Additional software	Any modern browser, preferably Google Chrome or Microsoft Edge.

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 user 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. **Note:** This account will only be used during for the product installation.	Sufficient permissions to create objects in the Active Directory forest. For example, you can use an account that is a member of the **Domain Admins** group.
Current user account	The account running the installation. During the installation, Cygna Auditor will create and start a service.	Permissions to create services. For example, your account should be a member of local **Administrators** group.
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. This	The **dbcreator** server role. **Note:** Once the database is created, you can revoke the **dbcreator** server role and grant the **db_owner** role on the database instead.

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
	database will be used to store audit data.	
Customer portal account	Credentials you use to log in to Cygna customer portal. During the installation, Cygna Auditor will automatically retrieve your license key. Later, these credentials will be used to periodically check and update your license status.	Any user registered with Cygna customer portal.

Installing the Product

QUICK TIP: Have you read the Planning Deployment chapter? Ensure the computer where you plan to install Cygna Auditor has .NET Framework 4.6 (including ASP.4.6) and Web server (IIS) role enabled.

1. Log in to Cygna customer portal. In the portal, check your license status or request a trial, and then download Cygna Auditor.
2. Double-click the installer to start the setup wizard.
3. On the **End User License Agreement** page, carefully read the license text and then accept the license terms if you agree with them.
4. On the **Destination Folder** page, review a default installation path (*C:\Program Files\Cygna Labs*) or click **Change** to specify an alternative installation folder.
5. On the **Active Directory Credentials** page, specify our corporate Active Directory forest and enter user credentials.

   Cygna Auditor prepopulates the forest and user fields with the name of your domain and your current user account; update them if necessary. Make sure the account you specify has sufficient permissions to create objects in Active Directory.
6. On the **Cygna Auditor repository** page, 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.
7. On the **Database Creation Credentials** page, enter the user credentials, authentication type (SQL or Windows), and test connection. The user account you specify must have sufficient permissions to create a database on your SQL Server instance. Cygna Auditor will use this database to store collected audit data.

   Note: SQL authentication is a recommended method. If you select Windows authentication method, make sure to check out Updating Application Pool Identity.
8. On the **Cygna Customer Portal Credentials** page, provide credentials you use to log in to Cygna customer portal. The product will verify the license key and continue to

use these credentials to periodically check and update your license status.

Note: The product requires internet access to verify the license. If the computer where you install Cygna Auditor has no internet access, contact Cygna Labs sales representative to discuss the possible options.

9. On the **Ready to install Cygna Auditor** page, click **Install**. During the installation, all necessary files and folders will be created, services started, Cygna Auditor web-console will be deployed as a website on your IIS, and the audit database will be created in a specified SQL Server instance.

Post-Installation Steps

These post-installation steps are only required if you

- Selected Windows authentication method to connect to SQL Server. Go to Updating Application Pool Identity.
- Use SQL Server Express as a storage for your audit data. Go to Configuring Additional Steps for SQL Server Express.

Updating Application Pool Identity

During the installation, if you opted for Windows authentication on the **Database Creation Credentials** page, you must manually update the application pool identity on your Web server (IIS). Otherwise, the Cygna Auditor web-console will not be able to connect to its audit database.

To check and update application pool identity:

1. Navigate to IIS Manager.
2. In the **Application pools**, select **Cygna Labs Web Console** and click **Advanced Settings** on the right.
3. In the **Process Model** section, locate the **Identity** item and expand it.
4. In the **Application Pool Identity** dialog, specify **Custom account**, click **Set** and provide the same user credentials you specified for Windows authentication in your SQL Server instance.

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.

Starting the Product

To start Cygna Auditor on a local computer:

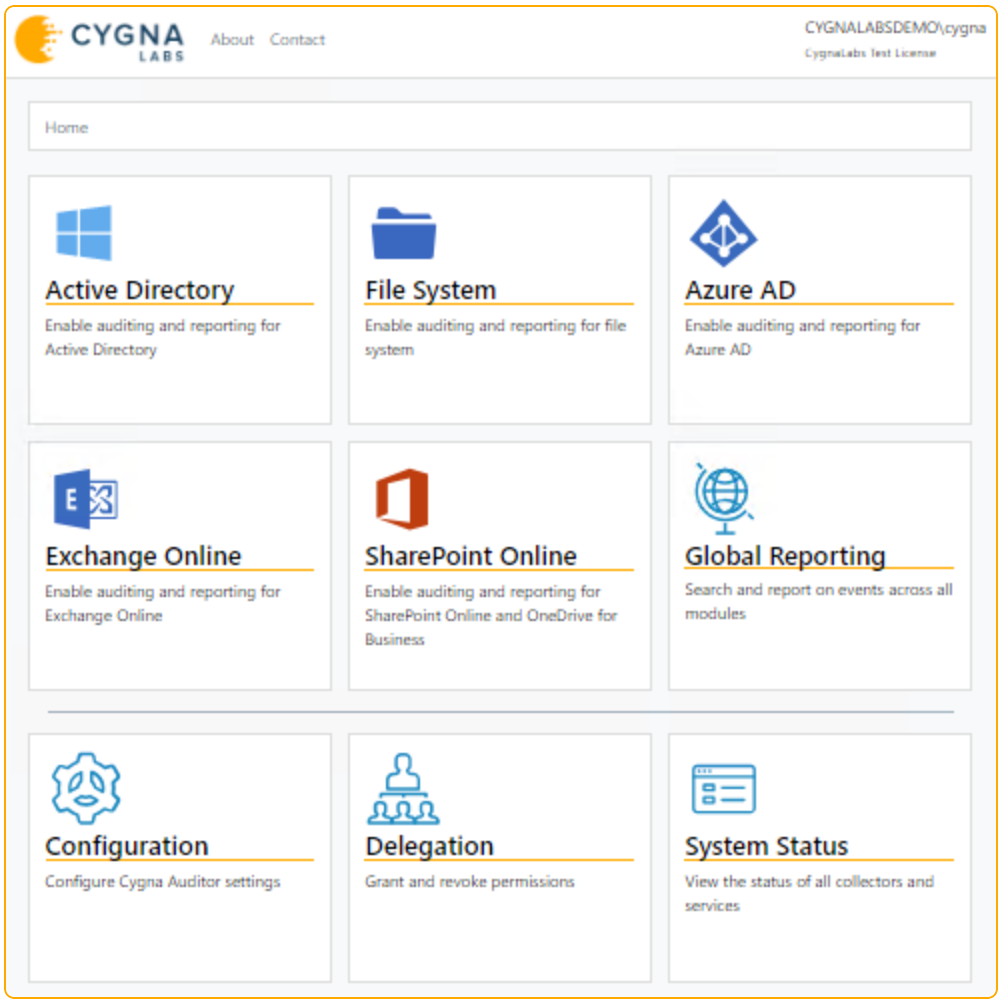
- Open a web browser and type "http://localhost/cygna".

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 "http://CygnaAuditorMachineName/cygna", where CygnaAuditorMachineName is a name of computer where Cygna Auditor was deployed. For example: *http://cygnaconsole/cygna*.
2. Enter your user credentials.

As you log in, you will see the Cygna Auditor home page with everything you need to start auditing your environment. It is up to you whether you want to configure delegation and other administration tasks first or jump right away to the audited system that requires your immediate attention.



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.

Audited Systems

Use this quick reference to find out what audited systems are currently supported by Cygna Auditor.

AUDITED SYSTEM	VERSIONS
Active Directory	Windows Server 2008 R2 Windows Server 2012 / Windows Server 2012 R2 Windows Server 2016
Azure AD	As distributed with Office 365
Exchange Online	As distributed with Office 365
SharePoint Online	As distributed with Office 365
Windows File System	Windows Server 2008 R2 Windows Server 2012 / Windows Server 2012 R2 Windows Server 2016 Windows 7 Windows 8.1 Windows 10

To ensure successful data collection, most audited systems require some configuration on their side. Check out Cygna Auditor online documentation portal for more information and detailed instructions.

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.

Basically, Cygna Auditor reports the following actions in Active Directory:

Create	Modify	Delete
Restore	Move	Rename

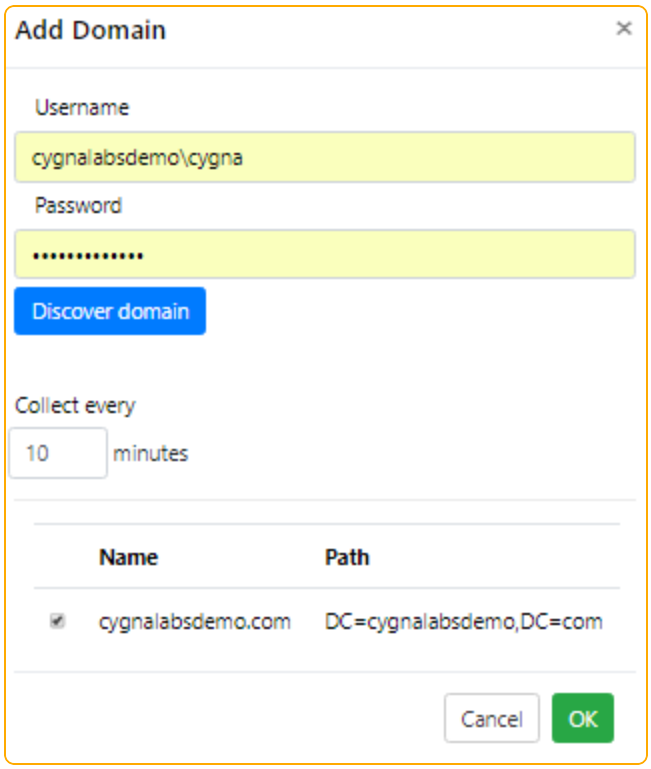
Enabling Audit

QUICK TIP: Have you configured your domain for auditing? Check out Cygna Auditor online documentation portal for more information and detailed instructions.

1. On the Cygna Auditor home page, click the **Active Directory** tile and then drill-down to **Configuration** / **Domains**.
2. Click **Add**.
3. In the pop-up dialog that opens, complete the fields:

OPTION	DESCRIPTION
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. For successful data collection, the account must have access to domain controllers' event logs.
Collect every	Specify how often do you want Cygna Auditor to collect audit events. By default, every 90 minutes. It means it will take up to 90 minutes for change records to become available for search and reporting.

4. Click **Discover domain** to look up for domains available for auditing. Check those you want to audit and click **OK**.



The domains you specified will appear in the list, with status and data collection frequency for each domain.

Name	Path	Frequency (minutes)	Status
cygnalabsdemo.com	DC=cygnalabsdemo,DC=com	3	OK

Continue reading:

Search

Reports

Activity Widgets

Alerts

Global Search

Global Reports

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.

Basically, Cygna Auditor reports the following actions on your file servers:

Open	Close	Read	Write
Create	Delete	Rename	Set attribute
Set permission	Recycle	Restore	Duplicate

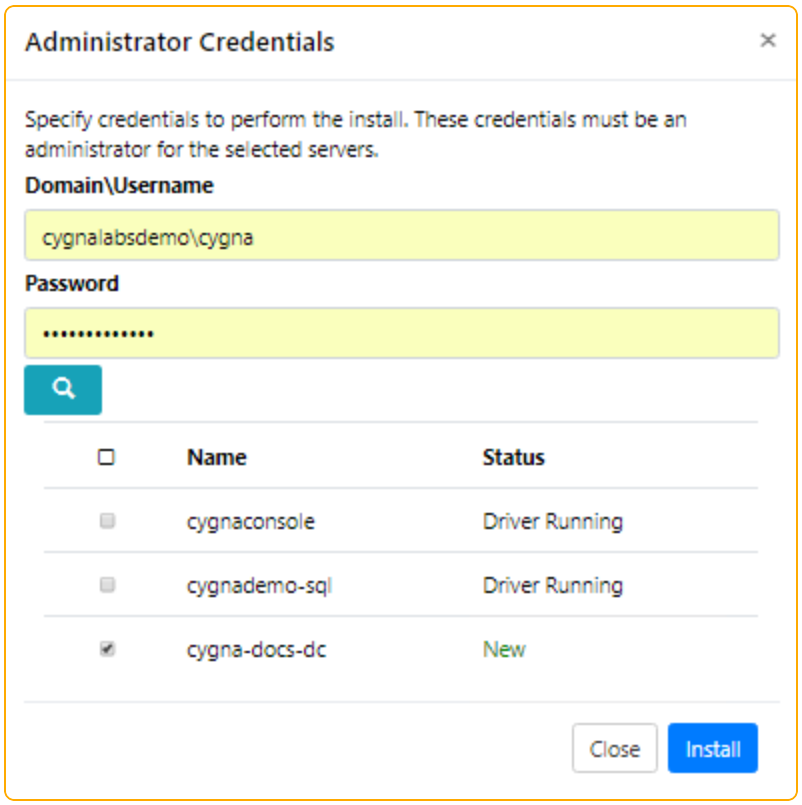
Enabling Audit

1. On the Cygna Auditor home page, click the **File System** tile and then drill-down to **Configuration / Servers**.
2. 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. You can deploy a service automatically or manually.

   Note: If you plan to audit Cygna Auditor application server for file system changes, install the service manually.

   - **Manually:** Click (the question mark button) and click the link to download the File System auditing service installer package. On each server you want to audit, install the service and start it.
   - **Automatically:** Click (the Add server button). In the dialog that opens, provide administrator credentials and click . Cygna Auditor will look up for servers and show the list of available servers. Select servers you want to audit and click **Install**.

     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. Specify folders for auditing. To do this, navigate to **File System / Alerts** and create a new alert for a folder you want to monitor. There is no need to add any actions. See Creating Alerts for detailed instructions.
4. Check the data collection status in the audited servers list.

Name	Status	Alert Count	Last Update
CYGNACONSOLE	Driver Running	1	Oct 25, 2018 12:49 PM

Continue reading:

Search

Reports

Activity Widgets

Alerts

Global Search

Global Reports

Office 365 Apps and Azure AD

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 and gain so much needed transparency in your Azure AD and Exchange Online activity. Cygna Auditor helps you detect potential threats and mitigate risks of internal and external attacks in the Cloud.

Configuring Office 365 Settings

Currently, Cygna Auditor allows collecting data from a single tenant. It means your Office 365 apps should belong to the same tenant, i.e. be in the same Azure AD domain.

1. On the Cygna Auditor home page, select **Configuration** / **Office 365**.

   Alternatively, you can click the **Azure AD**, **Exchange Online**, or **SharePoint Online** tile and then drill-down to **Configuration**.

2. Specify the polling interval. By default, 3 minutes. This value controls how often Cygna Auditor will check for updates in your Office 365 apps.

3. Click **Reauthorize** to deploy and authorize the Cygna Labs application in your Office 365. You will be prompted to enter your Microsoft account credentials. The user you specify must have sufficient permissions to deploy applications in Office 365, i.e. be granted the **Global administrator** role in your Azure AD domain.

   Make sure, the computer from which you authorize (Cygna Auditor application server, your proxy server, or a computer where you opened the Cygna Auditor web console) have access to the following Office 365 URLs:

   cygnacloud.azurewebsites.net

   graph.microsoft.com

   login.microsoftonline.com

   login.windows.net

   *.microsoftonline-p.com

   manage.office.com

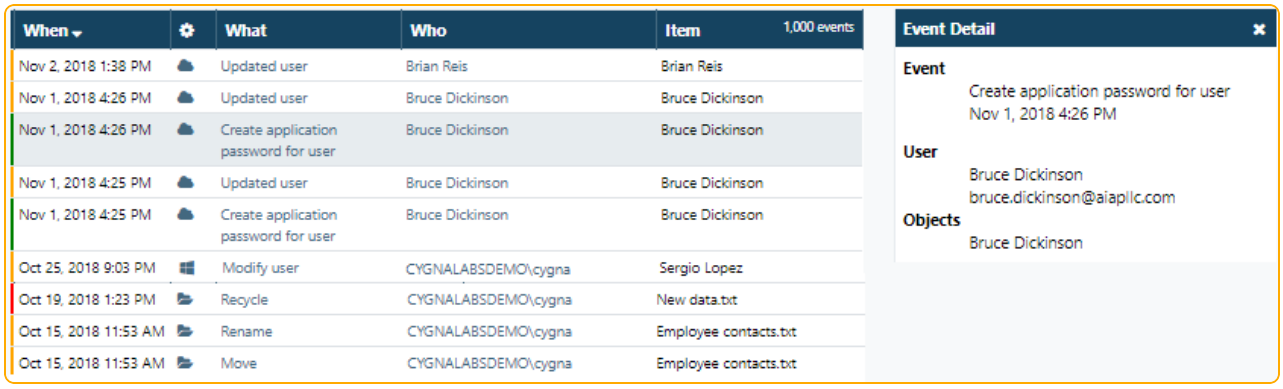
Once you configure Office 365 settings, data collection will start automatically for Azure AD, Exchange Online, and SharePoint Online.

Continue reading:

Search

Key Features

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



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

FEATURE	WHAT IS IT GOOD FOR?
Global Search	• Digging into security incidents • Investigating user actions across all audited systems • Focusing on event chains—subsequent events leading to a breach or security issue • Identifying potentially harmful users and security breaches in your environment
Search	Same as Global Search but with a focus on details specific to each audited system
Custom Global Reports	• Analyzing your environment structure and safe activity patterns across the entire organization • Identifying potential bottlenecks and their impact on your organization
Built-in Reports	• Proving compliance with security standards and regulations (PCI, HIPAA, SOX, etc.) • Passing internal and external audits

FEATURE	WHAT IS IT GOOD FOR?
Activity Widgets	Getting an activity digest. Widgets provide a visual overview of your audited system and help you check that everything goes well and no unusual activity was detected.
Alerts	Detecting threats as they occur. Alerts are sent immediately as a potentially harmful action is detected and processed by the product.

Global Search

Get the data at your fingertips with Global Search—review activity across all modules 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 audited system and see a bigger picture.

To review activity in your environment and start creating data searches, go to **Home** / **Global Reporting** / **Search**. You will see all changes right away. Then, you can narrow down your search to what bothers you the most. Creating a search 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. If you like the search you created, you can save it as a report to use it later.

The Global 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 from Search
- Distilling Search Results

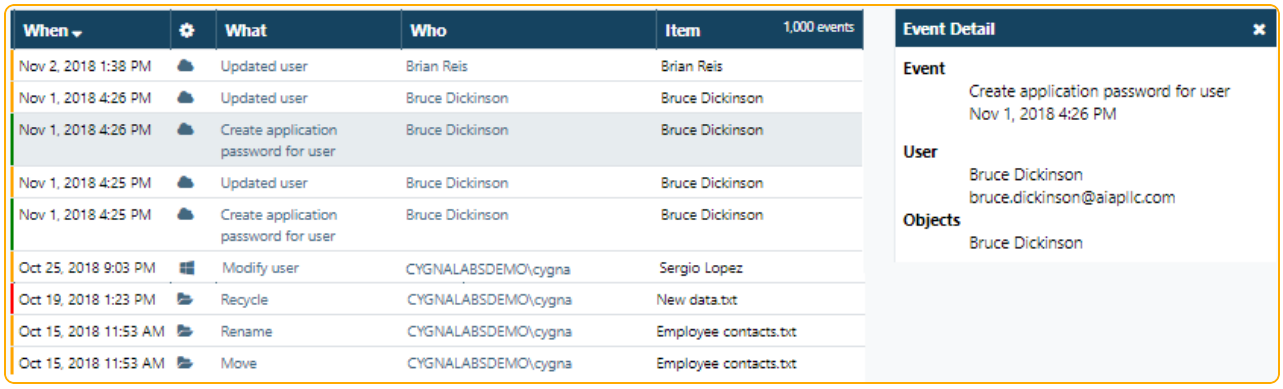
You can use these techniques interchangeably or supplementing each other. A good idea is to always start with all changes on the screen and then drill-down to more specific events.

Reviewing All Changes

To have a look on whats' going on in your corporate environment, go to Global Search and start browsing changes. Cygna Auditor is designed to display 1,000 newest events to ensure you can review the latest changes across all audited systems you are authorized to work with.

Each record includes a date when the activity took place, the audited system, what was made, the user who made the change, and the item or object that was affected. To get more information, click on the record—the details pane will appear on the right.

Reviewing all records is handy if you want to execute control over your data flow.



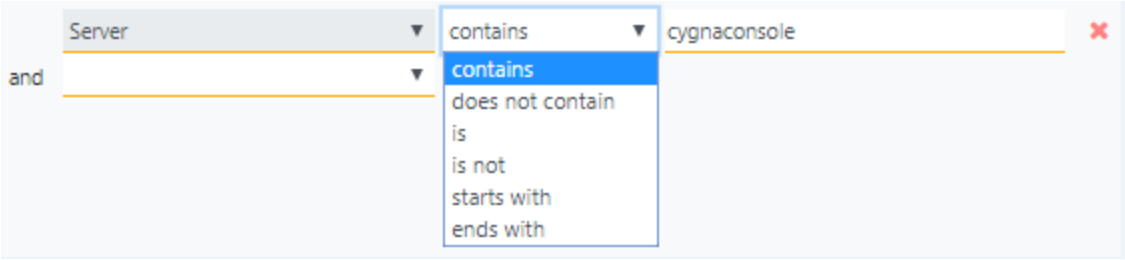
If you are interested in some particular changes, you can construct a search query by adding search conditions or adjust your search right from the data pane.

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.

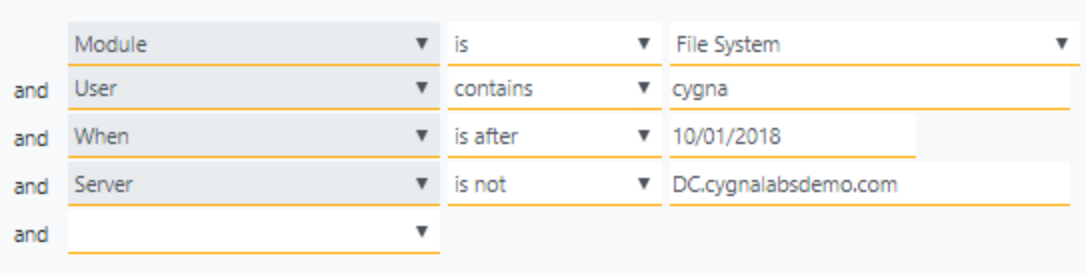
The search conditions basically describe what you are looking for. Each entry consists of three fields: the filter, the match type, and the value. You can add as many search entries to your search as you want, Cygna Auditor will look for records that match all search conditions at once.

FIELD	DESCRIPTION
Filter	The filter corresponds to the information you are searching. For example, *user*, *server*, or *when*.
Match type	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 entry that *starts with* or *ends with* a certain value. Exact and broad search can be negative as well (*is not* and *does not contain*).
Value	The value field is the area where you specify a value to be searched. For example, the name of a user or a server. 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:



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 includes "cygna" (e.g., cygnalabsdemo\cygna, cygnaconsole\cygnaadmin, etc.)
- On any server except "dc.cygnalabs.demo" (this server is specified with "is not" match type)
- That happened after October 1, 2018
- That is tracked within the File System module

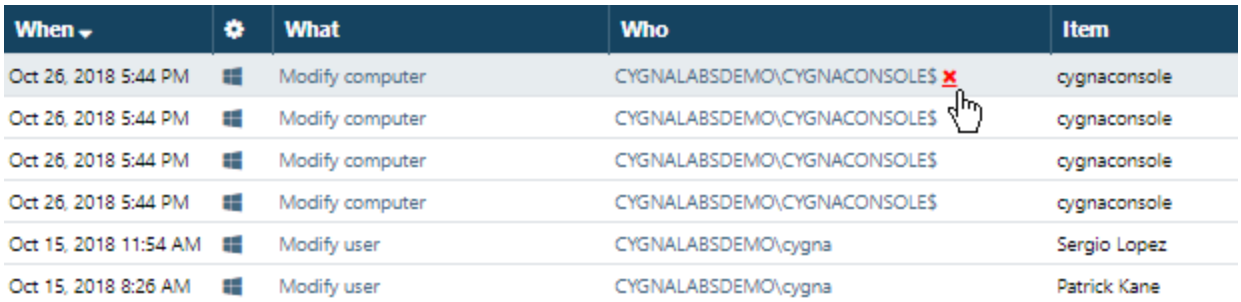
When	What	Who	Item
Oct 15, 2018 11:53 AM	Create	CYGNALABSDEMO\cygna	New folder
Oct 12, 2018 11:21 AM	Create	CYGNALABSDEMO\cygna	New Text Document.txt
Oct 12, 2018 11:20 AM	Create	CYGNALABSDEMO\cygna	New folder
Oct 12, 2018 8:52 AM	Create	CYGNALABSDEMO\cygna	New Compressed (zipped) Folder.zip
Oct 15, 2018 11:53 AM	Move	CYGNALABSDEMO\cygna	Employee contacts.txt
Oct 12, 2018 11:21 AM	Move	CYGNALABSDEMO\cygna	Archive with files.zip
Oct 23, 2018 2:08 PM	Open	CYGNALABSDEMO\cygna	Cygna Documents

Excluding Bias from Search

As you browse changes with Global Search, 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 cross. 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.

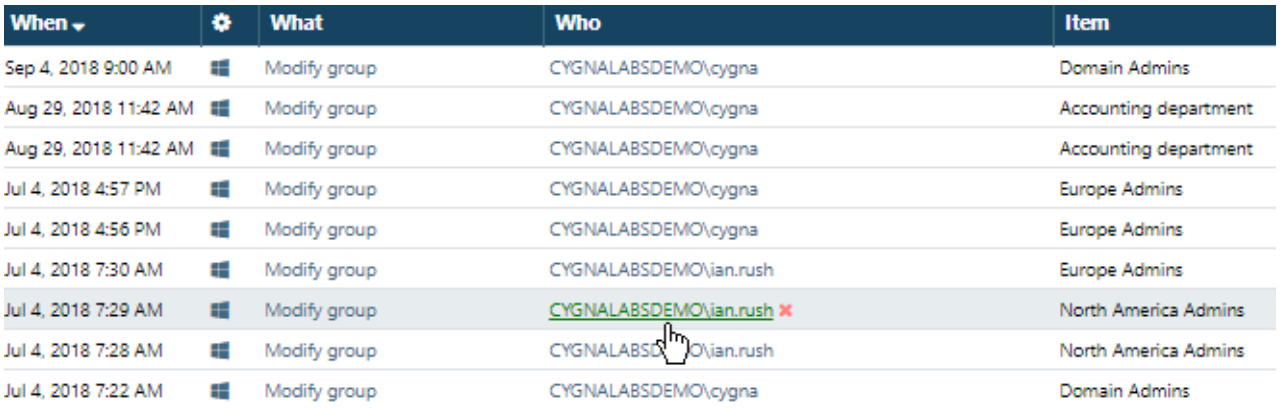


Distilling Search Results

As you browse changes with Global Search, 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, wait until it gets highlighted and underlined green and click on it. 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		What	Who	Item
Sep 4, 2018 9:00 AM		Modify group	CYGNALABSDEMO\cygna	Domain Admins
Aug 29, 2018 11:42 AM		Modify group	CYGNALABSDEMO\cygna	Accounting department
Aug 29, 2018 11:42 AM		Modify group	CYGNALABSDEMO\cygna	Accounting department
Jul 4, 2018 4:57 PM		Modify group	CYGNALABSDEMO\cygna	Europe Admins
Jul 4, 2018 4:56 PM		Modify group	CYGNALABSDEMO\cygna	Europe Admins
Jul 4, 2018 7:30 AM		Modify group	CYGNALABSDEMO\ian.rush	Europe Admins
Jul 4, 2018 7:29 AM		Modify group	CYGNALABSDEMO\ian.rush	North America Admins
Jul 4, 2018 7:28 AM		Modify group	CYGNALABSDEMO\ian.rush	North America Admins
Jul 4, 2018 7:22 AM		Modify group	CYGNALABSDEMO\cygna	Domain Admins

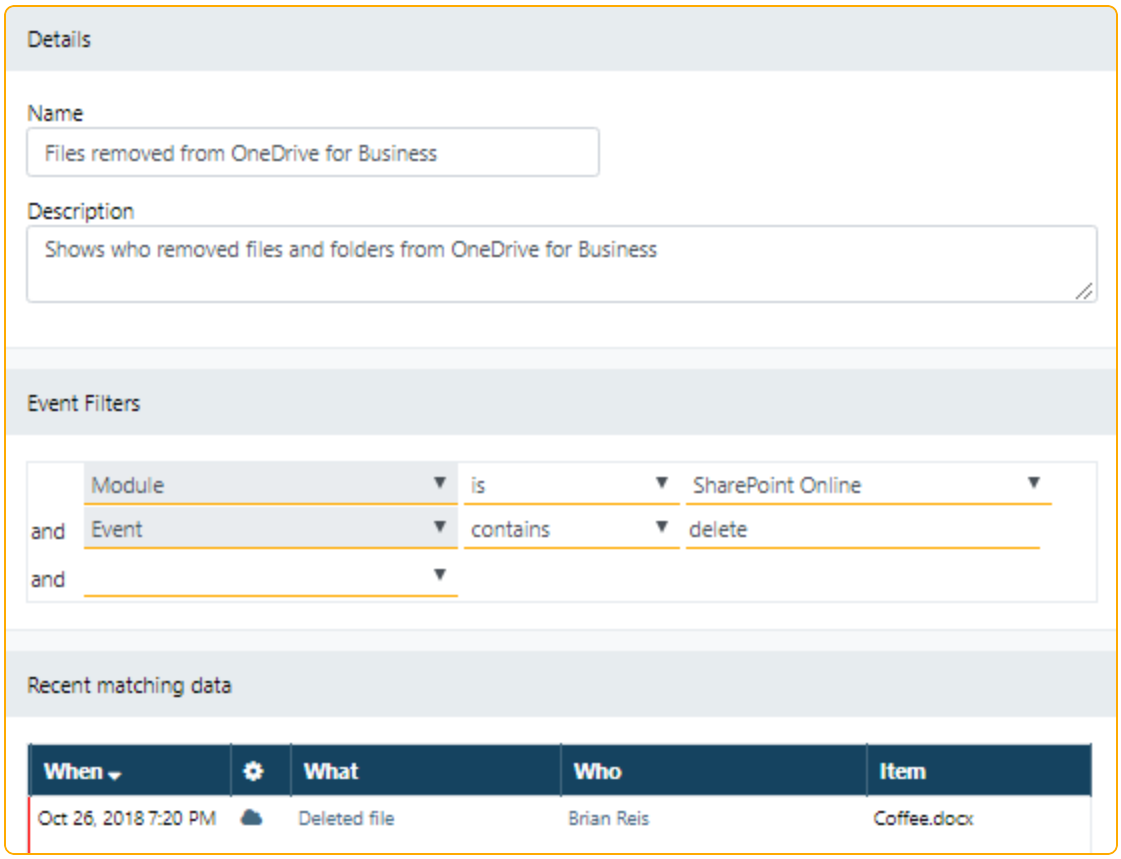
Global Reports

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 audited system, Cygna Auditor enables you to create custom cross-system reports based on Global Search.

Leveraging flexible filters of Global Search, Global reports 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 **Global Search** page or go to **Home** / **Global Reporting** / **Reports** and click **Create** to set up a new report.

For your convenience, Global Reports are featuring the same search techniques and data presentation as Global Search. If you are not familiar with these search techniques, refer to Global Search for more information.



Search

With search, you can explore activity and monitor changes across the entire audited system or drill-down and examine a security incident down to the tiniest detail.

Investigations and security analysis are much easier with Cygna Auditor intuitive search so you can focus on getting your work done instead of fighting your way through the auditing workflow.

Learn more about Creating Search Queries and Reading Search Results.

Creating Search Queries

QUICK TIP: Try asking yourself, "What am I looking for?" and spell out your query in filters or exclusions.

For example: I'm looking for all modifications (What) Ian Rush (Who) made during the last 24 hours (When). Or I'm looking for changes made by members of the Domain Admins group (Who) except for a trustworthy administrator called James Good (exclude Who).

To search for audit data:

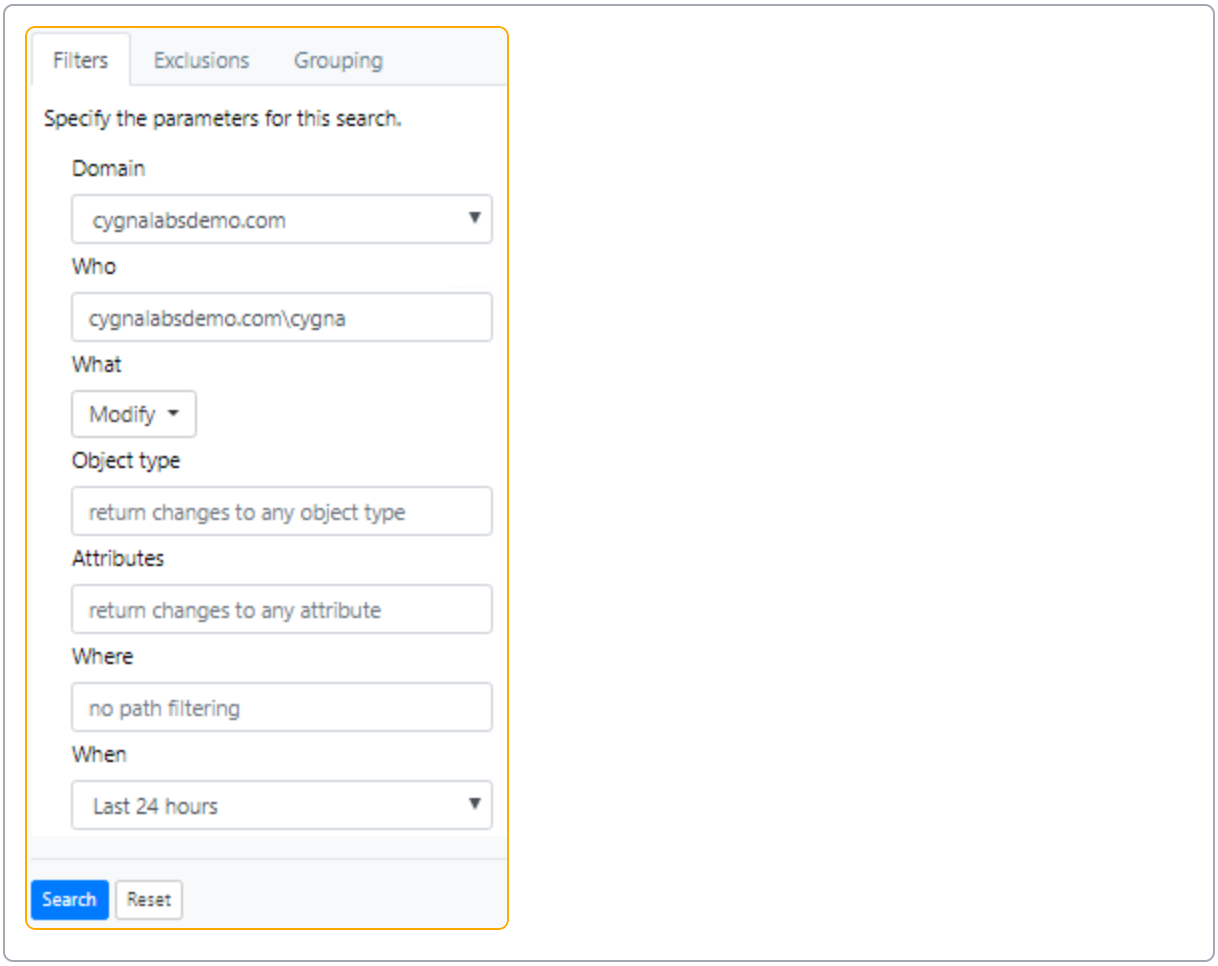
Note: The procedure below applies to the Active Directory module. Running search may vary slightly for other modules.

1. On the home page, select an audited system.
2. Select **Search**.
3. Customize your search—create a search query tailored to look for the information you are specifically interested in. Make sure to use full names as filters are designed to search for exact entries (e.g., cygnalabsdemo.com\ian.rush instead of ian.rush). To retrieve all activity, keep the search filters blank.
   - On the **Filter** tab, specify parameters to narrow down your search results (for example, specify a user name in the **Who** filter to narrow down your search to activity of a specific user).
   - On the **Exclusions** tab, specify entities you do not care about at the moment and do not want to show up in this search query (for example, a trustworthy administrators group).
   - On the **Grouping** tab, update your grouping preferences if you want to bundle change records based on a certain rule (for example, by user or by action type).

   You can run search without filters or exclusions to get all change records for your audited system.

   EXAMPLE:

   In the image below, filters are configured to search for all modifications the user Ian Rush made during the last 24 hours.

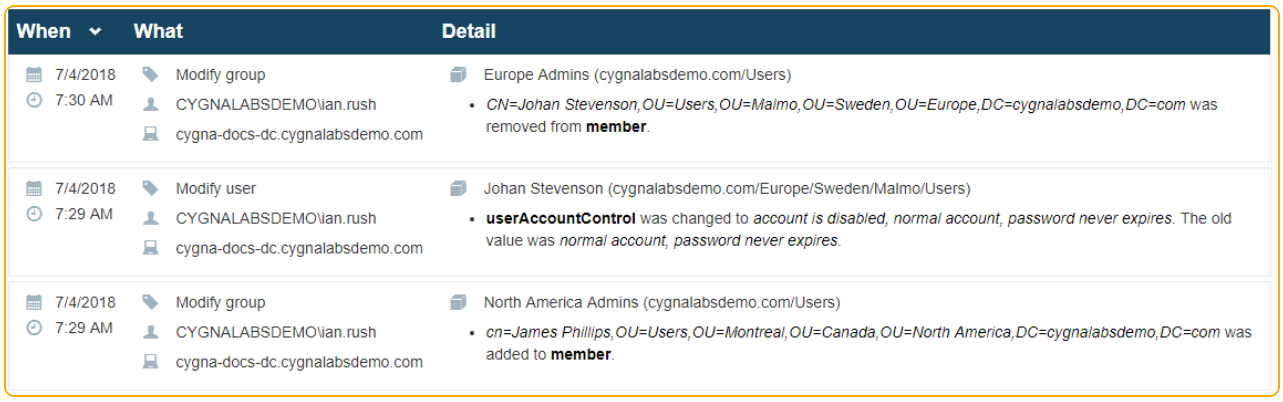


4. Select **Search**. Cygna Auditor will run your query and list all records found based on parameters you specified. For more information on how to view search results, refer to Reading Search Results.

QUICK TIP: Do you like your search query? Save it as a custom report and run it any time you like. Click the **Save as report** button in the upper right corner of your search results. Click **Export** to download the results as a pdf or xml document.

Reading Search Results

In the image below, you can see the search results. Cygna Auditor lists all modifications made by Ian Rush. This user modified Europe Admins and North America Admins groups and disabled a user account.



Icon	Description
	The date when the change occurred.
	The time when the change occurred.
	The action and object type.
	The user who made the change.
,	The computer where the change occurred.
, ,	More details regarding the change. For example, the name of the object that was changed, attributes, etc.

Reports

Cygna Auditor is shipped with audited system-specific reports that can 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?". You can browse the reports list and read report descriptions, or filter reports by tags. Cygna Auditor allows you to run built-in reports out of the box since 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.

To reduce the attack surface specific to your organization, create custom reports based on search. Unlike one-off searches you construct from scratch every time, custom reports are preserved in Cygna Auditor so that you and your colleagues can use them later. For your custom reports, you can add tags and set privacy settings making the reports public or invisible to others.

Learn more about Generating Reports. For your convenience, Cygna Auditor presents report results in the same format as search. To understand how to interpret results correctly, refer to Reading Search Results.

TASK	GO TO
Running built-in reports designed for your audited system	Home / your audited system / Reports / Reports tab
Creating a new custom search	Home / your audited system / Reports / Custom Reports tab **Note:** You can also create a custom report by clicking **Save as report** right from Search.
Analyzing the report execution history and making sure reports are reviewed on time and by appropriate employees	Home / your audited system / Reports / History tab

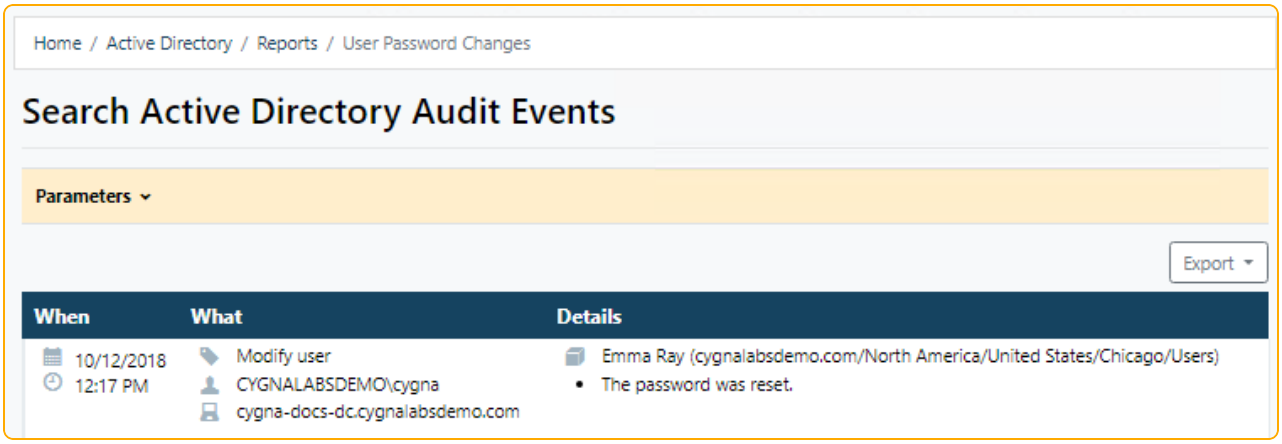
Generating Reports

To generate a report:

Note: The procedure below applies to the Active Directory module. Report generation may vary slightly for other modules.

1. On the home page, pick an audited system.
2. On your audited system landing page, select **Reports**.
3. Select a preset report from the list or go to the **Custom Reports** tab to see reports you created. Once you specify the report, Cygna Auditor will automatically run it.
4. Review the audit data. By default, the report shows data for the last 24 hours.
5. Click **Parameters** if you want to fine-tune your report results, for example, to filter out some users or modify a timeframe. Make sure to use full names as filters are designed to search for exact entries (e.g., cygnalabsdemo.com\ian.rush instead of ian.rush). Click **Run** to update the results.

The example below applies to the User password changes report. As you can see, CYGNALABSDEMO\cygna has reset password for the user Emma Ray.



If compliance regulations or in-house security procedures require you to keep reports, click **Export** to download report data as a pdf or xml document.

For more information on interpreting the data, refer to Reading Search Results.

Activity Widgets

Widgets provide a quick and clear overview of activity in your audited system. 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.

Here in Cygna Labs, we developed widgets for each audited system individually to ensure you get the most demanded activity metrics for your critical assets. You can always review activity widgets under a corresponding tile or add the most important charts right to the audited system landing page.

To learn how to add a widget to a landing page of your audited system, go to Enabling Widgets.

Enabling Widgets

To review widgets and add them on the audited system landing page for quick access:

1. On the home page, select an audited system.
2. Select **Activity Widgets**.
3. Review charts. The widget sets differ for each audited system and are designed to help you identify potential threats such as activity peaks or mass file modifications.
4. Click next to the widget name to add it to the audited system landing page. The widget will appear on the audited system page.

   Some modules (for example, Active Directory) enable you to fine-tune widgets—adjust the data time range, etc.

To hide widgets:

- On the audited system landing page, switch the **Show widgets** slider to *"No"*.

Alerts

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 the Search or Reports functionality. Sent directly to email or as SMS, alerts warn your authorized personnel about a possible threat once the triggering action occurs and is processed by the product.

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. To learn more about alert configuration, go to Creating Alerts.

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

Creating Alerts

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.

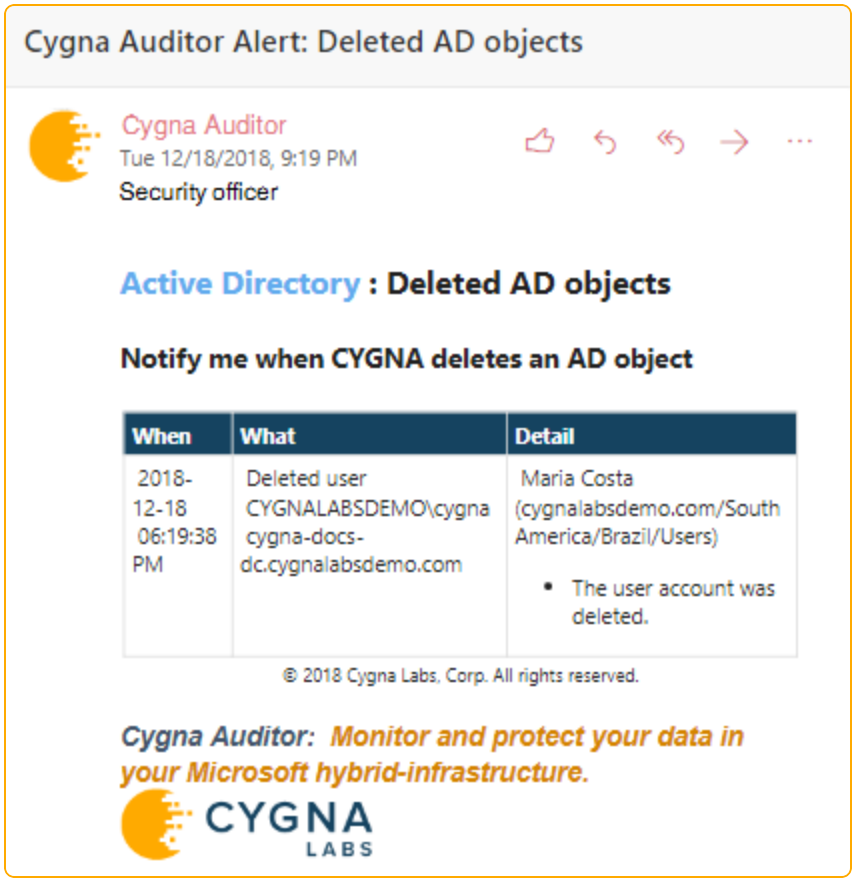
To create a new alert:

Note: The procedure below applies to the Active Directory module. Alert creation may vary slightly for other modules.

1. On the home page, pick an audited system.
2. Select **Alerts**.
3. Select **Create** to create a search-based alert.
4. Customize your search—create a search query tailored to look for the information you are specifically interested in. Make sure to use full names as filters are designed to search for exact entries (e.g., cygnalabsdemo.com\ian.rush instead of ian.rush). To retrieve all activity, keep the search filters blank.
   - On the **Filter** tab, specify parameters to narrow down your search results (for example, specify a user name in the **Who** filter to narrow down your search to activity of a specific user).
   - On the **Exclusions** tab, specify entities you do not care about at the moment and do not want to show up in this search query (for example, a trustworthy administrators group).
   - On the **Actions** tab, specify alert recipients.
5. Click **Save**.
6. In the **Save Alert** dialog, specify a new alert name and provide description. Set the **Enabled** status to *"Yes"* to turn on the alert. Also, you can assign tags to your alerts. e.g., *security*, *critical*, *moderate risk*.

After saving, a new alert will appear in the list. Later, you can update, disable, or delete your alerts.

The example below demonstrates the alert email that notifies about a user being deleted in your Active Directory domain.



For more information on interpreting the data, refer to Reading Search Results.

Summary

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

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

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

Index

R

S

W