

Cygn Auditor

Proof of Concept Guide

Published 6/28/2022

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

Proof of Concept	4
System Requirements and Prerequisites	5
Account and Permissions Checklist	7
Simple Installation	9
Initial Configuration Wizard	10
Architecture and Data Flow	11
Cygna Auditor Web Console	13
Security and Control of Your Data Flow	14
Delegation & Personas	16
Sources	18
Active Directory	19
Amazon Web Services	21
Windows File System	23
On-Premises Exchange	25
Microsoft Subscription	27
VMware	29
Dashboard—Get Bird's Eye View	30
Auditing & Reports—Keep Tabs on Activity and Changes	31
Active Directory Rollback and Recovery	33
Recovery	33
Rollback	33
Azure AD Recovery	35
Recovering Changes	35
SIEM Integration with Remote Logging	37
Seeing Cygna Auditor in Action	38
Summary	39

Proof of Concept

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.

This guide is designed to facilitate your PoC process and help you make an informed decision. The Proof of Concept guide outlines the main Cygna Auditor features and describes basic scenarios. For your convenience, each chapter comes with the checklist and comments section where you can write down specific requirements and compare Cygna Auditor with other competitors, or just add notes. As you start the PoC, you can identify your goals here:

1. _____
2. _____
3. _____
4. _____
5. _____

For information regarding product licensing, support, and distribution, please contact Cygna Labs sales engineers.

For detailed system requirements, setup and usage instructions as well as tutorials and best practices, visit [Cygna Auditor online documentation](#).

System Requirements and Prerequisites

Cygna Auditor system requirements and installation prerequisites are relatively easy to meet and do not require any major modifications to your corporate infrastructure. The recommended configuration includes:

1. For medium and enterprise environments—Distributed deployment on two servers



Cygna Auditor application server **Software configuration:** A clear Windows Server 2019 with preinstalled IIS (including Windows Authentication, ASP.NET), Group Policy Management, and .Net Framework 4.8.

Hardware configuration: Any modern processor, 4 GB RAM (min) or 8 GB RAM (recommended), HDD 100 MB.

Firewall configuration: 80 or 443 TCP port for inbound connections; 135, 443, and 1433 TCP ports for outbound connections.



Database server **Software configuration:** The server with SQL Server 2019 Standard Edition for data storage.

Hardware configuration: Minimum 2 GB free storage space, 8 GB RAM (min) or 16 GB RAM (recommended).

Firewall configuration: 1433 TCP port for inbound connections.

2. For PoC and small businesses—Simple deployment on a single server



Cygna Auditor application server and Database server **Software configuration:** A clear Windows Server 2019 with preinstalled IIS (including Windows Authentication, ASP.NET), .Net Framework 4.8, Group Policy, and SQL Server 2019.

Hardware configuration: Any modern processor, 12 GB RAM (min), HDD 4 GB (min) free storage space.

Firewall configuration: 80 or 443 TCP port, and 1433 TCP port for inbound connections; 135, 443 ports for outbound connections.

Besides recommended configuration, Cygna Auditor supports more operating systems and software components and allows you to set up a product environment in a way that works best for you.

- In addition to Windows Server 2019, Cygna Auditor supports installation on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2022.
- The audit database runs on SQL Server 2016 - 2022. Standard Edition or higher.
- Cygna Auditor web console can be hosted on IIS web server 8.5 or above (including Windows Authentication, ASP.NET 4.8) provided that the web server is deployed on the same machine as Cygna Auditor platform.
- Cygna Auditor requires access to docs.cygnalabs.com (online help), msdl.microsoft.com, *.core.windows.net, and the following URLs—allow HTTPS connections on your Cygna Auditor app server or leverage your in-house proxy server.

cygnacloud.azurewebsites.net (GET and POST)

m365.cygnalabs.com (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)

*.amazonaws.com (GET and POST)

Benefits:

1. Wide range of supported operating systems and database engines.

2. Minimal impact on your corporate environment.

3. The deployment scales to your business size.

4. Deployment on premises, on virtual machine, and in the Cloud.

Comparison checklist

	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Account and Permissions Checklist

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

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

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
	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.	The db_owner and public roles for the audit database.

Comparison checklist

	CygnA Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Simple Installation

Cyigna Auditor installs in minutes, without requiring professional services. Since Cyigna Auditor is part of the unified Cyigna Auditor platform, enabling additional Auditor functionality is as simple as turning on product modules—no additional installation required.

Run the Cyigna Auditor installation package as administrator and it will:

- Create and start all the necessary services and components
- Deploy a web UI on your web server



Benefits:

1. Install Cyigna Auditor once and access it from any computer within your corporate domain.

2. Up and running in minutes.
3. No need to reinstall the product when you add a new source to your license profile.

4. Easy license management.

Comparison checklist

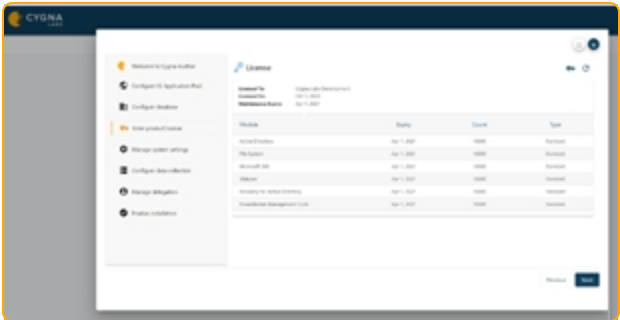
	Cyigna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Initial Configuration Wizard

Set up everything in minutes. On your first start, follow along the wizard to configure all the essential Cyigna Auditor settings such as:

- IIS application pool and database
- License
- Access to the product (delegation)
- Data collection
- System settings



Benefits:

1. Guided setup procedure. No need to explore on your own or hire a configuration manager.

2. Up and running in minutes.
3. Prepare everything you need to start auditing in the right order.

4. Easy license management and data collection configuration.

Comparison checklist

Cyigna Auditor

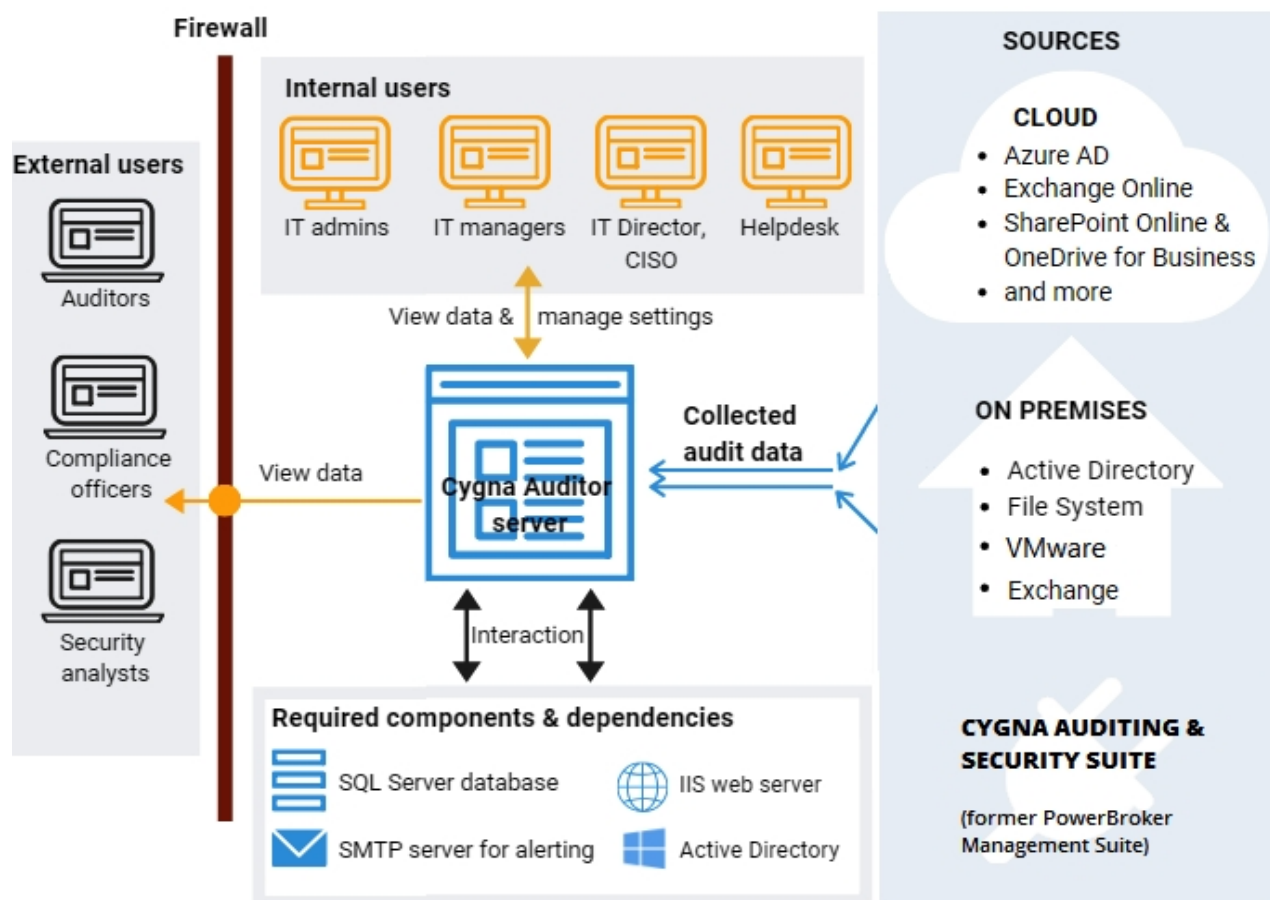
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Architecture and Data Flow

Cygna Auditor platform is designed to adopt to changes in your environment and to facilitate data collection and analysis. The server-side can be deployed on-premises, on a virtual machine, or in the Cloud. The management interface is web-based. Cygna Auditor allows multiple users to use it simultaneously in their browsers. The audit data collected by the product is written straight to the fine-tuned and optimized SQL Server-based data storage. Whether you are monitoring a few servers—or a few thousand—Cygna Auditor is highly scalable and extremely responsive to changes in your environment.

Employees within your corporate domain (IT managers and administrators, helpdesk personnel, etc.) as well as authorized users from outside the company (compliance officers, certified auditors, etc.) can leverage Cygna Auditor's web interface through secured HTTPS connection. Depending on assigned roles, users can review data from a specific data source, manage data collection settings, and much more.



Cygna Auditor relies on several components such as SQL Server for storing collected data, SMTP mail server for sending alert notifications, IIS web server for hosting the web console, and Active Directory for providing authentication and authorization services.

Cygna Auditor enables you to collect data from various systems and applications, both on premises and in the Cloud, including but not limited to Active Directory, Windows file servers, Azure AD, hybrid Exchange. On top of that, Cygna Auditor integrates seamlessly with former PowerBroker Management Suite (now Cygna Auditing & Security Suite).

Cygna Auditor collects and securely transfers audit data with no impact on your system's operability. Cygna Auditor employs non-intrusive agents to collect data and can as well be set without them. The product architecture is specifically designed to minimize complexity while keeping the attack surface to a minimum.

Benefits:

1. Scalable architecture adapts to your company growth.

2. Web interface enables easy and secure access from multiple workstations and does not require additional installations.
3. Zero impact on your corporate environment.

4. Deployment on premises, on virtual machine, and in the Cloud.

Comparison checklist	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

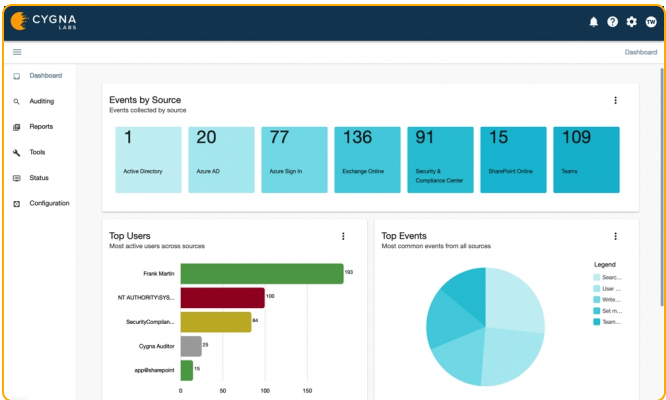
Comments

Cygna Auditor Web Console

Intuitive and easy-to-use web interface streamlines access to Cygna Auditor platform. There is nothing easier than opening a browser and starting using the product, from any location and any device.

Once you log in, you will see all your options right in front of you. Depending on assigned role, a user can have access to:

- Collected events in [Auditing search, reports, and alerts](#) and on a [Dashboard](#)
- Data collection configuration
- Product settings, including license, [proxy](#) settings, and [role delegation](#)



Benefits:

1. Unlike other auditing solutions, Cygna Auditor enables access to its functionality through a web browser.
2. Use the product anywhere and from any device, including iPad and Android tablets.
3. No need to install and take care of multiple instances of management console.
4. Clear interface with easy access to all the necessary features.

Comparison checklist

	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Security and Control of Your Data Flow

Security of data and operations is the top priority for Cygna Labs. Since Cygna Auditor platform leverages web interface, you are encouraged to switch to using a secured protocol (HTTPS) with encrypted certificate you utilize for your company's resources.

Organizations operating in highly regulated environments are seeking for full transparency in product operations and data flow as well as for ability to enforce strict security rules while preserving the product operability. Cygna Auditor is designed to be flexible and allows you to customize most demanded security options right in its web-console.

In addition to the flexible role delegation system that prevents unauthorized access to data and configuration—see [Delegation & Personas](#)—Cygna Auditor allows you to establish overall control over data traffic and service accounts used by product. These settings can be applied on the **Configuration / System** page.

Add a custom proxy server to reroute traffic through a secured gateway. Allow connection to:

System Configuration

Email Proxy Service

Proxy Server

☒ Use a proxy server for Internet access during data collection

Server
proxysrv.cygnalabsdemo.com

Port
8084

☒ Connect to the proxy server as a specific user

Account Name
cygnalabsdemo.com\proxy.user

Password
.....

Verify

cygnacloud.azurewebsites.net (GET and POST)

m365.cygnalabs.com (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)

*.amazonaws.com (GET and POST)

To see online help, you will also need access to: docs.cygnalabs.com.

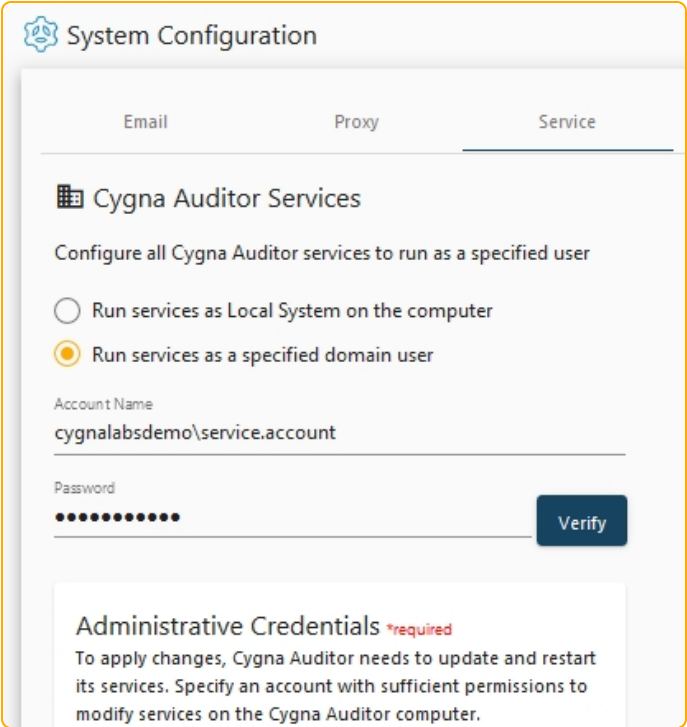
For agent-based Active Directory auditing, allow access to:

msdl.microsoft.com/download/symbols

msdl.microsoft.com

*.core.windows.net (GET)

If you utilize a specific account to run Windows services in your corporate environment, you can update Cygna Auditor settings and specify a designated account instead of Local System that is used by default. This user will operate services responsible for data collection and platform operations.



Benefits:

1. Allows switching to encrypted HTTP.
2. Reroute Microsoft 365 data collection traffic through your in-house proxy server.
3. Ability to assign Cygna Auditor to use a specific account for its Windows services.
4. Flexible delegation model that is integrated in the product.

Comparison checklist

	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Delegation & Personas

With built-in delegation functionality, Cygna Auditor takes care of configuration and data security. To ensure that only authorized personnel can review data and update auditing configuration, Cygna Auditor enables you to delegate permissions within the product.

The delegation model is flexible. Creating custom roles is simple and intuitive. Grant access to certain features, data sources, or settings.

Manage Role Permissions

Name *

Helpdesk

Description

This role is for helpdesk administrators who help resolve AD and Azure AD issues.

☐

Grant Global Administrator access

☐ Check all

Filter...

Data Sources (View)

☒ Active Directory Data

☒ Azure AD Data

☒ Azure AD Sign-ins Data

☐ Cygna Auditor Self Audit Data

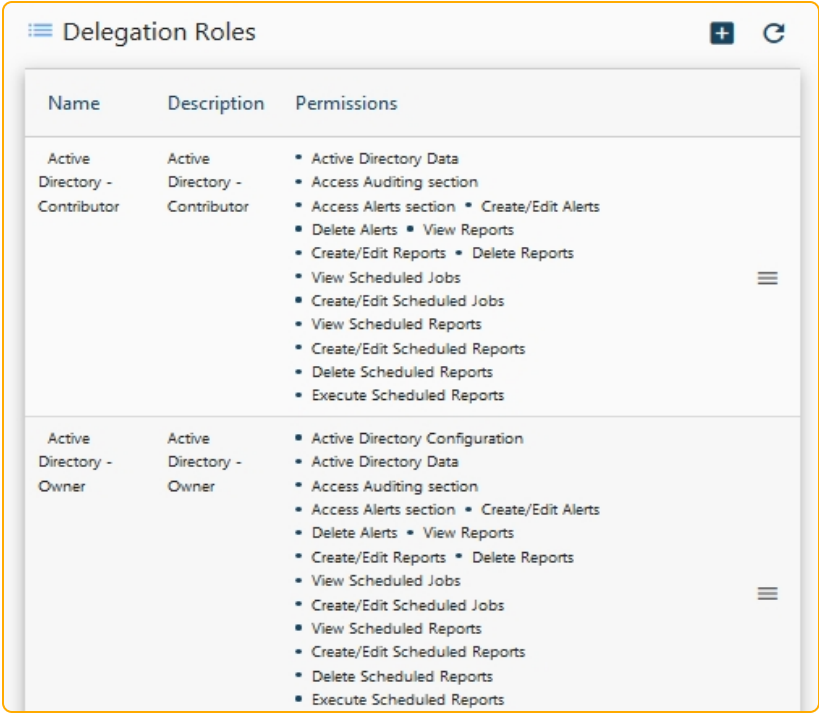
☐ Exchange Online Data

☐ File System Data

☐ SharePoint Online Data

Cancel

Save



Depending on workflows in your organization, you can leverage built-in roles or create custom roles and grant permissions to data and settings. Both users and groups can be assigned roles and permissions.

Benefits:

1. Besides simple login authorization, Cyigna Auditor ensures that users see only the features and data they are authorized to see.
2. Flexible delegation model. Assign atomic permissions or grant access to audit source.
3. Delegation is fully integrated with Active Directory. Manage delegation through Active Directory groups or on user level.
4. Tailor delegation model to your specific needs.

Comparison checklist

Cyigna Auditor

Comments

Sources

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

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

Active Directory

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

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

Adding a domain for auditing is easy. Provide user credentials—Cygna Auditor will automatically find domains. Fine-tune data collection settings as necessary.

Manage Domain Auditing

1 Domain Selection

2 Collection Settings

3 Domain Controllers

4 Save Changes

Please choose the preferred collection method.

Select collection method (Unable to change the collection method while Cygna Agents ...)

Cygna Auditor Agent

☒ Combine similar events occurring within the specified interval 5000 ms

☒ Attempt to locate workstation information for events

☒ Perform reverse name lookup when events only include an IP address for the remote workstation

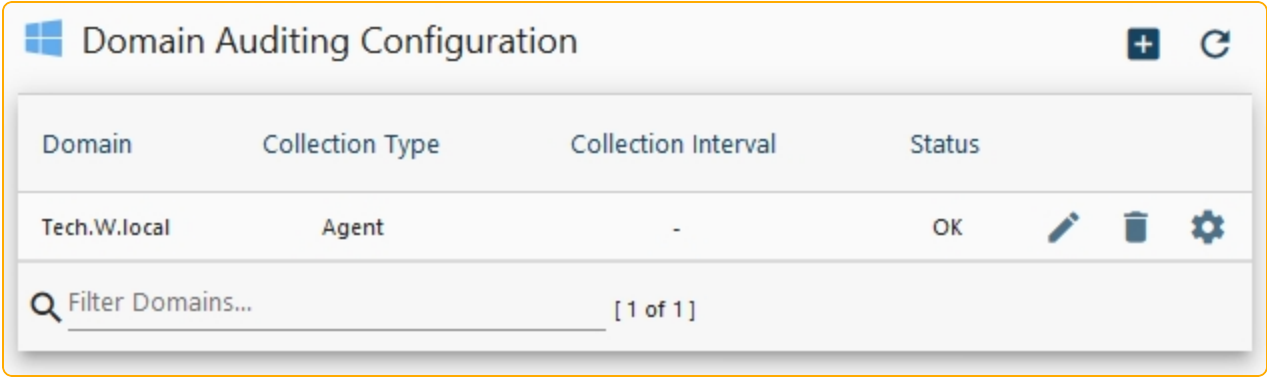
☒ Ignore login events

☐ Enable nested group alerting and auditing

Advanced collector settings

Supported domain controller versions:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022



Available auditing features:

-  Event Auditing
-  Reporting
-  Dashboard widgets
-  Alerting

On top of that, Cyigna Auditor has one-of-a-kind [recovery and rollback](#) features designed specifically for Active Directory.

Benefits:

1. Cyigna Auditor for Active Directory detects all changes to the directory.

2. Cyigna Auditor enables you to rollback unwanted changes and recover AD objects.
3. Scalable. No matter how many domain controllers you have, two or two hundred.

4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

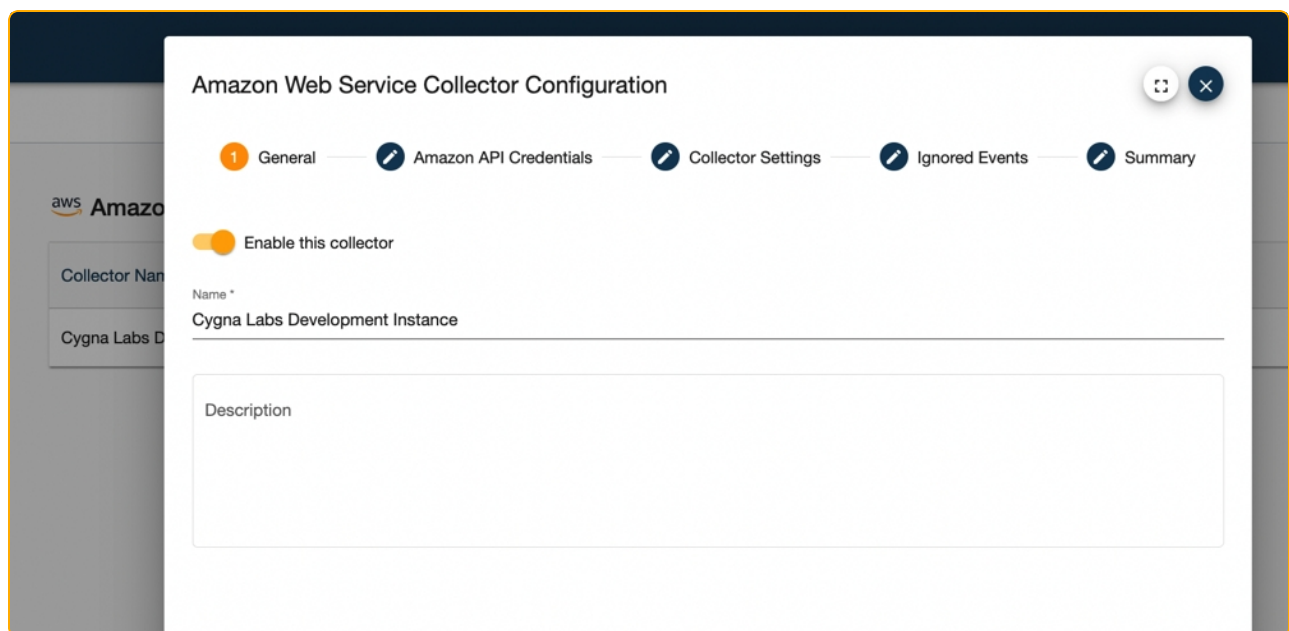
<i>Comparison checklist</i>	Cyigna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Comments</i>			

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.

Authorize Cygna Auditor application to connect to your Amazon IAM – Cygna Auditor will start collecting audit data automatically for the AWS regions that IAM account has access to.



Cygna Auditor for AWS reports changes to:

- EC2
- IAM
- Logging
- Route 53
- ELB
- VPC
- and many more

Available auditing features:

 Event Auditing

 Reporting

 Dashboard widgets

 Alerting

Benefits:

1. Cygn Auditor tracks changes to identity and access management configuration.

2. Cygn Auditor provides comprehensive analysis of AWS configuration and helps identify issues faster.
3. With a single authorization, Cygn Auditor starts collecting data for multiple AWS regions.

4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

Comparison checklist

	Cygn Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

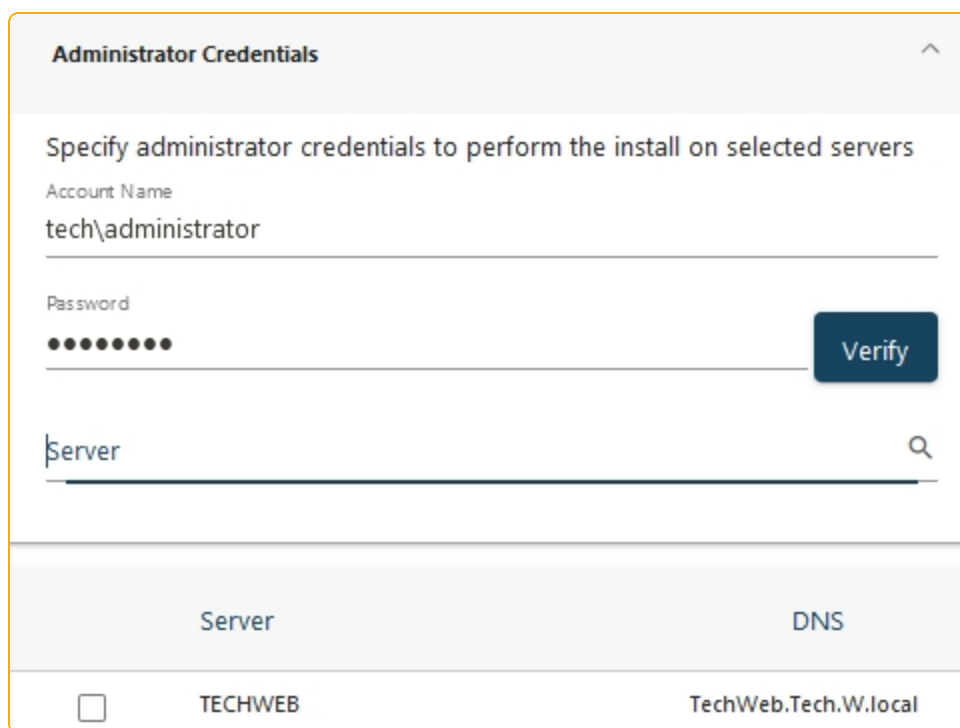
Comments

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.

Install an optimized and lightweight service on your file server—and Cygna Auditor will automatically start collecting data. You can always check the data collection status in webconsole.







The image shows a web form titled "Administrator Credentials" with a collapse icon. The form contains the following elements:

- A heading: "Specify administrator credentials to perform the install on selected servers"
- An "Account Name" field with the text "tech\administrator".
- A "Password" field with masked characters (dots) and a "Verify" button to its right.
- A "Server" field with a search icon to its right.
- A table with two columns: "Server" and "DNS".
- A row in the table with a checkbox, the text "TECHWEB", and the text "TechWeb.Tech.W.local".

Supported OS:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows 8.1

- Windows 10
- Windows 11

<input type="checkbox"/> Server	Alert Count	Last Active	Driver Version	Status	
<input type="checkbox"/> TECHDB	0	4/22/21, 4:09 PM	1.4.1.3	Driver running	 
<input type="checkbox"/> TECHDC1	0	4/22/21, 11:10 AM	1.4.1.3	Driver running	 
<input type="text" value="Filter Servers..."/> [2 of 2]					

Available auditing features:

-  Event Auditing
-  Reporting
-  Dashboard widgets
-  Alerting

Benefits:

1. Cygna Auditor for File System tracks file and folder creation, change, and deletion, who made the change, and when the change was made.
2. Insight into both successful and failed actions as well as permission changes.
3. Scalable. No matter how many servers you monitor, two or two hundred, or how big they are.
4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

Comparison checklist

	Cygn Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

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.

Adding an Exchange organization for auditing is a straightforward process. After providing the Exchange Server name and adding user credentials that will be used to run data collections, you can specify the auditing schedule. Set a workflow that fits your monitoring goals best: collect data every couple of minutes, hours, daily, weekly, quarterly, or annually.

Configure On-Premises Exchange collector

1 General 2 Exchange server 3 Collection Schedule 4 Summary

☒ Enable this collector

Name *
Exchange

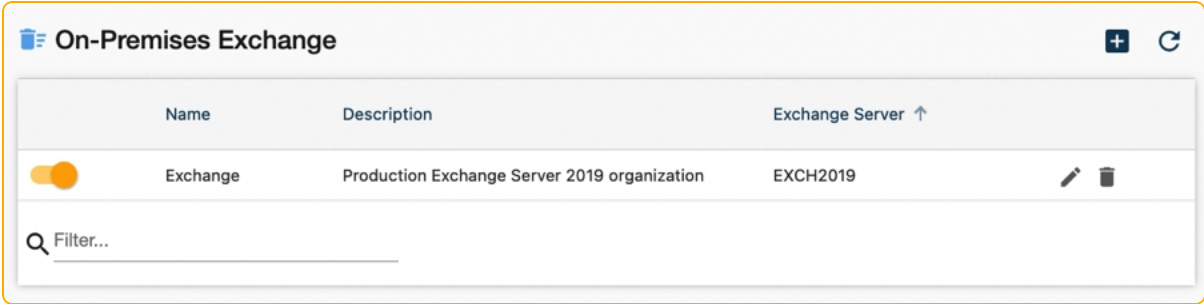
Description
Production Exchange Server 2019 organization

Cancel Next

To reduce the amount of collected events and help you focus on the most critical cases, Cygna Auditor provides you with ability to pre-filter events and skip certain events such as an owner opening an email. Flexible filters streamline monitoring and make it more efficient.

Supported on-premises Exchange Server versions:

- Exchange Server 2016
- Exchange Server 2019



Available auditing features:

- Event Auditing
- Reporting
- Dashboard widgets
- Alerting

Benefits:

- 1. Cygna Auditor for Exchange detects all changes to on-premises Exchange organization, including non-owner changes.
- 2. Cygna Auditor supports hybrid Exchange deployment and allows auditing on-premises Exchange and Exchange Online.
- 3. Supports businesses by auditing up to 2500 mailboxes per Exchange organization, no limits on administrative or configuration event auditing.
- 4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

Comparison checklist

Cyigna Auditor

Comments

Microsoft Subscription

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.

Authorize Cygna Auditor application in Office 365—and that's it, Cygna Auditor will start collecting audit data automatically for all Office 365 tenants you have access to.

CYGNA LABS

Dashboard / Configuration / Microsoft Subscriptions

Microsoft Subscription Configuration

Cygna Labs Corp. will require authorization to collect event data from your Microsoft subscription.
Note: A window will appear from Microsoft requiring administrative credentials for your organization, followed by a prompt to approve the addition of Cygna Auditor to your Tenant.

Name	Microsoft 365 Enabled?	Azure Enabled?	Polling Interval
Cygna Labs LLC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10

Verifying internet connectivity

*Microsoft subscription data collection requires access to the Internet. Use this option to verify connectivity to the required Microsoft URLs from the Cygna Auditor server.

Verify Connectivity

Microsoft Cloud-based apps:

- Azure AD, including Logins
- Exchange Online
- SharePoint Online and OneDrive for Business
- Microsoft Teams

Available auditing features:



On top of that, Cygna Auditor enables you to rollback object and revert changes to attributes with Azure AD Recovery.

Benefits:

1. Cyigna Auditor tracks Azure AD user activity and sign-ins, allowing you to identify compromised accounts and potential threats.

2. Cyigna Auditor provides comprehensive user email auditing as well as helps prevent data loss by tracking SharePoint Online document deletions.
3. With a single authorization, Cyigna Auditor starts collecting data for multiple Office 365 tenants.

4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

Comparison checklist

	Cyigna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

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.

Available auditing features:

 Event Auditing

 Reporting

 Dashboard widgets

 Alerting

Benefits:

1. CygnA Auditor for VMware tracks changes to virtual machines and helps prevent critical data loss.

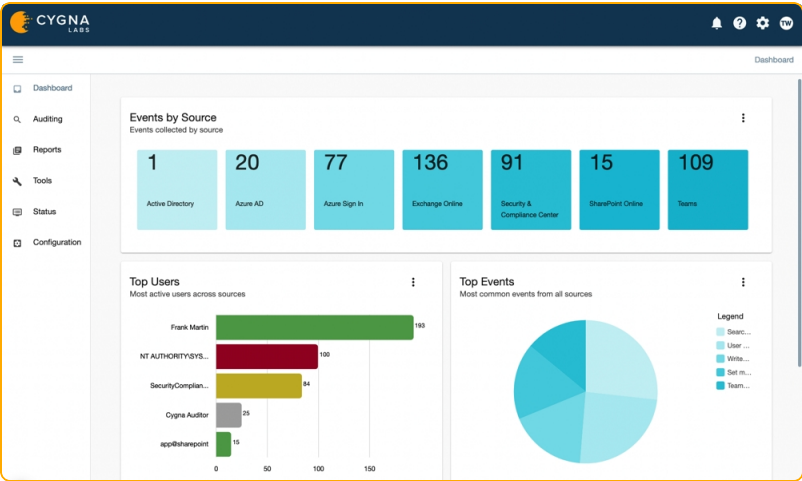
2. Insight into VMware activity.
3. Scalable. No matter how many VMware servers you monitor, two or two hundred, or how big they are.

4. Easy access to audit data. Search, reports, widgets, and alerts are right in front of you.

Comparison checklist	CygnA Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments			

Dashboard—Get Bird's Eye View

The activity 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.



Benefits:

1. Widgets are designed to ensure you get the most demanded activity metrics for your critical assets.

2. Most important activity charts.
3. Activity widgets for Active Directory, File System, Azure AD, Exchange Online, and SharePoint Online.

4. Quick and clear overview of activity in your audit sources.

Comparison checklist

Cygna Auditor

☐

☐

☐

☐

☐

☐

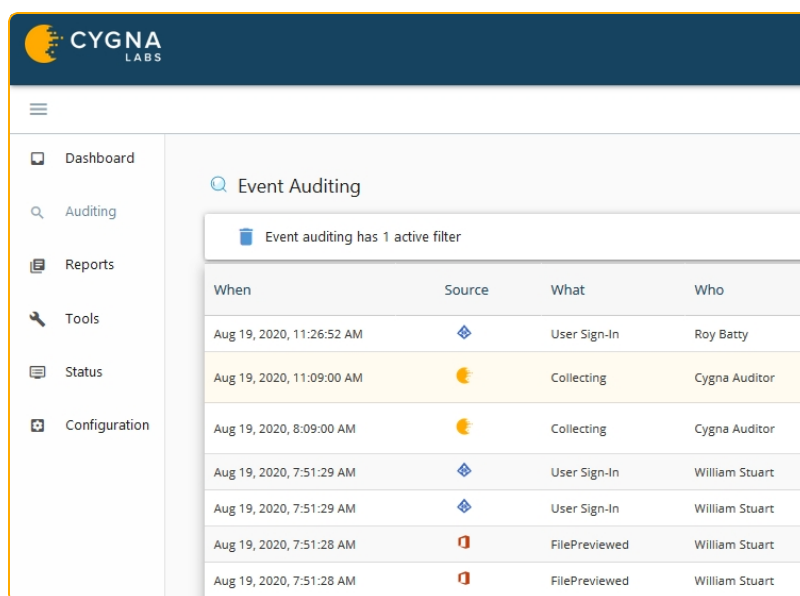
Comments








Auditing & Reports—Keep Tabs on Activity and Changes

Investigating security incidents and unraveling event chains that led to them in the first place is crucial if you want to keep your data under control and minimize the potential threats in the future. With Cygna Auditor's event auditing, you can keep tabs on activity and changes from all sources, run searches, generate reports, and configure alerts.

Auditing Search

Get a grip on what's going on in your environment—review all activity in one place and then narrow down your search to what bothers you the most. With Cygna Auditor's flexible filters and intuitive search investigating who did what has never been easier.



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

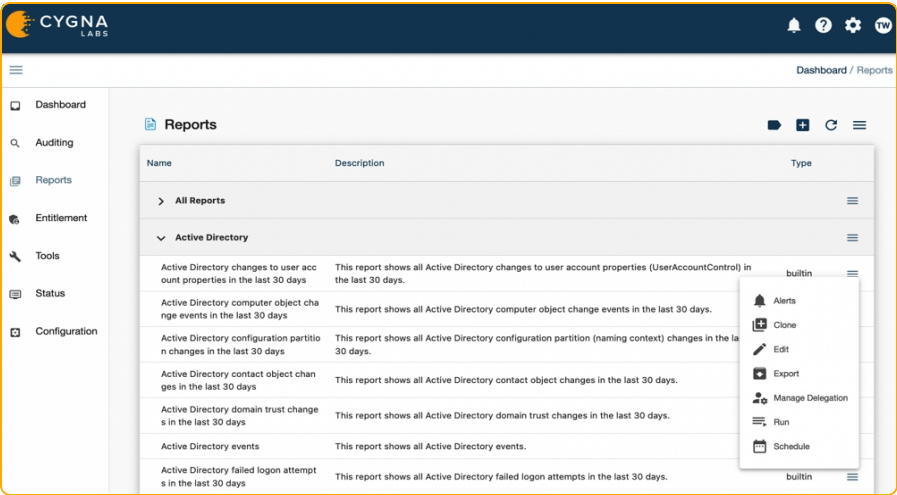
Reports

Meeting industry compliance requirements such as GDPR, FISMA, HIPAA, and NIST is bothersome in regulated industries such as education and healthcare. Cygna Auditor helps you pass compliance audits by providing reports designed to satisfy these requirements.

Cygna Auditor is shipped with built-in reports that were specifically designed to help you prove compliance and answer most everyday security administration questions such as "were there any changes to security groups?" or "what users got their passwords reset?"

In addition to that, Cygna Auditor enables you to save auditing searches as custom reports. These reports are shared with other Cygna Auditor users in your organization so everyone

can run these reports from their computers or receive them as subscription. You can subscribe to any report and receive alerts to your email once a similar activity is captured.



Benefits:

1. Flexible, almost human language-like filters enable you to search for any action across all sources.
2. The search results are updated on the fly when you specify a filter.
3. Saving your favorite searches as custom reports to reuse them later and alerting on changes.
4. Search results that are easy to review. Clear presentation of who did what, where, and what are the details.

Comparison checklist

Cygna Auditor

☐

☐

☐

☐

☐

☐

Comments

Active Directory Rollback and Recovery

Enterprise-scale Active Directory is a living and breathing system with hundreds of changes per hour that should be closely monitored. With Rollback and Recovery features, Cygna Auditor enables you to address Active Directory issues and revert unwanted changes in no time. Whenever the change was done by mistake or with malicious intent in mind, you can fix it right in Cygna Auditor web console.

Intelligent Recovery and Rollback features speed up the response time and help your system withstand security threats.

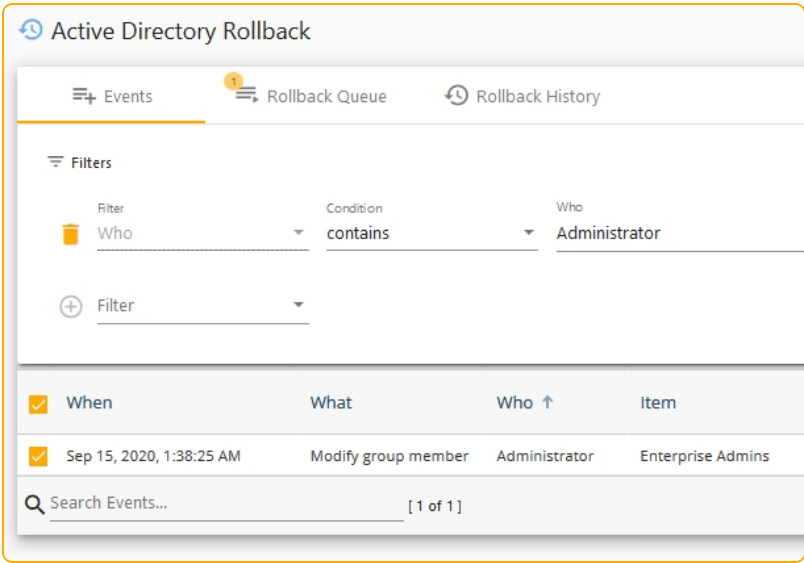
Recovery

Restore Active Directory objects such as deleted users or Active Directory groups. Cygna Auditor stores snapshots of your Active Directory domain and enables you to recover objects from the AD Recycle Bin and restore their properties to the state they were at a specific moment in time.

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:7cf9675f-5c9a-4d77-9856-6860d90438e2,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:dc50951-c1ce-41e4-d-94ec-becd45fcb3c,CN=Deleted Objects,DC=TechENV,DC=com	167 days
.._msdcs	dnsNode	Sep 15, 2020, 12:21:29 AM	DC=..Deleted-TechENV.com\0ADEL:dc50951-c1ce-41e4-d-94ec-becd45fcb3c,CN=Deleted Objects,DC=TechENV,DC=com	167 days

Rollback

Roll back unwanted changes such as changes to group membership or user properties. Cygna Auditor is the only auditing and security solution that allows reverting changes up to specific attributes.



Cygn Auditor stores snapshots of your Active Directory domain meaning that you can roll back objects to the state they were just before the change as well as explore the whole change history.

Benefits:

1. Address security issues in seconds.
2. No additional software – recover objects and roll back changes right in Cygn Auditor web console.
3. Precise. Restore objects up to specific attributes.
4. Active Directory snapshots keep history. Compare how the objects changed over time and specify the best state to revert to.

Comparison checklist

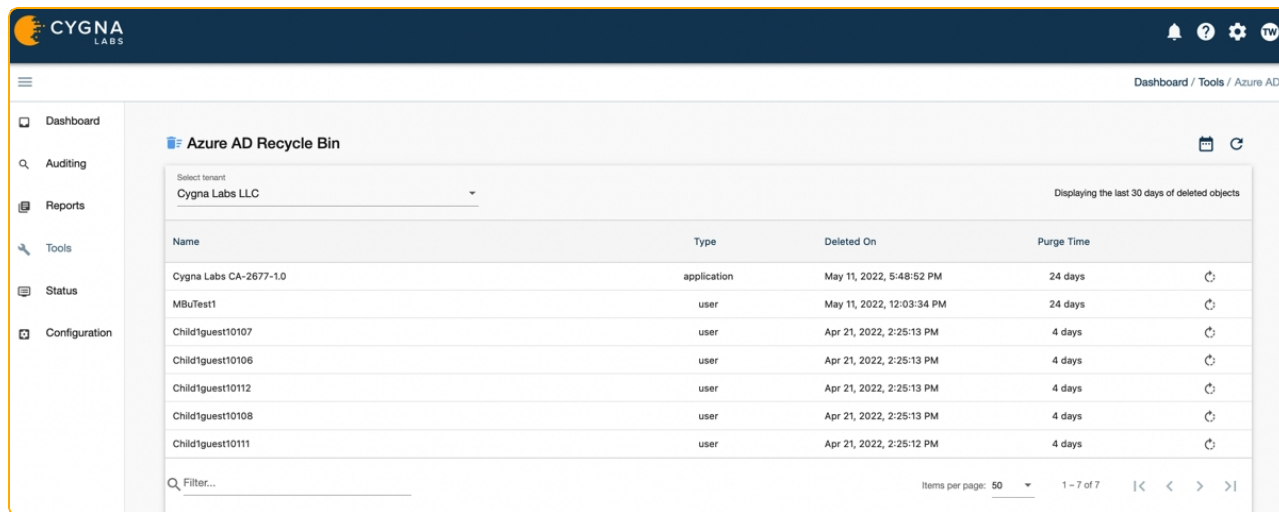
Cygn Auditor

Comments

Azure AD Recovery

Cygna Auditor enables you to recover unwanted changes to users and groups in your Azure AD. With the recovery functionality, you can revert entire objects to their previous state or roll back specific attributes.

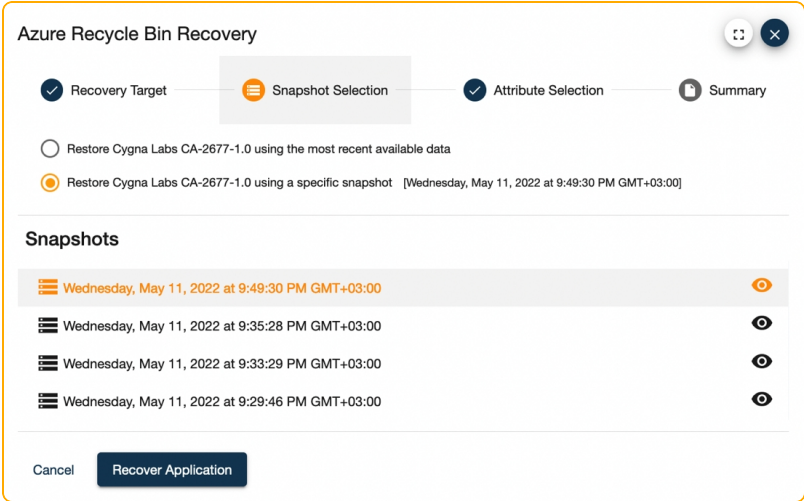
Recovery for Azure AD is the next step after setting an ongoing auditing and monitoring of your tenant. With the recovery, you can address Azure AD issues and revert unauthorized changes in no time.



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

Recovering Changes

1. Before you can start rolling back changes, ensure that the Cygna Auditor application is registered in your Azure AD tenant account and is allowed collect snapshot data.
2. Provide your client key and secret to enable Cygna Recovery to collect and recover data in your Azure AD.
3. Scan through the list of Azure AD changes either in the Auditing search or in a dedicated dashboard. You can find it under **Tools / Azure AD Recovery**.
4. Pick a record to recover and review what exactly has changed there.



Cyigna Auditor stores snapshots of your Azure AD and enables you to roll back objects to the state they were just before the change as well as explore the whole change history.

Benefits:

1. Address security issues in seconds.

2. No additional software – recover objects and roll back changes right in Cygna Auditor web console.
3. Precise. Restore objects up to specific attributes.

4. Azure AD snapshots keep history. Compare how the objects changed over time and specify the best state to revert to.

<i>Comparison checklist</i>	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Comments</i>			

SIEM Integration with 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. Take the most out of both solutions.

Cygna Auditor seamlessly integrates into your SIEM data flow. All you have to do to configure integration is to provide a path to your SIEM solution and enable alerts with remote logging.

System Configuration

Email

Proxy

Service

Remote Logging

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

Save

Reset

Benefits:

1. Supplement your SIEM solution with Cygna Auditor data.

2. Easy-to-configure integration.
3. Data is feed to your SIEM solution in its native format.

4. Get notifications immediately.

Comparison checklist

	Cygna Auditor		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comments

Seeing Cygna Auditor in Action

To appreciate what Cygna Auditor can do to your organization, you should see it in action. Here is the list of recommended test actions you can perform on your systems and then see them reported in the product. Make sure to configure auditing settings and enable data collection in advance.

SOURCE	TEST ACTION
Active Directory	On a domain controller, add a new user through Active Directory Users and Computers and then disable this user.
Windows File System	Create a new folder on the audited file server and then rename or move it.
Azure AD	Log in with your Office 365 account to Azure AD admin center, add a new user, and then disable it.
Exchange Online / On-premises Exchange	Log in Exchange admin center, create a new mailbox and update its properties.
SharePoint Online and OneDrive for Business	Log in to your Office 365 account, open a SharePoint site, and add a new file.

After waiting for the product to collect data, see how these changes are reported in Global Reporting all together and in Search and Reports sections for each source individually.

<i>Comparison checklist</i>	Cygna Auditor
<hr/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<hr/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<hr/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<hr/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<hr/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<i>Comments</i>	
<hr/>	
<hr/>	

Summary

Thank you for reviewing Cygna Auditor, your feedback is important to us as here, in Cygna Labs, we are constantly working on improving the product.

Here you can add your major PoC takeouts or comments:

1. _____
2. _____
3. _____
4. _____
5. _____

Here is a list of resources that are meant to assist you during the onboarding:

1. [Complete user guide](#) that you can download and use offline
2. [Online documentation](#) where you can find setup and usage instructions, and more
3. [Cygna Auditor system requirements](#) with deployment options and recommendations
4. Detailed instructions on how to [install the product](#)
5. The most up-to-date list of [supported audit sources](#)
6. The checklist of [auditing configuration settings](#)