CYGNA LABS

Cygna Entitlement and Security

User Guide



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

Published 10/14/2026

Copyright © 2026

Version 3.10

Copyright

©2026 Cygna Labs Corp. ALL RIGHTS RESERVED.

Trademarks

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

Disclaimers

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

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

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

Contents

- Welcome, and Let's Get Started ... 6
- Planning Deployment ... 7
  - System Requirements ... 7
    - Distributed Deployment–Medium and Enterprise Environments ... 8
      - Cygna Application Server ... 8
      - Cygna Entitlement and Security Server ... 8
      - Database Server ... 9
    - Single Server Deployment–Small Businesses and PoC ... 10
    - Recommended Database Maintenance ... 11
  - Ports and Network Resources Reference ... 11
    - Cygna Platform ... 13
    - Entitlement and Security Server ... 13
    - Database server ... 14
    - Active Directory DCs ... 14
  - Account and Permissions Checklist ... 14
  - Entitlement Sources ... 16
- Installing the Product ... 17
- Starting the Product ... 18
- Granting Access to Cygna Platform ... 19
  - Cygna Roles ... 19
  - Assigning Roles to Users ... 19
- Configuration ... 20
  - Setting up Entitlement Service ... 20
  - Enabling Active Directory Data Collection ... 21
  - Enabling Entra ID Data Collection ... 22
- Security Audit Reports ... 24
  - Viewing Reports ... 24
  - Creating Custom Reports ... 25

Configuring Report Details ... 26
Adding Filters ... 26
Filtering Results ... 26
Specifying a Filter Target ... 26
Building a Filter ... 26
Defining Filter Logic ... 27
Understanding Fields ... 29
Entitlement Explorer ... 33
Understanding How Entitlement Explorer Works ... 33
Specifying the Server ... 34
Changing Collection Timeline ... 34
Browsing Domain ... 35
Searching Data ... 36
Exploring Entitlement Data ... 37
Switching Views ... 37
Filtering Results ... 37
Fine-Tuning ... 39
Entitlements – Access ... 40
Security – Permissions ... 41
Trustees – Expanded Permissions ... 42
Group Members ... 43
Group Membership ... 44
Entra ID Views ... 45
Ownership and Relationships ... 46
Ownership ... 47
Management ... 47
Sponsorship ... 47
Devices ... 47
Roles and Privilege ... 47
Views ... 47

Access Packages and Governance 48
Views 48
Applications 49
Views 49
Policies 50
Views 50
Authentication Methods 50
Views 51
Consent and Admin Review 51
Views 51
Agent Identities 52
Views 52
Tenant Configuration 52
Views 52
Identity and Licensing 53
Views 53
Policy Settings 54
Viewing GPO Settings and Links 54
Viewing Resultant Policy for an Object 55
Auditing Policy Application Over Time 55
Index 57

Welcome, and Let's Get Started

Cygna Entitlement and Security provides the ability to gather and report on entitlements and group membership across Active Directory, Entra ID, and Group Policy Objects (GPOs), and search and report on the latest or historical point-in-time collections. Secure your infrastructure and gain control over the assignments by getting direct answers to your auditing questions:

Where does a user or group have rights in the environment?

- Verify appropriate permissions for role
- Ensure permissions have been revoked when moving roles or leaving

Where is a particular permission set configured in the environment?

- Show which resources have full control permissions set

What permissions are set on this object?

- See the effective permissions on objects

Cygna Entitlement and Security helps you enforce the least privilege model and keep your environment accountable and secure. With regular entitlement and permissions review, you can eliminate the risk of granting unrestricted access to accounts in your environment and permission misuse.

Cygna Entitlement and Security can be installed alongside Cygna Auditor or as a stand-alone product.

Planning Deployment

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

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

1. A clean Windows Server 2022 with preinstalled IIS, the .NET Desktop Runtime 10.0, and the ASP.NET Core Runtime 10.0 Hosting Bundle for Cygna platform.
2. A high load Windows Server 2022 for Entitlement and Security server (64 GB RAM, 8 cores).
3. The other server with SQL Server 2019 Standard Edition.

Check all servers are in your corporate Active Directory domain.

Continue reading:

System Requirements 7
Distributed Deployment–Medium and Enterprise Environments 8
Single Server Deployment–Small Businesses and PoC 10
Recommended Database Maintenance 11
Ports and Network Resources Reference 11
Cygna Platform 13
Entitlement and Security Server 13
Database server 14
Active Directory DCs 14
Account and Permissions Checklist 14
Entitlement Sources 16

System Requirements

Read this section to learn more about the Cygna platform, Cygna Entitlement server and database server system requirements. Depending on your company size and the Active Directory structure, the requirements can vary significantly. Use the metrics below as a general guideline and consider scaling your Cygna Entitlement and Security 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 three servers.

Cygna Application Server

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

COMPONENT	REQUIREMENTS
Hardware	• **CPU**: Any modern processor with 4 cores • **RAM**: 8 GB (minimum), 16 GB (recommended) • **HDD**: 20 GB
Operating system	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Server roles and features	• **Web Server (IIS)**: Microsoft IIS 8.5 or above, including Windows Authentication **Note:** Depending on the OS, you might need to install ASP.NET manually.
Additional software	• Any modern browser, preferably Google Chrome or Microsoft Edge. • ASP.NET Core Runtime 10.0 Hosting Bundle • .NET Desktop Runtime 10.0 Windows x64

Cygna Entitlement and Security Server

Make sure the computer where you plan to set up the Cygna Entitlement and Security server (deploy the agent), meets the following hardware and software requirements and has all necessary software components and roles enabled.

COMPONENT	REQUIREMENTS
Hardware	• **CPU**: Any modern processor with 8 cores (minimum), 16 cores (recommended), more for large environments • **RAM**: 16 GB (minimum), 64 GB (recommended) • **HDD**: 1 TB For better performance, adjust your hardware configuration based on the number of entities in your Active Directory. The bigger your AD is, the more impact on your database server. The disk space required for the entitlement data can grow significantly over time.
Operating system	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025

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**: 100 GB (minimum). For better performance, adjust your hardware configuration based on the number of entities in your environment. The bigger your environment is, 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 2019 • SQL Server 2022 Standard and Enterprise editions are supported. Note that SQL Express edition is not supported.

Single Server Deployment–Small Businesses and PoC

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

COMPONENT	REQUIREMENTS
Hardware	• **CPU**: Any modern processor with 8 cores • **RAM**: 32 GB (minimum), 64 GB (recommended) • **HDD**: 1 TB For better performance, adjust your hardware configuration based on the number of entities in your environment. The bigger your environment is, the more impact on your database server. The disk space required for the audit data can grow significantly over time.
Operating system	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Server roles and features	• **Web Server (IIS)**: Microsoft IIS 8.5 or above, including Windows Authentication **Note:** Depending on the OS, you might need to install ASP.NET manually.
Database	• SQL Server 2019 • SQL Server 2022 Standard and Enterprise editions are supported. Note that SQL Express edition is not supported.
Additional software	• Any modern browser, preferably Google Chrome or Microsoft Edge. • ASP.NET Core Runtime 10.0 Hosting Bundle • .NET Desktop Runtime 10.0 Windows x64

Recommended Database Maintenance

Cygna Labs recommends a weekly SQL Server maintenance job that includes the following elements. These items may be added using the SQL Server Maintenance Plan Wizard. See the Microsoft SQL Server documentation for details.

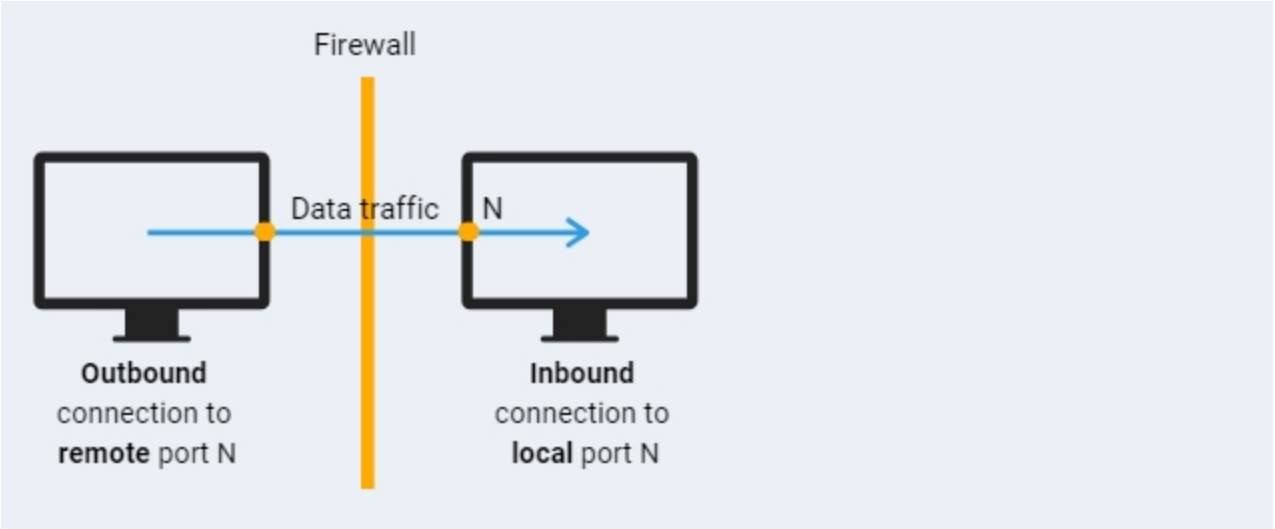
- Shrink Database
  - Allow 10% free space after shrink
  - Return freed space to the operating system
- Rebuild Index
  - Rebuild indexes if fragmentation exceeds 20% and the page count exceeds 500 pages
- Update Statistics
  - All existing statistics
  - Full scan
- Backup Database

Cygna Labs recommends using the archive and purge features only to retain the level of data required for compliance at your organization. If these features are not enabled at install time, the first few operations will be completed successfully but will have a higher SQL load than usual. The jobs should not be scheduled to run at the same time as your SQL Maintenance Plan.

Ports and Network Resources Reference

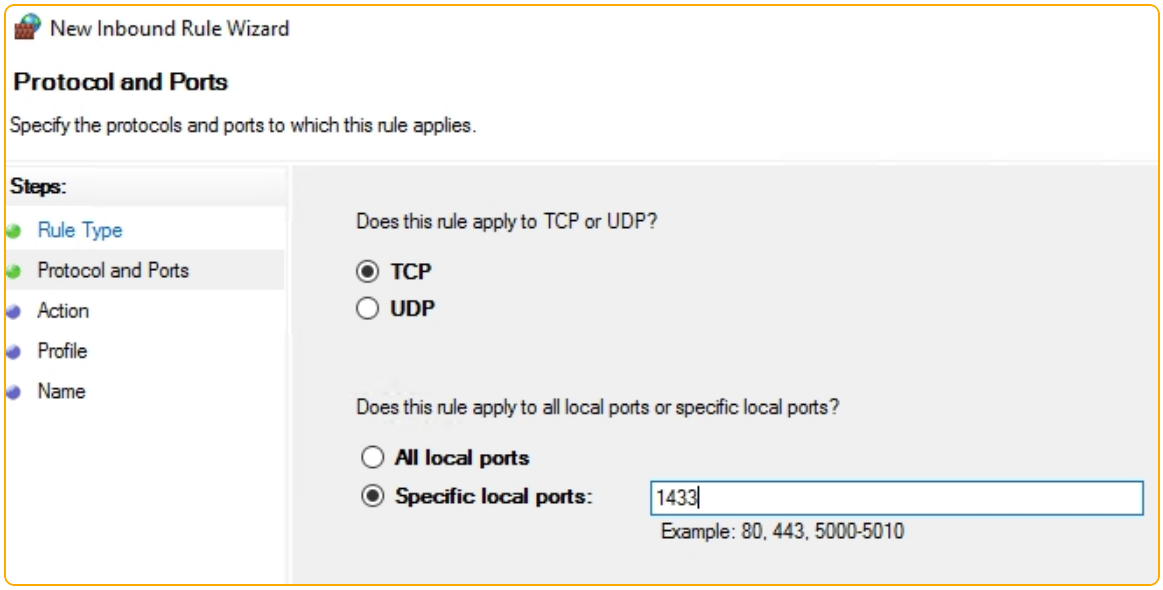
Check this reference and ensure your firewall is configured to allow inbound and outbound connections to the following ports. This port configuration is essential to product operability since facilitates data collection, acquisition, and transmission between the product components and audit sources.

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



Configuring Windows Firewall Rules

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



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

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

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

4. Ensure the newly created rule is enabled.

Cygna Platform

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

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	80 (http) 443 (https)	IIS
Outbound	Remote	TCP (HTTP/2)	6656	Interaction with Cygna Entitlement servers.
Outbound	Remote	TCP	443 (https)	Access to Cygna Entitlement and Security online help at docs.cygnalabs.com.
Outbound	Remote	TCP	1433	Interaction with SQL Server-based data storage.

Entitlement and Security Server

The server collecting entitlement data should be configured to allow the following connections.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP (HTTP/2)	6656	Interaction with Cygna platform.
Outbound	Remote	TCP	389	Domain LDAP
Outbound	Remote	TCP	3268	Global catalog LDAP
Outbound	Remote	TCP	636	Domain LDAP

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
				over SSL (LDAPS)
Outbound	Remote	TCP	3269	Global catalog LDAP over SSL (LDAPS)

Database server

The server where entitlement database is located should be configured to allow the following connections.

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

Active Directory DCs

Domain controllers in the Active Directory domain you want to query for entitlement and user assignment data.

CONNECTION	PORT	PROTOCOL	PORT	REQUIRED FOR
Inbound	Local	TCP	389	Domain LDAP
Inbound	Local	TCP	3268	Global catalog LDAP
Inbound	Local	TCP	636	Domain LDAP over SSL (LDAPS)
Inbound	Local	TCP	3269	Global catalog LDAP over SSL (LDAPS)

Account and Permissions Checklist

When setting up the product and data collection, Cygna Entitlement and Security will prompt you to enter account credentials for specific services and applications the product

requires access to. For your reference, below is a complete list of accounts with required rights and permissions.

ACCOUNT	WHAT IS IT USED FOR?	REQUIRED PERMISSIONS
Domain account	Active Directory credentials used to connect to a domain and collect entitlement data. Note that collection is a read-only operation and doesn't make any changes in your Active Directory environment.	The use of **Domain administrator** account is recommended. Alternatively, ensure the account running entitlement collection has **"read all properties"** and **"read DACL"** enabled for every object in the monitored domains, including child domains and trusted domains. Contact Cygna Support if you cannot use the Domain administrator account and need help setting up an account with less privileges.
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.
Database account	Account with Windows or SQL Server authentication used to connect to the SQL Server instance. During the collection setup, Cygna Entitlement and Security will create a database on a SQL Server instance you specify. This database will be used to store entitlement data.	**SQL Authentication:** The SQL Server account must have **dbowner** role on the created Entitlement database in order to create the schema. **Windows Authentication:** The account that runs the Entitlement service (by default, LOCAL SYSTEM of the server it is running on), must have **dbreader** and **dbwriter** roles assigned. The account selected to create the database and schema must have rights to create the schema.

Entitlement Sources

Cygna Entitlement and Security enables you to collect entitlement data from Entra ID tenants and Active Directory domains. Supported Domain Controller operating systems are:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note: There are no prerequisites for collecting entitlement data from your Active Directory domains. No prior configuration is required on the AD side.

Note: Collecting data from a Microsoft Entra ID tenant requires an Entra ID application with specific API permissions granted. See the Recovery for Entra ID configuration in the Cygna Auditor configuration for details.

Installing the Product

Cygna Entitlement is enabled by applying a license to a Cygna Auditor installation. No Cygna Auditor licenses are required – you can apply only an Entitlement license to use Entitlement features, or combine Entitlement and Auditor licenses to use both. To get started, install Cygna Auditor using the instructions in Installing the Product, then return here to apply your Entitlement license to enable one or more Entitlement modules.

Starting the Product

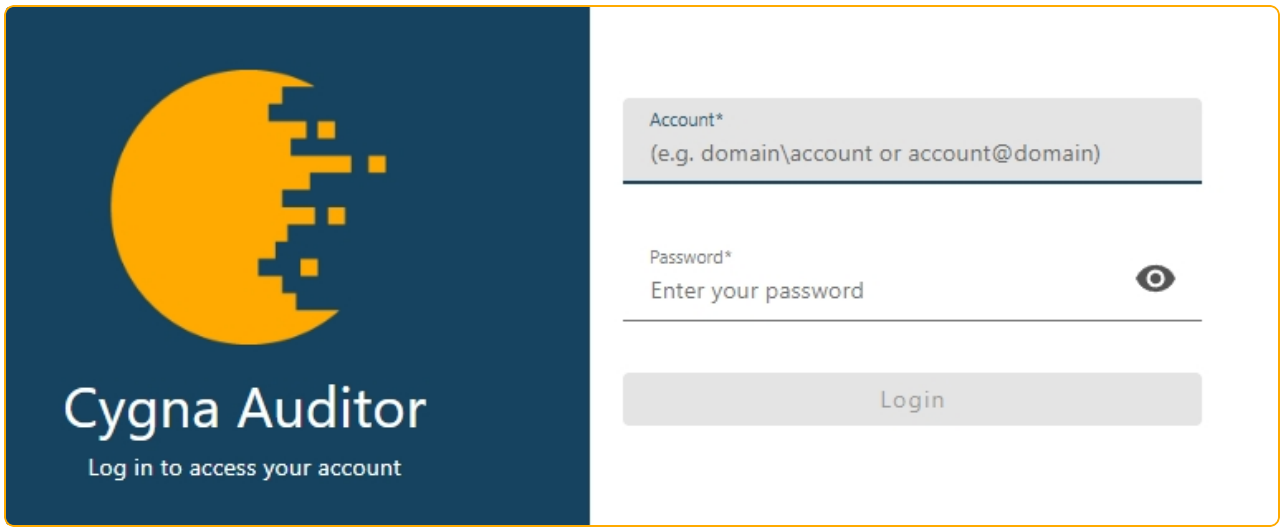
To start Cygna web console on a local computer:

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

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

To start Cygna web console on any computer in your corporate domain:

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



Granting Access to Cygna Platform

Cygna platform collects data in your organization so that you can be sure that no breach can occur. If distributed freely, such data can be a huge security issue of its own since internal attackers can use it to their own advantage. To secure collected data and ensure that only authorized personnel can review it and update configuration, the Cygna platform enables you to delegate access within the product.

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

Cygna Roles

Cygna platform comes with a set of built-in roles. These roles cannot be removed or modified. To view available roles, navigate to **Configuration / Delegation / Roles**. For Cygna Entitlement and Security, pay attention to the following roles:

- **Global administrator**–provides access to all product functionality, including role delegation. The first user to install the Cygna platform is granted the **Global administrator** role.
- **Entitlement Explorer - Owner**–provides extensive permissions to Entitlement data, reports, and configuration.

Assigning Roles to Users

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

Configuration

Before exploring entitlements, you must set up an Entitlement and Security server, databases, and data collection.

Continue reading:

Setting up Entitlement Service 20
Enabling Active Directory Data Collection 21
Enabling Entra ID Data Collection 22

Setting up Entitlement Service

You can use several Entitlement and Security Servers to collect data from your environment. The first server you deploy is set as primary. In a deployment with multiple Entitlement and Security Servers, the primary server manages the configuration and controls the other servers. Most environments do not require more than one server.

To set up a server and databases:

1. In the Cygna console, navigate to **Configuration / Entitlement / Servers** and set up a server.
2. On the **Deployment** step:
   - Select if you want to make this server the primary
   - Choose if you wish to deploy the Entitlement server on the Cygna Auditor host computer or a different one. Cygna Labs recommends using a different computer to distribute the load and improve performance.
   - Click Deploy Entitlement Service. The system will deploy the server and wait for the service to start before allowing you to continue. This step will take several minutes.
3. On the **Settings** step:
   - Configure the Entitlement and Security database. This database contains configuration information and will remain small.
   - Do not modify the Advanced options unless requested by Support or a Sales Engineer.
4. On the **Modules** step:

- Configure databases for any active modules. These databases store security information for the related module. This database will grow over time and will depend on your environment's size.

5. On the **Summary** step:
   - Select Finish to save the Server configuration

Enabling Active Directory Data Collection

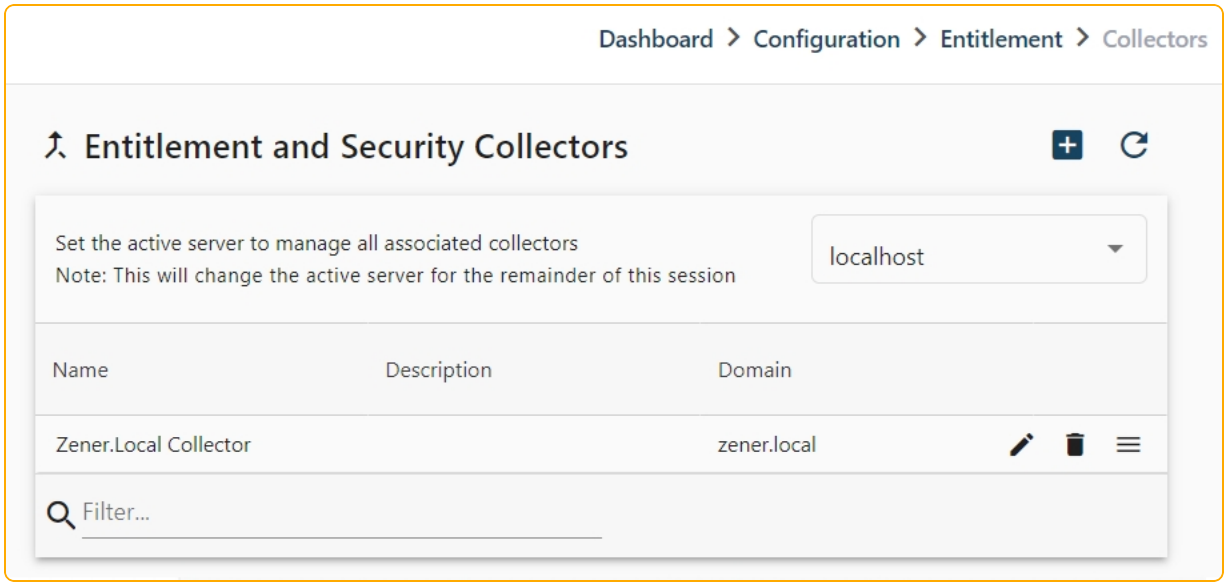
To start collecting entitlement data from your Active Directory domains, perform the following configuration steps. While there are no specific prerequisites for data collection that should be configured on the AD side, make sure you have sufficient permissions to perform data collection. See Account and Permissions Checklist for more information.

1. In the **Cygna** console, navigate to **Configuration / Entitlement / Collectors / Active Directory** and set up a new collector.
2. Complete the Deployment tab. If you are deploying
3. Complete the **General** tab – provide a name and description for your collection.
4. On the **Connection settings** tab:
   - Select **Enable LDAPS (LDAP over SSL)** to run all LDAP queries using a secure LDAP channel (LDAPS). Make sure LDAPS is configured in your AD.
   - Provide AD credentials. Consider using the domain administrator account.
   - Select **Verify connection information** to run a test collection.
   - Advanced settings should not be changed unless recommended by Cygna Labs Corp. technical personnel.

OPTION	DESCRIPTION
Collect Externally Trusted Domains	Enable collection of externally trusted domains. Cygna Labs Corp. recommends using a separate collector for these domains.
Domain Scope	Enable to stop referrals to external domains from being generated when data is collected.
Chase Referrals	Enable to allow collector to chase a referral provided that a referral is generated.
Use Active Directory provided DC lookups	By default, the Entitlement collector executes a site-aware Domain Controller & Global Catalog lookup to always execute the collection against the same set of

OPTION	DESCRIPTION
	Domain Controllers & Global Catalogs. Enable this option to let AD/DNS determine which Domain Controllers to connect to instead of the optimized site-aware selection.
Reorganize and rebuild database indexes after successful collection	This option will trigger index rebuild and reorganize operations at the end of a collection. It is recommended that index operations remain part of the standard SQL maintenance plan. If this option is enabled, the SQL user must be granted permission to perform index maintenance operations.

5. On the **Schedule** tab, configure the collection schedule. Cygna Labs recommends collecting data twice a week, preferably during off hours to avoid load on your system.
6. On the **Summary** tab, review collection settings.



Enabling Entra ID Data Collection

To collect entitlement data from your Entra ID tenant, perform the following configuration steps.

1. In the Cygna console, navigate to Configuration / Entitlement / Collectors / Entra ID and set up a new collector.
2. On the General tab:

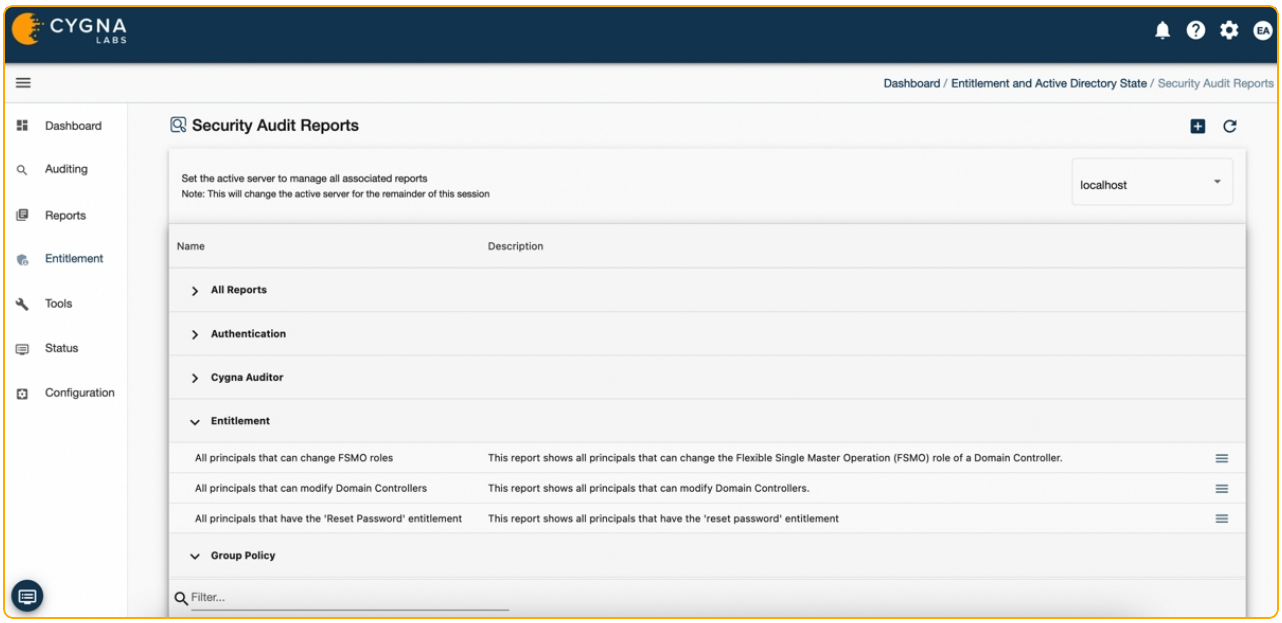
- Select a tenant configuration. Select an existing Microsoft 365 tenant configuration from Cygna Auditor, or register a new tenant by providing the tenant ID from Entra ID and other relevant details.
- Set a name and optional description for the collector.

3. On the Collector Settings tab:
   - If an existing tenant with an Entra ID Backup configuration was selected, the application ID and Secret will be pre-populated. If you added a new tenant, you must add an application in the Entra ID portal (see Recovery for Entra ID configuration in Cygna Auditor) and then provide the application ID and secret.
   - Do not modify the Advanced collection settings unless requested by Support or other Technical personnel from Cygna Labs.
4. On the Schedule tab:
   - Define a collection schedule for entitlement data. The minimum interval is once per day.
5. On the Summary tab:
   - Confirm the details and click Save.

Security Audit Reports

With Cygna Entitlement and Security, you can generate detailed reports on the distribution of your permissions. Reports help unveil security data and keep your infrastructure accountable. The products come with a curated list of reports out-of-the-box. You can also use advanced search functionality to craft custom reports.

For your convenience, the reports are grouped by category.



Continue reading:

Viewing Reports 24
Creating Custom Reports 25
Understanding Fields 29

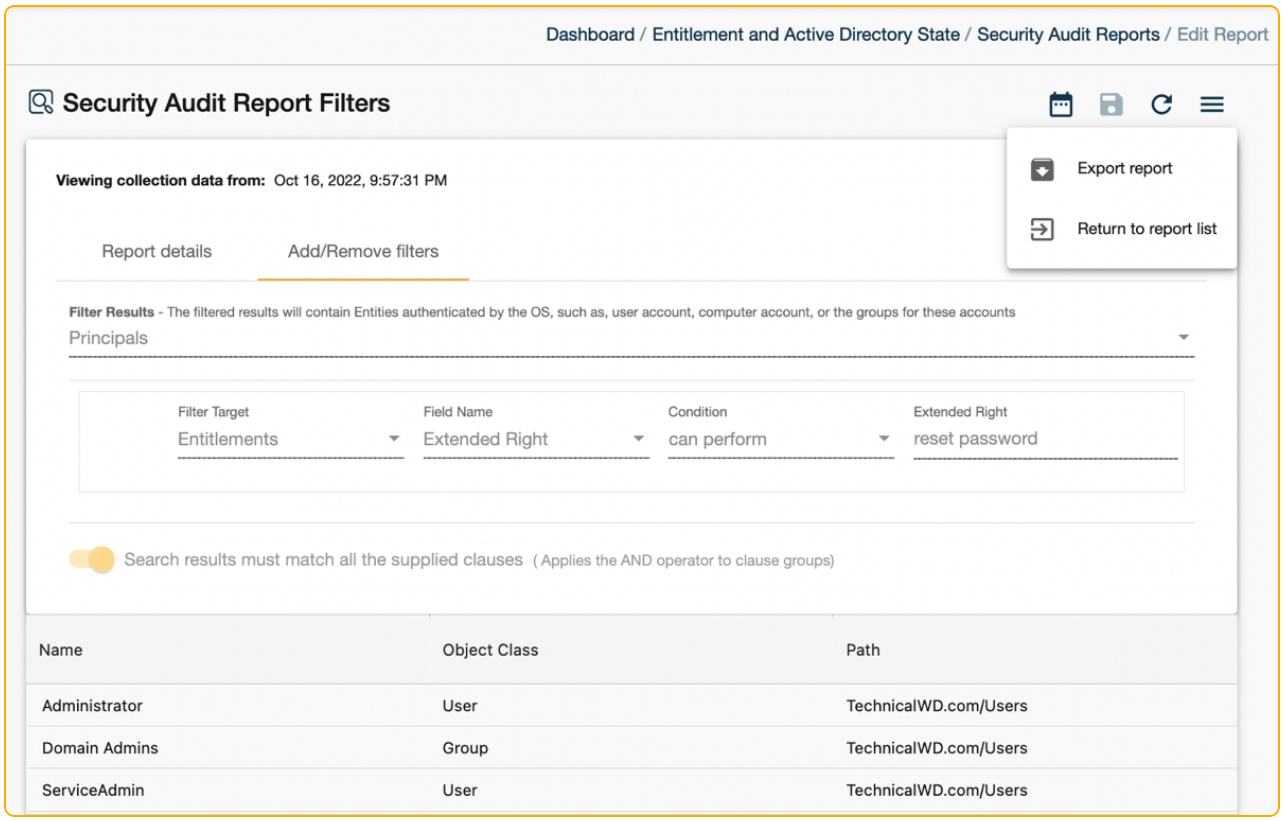
Viewing Reports

1. Navigate to **Entitlement / Security Audit**.
2. Select a report.
3. View report details and applied filters. The built-in reports are read-only but you can clone a report and modify its filter or create a custom report from scratch.
4. Cygna Entitlement and Security will search for events that match report's filters and display them.

For each report, you can:

- Clone the report–to create a new custom report based on an existing one

- Export results–to share the report data as PDF or CSV with executives who don't have access to the Cygna platforms
- Change the snapshot date–to create historical reports representing the state of your environment on a specific date.



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

Creating Custom Reports

Create custom reports to cater to your organization needs. Your custom reports will be stored alongside built-in reports. You can find them under **Entitlement / Security Audit**.

To create a report:

- Clone an existing report and customize it. To do it, select next to an existing report and specify **Clone**. The newly created report will appear in the list. Drill down to its

details to update this report.

- Create a new report from scratch. To do it, select . A draft report displays all data.

Configuring Report Details

On the **Edit report details** tab, add the report name and description. You can specify tags to find this report faster.

Adding Filters

On the **Add/Remove filters** tab, specify the search query to retrieve the data you need for your report.

When filters are empty, the report returns all data collected by Cygna Entitlement and Security. The filters help you discover and retrieve data that you are looking for.

Filtering Results

Specify the AD entities to return in your report results:

- **Principals**–returns user and computer accounts, as well as groups.
- **Objects**–returns security principals, containers, resources, applications, and services.
- **ImpliedTrustees**–returns objects matching directly or through group membership
- **ImpliedPermissions**–returns objects matching selected permissions criteria.
- **ImpliedEntitlements**–returns principals matching selected access criteria.

Specifying a Filter Target

If you select **Principals** or **Objects** in the **Filter results**, you can choose a target for each search. Select one of the following:

- Objects–queries entities such as security principals, containers, resources, and applications and checks if they match the search criteria.
- Trustees–queries objects and checks whether they match directly or through group membership.
- Permissions–queries objects and checks if they match selected permissions criteria.
- Entitlements–queries principals and checks if they match selected access criteria.

Building a Filter

The filter clause contains a field name, a matching condition, and a value. It defines a query to look for.

OPTION	DESCRIPTION
Field name	Pick a filter from the drop-down. The filter corresponds to the attribute you are searching for. For example, CN or adminCount.
Condition	Select a condition from a drop-down. Available conditions vary depending on the attribute you choose in the Filter name section. Select these conditions, • if you are looking for an exact entry (*equals*) • if you are looking for an entry containing the searched value (*contains*) • if you are searching for an entry that *starts with* or *ends with* a certain value. • if you are looking for opposite values such as *does not start with* and *does not contain* • if you are looking for any value (*exists*) Specific attributes allow other conditions.
Value	The value field is the area where you specify a value to be searched. Depending on the filter name, you can select a value from the drop-down list or enter it manually.

Defining Filter Logic

Create complex report queries with multiple filter clauses, organized with logical AND/OR operators. To add a new clause, start selecting the filter name in the empty clause section.

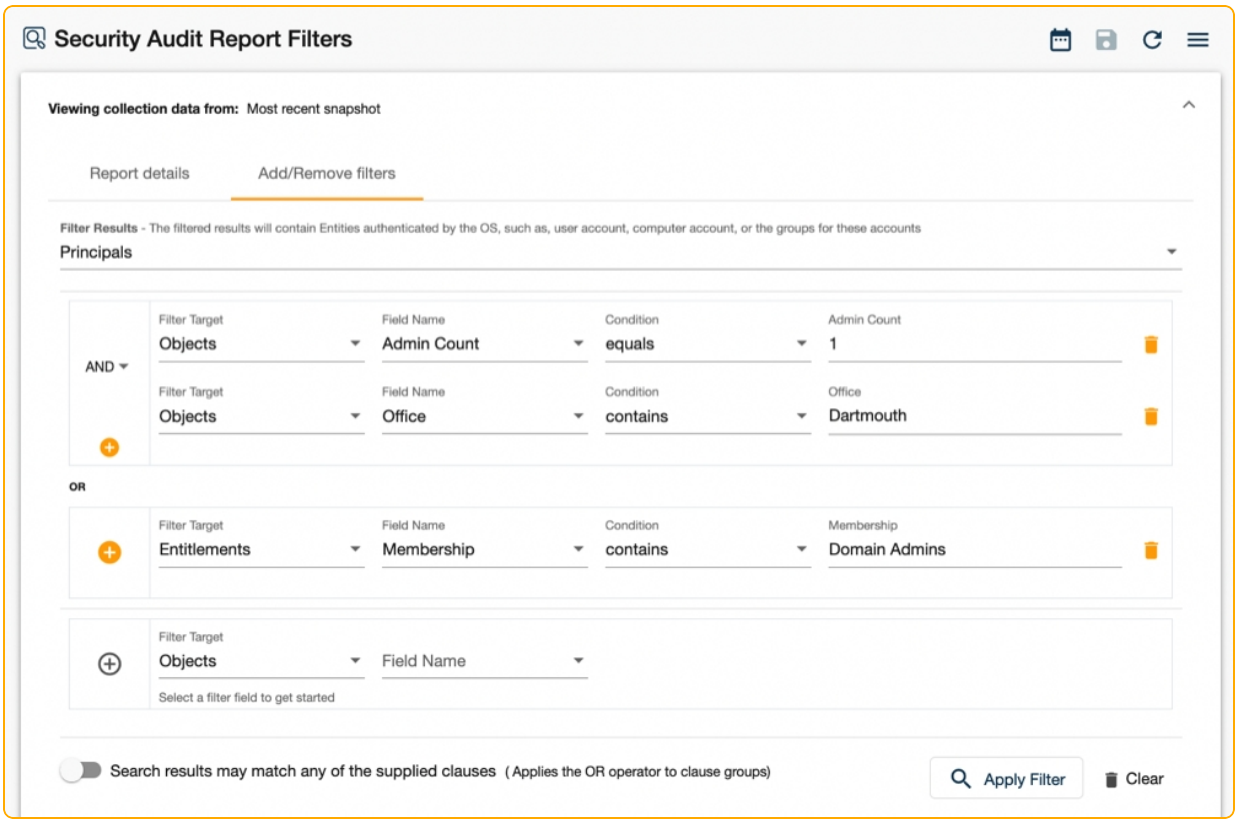
By default, Cygna Entitlement and Security returns data that matches all filter clauses at once (logical AND). You can change this behavior and instruct the product to return records that match at least one filter clause (logical OR). To do it, switch the toggle to the *off* position.

Additionally, you can organize filters into groups. To do it, click on the orange + to add a clause within a group where you can set a specific logic too.

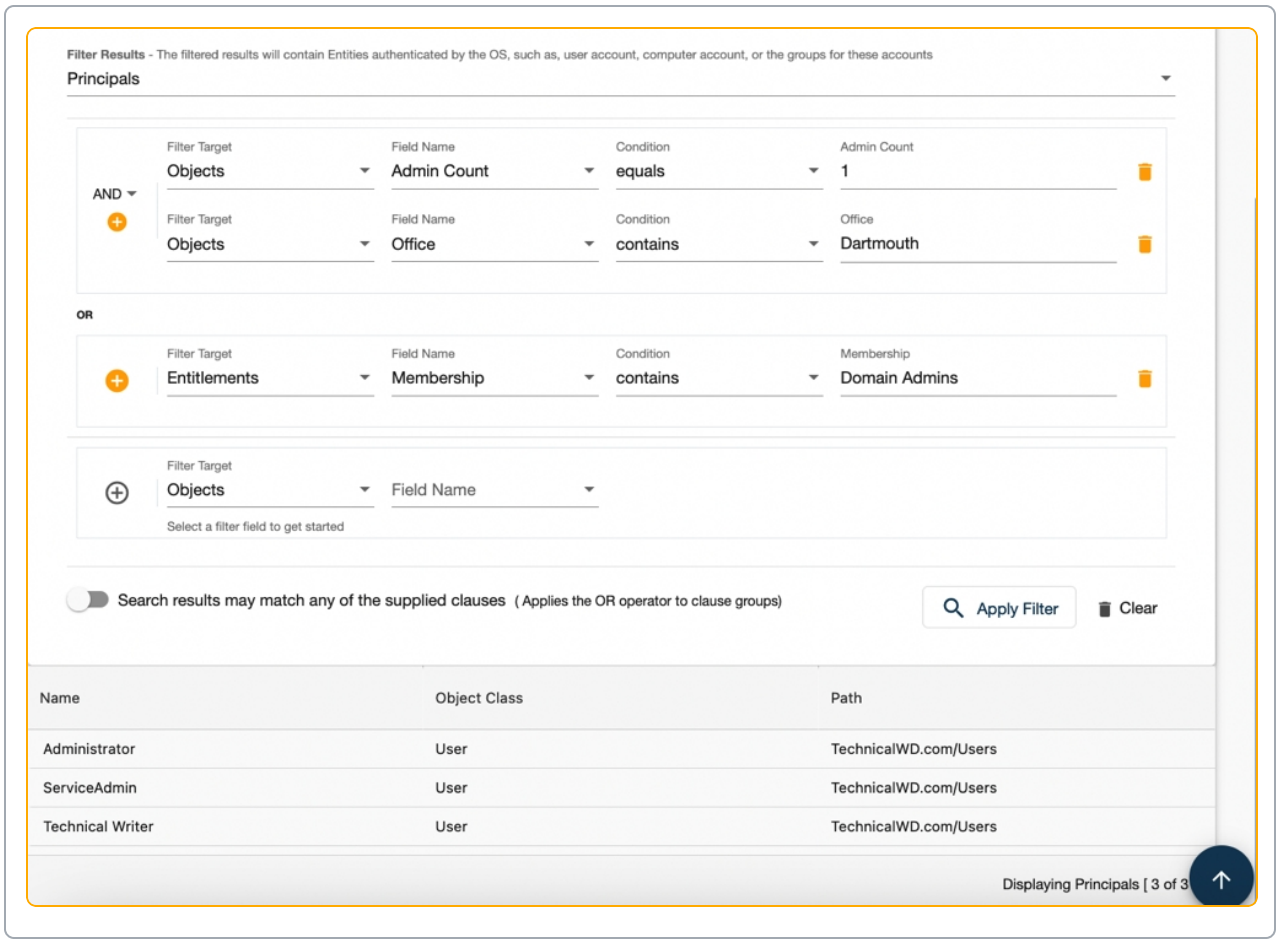
In result, you can create a filter query such *'[Clause 1 OR Clause 2] AND Clause 3'* or *' [Clause 1 AND Clause 2] OR [Clause 3 AND Clause 4]'*.

EXAMPLE:

For example, you want to locate principals residing in the Dartmouth office that were ever a member of the protected group. Additionally, in this report you want to see principals that are currently members of the Domain Admins.



To do it, you create a complex search query that includes a clause with two subclauses with AND relationship inside. And a second clause. The main clauses are in the OR relationship (the toggle is off and set to *"Search results may catch any of the supplied clauses"*). After clicking **Apply Filter**, check the results in pane below.



Understanding Fields

Below is a list of available field filters with descriptions. The filters correspond to Active Directory attributes.

FIELD	DESCRIPTION
Access	A selectable list of access rights
Ace Count	A count of unique Access Control Entries in the security descriptor associated with the object
Admin Count	The adminCount attribute
Allow	Combined direct and inherited allow rights on an object (context dependent on the qualifier)
Breaks Inheritance	Checks for inheritance break
Cn	The cn attribute

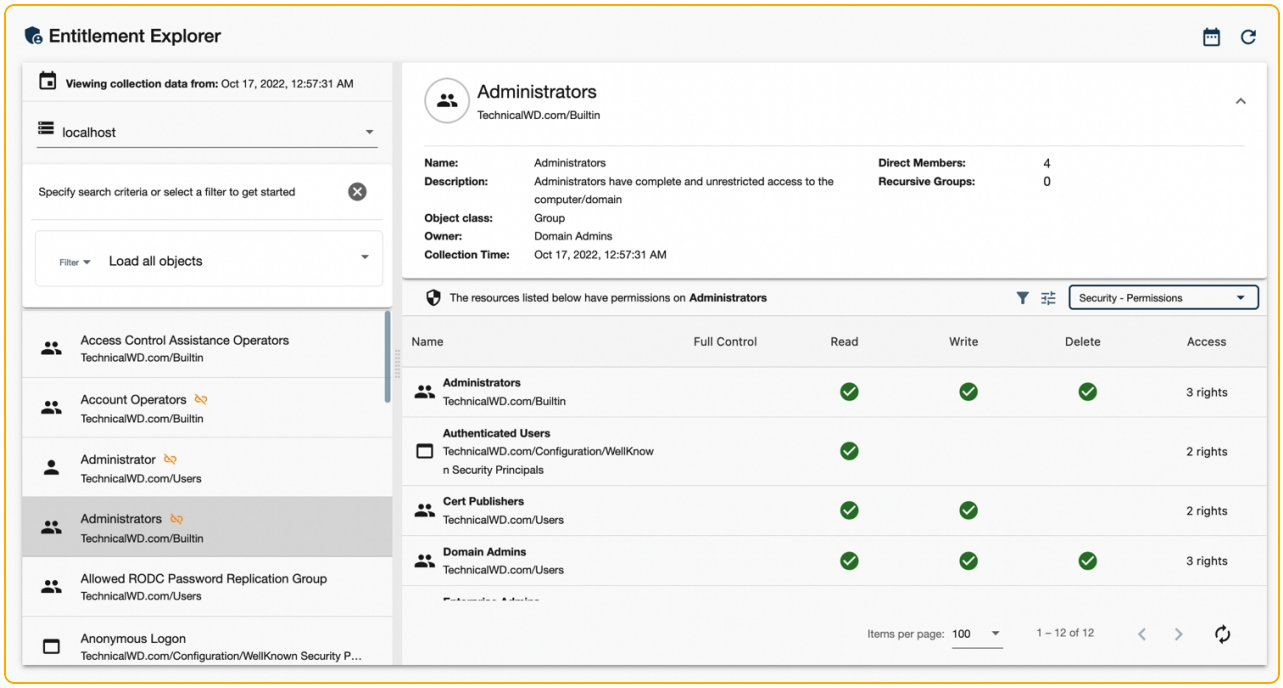
FIELD	DESCRIPTION
Company	The company attribute
Country	The country attribute
Create Child	The createChild permission (context dependent on qualifier)
Delegate	Rights applied to descendant objects of type (context dependent on qualifier)
Delete Child	The deleteChild permission (context dependent on qualifier)
Deny	Combined direct and inherited deny rights on an object
Department	The department attribute
Descendant Object	Rights applied to descendant objects of type (context dependent on the qualifier)
Description	The description attribute
Direct Allow	Direct allow rights on object (context dependent on the qualifier)
Direct Deny	Direct deny rights on object (context dependent on the qualifier)
Distinguished Name	The distinguishedName attribute
Domain	The Domain object the data was collected from
Email	The mail attribute
Extended Right	Extended Right on an object (context dependent on the qualifier)
Field	Existence check on the field
Group Type	The groupType attribute
Inherited Allow	Inherited allow rights on object (context dependent on the qualifier)
Inherited Deny	Inherited deny rights on object (context dependent on the qualifier)
Is Derived Through	How the right is applied to the object (context dependent on the qualifier)

FIELD	DESCRIPTION
Manager	The manager attribute
Member Count	Number of members in the group
Membership	Direct membership of a principal
Membership Count	Number of groups a principal is a member of
Name	The name attribute
Nested Membership	Nested membership of a principal
Object Class	The objectClass attribute
Object Guid	The objectGuid attribute
Object Sid	The objectSid attribute
Office	The office attribute
Operating System	The os attribute
Operating System Hotfix	The operatingSystemHotfix attribute
Operating System Service Pack	The operatingSystemServicePack attribute
Operating System Version	The operatingSystemVersion attribute
Owner	Owner of the object
Path	Path of the object
Primary Group	The primaryGroupId attribute
Read Property	Read property on object (context dependent on the qualifier)
Read Property Set	Read property set on object (context dependent on the qualifier)
Service Principal Name	The servicePrinicpalName attribute
Show In Advanced View Only	The showInAdvancedViewOnly attribute

FIELD	DESCRIPTION
State	The state attribute
Superior	Nested manager
System Flags	The systemFlags attribute
Title	The title attribute
User Account Control	The uac attribute
Write Property	Write property on the object (context dependent on the qualifier)
Write Property Set	Write property set on the object (context dependent on the qualifier)

Entitlement Explorer

Explore entitlement and permission data in your environment and delve into history snapshots.



Continue reading:

Understanding How Entitlement Explorer Works 33

Exploring Entitlement Data 37

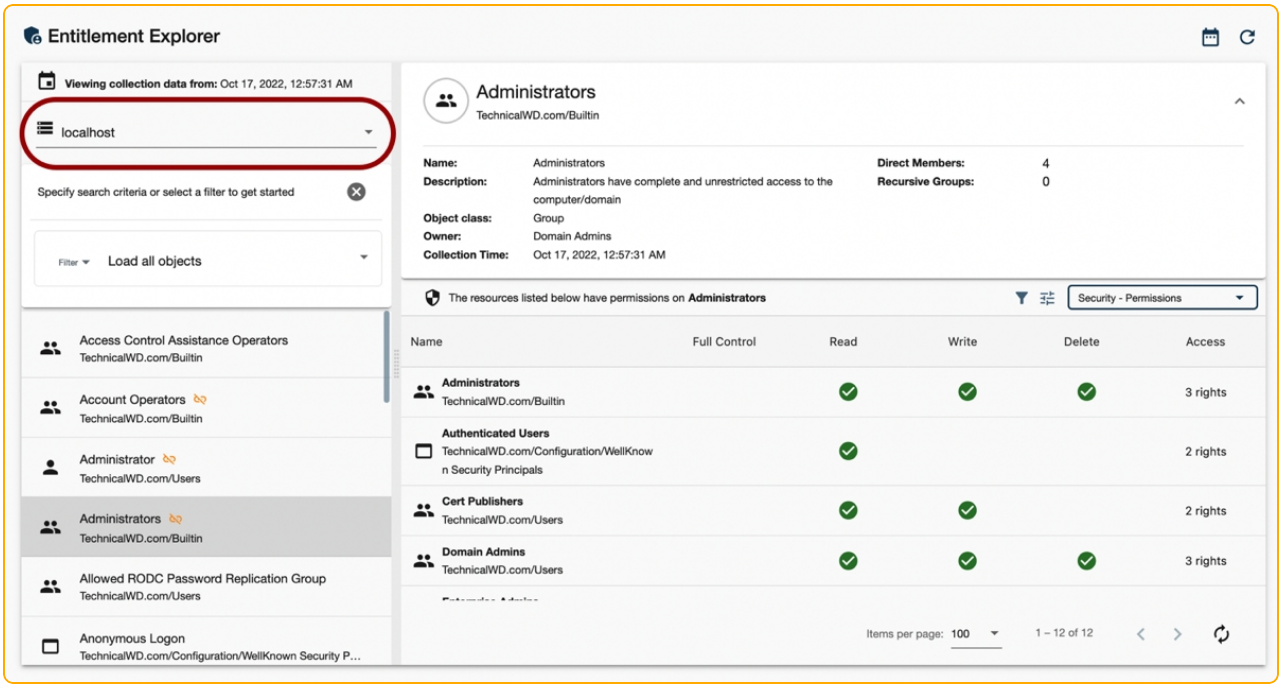
- Entitlements – Access 40
- Security – Permissions 41
- Trustees – Expanded Permissions 42
- Group Members 43
- Group Membership 44
- Entra ID Views 45

Understanding How Entitlement Explorer Works

The Entitlement Explorer is a versatile tool that enables you to reach the same objects and entitlements using different approaches. Before you start reviewing entitlement data, learn about the Explorer capabilities to use it fully.

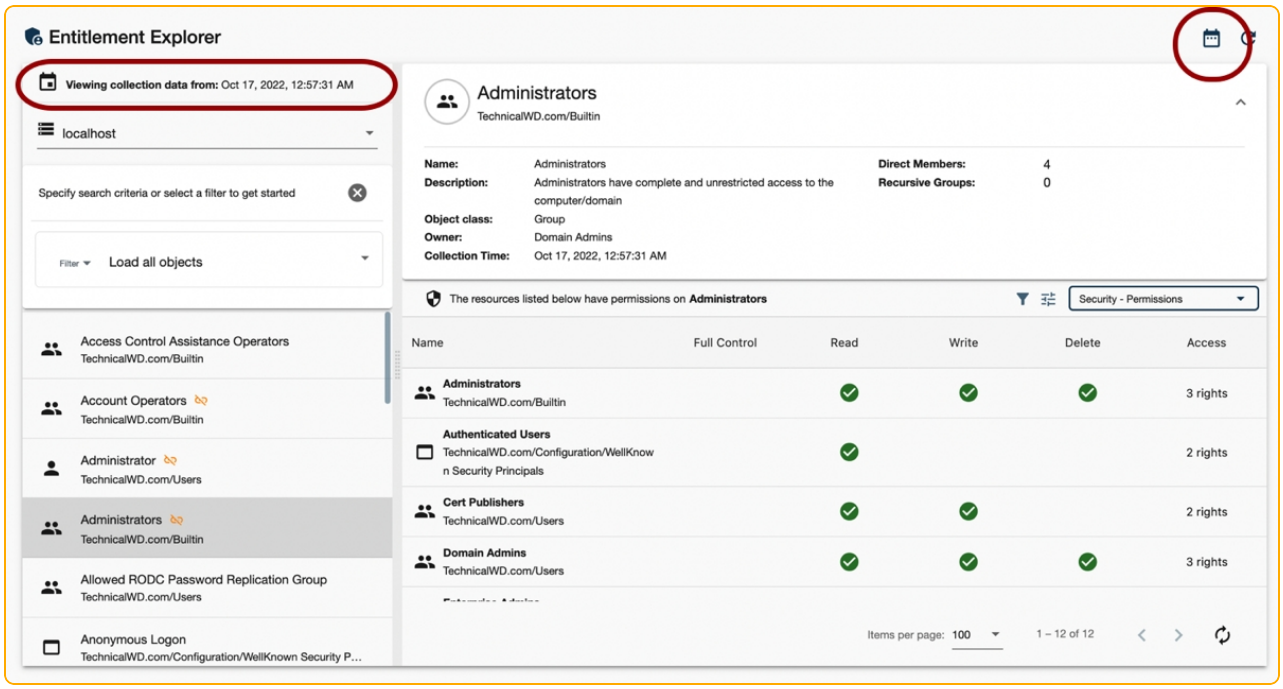
Specifying the Server

Before browsing data, select the Entitlement server. The explorer displays data from the primary server by default, but you can always switch to another server.



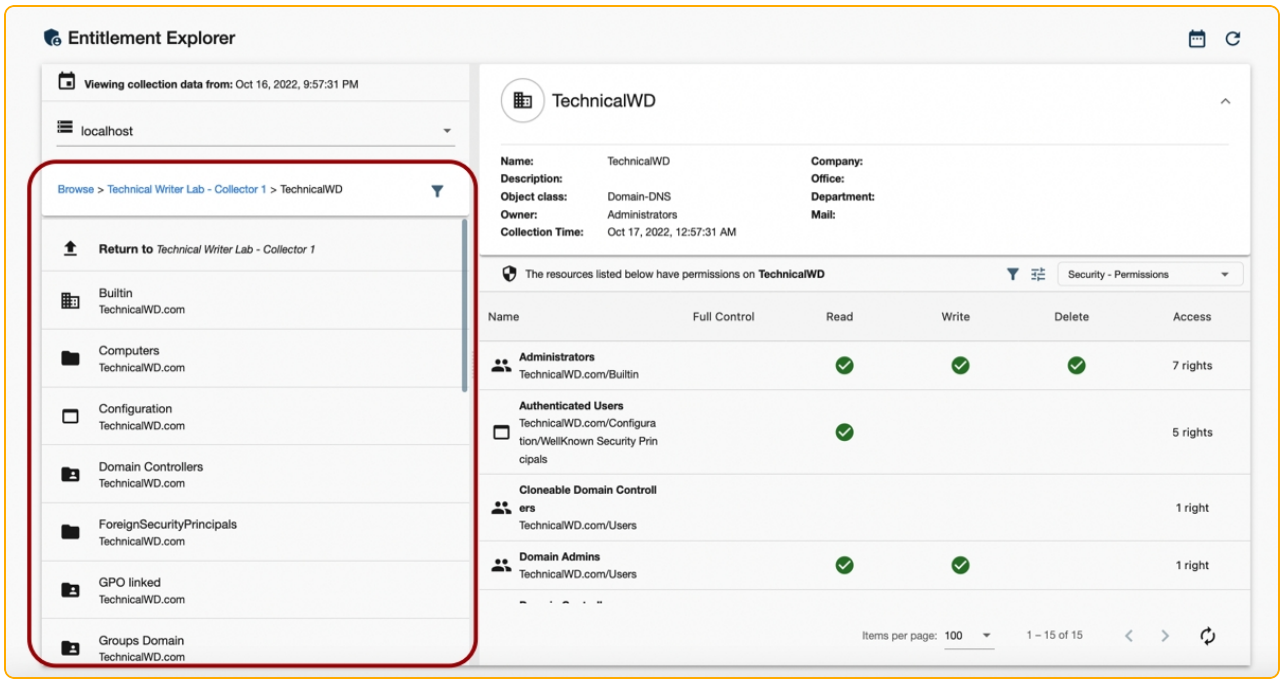
Changing Collection Timeline

By default, you can see the most recent data collected by Cygna Entitlement and Security. The last data collection date is displayed on the top of the page. If you are interested in entitlement data relevant for a specific point in time, select the snapshot closest to this date. Pick a date and time and set a new timeline.



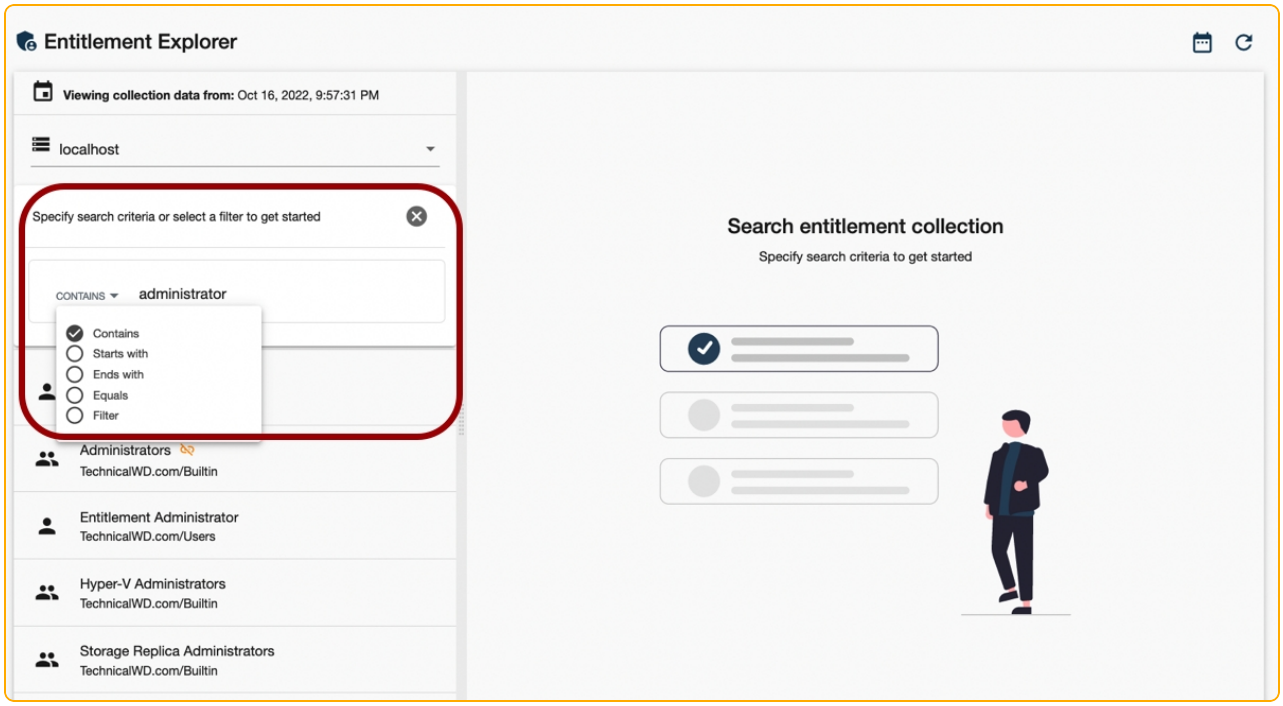
Browsing Domain

Drill-down into your AD domains to get a better understanding of the overall domain structure. Double-click your collection, pick a domain and delve into objects and groups. Select an object to see its entitlements and permissions.

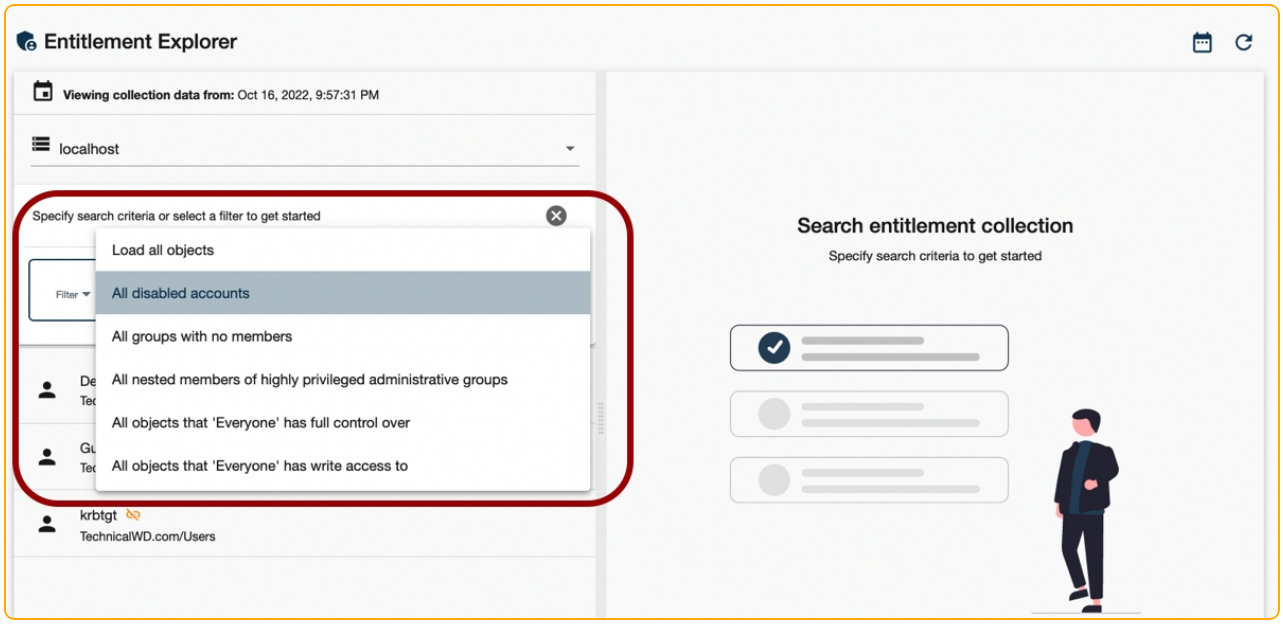


Searching Data

To locate objects you are interested in faster, use search capabilities. Use one of the condition operators (*contains*, *starts with*, *ends with*, or *equals*) and provide an object name. The Entitlement Explorer will display entities with matching names.



Alternatively, you can search for objects using preset filters. To do it, select *Filter* and then pick a query. The queries are the same as listed in the Security Audit Reports. The Entitlement Explorer will locate the objects matching the entire query. Note that you can create custom reports and use their queries when using the Entitlement Explorer. In case you want to retrieve all entities without preliminary filtering, set the filter to *"Load all object"*.



Exploring Entitlement Data

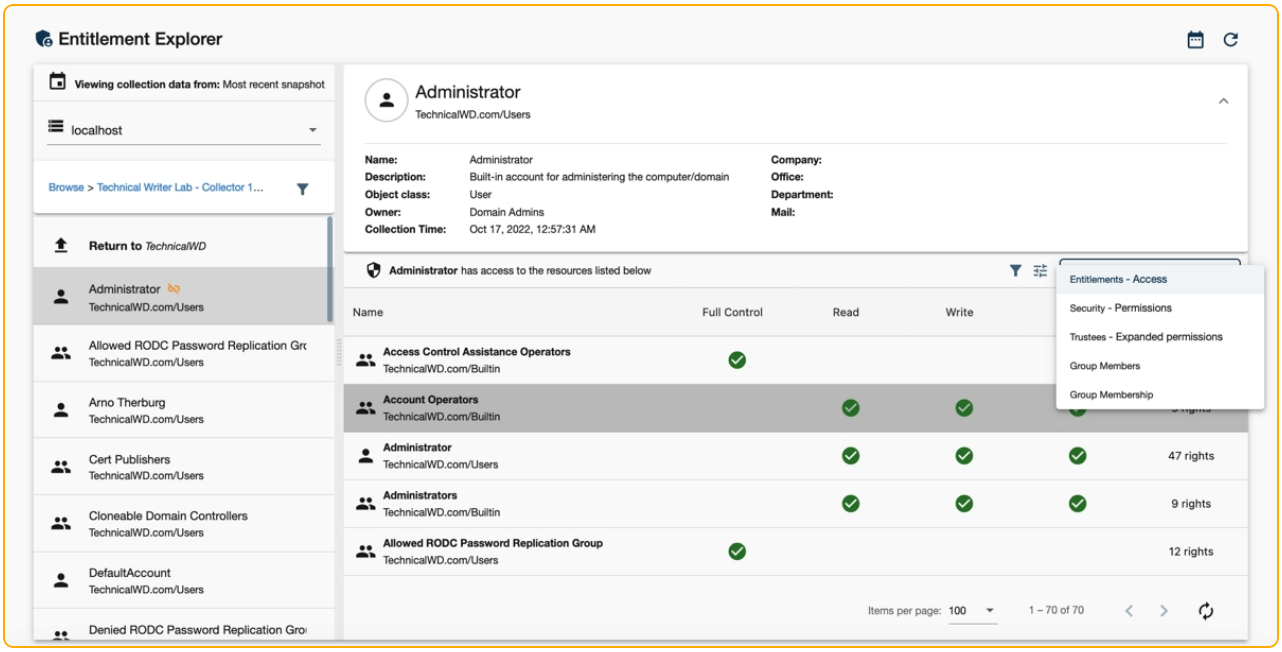
Once you locate an entity you are interested in, select it to see more details in the right-hand pane. While the top part displays general information such as the name, descriptions, class, and owner, the bottom section changes depending on the type of entitlement data you want to see for this particular object.

Switching Views

Select the type of data you want to see:

- Entitlements – Access
- Security – Permissions
- Trustees – Expanded Permissions
- Group Members
- Group Membership

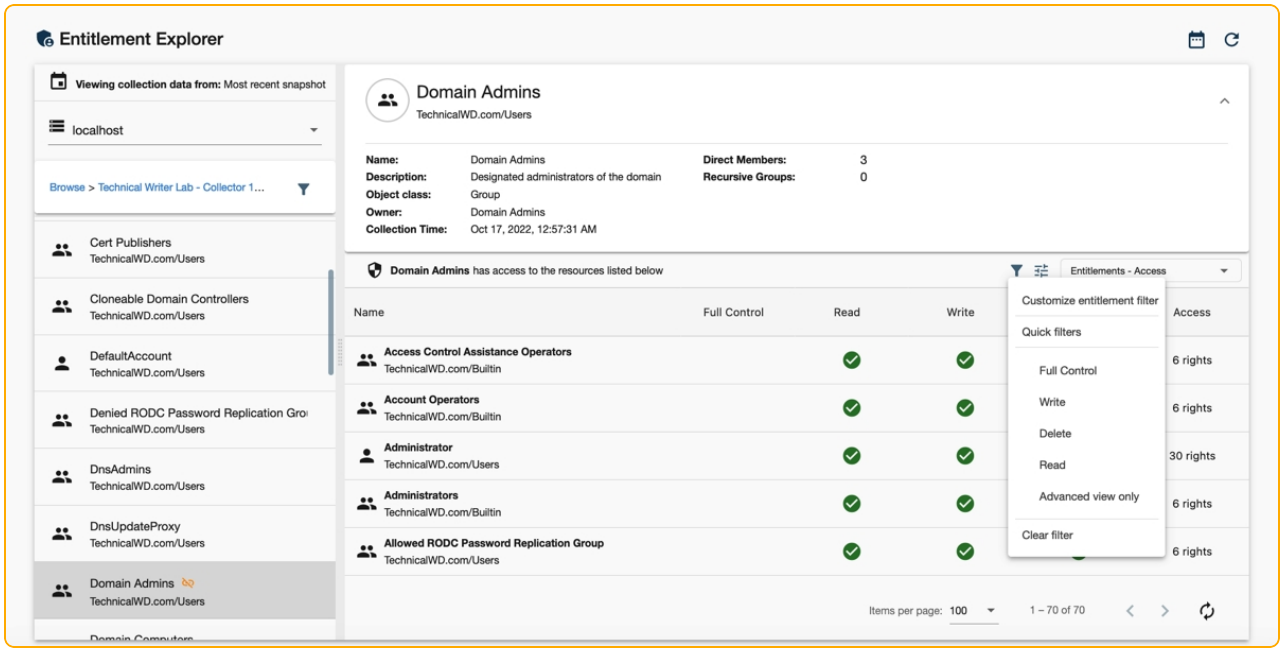
The views listed above apply to Active Directory objects. Entra ID objects provide a considerably larger set of views, covering roles and privilege, access packages, applications, policies, authentication methods, and tenant configuration. These are described in Entra ID Views.



Filtering Results

To narrow down the list of the entities in the bottom section, use filtering. You can either use a quick filter (e.g., full control) or create a custom filter and search for specific

attributes.



To build a custom filter:

The filter clause contains a field name, a matching condition, and a value. It defines a query to look for.

OPTION	DESCRIPTION
Field name	Pick a filter from the drop-down. The filter corresponds to the attribute you are searching for. For example, CN or adminCount.
Condition	Select a condition from a drop-down. Available conditions vary depending on the attribute you choose in the Filter name section. Select these conditions, • if you are looking for an exact entry (*equals*) • if you are looking for an entry containing the searched value (*contains*) • if you are searching for an entry that *starts with* or *ends with* a certain value. • if you are looking for opposite values such as *does not start with* and *does not contain* • if you are looking for any value (*exists*) Specific attributes allow other conditions.

OPTION	DESCRIPTION
Value	The value field is the area where you specify a value to be searched. Depending on the filter name, you can select a value from the drop-down list or enter it manually.

Create complex report queries with multiple filter clauses, organized with logical AND/OR operators. To add a new clause, start selecting the filter name in the empty clause section.

By default, Cygna Entitlement and Security returns data that matches all filter clauses at once (logical AND). You can change this behavior and instruct the product to return records that match at least one filter clause (logical OR). To do it, switch the toggle to the *off* position.

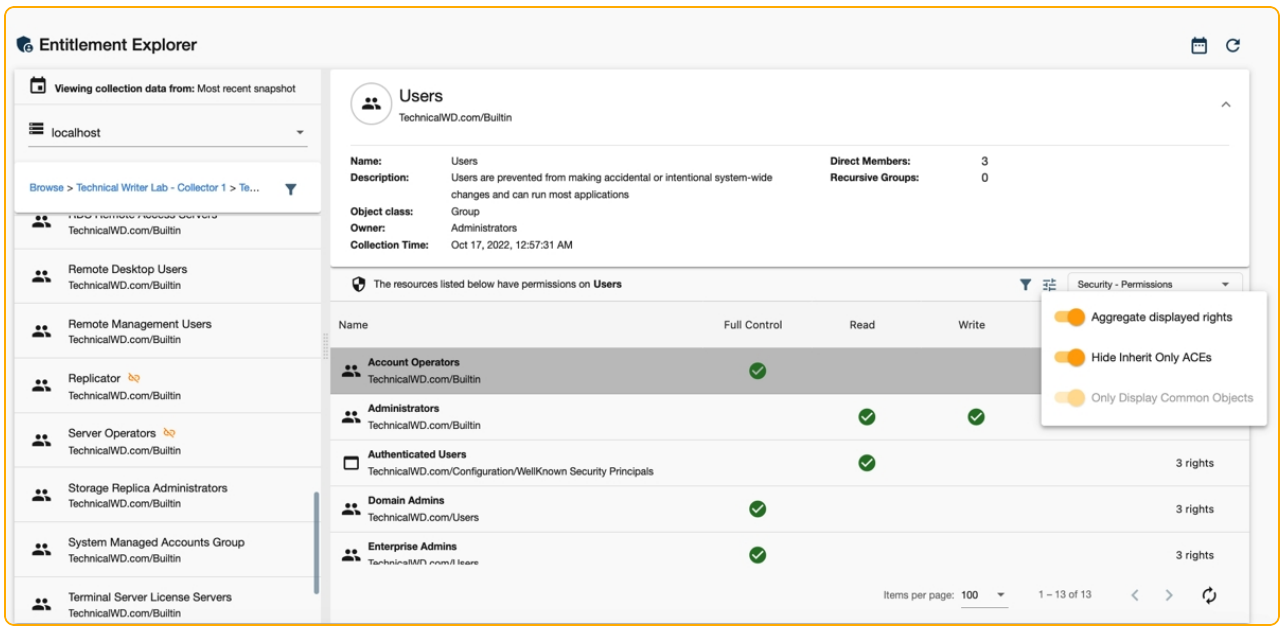
Additionally, you can organize filters into groups. To do it, click on the orange + to add a clause within a group where you can set a specific logic too.

In result, you can create a filter query such *'[Clause 1 OR Clause 2] AND Clause 3'* or *'[Clause 1 AND Clause 2] OR [Clause 3 AND Clause 4]'*.

Fine-Tuning

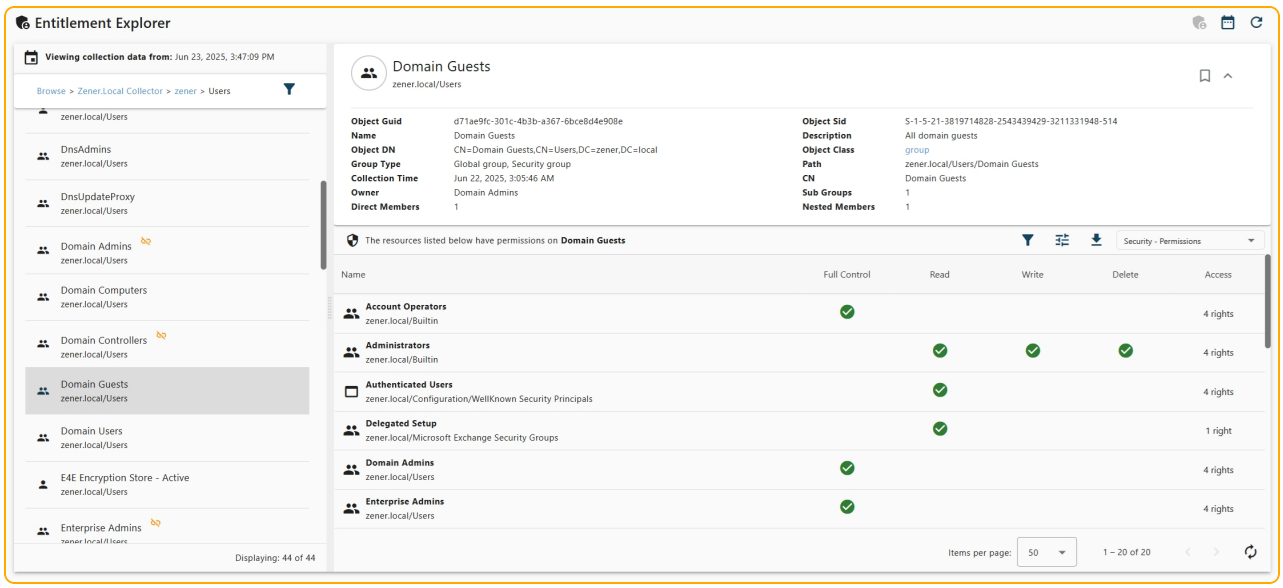
Choose the way you want to see the entitlement data and fine-tune results.

- Aggregate displayed rights
- Hide inherit only ACEs
- Only display common objects



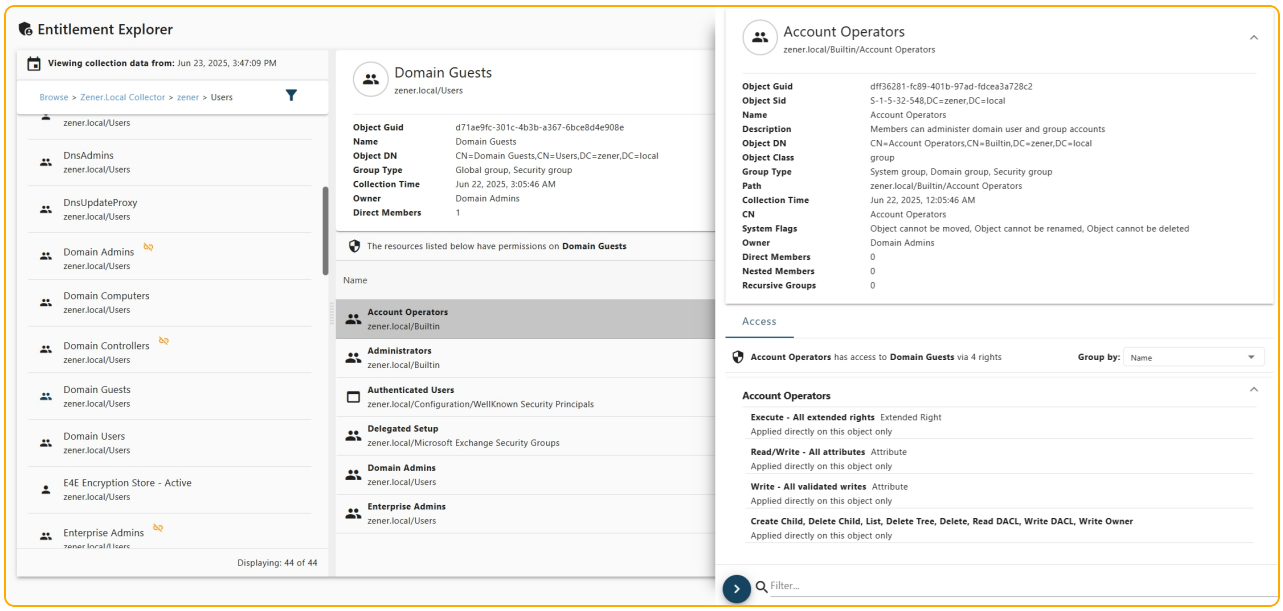
Entitlements – Access

Use the **Entitlement – Access** view to see resources the object has access to and unveil any irrelevant or elevated permissions. For example, check user entitlements to ensure appropriate access has been revoked when a user changes roles or leaves an organization. Or verify that a user's access aligns with their role.



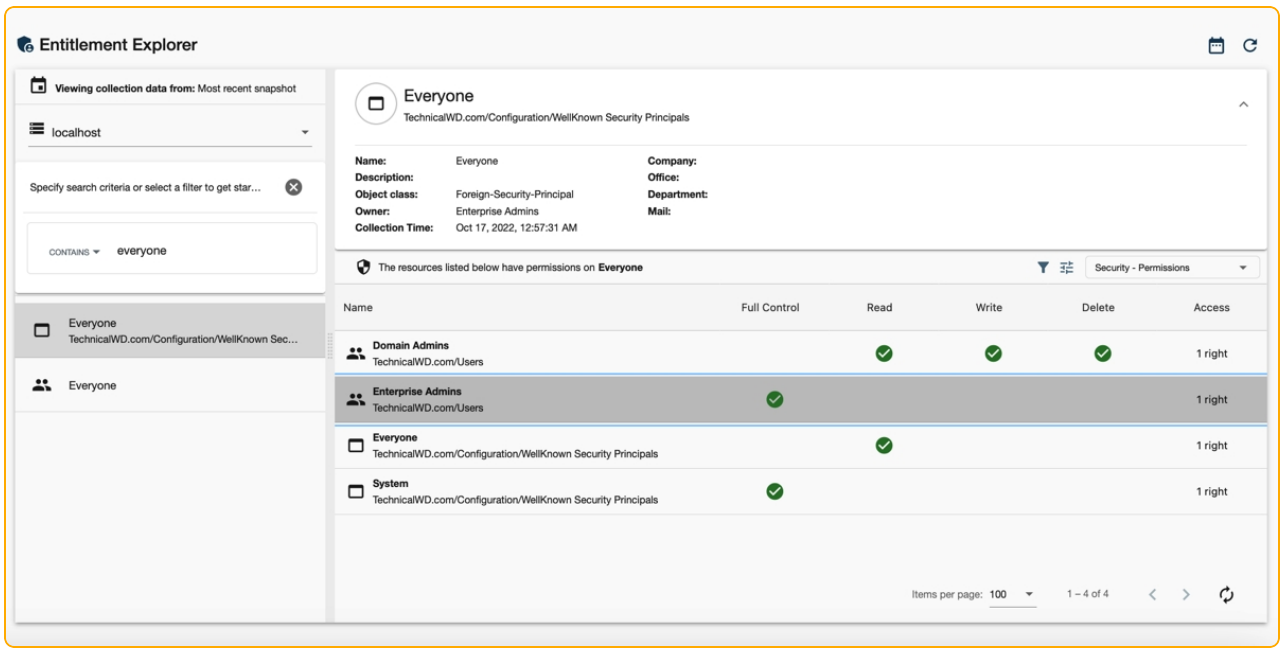
The full control, read, write, and delete access settings are marked visually for your convenience.

To learn more about the exact rights and group membership that resulted in granting access to a particular resource, select this resource to expand details.



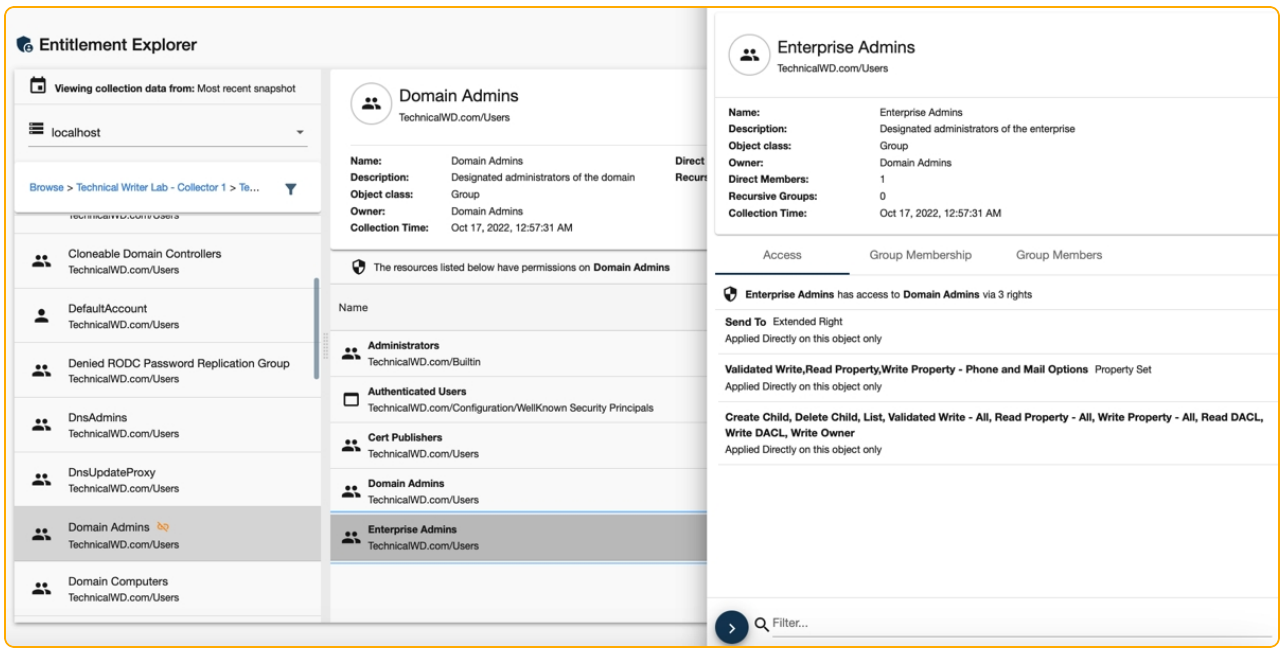
Security – Permissions

Use the **Security – Permissions** view to see resources with access to the specified entity. With the help of this view, you can locate potentially high-risk settings (such as regular users being granted **Full Control** to *Everyone* or *Everyone* having extended access to sensitive data) or troubleshoot your environment by locating explicit write denies.



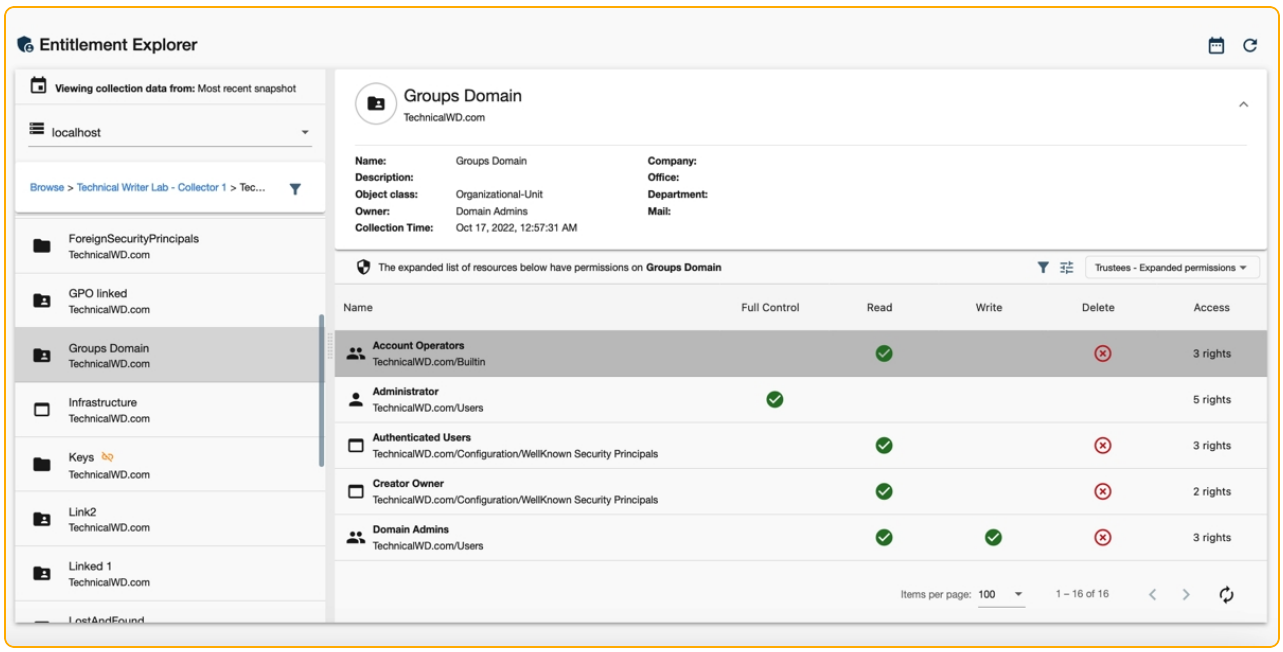
The full control, read, write, and delete permissions are marked visually for your convenience.

To learn more about the exact rights and group membership that resulted in a particular resource having rights to the object, select this resource to expand details.



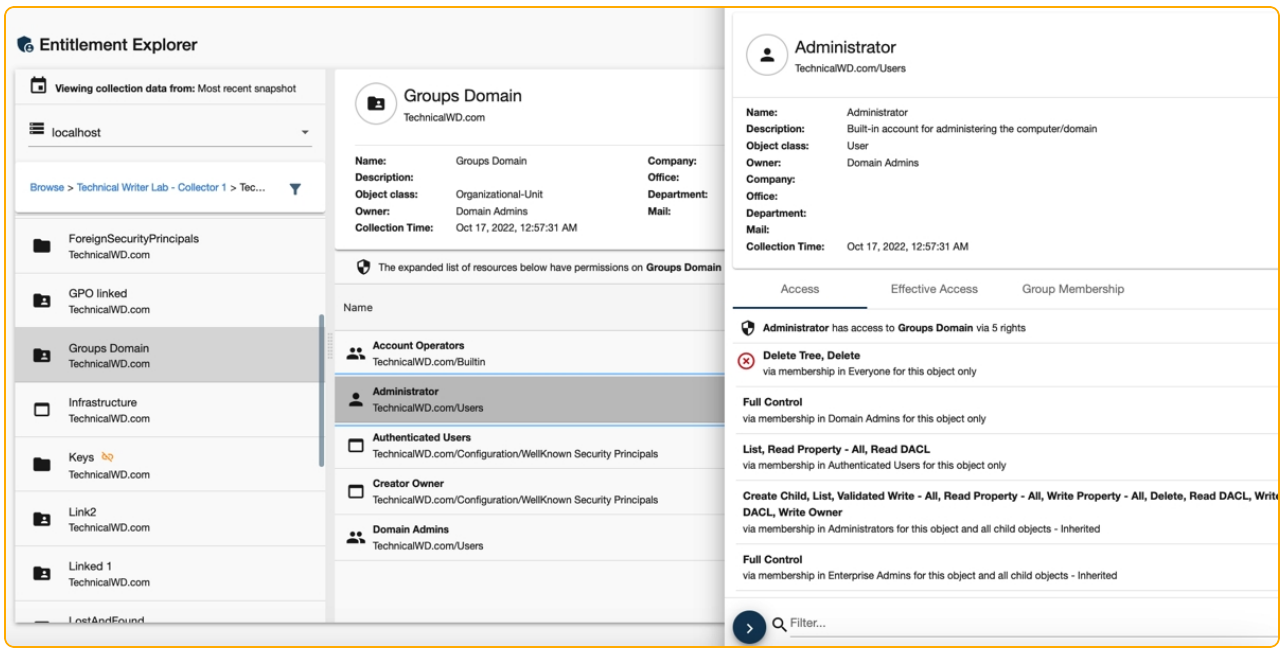
Trustees – Expanded Permissions

Use the **Trustees – Expanded Permissions** view to see effective permissions on a specified object. With the help of this view, you can discover effective permissions, including those inherited through group membership, and locate excessive permissions granted to sensitive OUs or groups.



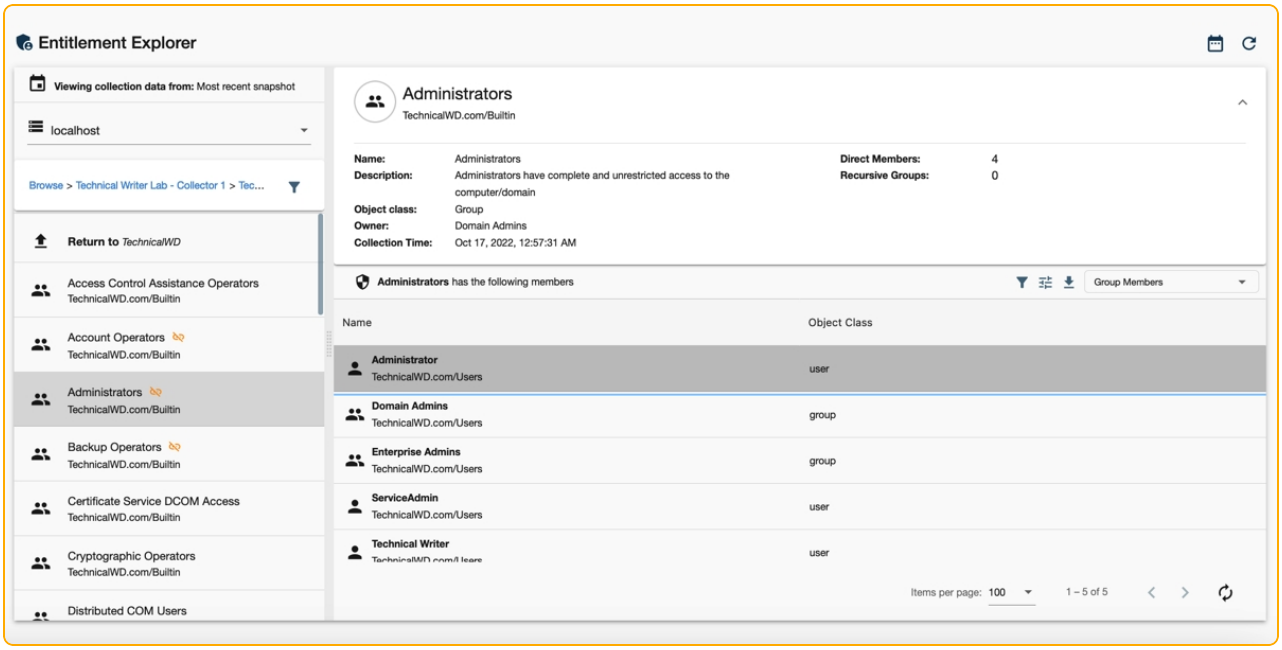
The full control, read, write, and delete permissions are marked visually for your convenience.

To learn more about the exact rights and group membership that resulted in a particular resource having rights to the object, select this resource to expand details.



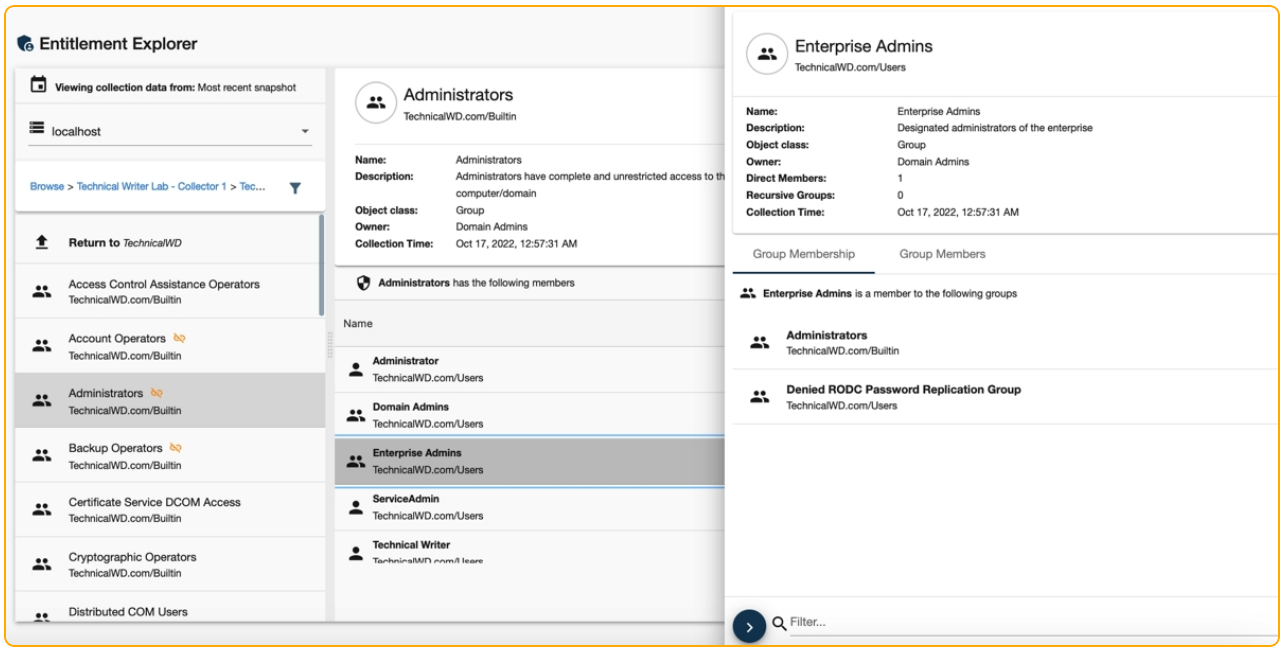
Group Members

Use the **Group Members** view to see the list of members of a particular group. For example, check who was ever a member of administrative groups such as Enterprise Admins or Domain Admins. Export the member list and save it as a PDF report for external auditors.



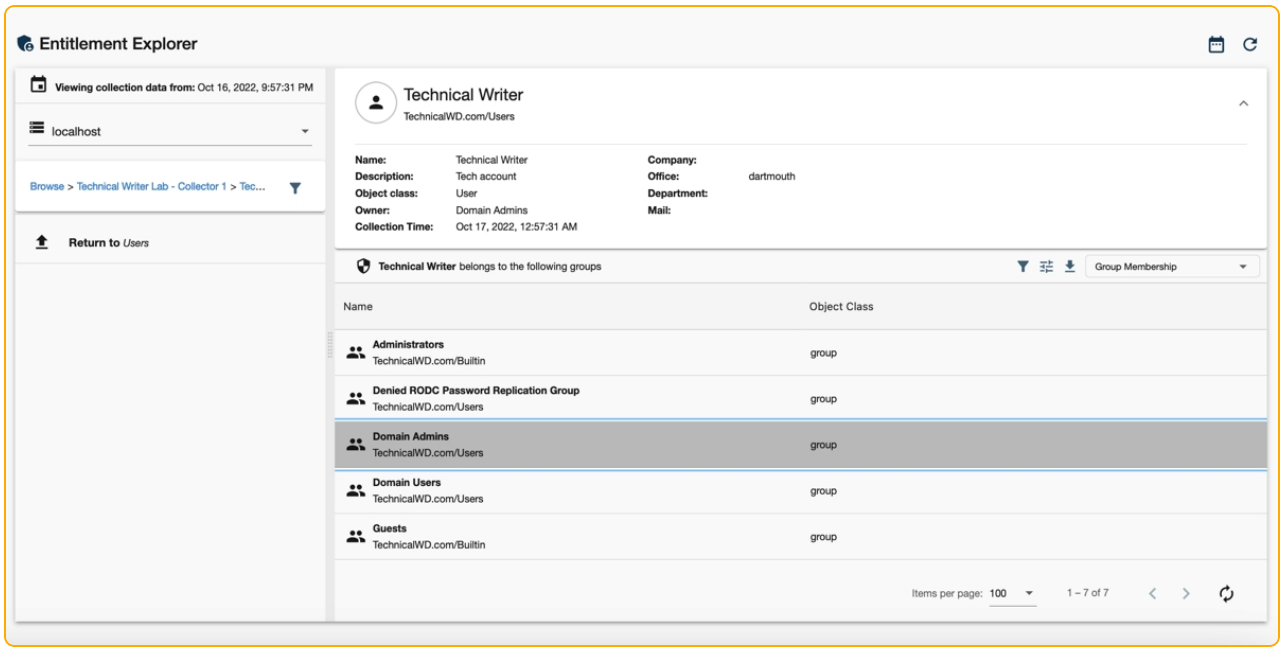
The full control, read, write, and delete permissions are marked visually for your convenience.

To learn more about the group membership and members of a specific resource, select this resource to expand details. For each resource, you can see the list of groups where the resource belongs to. For groups, you can also see a list of members.



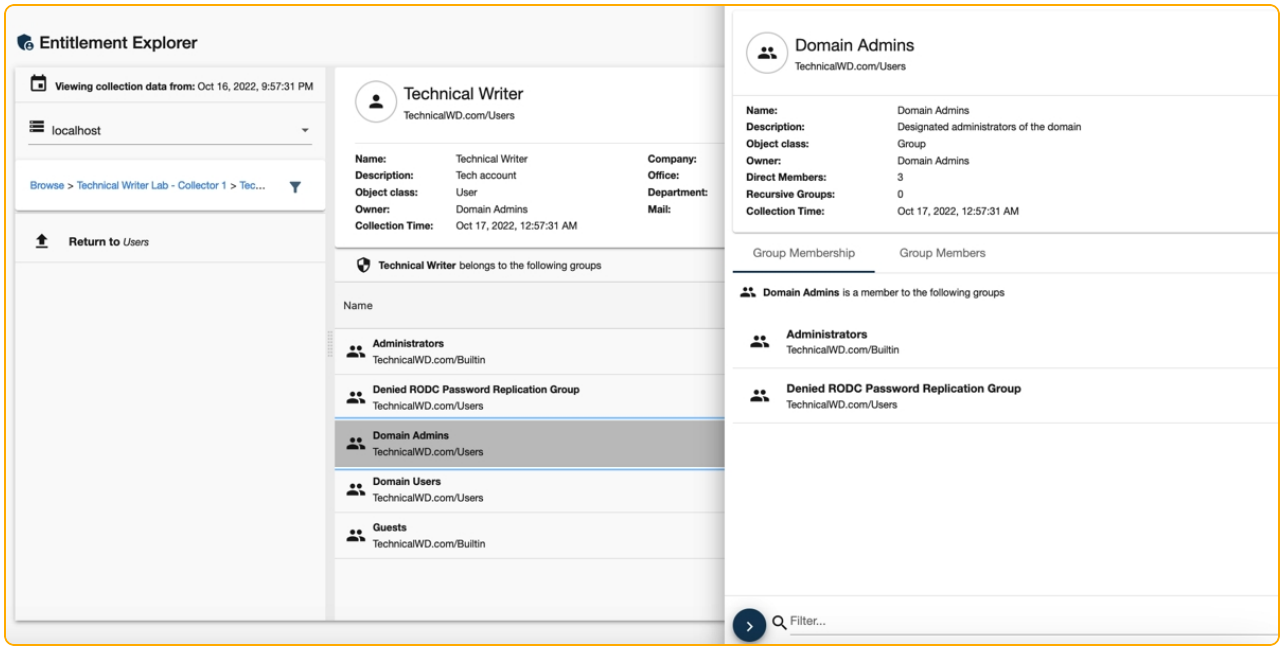
Group Membership

Use the **Group Membership** view to see the groups the object is a member of. Check if the object was ever granted administrative permissions via group membership. Export the group list and save it as a PDF report for external auditors.



The full control, read, write, and delete permissions are marked visually for your convenience.

To learn more about the group membership and members of a specific resource, select this resource to expand details. For each resource, you can see the list of groups where the resource belongs to. For groups, you can also see a list of members.



Entra ID Views

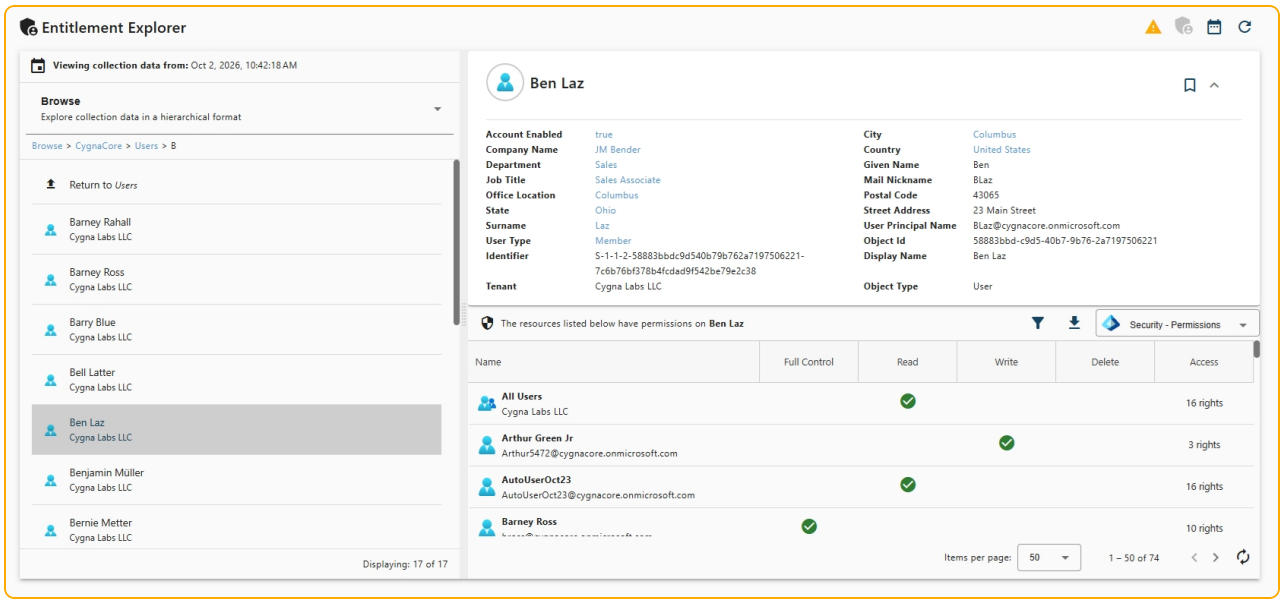
When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. Entra ID provides a considerably larger set of views than Active Directory, reflecting the range of roles, policies, and relationships that Entra ID maintains.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

The Entitlements – Access, Security – Permissions, Trustees – Expanded Permissions, Group Members, and Group Membership views apply to Entra ID objects as well as Active Directory objects. The remaining views are specific to Entra ID and are grouped by the kind of data they show:

- Ownership and Relationships–who owns, manages, and sponsors an object, and which devices a principal can reach.
- Roles and Privilege–role assignments and eligibility, role management policies, activation requirements, and effective privilege.
- Access Packages and Governance–access package governance, assignment policies, requestors and approvers, custom extensions, and terms of use.

- Applications–application credentials and restrictions, pre-authorized applications, application roles, and lock configuration.
- Policies–the principals, applications, locations, and authentication contexts a policy applies to, and the policies that apply to an object.
- Authentication Methods–authentication method policies and principals, and allowed authentication strength combinations.
- Consent and Admin Review–consent posture, condition sets, permission grant policies, and admin consent reviewers and their scopes.
- Agent Identities–agent identities, agent identity blueprints, and the applications that created them.
- Tenant Configuration–security defaults, external identities, guest and member default permissions, self-service sign-up, and device registration settings.
- Identity and Licensing–sign-in identities, security identifiers, license assignments, and administrative unit membership.



Ownership and Relationships

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views in this chapter describe how an object relates to other objects in your tenant–who owns it, who manages it, and what it can reach.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Relationship views come in pairs, so you can follow a relationship from either direction. For example, **Owners** lists the principals that own the selected object, while **Owned Resources** lists the objects that the selected principal owns.

Ownership

- **Owners**–the principals that own the selected object.
- **Owned Resources**–the resources that the selected principal owns.

Management

- **Managers**–the principals recorded as managers of the selected object.
- **Managed Resources**–the resources that the selected principal manages.

Sponsorship

- **Sponsors**–the principals that sponsor the selected object. Sponsors are typically used for guest and external identities.
- **Sponsored Resources**–the objects that the selected principal sponsors.

Devices

- **Owned Devices**–the devices that the selected principal owns.
- **Accessible Devices**–the devices that the selected principal can access.
- **Principals With Device Access**–the principals that can access the selected device.

Roles and Privilege

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover role assignments and eligibility, the policies that govern them, and the privilege a principal effectively holds.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Activation Requirements**–the resultant requirements a principal must satisfy to activate the selected role.
- **Assigned Role Eligibility Schedule**–the role eligibility schedule requests raised for the selected principal.
- **Assigned Scoped Roles**–the scoped role assignments held by the selected principal.

- **Effective Privilege**–the privilege the selected principal effectively holds once role assignments and eligibility are resolved.
- **Entitlement Role Actions**–the entitlement management actions permitted by the selected role.
- **Governed Roles**–the roles governed by the selected role management policy.
- **Role Actions**–the individual actions permitted by the selected role.
- **Role Eligibility**–the roles the selected principal is eligible to activate.
- **Role Eligibility Schedule**–the role eligibility schedule requests raised for the selected role.
- **Role Management Policy**–the role management policy that governs the selected role.
- **Role Members**–the principals assigned to the selected role.
- **Role Membership**–the roles assigned to the selected principal.
- **Role Policies**–the policies that apply to the selected role.
- **Rules**–the rules defined by the selected role management policy.
- **Scoped Role Members**–the principals that hold the selected role within an administrative unit scope.
- **Sign-In Requirements**–the resultant sign-in requirements that apply to the selected object.

Access Packages and Governance

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover entitlement management access packages: how they are governed, who may request them, and the terms of use they require.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Assignment Policies**–the assignment policies defined for the selected access package.
- **Custom Extensions**–the custom extensions invoked by the selected access package.
- **Governance**–the governance settings applied to the selected access package.
- **Policies Requiring Terms of Use**–the policies that require the selected terms of use.

- **Requestors and Approvers**–the principals that may request the selected access package, and those that approve requests.
- **Terms of Use**–the terms of use that the selected policy requires.

Applications

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover application registrations: the permissions they hold, the credentials they use, and the restrictions placed on them.



Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **API Permission**–the API permissions assigned to the selected application.
- **Application Role**–the application roles the selected object is assigned.
- **Application Role Assignments**–the application role assignments made against the selected application.
- **Application Timeouts**–the activity-based timeouts the selected policy sets for applications.
- **Assigned Application Roles**–the application roles assigned to the selected principal.
- **Credential Restrictions**–the credential restrictions that apply to the selected application.
- **Credentials**–the credentials registered for the selected application.
- **Federated Credentials**–the federated identity credentials registered for the selected application.
- **Idle Timeout**–the idle timeout that applies to the selected application.
- **Lock Configuration**–the lock configuration protecting the sensitive properties of the selected application.
- **Oauth2 Permission Scope**–the OAuth2 permission scopes the selected application exposes.
- **Pre-Authorized Applications**–the applications that the selected application pre-authorizes.
- **Pre-Authorized On**–the applications on which the selected application is pre-authorized.

Policies

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover how a policy relates to the principals, applications, locations, roles, and authentication contexts it applies to.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Application Policies**–the policies assigned to the selected application.
- **Assigned Applications**–the applications the selected object is assigned to.
- **Assigned Policies**–the policies assigned to the selected object.
- **Authentication Context Policies**–the policies that use the selected authentication context.
- **Authentication Contexts**–the authentication contexts the selected policy defines.
- **Authentication Strength Policies**–the policies that require the selected authentication strength.
- **Location Policies**–the policies that reference the selected location.
- **Policy Applications**–the applications the selected policy is assigned to.
- **Policy Authentication Strengths**–the authentication strength policies the selected policy requires.
- **Policy Locations**–the locations the selected policy is assigned to.
- **Policy Principals**–the principals the selected policy is assigned to.
- **Policy Roles**–the roles the selected policy is assigned to.
- **Principal Policies**–the policies assigned to the selected principal.

Authentication Methods

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover which authentication methods are available, who they apply to, and the combinations an authentication strength allows.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Allowed Combinations**–the authentication method combinations the selected authentication strength allows.
- **Authentication Method Policies**–the authentication method policies that target the selected principal.
- **Authentication Method Principals**–the principals the selected authentication method policy applies to.
- **Authentication Methods**–the authentication methods registered for the selected principal.
- **Methods**–the authentication methods configured for the selected policy.

Consent and Admin Review

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover how consent is granted and reviewed in your tenant.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Admin Consent Reviewer Scopes**–the policies for which the selected principal reviews admin consent requests.
- **Admin Consent Reviewers**–the reviewers responsible for admin consent requests for the selected policy.
- **Authorization Policies**–the authorization policies that enable the selected capability, or that assign the selected guest user role.
- **Condition Sets**–the condition sets defined by the selected permission grant policy.
- **Consent Posture**–the resultant consent posture for the selected object.
- **Permission Grant Policies**–the permission grant policies referenced by the selected authorization policy.
- **Referencing Authorization Policies**–the authorization policies that reference the selected permission grant policy.
- **Request Settings**–the admin consent request settings defined by the selected policy.

Agent Identities

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover agent identities, the blueprints they were created from, and the applications that created them.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Agent Identities**–the agent identities created from the selected blueprint.
- **Agent Identity Blueprint**–the blueprint the selected agent identity was created from.
- **Created Agent Identities and Blueprints**–the agent identities and blueprints created by the selected application.
- **Created By Application**–the application that created the selected agent identity or blueprint.

Tenant Configuration

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover tenant-wide settings that affect how identities, devices, and external access behave.

Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Default External Access**–the default cross-tenant access configuration.
- **External Identities**–the external identities settings configured for the tenant.
- **Guest User Role**–the guest user role the selected policy assigns.
- **Lifecycle**–the lifecycle settings applied to the selected group.
- **Member Default Permissions**–the default permissions the selected policy grants to members.
- **Partner Tenant**–the partner tenants configured in the cross-tenant access policy.
- **Registration Settings**–the device registration settings.
- **Security Defaults**–whether security defaults are enabled for the tenant.

- **Self-Service Sign-Up**–the self-service sign-up configuration.
- **Setting Values**–the setting values defined for the selected group.
- **Web Settings**–the web settings configured for the tenant.

Identity and Licensing

When you select an Entra ID object in the Entitlement Explorer, the lower section of the right-hand pane shows the views available for that object. The views described here cover sign-in identities, security identifiers, license assignments, and administrative unit membership.



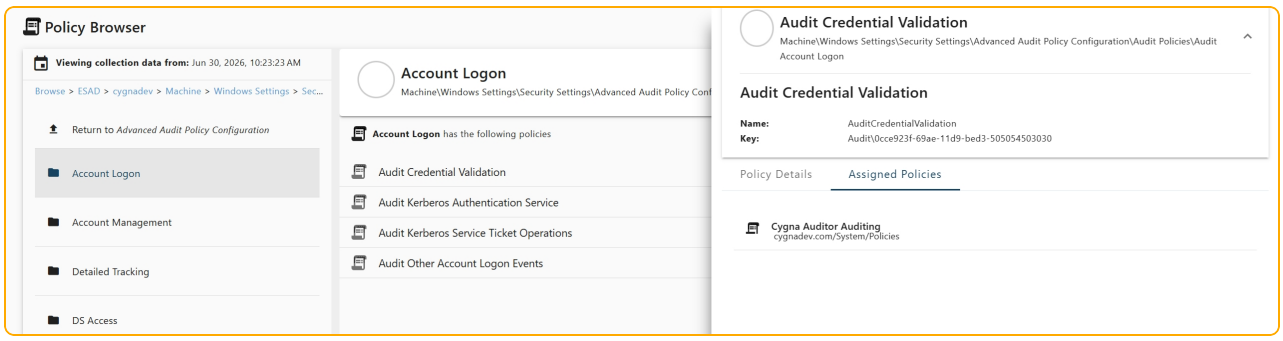
Note: Not every view is available for every object. Cygna Entitlement and Security shows only the views that apply to the type of object you selected.

Views

- **Administrative Unit Members**–the members of the selected administrative unit.
- **Administrative Unit Membership**–the administrative units the selected object belongs to.
- **License**–the licenses assigned to the selected object.
- **Licensed Object**–the objects the selected license is assigned to.
- **Security Identifiers**–the alternative security identifiers recorded for the selected object.
- **Sign-in Identities**–the identities the selected principal can sign in with.

Policy Settings

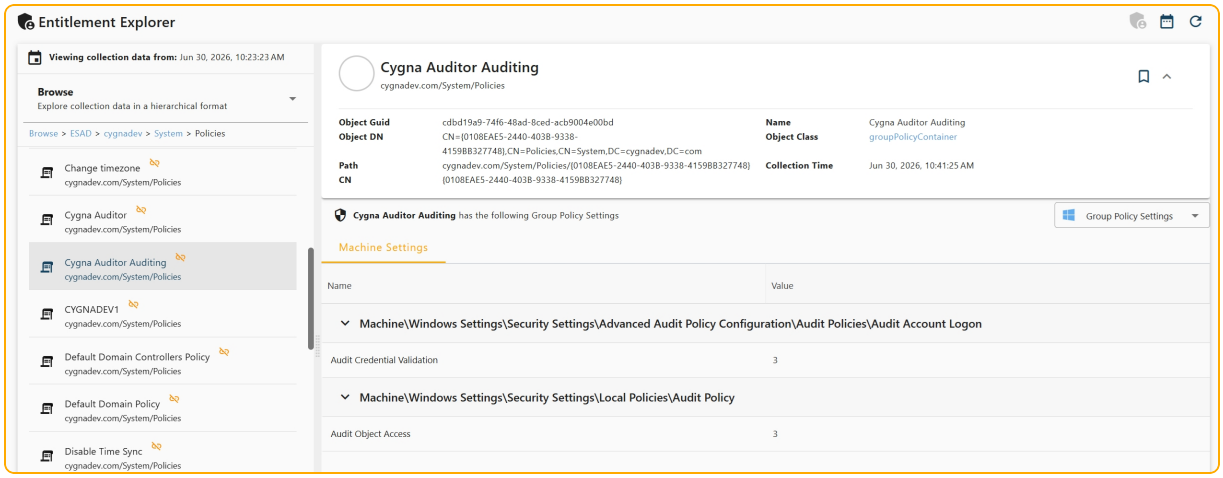
Policy Settings provides a reference of all GPO settings available for use in Group Policy Objects. Use it to understand what settings exist, which GPOs use any given setting, where GPOs are applied across your environment, and what policies are ultimately in effect for any given object.



Viewing GPO Settings and Links

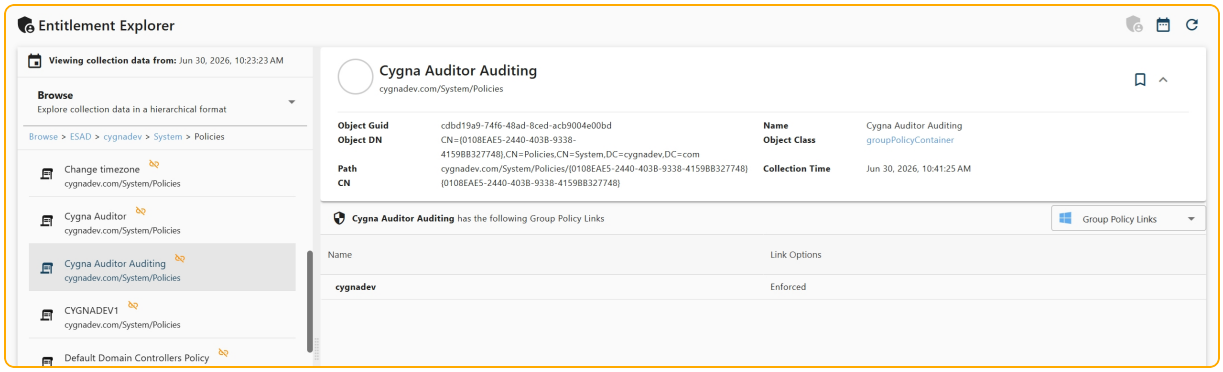
Selecting any setting in Policy Settings displays all GPOs that use that setting, making it easy to understand its scope across your environment. To inspect a specific GPO further, select it in the Active Directory module and use the following menu options:

- **Group Policy Settings** – displays all settings configured within the selected GPO.



- **Group Policy Links** – shows the domains where the selected GPO is linked, giving you

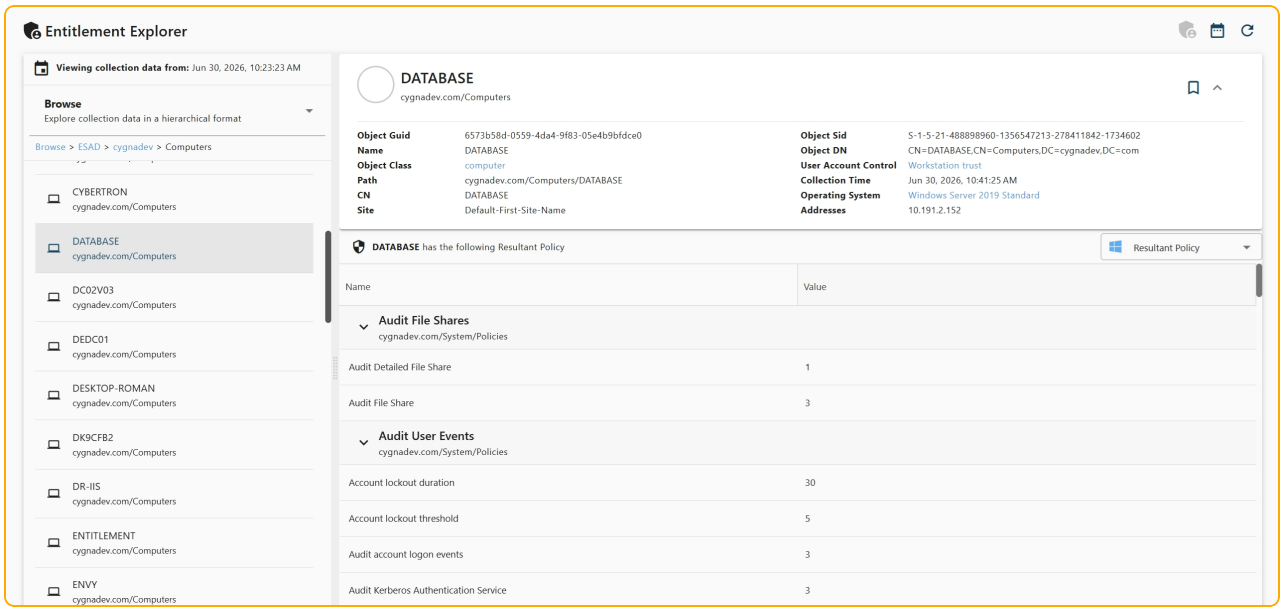
a clear picture of its scope across your environment.



Viewing Resultant Policy for an Object

When viewing a specific object, select the **Resultant Policy** menu option to see the effective GPO policy applied to that object – the combined result of all GPOs in scope. This allows administrators to confirm that the expected settings are being applied where they should be.

Select any individual setting in the Resultant Policy view to see which GPO or GPOs contributed to that setting being applied.



Auditing Policy Application Over Time

Policy Settings is not limited to current data. By adjusting the collection date, administrators can step back in time to see exactly which policies were in effect at any given point. This makes it straightforward to answer questions like whether a setting was applied before a change was made, or to confirm the state of an environment at the time of an incident.

Combined with the ability to trace any resultant setting back to its source GPO, administrators have a clear and auditable picture of what is applied, where it is applied, and how that has changed over time.

Index

A

Access Packages and Governance 48
Accounts 14
Active Directory 16
Agent Identities 52
Applications 49
Audit database
  Requirements 9
Authentication Methods 50

C

Consent and Admin Review 51

D

Database requirements 7
Delegation 19
Deployment, planning 7

E

Entitlement Explorer 33
  Entitlements - Access 40
  Entra ID views 45-53
  Explore data 37
  Group Members 43
  Group Membership 44
  How it works 33
  Security - Permissions 41
  Trustees - Expanded Permissions 42

G

Grant permissions 19

H

Hardware requirements 7

I

Identity and Licensing 53
Installation 17
  Ports 11

M

Managers 46

O

Ownership 46

P

Policies 50
Policy Settings 54
Ports 11
Product, launch 18

R

Reports 24
Reports, custom 25
Reports, understand fields 29
Reports, view 24
Roles and Privilege 47

S

Software requirements 7
Sponsors 46
System requirements 7

T

Tenant Configuration 52