AdminDroid

AdminDroid 365

Active Directory Auditing

Pre-Configuration Guide

Table of Contents

Active Directory Auditing
Pre-Configuration Guide

AdminDroid Active Directory management tool helps monitor critical activities across your Active Directory environment. However, certain configurations must be enabled in Active Directory to ensure the required events are recorded and available for tracking.

Without these pre-configurations, important Active Directory domain activities may not be logged, resulting in limited visibility and incomplete audit reports.

Required Pre-Configurations in Active Directory

AdminDroid Active Directory auditing tool relies on Windows Security event logs to audit Active Directory activities. The following configurations ensure that the required events are generated and can be collected successfully.

1. Advanced Audit Policies

Advanced Audit Policy configuration provides granular control over which activities are recorded in the Windows Security event log. Configuring these policies ensures that the required Active Directory activities are captured for auditing.

2. Windows Firewall Rules

To enable remote collection of event logs, domain computers must allow specific inbound Windows firewall connections. These firewall rules allow AdminDroid to remotely collect, monitor, and centrally access security event logs.

3. Object-Level Auditing (SACLs)

Object-level auditing uses System Access Control Lists (SACLs) to define which operations on selected Active Directory resources are audited. It enables detailed tracking of changes made to selected objects, containers, and directory partitions.

Now, let's walk through the steps required to configure the Active Directory environment for AdminDroid AD Reporter.

Configure Active Directory Auditing Prerequisites

You can configure the required Active Directory auditing prerequisites using one of the following methods:

- Manual Configuration (Active Directory consoles)
- Automated Configuration (AdminDroid)

Manual Configuration Of Active Directory Auditing Pre-Configuration

This section explains how to manually configure the required auditing policies and settings directly in Active Directory. Here, you will configure:

1. Advanced Audit Policies
2. Windows Firewall rules
3. Object-level auditing

Before proceeding, make sure you have the required permissions to configure auditing in your domain.

- Permission to create or update Group Policy Objects.
- Permission to create and manage Active Directory groups.

1. Configure Active Directory Advanced Audit Policies

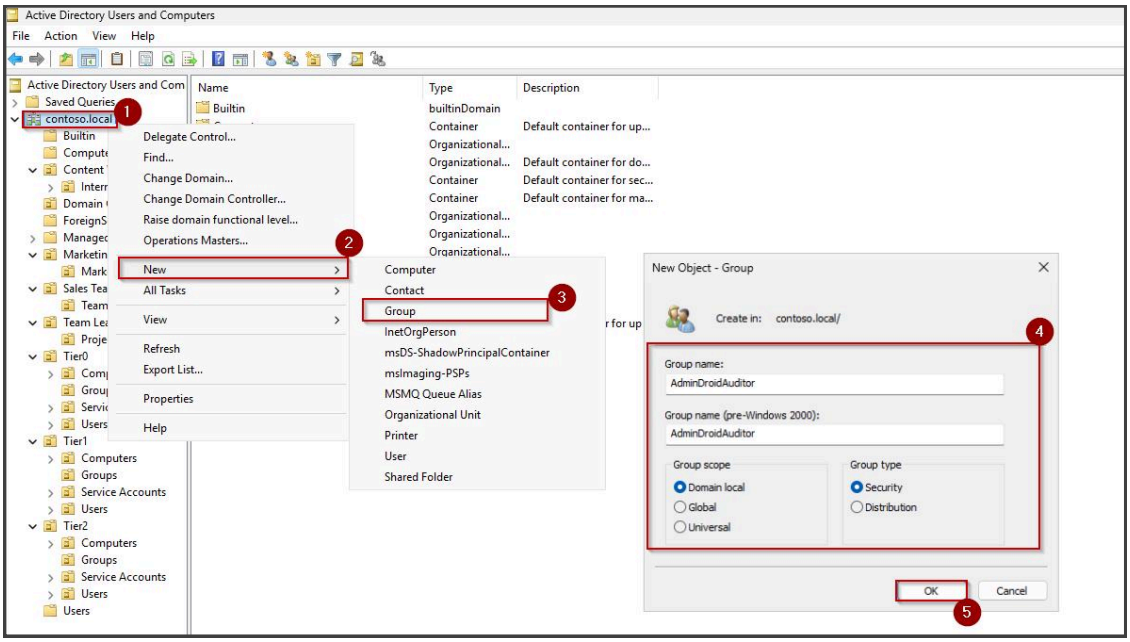
Follow the steps below to manually configure Advanced Audit Policies in the Active Directory environment.

Step 1.1: Create a Security Group in Active Directory

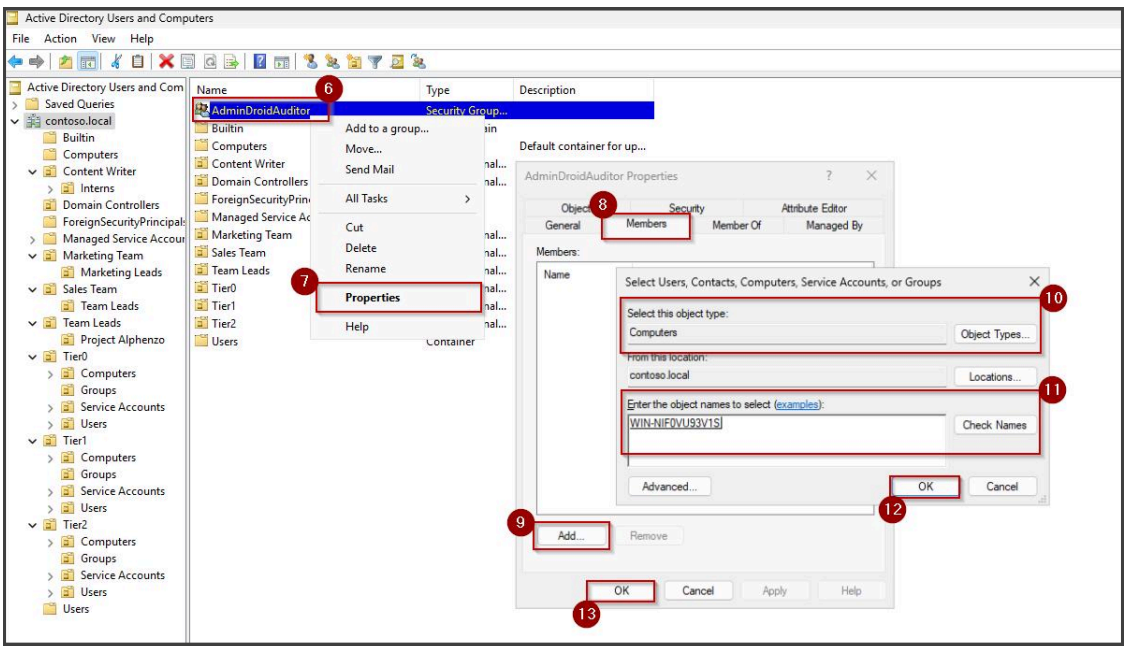
Create a dedicated security group and add all computers that need to be audited through AdminDroid. Using a security group helps apply the auditing GPO only to the required systems instead of the entire domain.

1. Open **Active Directory Users and Computers** (ADUC).
2. Right-click the domain name, select **New**, then choose **Group**.
3. Name the group (e.g., AdminDroidAuditor) and ensure the **Group Scope** is set to Domain local and the **Group Type** is Security.

4. Then, click **OK** to complete the group creation.



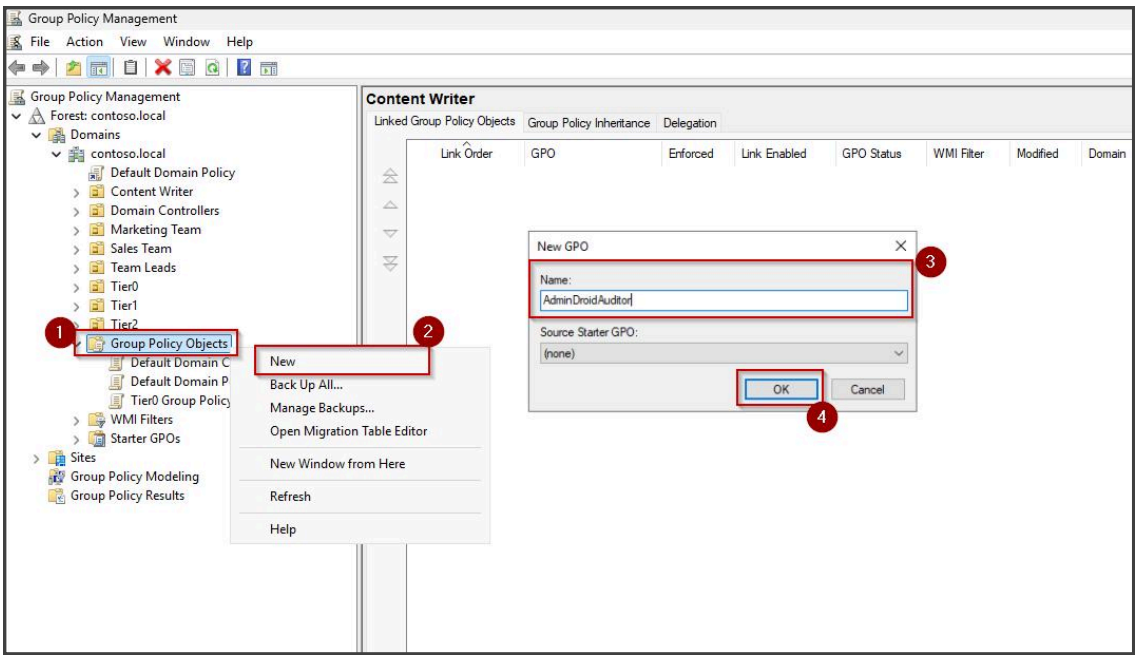
5. Once created, right-click the newly created group and choose **Properties**.
6. Navigate to the **Members** tab and click **Add**.
7. Click **Object Types**, choose **Computers**, and click **OK**.
8. Enter the names of the computers you wish to audit and click **Check Names** to verify them.
9. Click **OK** to add them to the list. Repeat these steps until all required computers are included in the group.
10. Once finished, click **OK** to save your changes and close the Properties window.



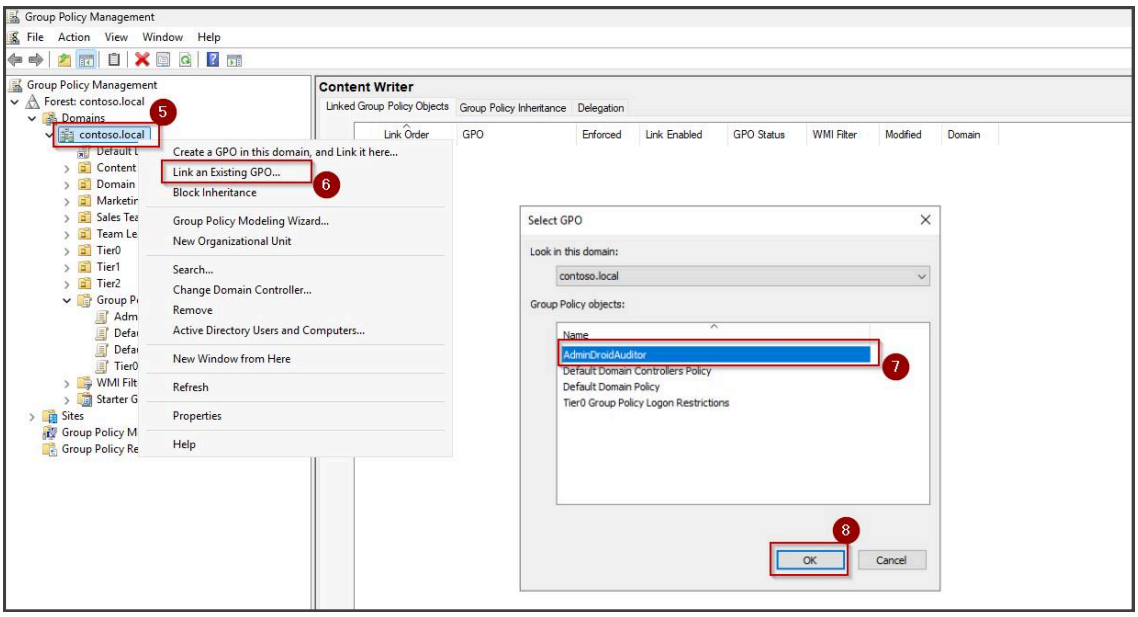
Step 1.2: Create a Group Policy Object in Active Directory

Once the security group is ready, you need to create a GPO to host the audit settings and link it to your domain.

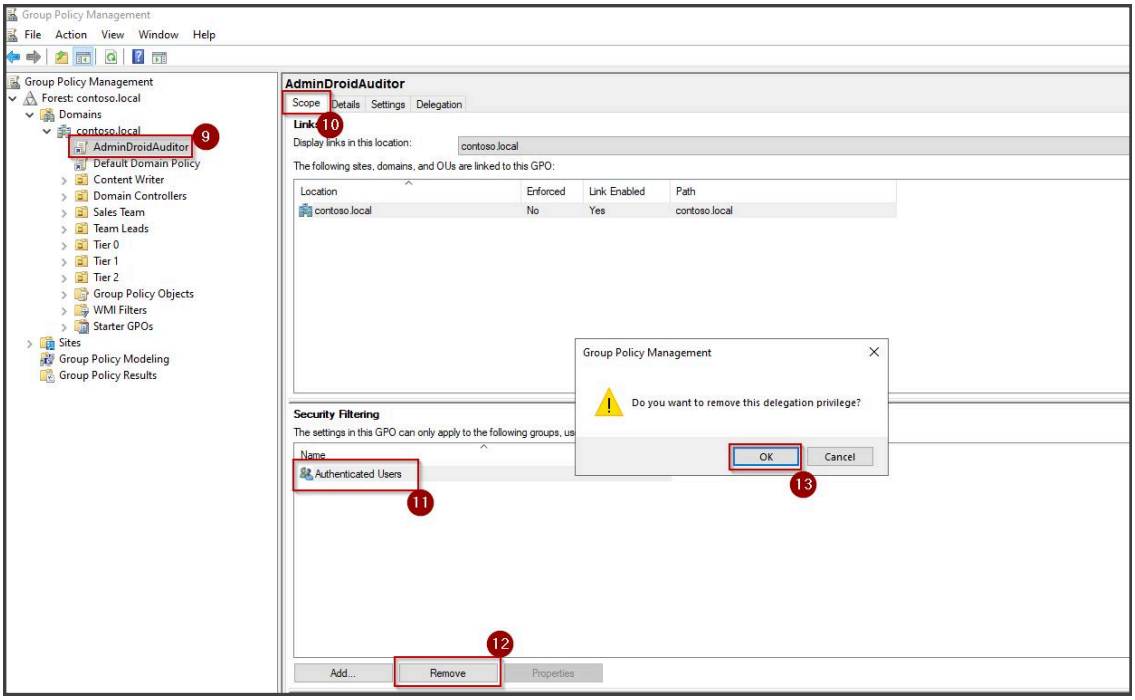
1. Open the **Group Policy Management Console.**
2. Expand the Forest, then expand Domains, and right-click **Group Policy Objects** container.
3. Select **New**, enter a meaningful name for the GPO (e.g., AdminDroidAuditor), and click **OK**.



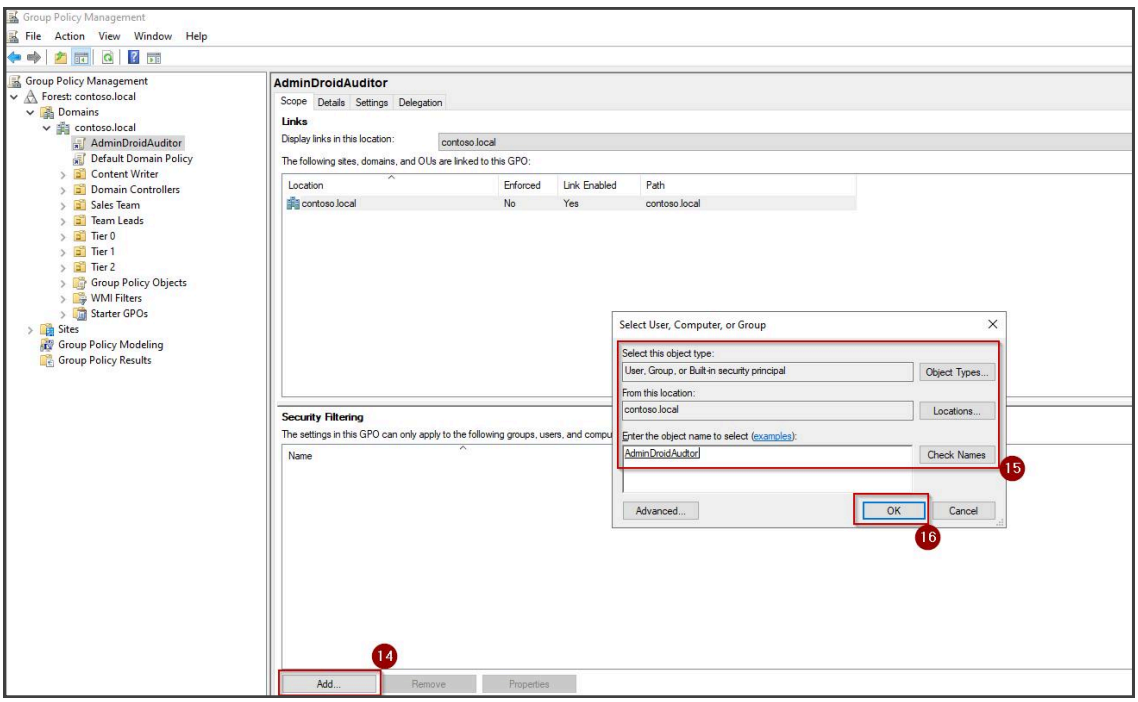
4. Right-click your domain name and click **Link an Existing GPO.**
5. From the Group Policy objects list, choose the GPO you just created and click **OK**.



6. Then, select the newly linked GPO and go to the **Scope** tab.
7. Here, click **Authenticated Users** under 'Security Filtering', choose **Remove**, and click **Yes** in the confirmation prompt.



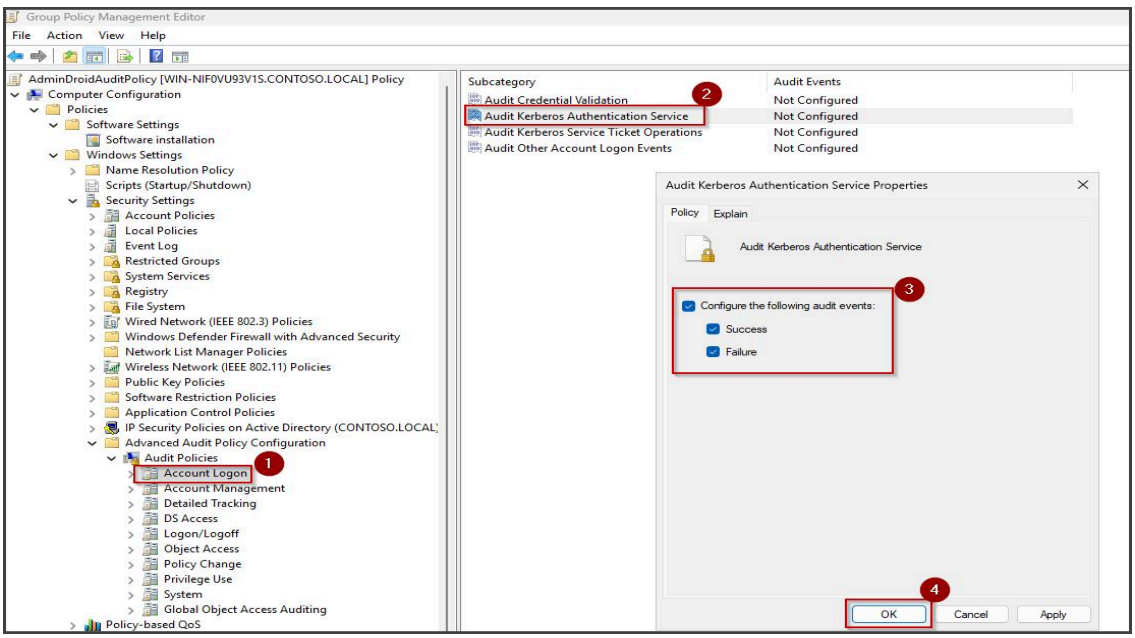
8. Then, click **Add** and type the name of the security group (AdminDroidAuditor) you created, and click **OK**.



Step 1.3: Enable Advanced Audit Settings in the Active Directory GPO

The newly created GPO does not yet enforce any Advanced Audit Policy settings. Configure the required audit policy categories and subcategories by following the steps below to ensure the necessary security events are recorded in your domain.

1. Right-click the newly created GPO (AdminDroidAuditor) and click **Edit** to open the Group Policy Management Editor.
2. Navigate to *Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies*.
3. Select **Account Logon** and double-click “Audit Kerberos Authentication Service”.
4. Select **Configure the following audit events**, enable Success and Failure, and then click **OK**.



5. Repeat steps 3 and 4 for all required audit subcategories by navigating through each category. Then, enable the Success and Failure as specified in the configuration table below.

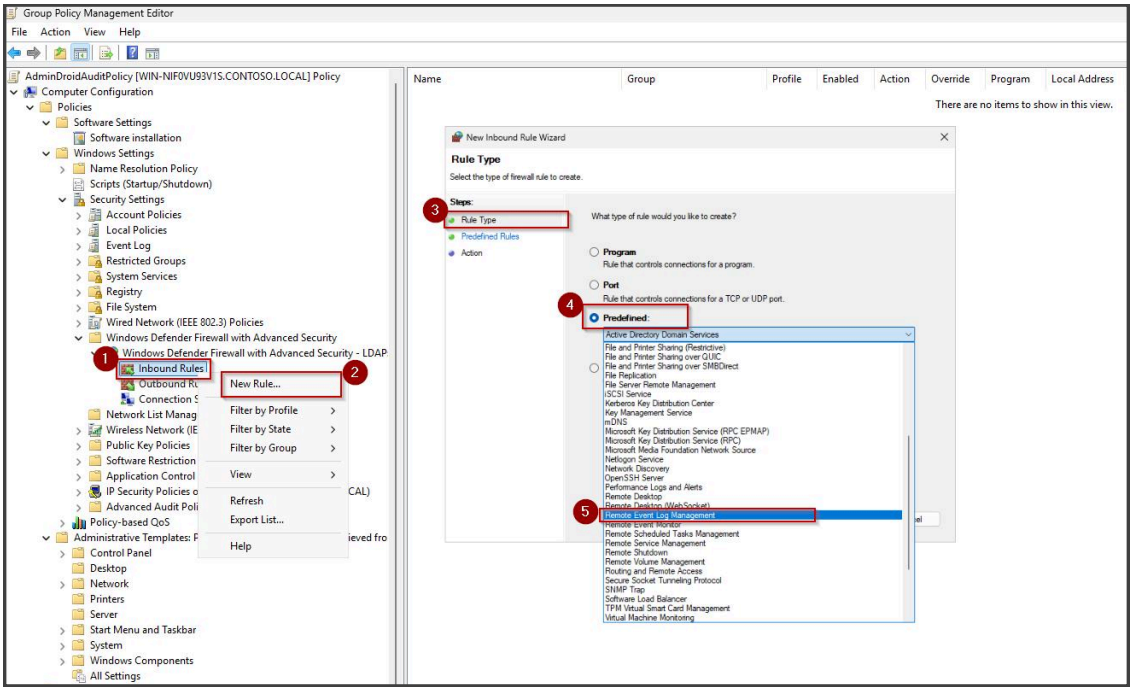
Microsoft 365 Application	Subcategory	Refresh frequency
Account Logon	Kerberos Authentication Service	Success and Failure
	Kerberos Service Ticket Operations	Success and Failure
Account Management	User Account Management	Success and Failure
	Computer Account Management	Success
	Distribution Group Management	Success

	Security Group Management	Success
	Other Account Management	Success
Detailed Tracking	Process Creation	Success
	Process Termination	Success
	PNP Activity	Success
DS Access	Directory Service Access	Failure
	Directory Service Changes	Success
Logon/Logoff	Account Lockout	Failure
	Group Membership	Success
	Logoff	Success
	Logon	Success and Failure
	Other Logon/Logoff	Success and Failure
	Special Logon	Success
Policy Change	Audit Policy Change	Success
	Authentication Policy Change	Success
	MPSSVC Rule Level Policy Change	Success and Failure
	Other Policy Change	Failure
Privilege usage	Sensitive Privilege Use	Success and Failure
	Non-Sensitive Privilege Use	Failure
Object Access	Other Object Access Events	Success and Failure
	Removable Storage	Success and Failure
System	Security State Change	Success
	Security System Extension	Success
	System Integrity	Success and Failure
	Other System Events	Success and Failure

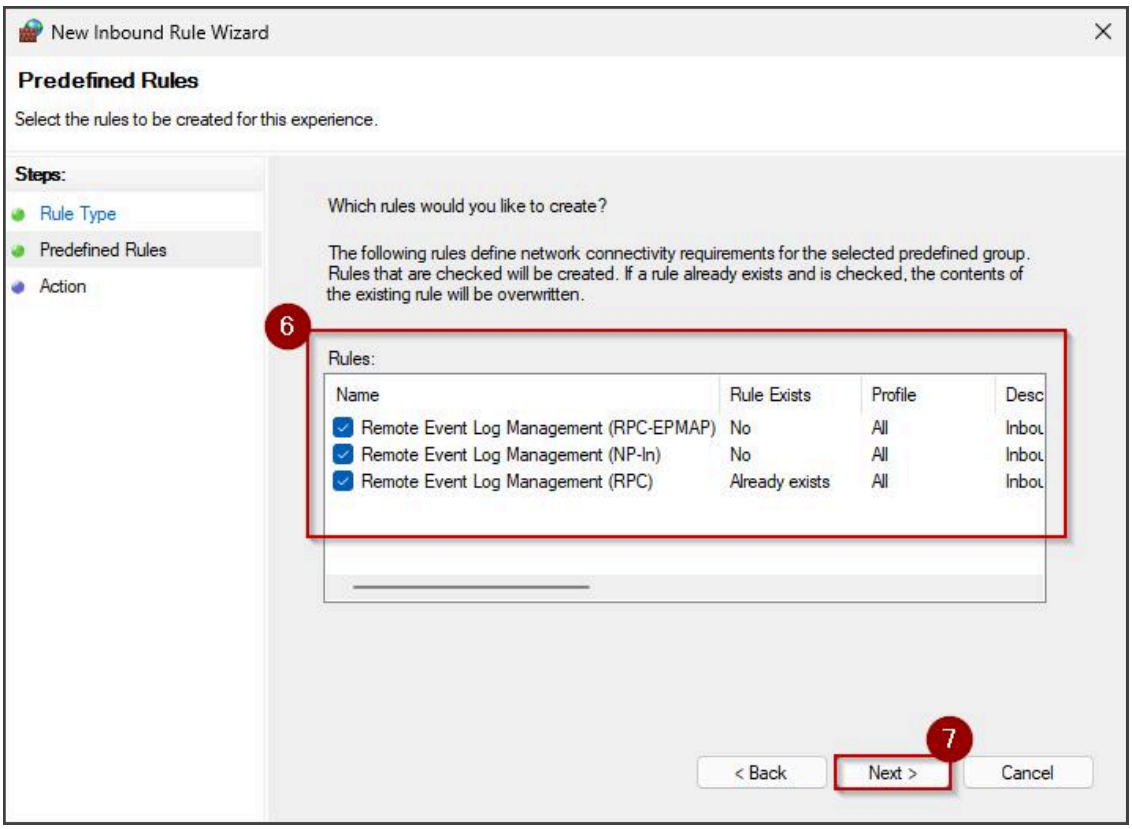
2. Configure Firewall Rules For Remote Event Log Collection

Once audit policies are configured, follow the steps below to enable the required firewall rules in the GPO.

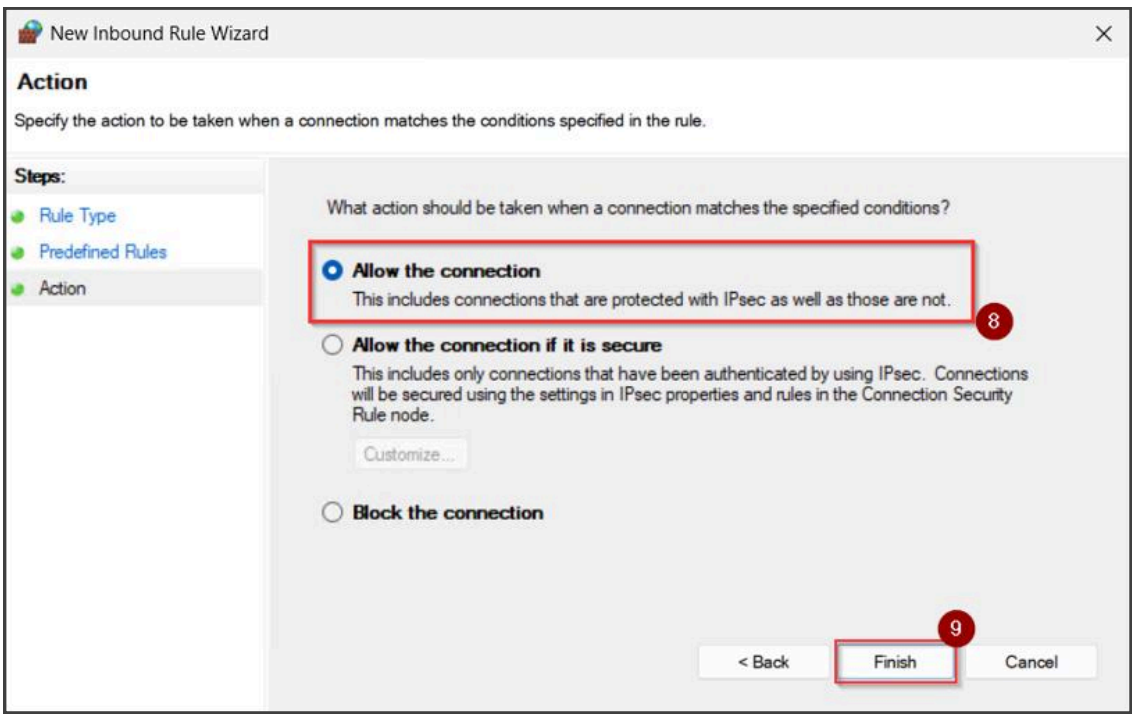
1. Right-click the newly created GPO (AdminDroidAuditor) and click **Edit**.
2. In the Group Policy Management Editor, navigate to the following path: *Computer Configuration > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security > Windows Defender Firewall with Advanced Security - LDAP value > Inbound Rules.*
3. Right-click **Inbound Rules** in the left pane and select **New Rule**.
4. In the Rule Type window, select **Predefined**, choose “Remote Event Log Management”, and then click **Next**.



5. In the Predefined Rules window, ensure the following three rules are selected and hit **Next**.
   a. Remote Event Log Management (RPC-EPMAP)
   b. Remote Event Log Management (NP-In)
   c. Remote Event Log Management (RPC)

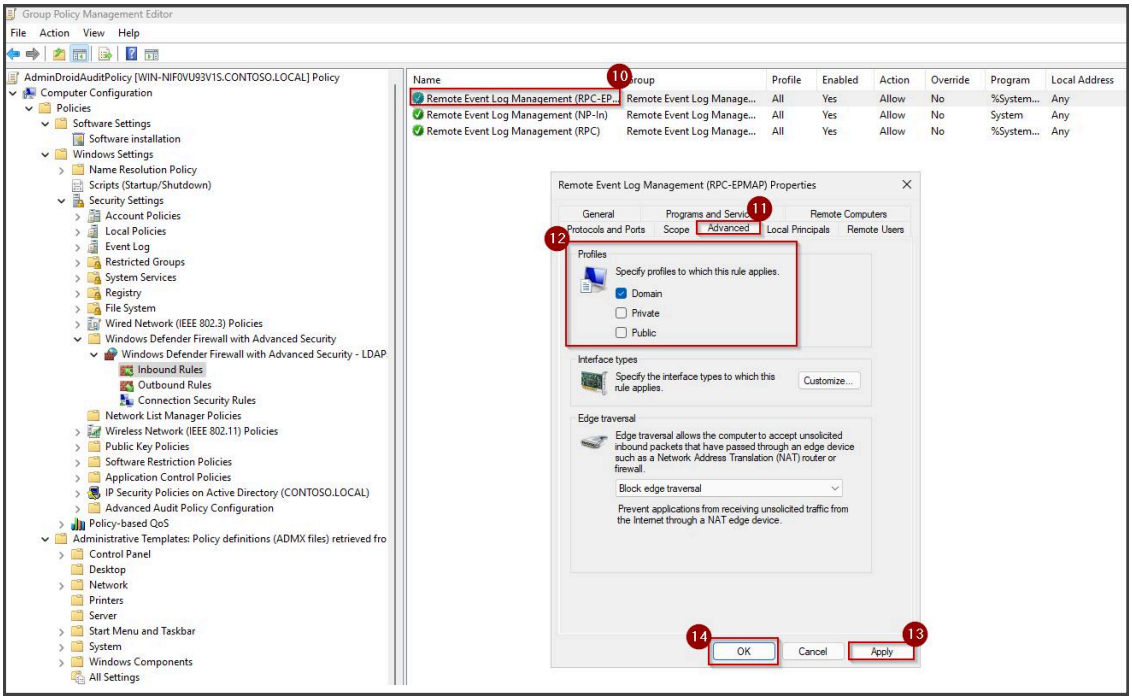


6. Select **Allow the connection** and select *Finish*. This will create all the required inbound firewall rules within the GPO.



By default, these rules apply to Domain, Private, and Public profiles. For better security, limit these rules to the **Domain** profile only.

7. Double-click the each newly created firewall rule and go to the **Advanced** tab.
8. Deselect Private and Public, leaving only **Domain** selected.
9. Click **Apply** and then “OK” to save the changes.



This completes the required firewall rules pre-configuration in your Active Directory domain.

3. Configure Object-Level Auditing In Active Directory

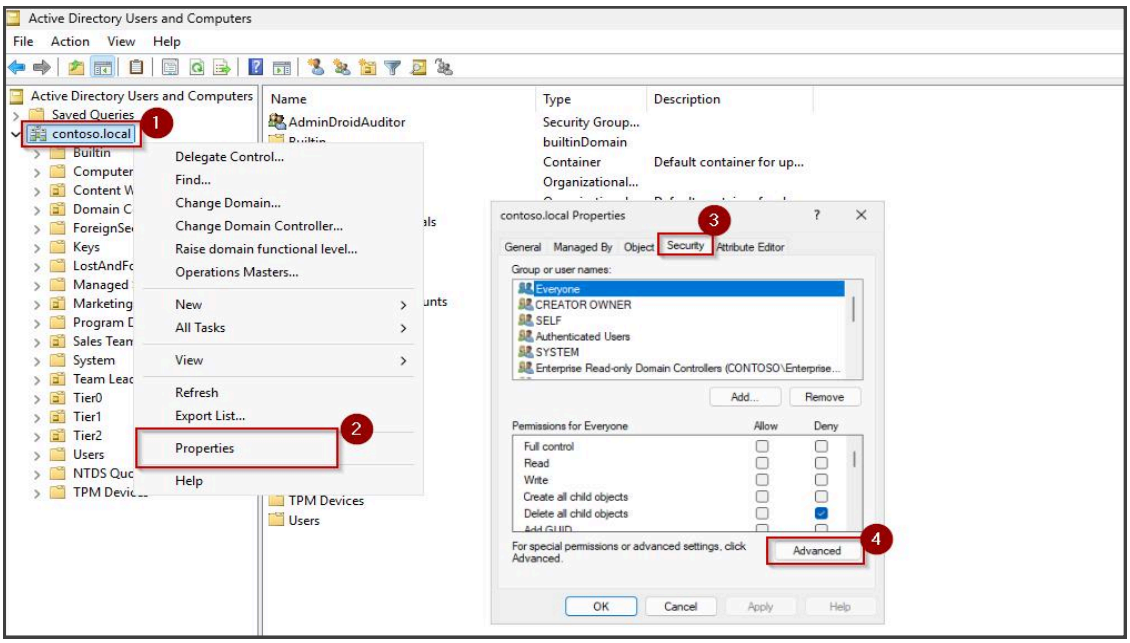
Follow the steps below to enable auditing for the applicable Active Directory objects in your domain. You’ll configure auditing for the following objects:

1. Active Directory domain objects
2. Active Directory containers
3. Password Settings Objects (PSOs)
4. Active Directory partitions

Step 3.1: Active Directory Domain Objects

Enable object-level auditing for Active Directory domain objects to maintain a complete audit trail of changes to users, groups, computers, and organizational units (OUs) across your domain.

1. Log in to the domain controller with the admin credentials.
2. Open Active Directory Users and Computers, right-click your domain, and select **Properties.**
3. Select the **Security** tab, and then click “Advanced”.

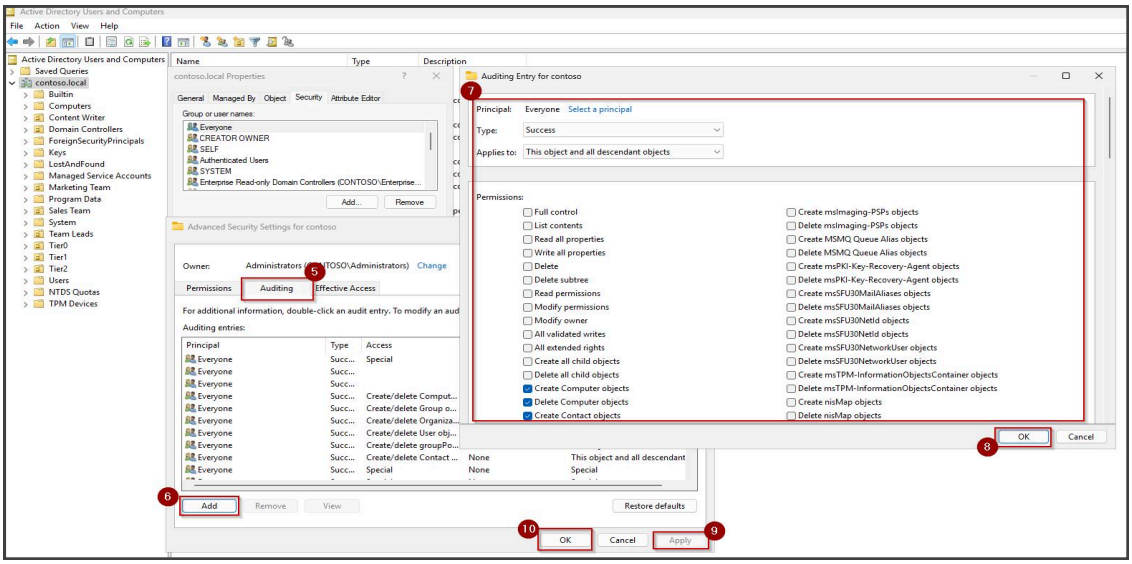


4. Go to the **Auditing** tab and select **Add**.
5. Click Select a principal, choose **Everyone**, and set Type to **Success**.
6. Configure Permissions and Applies to as listed in the following audit configuration table.

Applies to	Permissions
This object and all descendant objects	• Create User objects • Delete User objects • Create Group objects • Delete Group objects • Create Computer objects • Delete Computer objects • Create Contact objects • Delete Contact objects • Create Organizational Unit objects • Delete Organizational Unit objects • Create groupPolicyContainer objects • Delete groupPolicyContainer objects
Descendant User objects	• Write all properties • Delete • Modify permissions • All extended rights

Descendant Group objects	• Write all properties • Delete • Modify permissions • All extended rights
Descendant Computer objects	• Write all properties • Delete • Modify permissions • All extended rights
Descendant Contact objects	• Write all properties • Delete • Modify permissions
Descendant groupPolicyContainer objects	• Write all properties • Delete • Modify permissions
Descendant Organizational Unit objects	• Write all properties • Delete • Modify permissions

7. After configuring each entry in the above table, click **OK** in the Auditing Entry window and select **Apply** to save it. Then click **Add** again on the Security Settings window to configure the next permission set. Continue this process until all listed entries are configured.
8. Then, click **OK** in the Advanced Security Settings window to save the configuration changes.

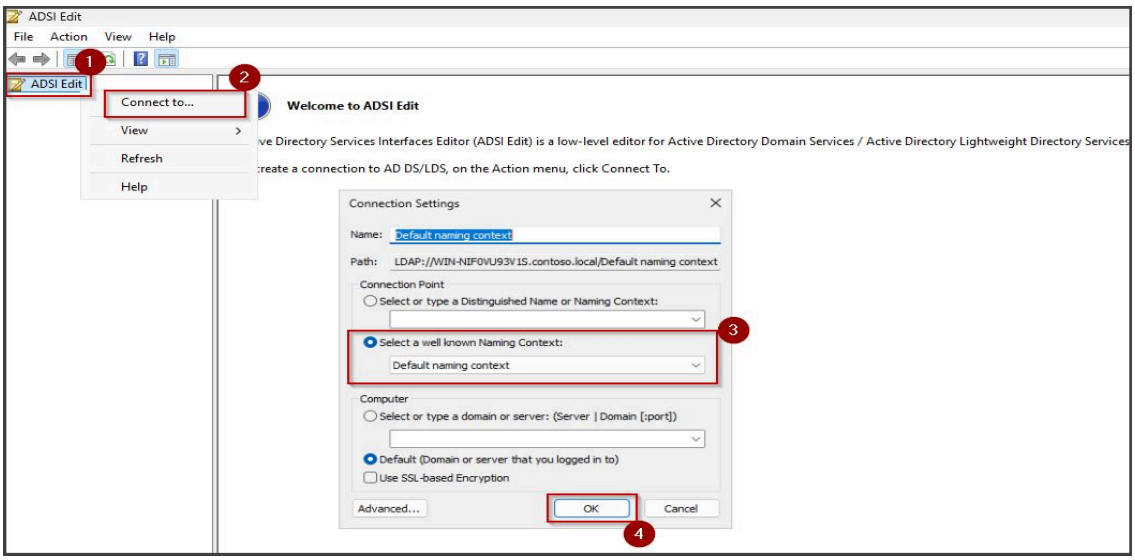


Step 3.2: Active Directory Container Objects

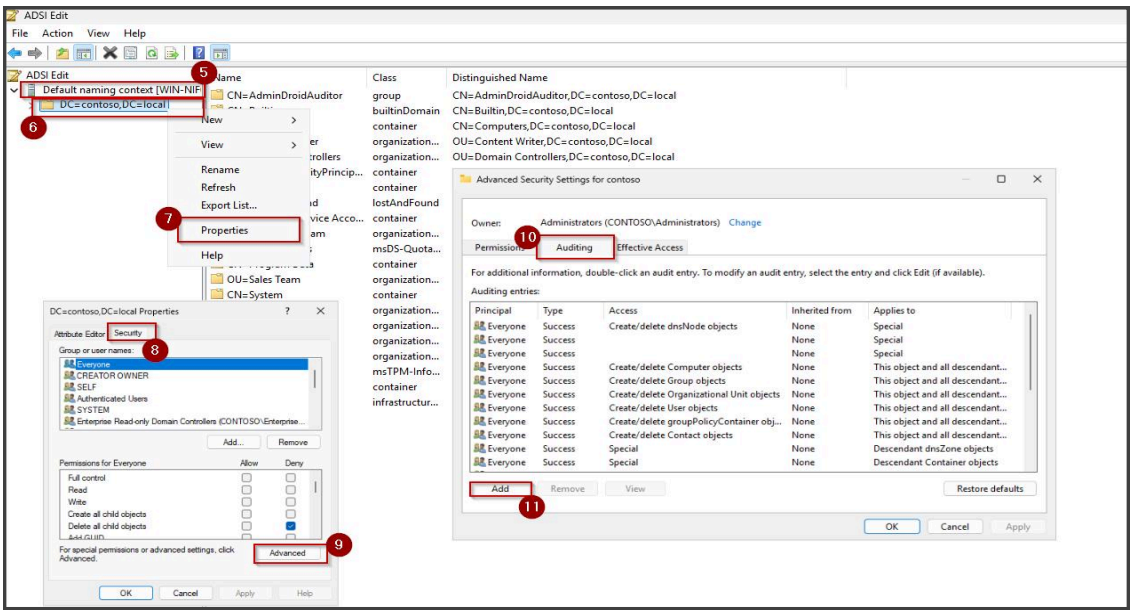
Active Directory containers store critical domain-wide configuration data that is not associated with standard domain objects such as users, groups, computers, or organizational units. Configuring object-level auditing for these containers helps ensure that changes to these resources are recorded.

Follow the steps below in the ADSI Edit console to enable auditing for directory containers.

1. Open Server Manager on a domain controller and go to Tools > ADSI Edit.
2. Right-click **ADSI Edit** and select **Connect to**.
3. Under “Select a well known Naming Context”, choose the **Default naming context**, and select **OK**.

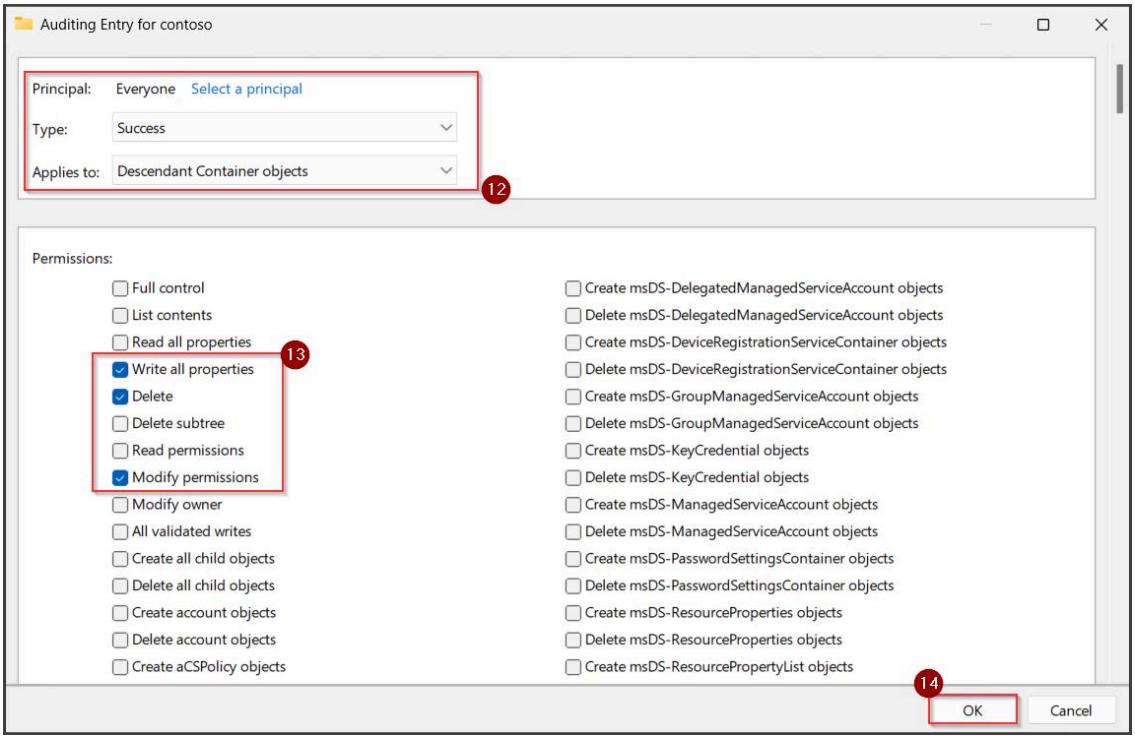


4. In the left pane, expand the naming context and right-click the domain distinguished name.
5. Go to *Properties > Security > Advanced > Auditing*.



6. Click **Add** and enter the following appropriate audit entry and select **OK**.

Principal	Type	Applies to	Permission
Everyone	Success	Descendant Container Objects	• Write all properties • Delete • Modify permissions

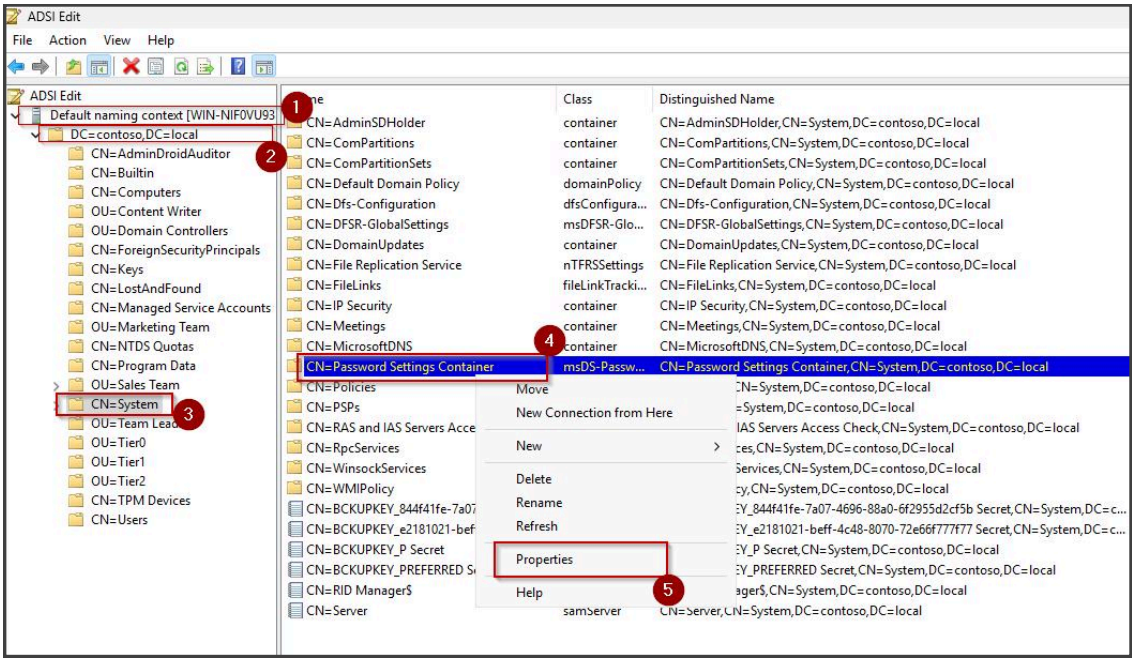


7. Then, click **Apply** and **OK** in the **Advanced Security Settings** window to save the changes.

Step 3.3: Active Directory Password Setting Objects

The Password Settings Container stores Password Settings Objects (PSOs), which define Fine-Grained Password Policies (FGPPs) for users and groups. Enable auditing for this container to track changes to password and account lockout thresholds that could impact your domain's security.

1. In ADSI Edit, expand the default naming context configured above for the container object.
2. Expand the domain distinguished name and select **CN=System.**
3. Right-click ‘CN=Password Settings Container’ and select **Properties.**



4. Navigate to *Security > Advanced > Auditing* and click **Add**.
5. Configure the following password settings container audit entries and click **OK**.

Principal	Type	Applies to	Permission
Everyone	Success	This object and all descendant objects	• Create msDS-PasswordSettings objects • Delete msDS-PasswordSettings objects
		Descendant msDS-PasswordSettings objects	• Write all properties • Delete • Modify permissions

6. Click **Apply** to save the configuration, and then click **OK** to close the **Advanced Security Settings** window.

Step 3.4: Active Directory Partitions

Follow the steps below to configure object-level auditing for Active Directory partitions, including the Configuration, Schema, and DNS partitions.

Step 3.4.1: Configuration Partition

1. Right-click ADSI Edit and select **Connect to**.
2. Under 'Select a well known Naming Context', choose **Configuration**.
3. Right-click the Configuration naming context and select **Properties**.
4. Go to *Security > Advanced > Auditing* and click **Add**.
5. Then, add the following audit entry and click **OK**.

Principal	Type	Applies to	Permission
Everyone	Success	This object and all descendant objects	• Create all child objects • Write all properties • Delete all child objects • Delete • Modify permissions • All extended rights

6. Click **Apply** in the **Advanced Security Settings** window, and then click **OK** to save and close the configuration window.

Step 3.4.2: Schema Partition

1. Right-click ADSI Edit in the left pane and select 'Connect to'.
2. Choose **Schema** under "Select a well known Naming Context".
3. Right-click the Schema partition and select **Properties**.
4. Navigate to *Security > Advanced > Auditing* and add the following audit entry.

Principal	Type	Applies to	Permission
Everyone	Success	This object and all descendant objects	• Create all child objects • Write all properties • Delete all child objects • Delete • Modify permissions • All extended rights

5. Select **OK**, and then select **Apply** and 'OK' in the Advanced Security Settings to save the changes.

Step 3.4.3: DNS Zones and Nodes

1. Right-click on ADSI Edit and select **Connect to.**
2. Choose **Select or type a Distinguished Name or Naming Context** under Connection Point.
3. Enter the distinguished name based on the partition where DNS zones are stored (domain or forest) and select **OK**.

Based on the partition you selected, choose the specific option

4. Type: Distinguish name of the domain
   - Click on the **Default naming context** you created and right-click the root (domain).
   - Go to *Properties > Security > Advanced > Auditing* and click **Add**.
   - Add the audit entry in the table below and select **OK**.
   - Then, select **Apply** and then **OK** to save the changes.

5. Type: Forest or Domain DNS Zones
    - Click the naming context you created and expand the DNS Zone.
    - Right-click on **CN=MicrosoftDNS** and select **Properties**.
    - Go to *Security > Advanced > Auditing* and click **Add**.
    - Add the appropriate permissions mentioned in the table below and select **OK**.
    - Click **Apply** to save the configuration, and then click **OK** to close the **Advanced Security Settings** window.

Principal	Type	Applies to	Permission
Everyone	Success	This object and all descendant objects	• Create dnsZone objects • Delete dnsZone objects • Write all properties • Delete • Modify permissions
		Descendant dnsZone objects	• Write all properties • Delete • Modify permissions • Create dnsNode objects • Delete dnsNode objects
		Descendant dnsNode objects	• Write all properties • Delete • Modify permissions

By completing these configurations, you have ensured that critical Active Directory object changes are consistently logged and available for auditing. AdminDroid can now collect and display detailed activity data, allowing you to monitor changes, investigate events, and maintain better security oversight across your domain.

Automate Active Directory Auditing Prerequisites With AdminDroid

Manually configuring Active Directory auditing requires navigating multiple management tools and applying several settings individually. AdminDroid simplifies this process by automatically configuring the required auditing settings with just a few clicks. Once configured, AdminDroid can collect and present a complete picture of activities across your domain, without gaps.

AdminDroid automates the following configurations in your Active Directory domain.

1. Advanced Audit Policy & Firewall configuration
2. Object-level auditing configuration

1. Automatically Configure Advanced Audit Policies & Firewall Rules

Here's a quick overview of what happens when you set up configuration with AdminDroid.

1. When you select the required computers and enable pre-configuration, a domain-level Group Policy Object (GPO) named **AdminDroidAuditor** is automatically created in your domain.
2. This GPO includes all the necessary configurations required for event auditing, such as advanced audit policies and firewall settings for event log collection.
3. Next, a security group named **AdminDroidAuditor** is created in the domain. All the selected domain computers are automatically added to this group.
4. The group is then used for GPO security filtering, ensuring that the auditing settings are applied only to the intended systems.

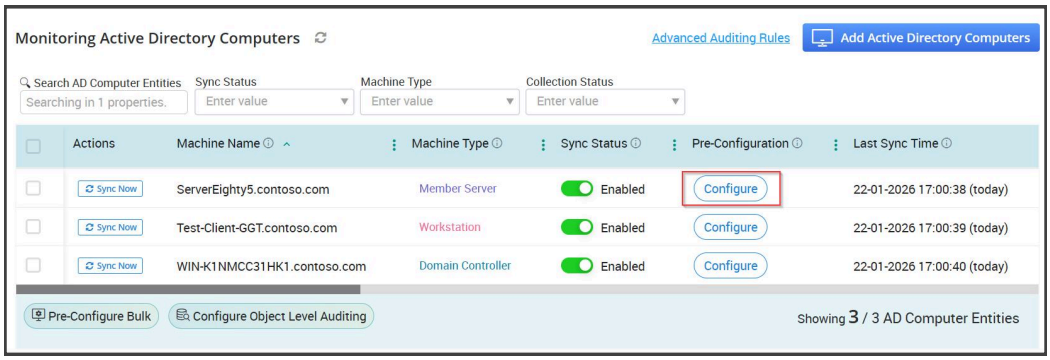
As a result, activities performed on these domain computers are logged in the Windows Event Viewer and collected by AdminDroid for auditing and reporting purposes.

Follow the steps below to configure the required Advanced Audit Policies automatically:

1. Log in to the **AdminDroid Active Directory Companion**.
2. Navigate to *Settings > Audit Settings*, select the computers you want to set up for auditing, and click **Next**.
3. A preview of the selected computers is displayed. Click **Next** to continue.
4. Set **"Configure Advanced Audit Policy and Firewall"** to **Yes**, then click **Start Auditing** to enable auditing for the selected computers.

   If you skipped this step during computer onboarding, you can configure it later from the **Audit Settings** page using the options below.

   a. Single computer – To configure auditing for an individual computer, click **Configure** in the "Pre-Configuration" column of the specific computer.

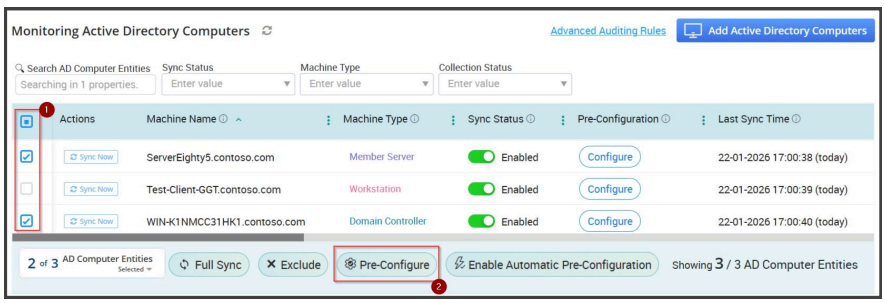


   b. Multiple computers – When configuring multiple computers, choose one of the following options based on your environment.

I. **Pre-Configuration** – This option immediately applies the required settings to all selected computers. If a computer is offline or unreachable at the time of configuration, the settings are not applied. You must run the configuration again later for those computers. Use this option when all selected computers are online.

To configure:

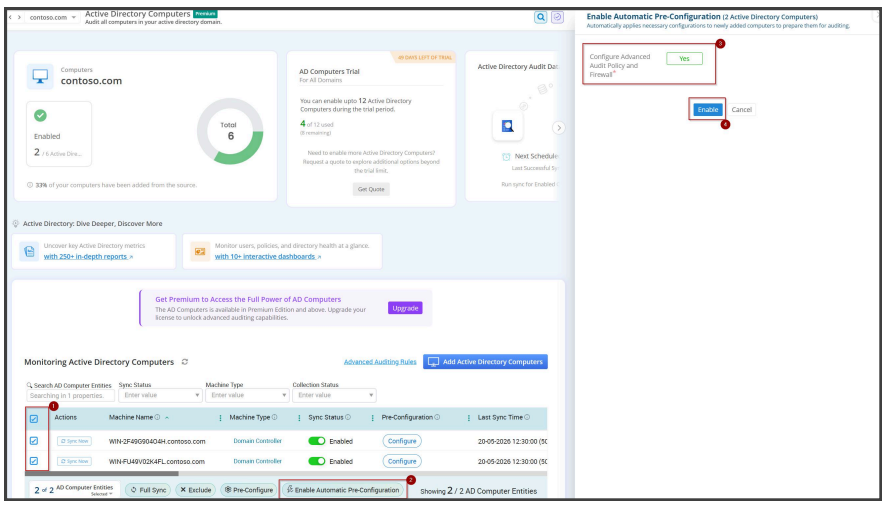
1. Select the required computers.
2. Click **Pre-Configure** in the bottom pane.
3. Click **Yes** on the confirmation prompt.



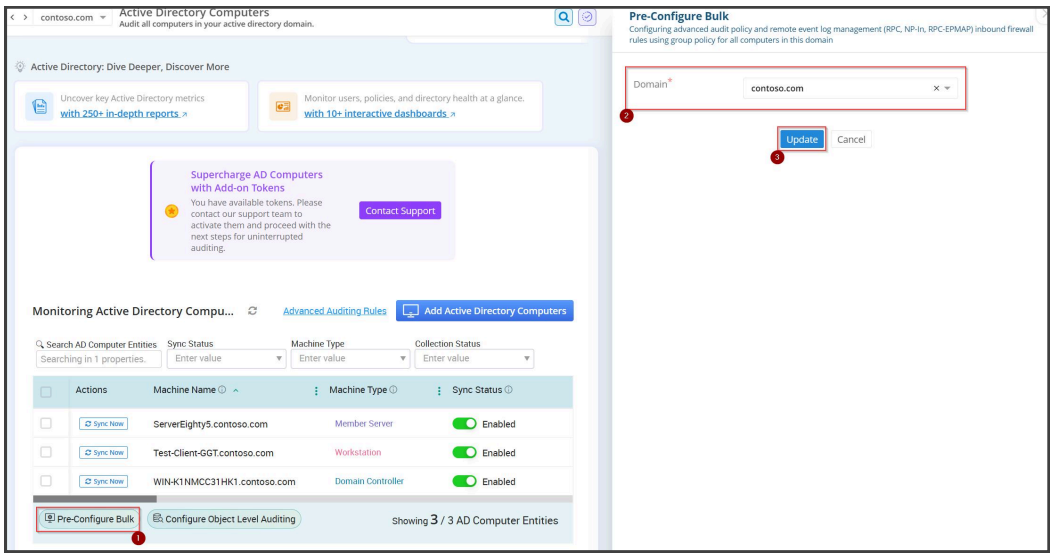
II. **Automatic Pre-Configuration** – Use this option when some selected computers are offline during configuration. AdminDroid immediately configures auditing on all available computers and continues to check the offline systems during each synchronization cycle until all required auditing prerequisites have been configured.

To configure:

1. Choose the required computers where you want to enable auditing.
2. Click **Enable Automatic Pre-Configuration** in the bottom pane.
3. Set ‘Configure Advanced Audit Policy and Firewall’ to **Yes**, and click **Enable**.



c. All computers – To configure auditing for all computers in a domain, click **Pre-Configure Bulk** in the bottom pane, select the domain, and then click **Update**. This option automatically applies the required auditing configuration to all computers that are configured for auditing in AdminDroid.

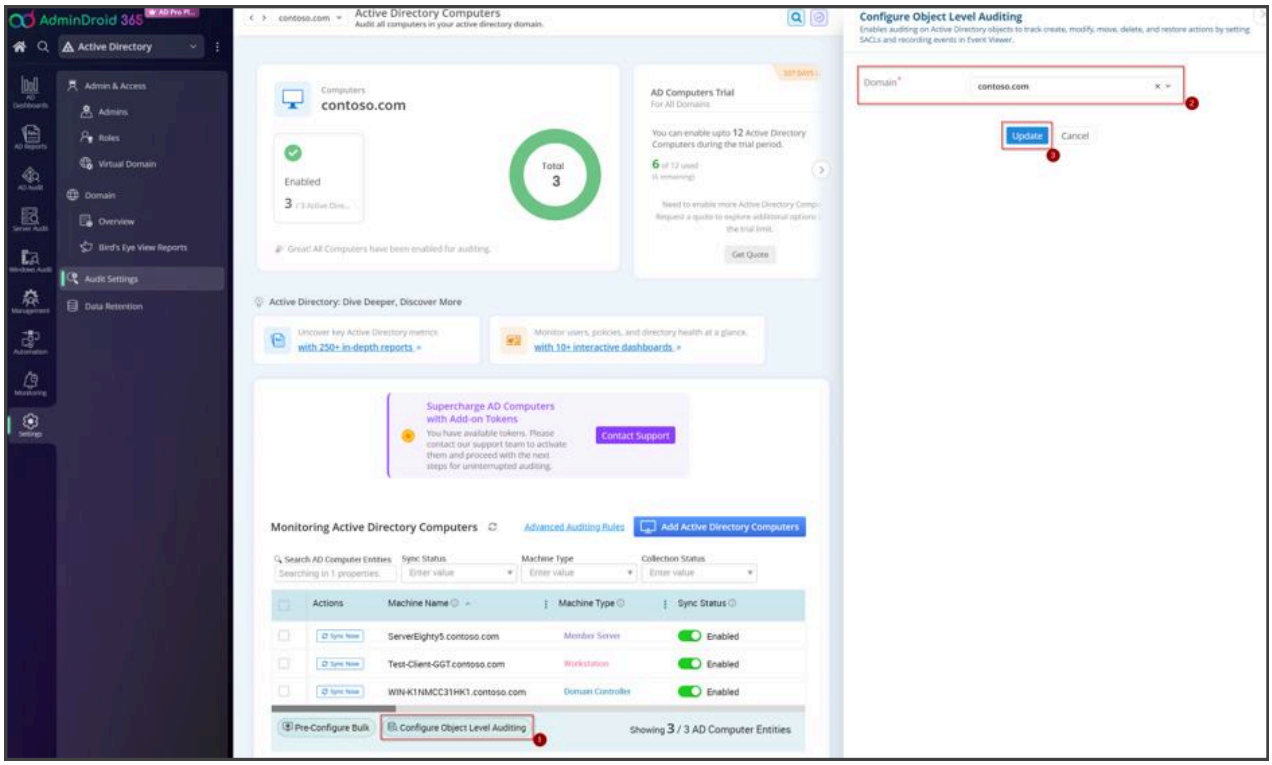


Once configured, events occurring on the selected computers will be audited automatically. To add a new computer for auditing, click Add Active Directory Computer and select the computer from your domain. Set “Configure Advanced Audit Policy and Firewall” to **Yes**, then set “Sync Status” to **Enabled** and click **Create**. This adds the computer to AdminDroid and configures the required advanced audit policies and Windows Firewall rules for event log collection.

2. Automatic Object-Level Auditing Configuration In Active Directory

Object-Level Auditing requires audit entries (SACLs) to be configured on multiple Active Directory partitions and containers. AdminDroid automatically enables the required audit entries across these locations in just a few steps.

To enable auditing for Active Directory object changes, click **Configure Object-Level Auditing** in the bottom pane. Then select the domain and click **Update**. This creates the required audit entries to log events that occur on Active Directory objects.



Once the policy configuration is complete, AdminDroid will start collecting the generated security events from all selected computers. You can verify the collected data in the relevant Active Directory reports and dashboards.