Cygna Protector for Active Directory

User Guide

Cygna Auditing & Security Suite

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

Published 1/11/2022

Version 5.9

Table of Contents

Introduction to Cygna Protector For Active Directory

This guide provides instructions for using Protector for Active Directory and information about product features, benefits, functions, unique concepts, and basic procedures.

Note for BeyondTrust Customers

Cygna Labs assures BeyondTrust's Auditor Suite customers continuity with on going product development, maintenance and support. Please find the information below on respective name changes.

Former name	Current name
PowerBroker Auditor for Active Directory BeyondTrust Auditor for Active Directory	Cygna Auditor for Active Directory
PowerBroker Auditor for Exchange BeyondTrust Auditor for Exchange	Cygna Auditor for Exchange
PowerBroker Auditor for File System BeyondTrust Auditor for File System	Cygna Auditor for File System
BeyondTrust Event Vault for Windows	Cygna Event Vault for Windows
PowerBroker Auditor for SQL Server BeyondTrust Auditor for SQL Server	Cygna Auditor for SQL Server
Change Manager for Active Directory	Cygna Change Manager for Active Directory
Privilege Explorer for Active Directory	Cygna Privilege Explorer for Active Directory
Privilege Explorer for File System BeyondTrust Privilege Explorer for File System	Cygna Privilege Explorer for File System
Protector for Active Directory BeyondTrust Protector for Active	Cygna Protector for Active Directory

Former name	Current name
Directory	
Recovery for Active Directory	Cygna Recovery for Active Directory

Product Overview

Cygna Protector for Active Directory provides real-time protection and automated policy enforcement for Active Directory. It locks down the critical parts of your Active Directory and protects them against unauthorized changes and deletions—even by a user with native access.

Even users and administrators who are authorized to make changes to critical objects and GPOs in the AD must follow strict policies designed to protect critical objects and GPOs from tampering and accidents. Only Cygna Protector allows you to automate the protection of your AD, with easily created policies and real-time alerts.

Features of Protector For Active Directory

- Streamlined policy creation and implementation
- Automated volume-based and object-based change control to protect against the deletion of large numbers of objects or entire OUs
- Real-time monitoring and control of mass updates
- Real-time alerts of unauthorized changes, set up any way you need them, to ensure that you're made aware of unauthorized changes in time to prevent harm
- Detailed policies that protect your critical AD objects from unauthorized changes

About Real-time Protection Policies

Protector for Active Directory is designed to provide real-time alerting for changes made to Active Directory objects. Additionally, it can provide a mechanism to prevent modifications to critical objects from occurring. Real-time protection policies gather information when an action occurs on the selected objects. Using real-time protection policies, you can monitor activities on objects and ensure that the changes are not committed to the Active Directory database.

Note: It can take up to 15 minutes for changes to be detected and implemented. Computer and user objects can only be protected from deletion but you can create alerts for creation, deletion, and modifications.

Packages I Need to Use This Feature

Module	Description	License Required?
Server/Console	The Server/Console module provides fundamental setup features such as deploying agents; configuring e-mail accounts; and creating schedules to associate with collectors, policies, and auditing.	✓
Cygna Auditor for Active Directory	The Auditor tracks changes to Active Directory and Group Policy objects. Each audit event includes who, what, where, and when for all changes. It also includes before and after values for all attributes. The Audit Viewer, built-in audits, and creating collector policies are key features provided by the Auditor module.	✓
Protector for Active Directory	Protector for AD locks down critical parts of Active Directory and protects them against unauthorized changes and deletions.	✓

Configure Active Directory Agents

Agent Requirements

Overview

When you deploy an agent, the following SQL Server changes will be attempted by the Management Server service account during deployment:

- Create a server login for the Domain Controllers (DC) group by default or the credentials supplied by the user on the Database page (db_securityadmin).
- Create user login on the Auditor database for the DC group (db_owner).
- Add the user login to the Auditor role (db_securityadmin or db_owner).

Agent Deployment Requirements

The account will need:

- Administrator access to the target host
- DBO access on the Auditor database
- Remote registry services
- DNS name resolution

Agent Service Account

The agent runs as Local System.

Deploy Active Directory Agents

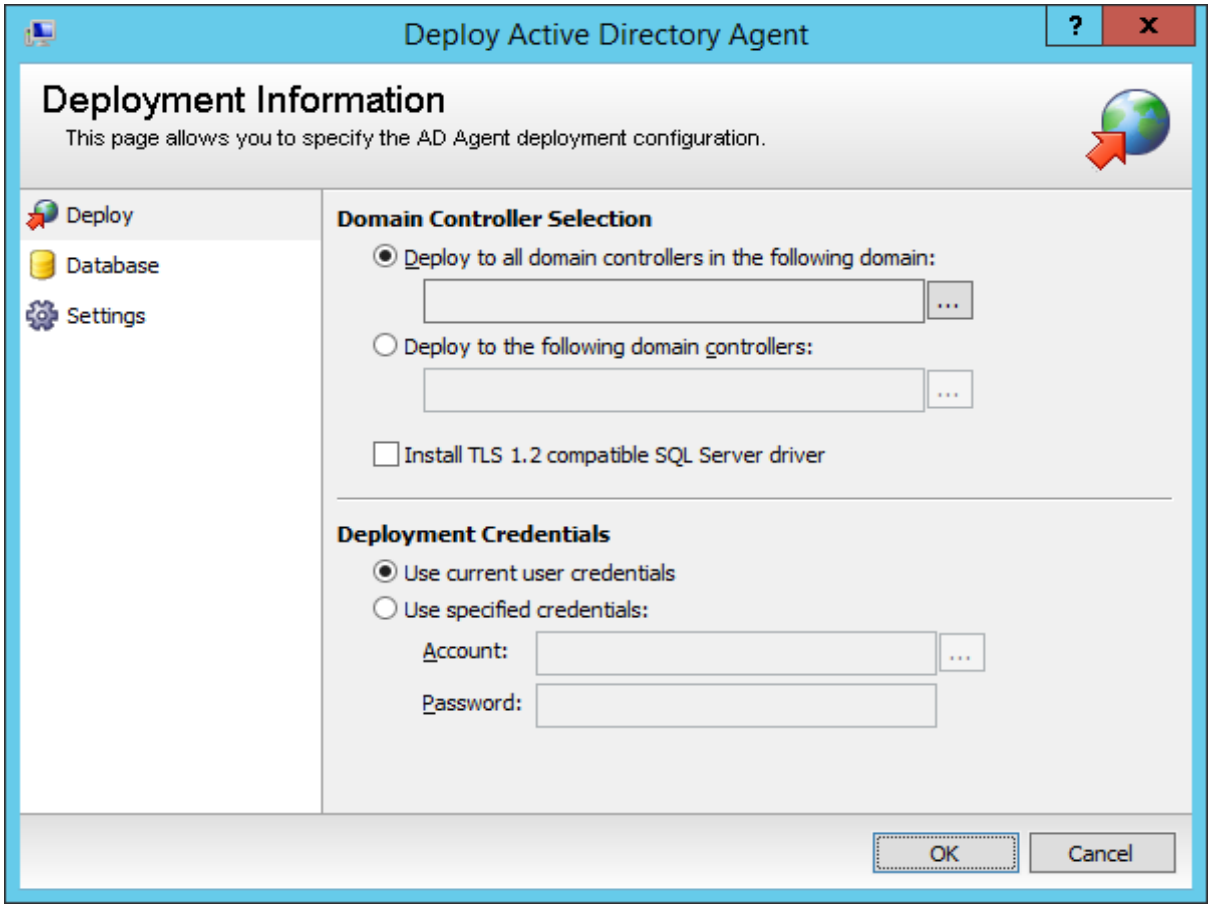
After the initial installation of Cygna Auditor for Active Directory, you must deploy an agent to every domain controller (DC) you want to monitor Active Directory objects on. The AD agent automatically collects all changes that occur in Active Directory. The events are tracked as they occur.

For full monitoring coverage, we recommend deploying an agent to every DC in your network. Otherwise, not all activity will be monitored. You can deploy an agent to any domain controller, regardless of the forest the domain controller exists in.

Do not deploy agents to read-only domain controllers (RODCs). Remove any agents previously installed on RODCs.

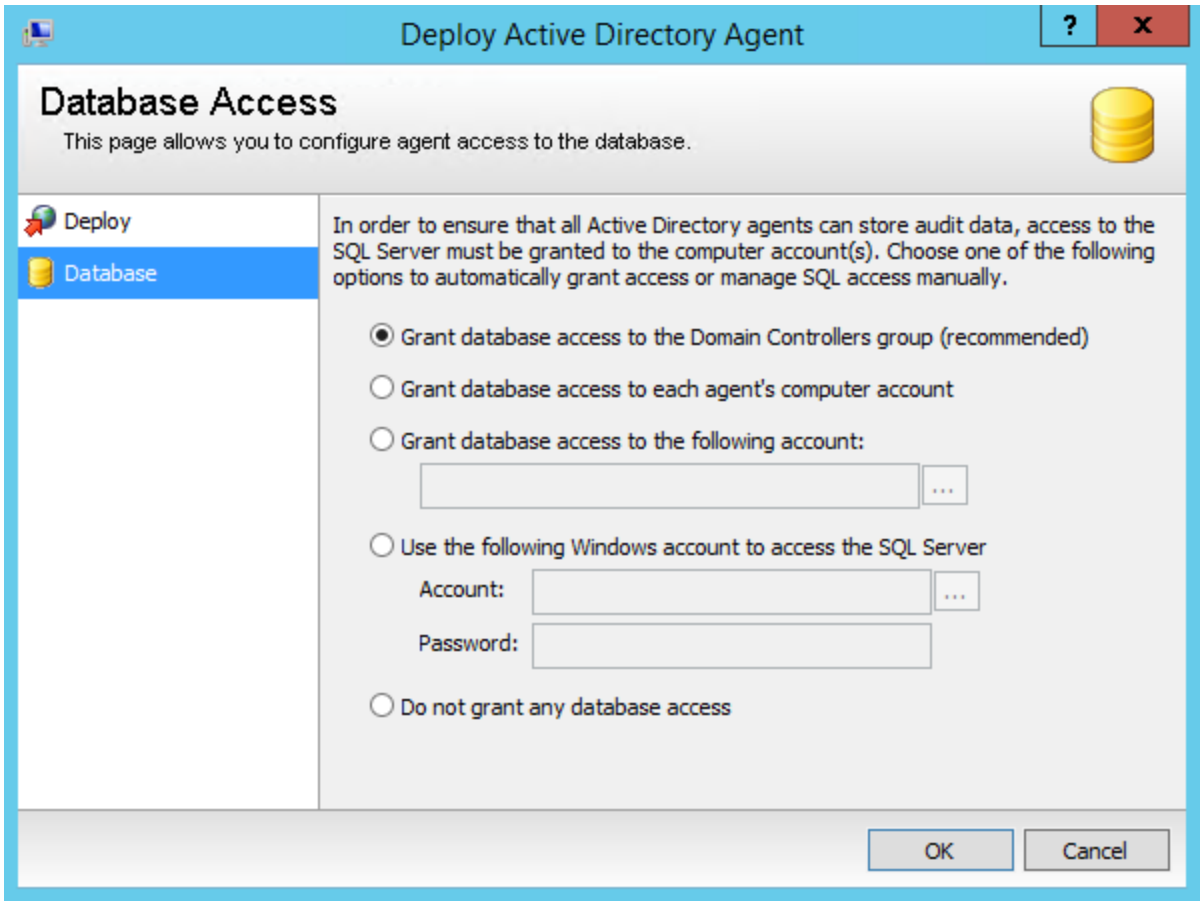
1. Start the console.
2. Expand Cygna Auditing & Security Suite.

3. Expand Active Directory.
4. Right-click Domain Controllers, and then select Deploy agent.



5. In the Deploy Active Directory Agent dialog box, under Domain Controller Selection, select the options as follows:
   - Deploy to all domain controllers in the following domain:
     - Click the browse button, then select the domain. Click OK.
   - Deploy to the following domain controllers:
     - Click the browse button, then select the domain. Click OK.
     - Select the DCs from the Domain Controller list.
     - To deploy agents to a DC in an external forest, click Change Forest. Provide the server name or IP address for the DC. Be sure to use credentials with read rights to connect to the external forest, and then click OK.
   - Select the Install the TLS 1.2 check box to install the SQL Server Native Client driver.

6. In the Deploy Active Directory Agent dialog box, under Deployment Credentials, provide the logon credentials for the remote agent deployment. This account must have administrative rights on the destination server.
   - Select Use specified credentials, and then provide the domain\username for the account. Alternatively, click the browse button to search for the user account.
   - Enter the password and click OK.



7. In the Deploy Active Directory Agent dialog box, select Database to open the Database Access page.
   - Verify authentication using either SQL or Windows authentication. If you choose Windows authentication, access to the database must be granted to the agents. If you choose SQL Server, no further authentication is required.
   - The Management Server service account requires sufficient access on the SQL Server to create logins and users on the SQL Server. If the service account does not have these rights, the AD agents will not have access to SQL Server and will remain in the Deployed or Starting status in the Management Console. The deployment will still be successful, however.

Note: All database activity originating from the destination DC will be executed using the credentials provided on this page.

Manage Agents

From the Domain Controllers node you can view the status of the agent and details of the DC such as OS & version, last update time, and the forest where the DC resides. You can also right-click a DC in the list and reload the settings, upgrade the agent, remove the agent, view the agent log file, restart, start, and stop the agent, and view its properties.

Uninstall and Upgrade the Agent

Note that it is not required that you restart to upgrade or uninstall the agent. However, you must restart the server to ensure all files are removed after an uninstall.

Troubleshoot Agents

If the agent's status is not Running, consider these questions:

- What is the agent's last update time?
- Is the remote machine running and can you log on to it?
- Is the agent service running?
- Are the agent service account user name and password correct?
- Does the machine have connectivity to the database and does the service account have permissions to the database?

Generally, there are two reasons why an audit event would not appear in Audit Views. Either the agent is not running, or the agent cannot communicate with the database.

Agent is not running

- What is the status of the agent in the console?
    - Offline: The agent hasn't updated its Last Update Time in the database in over 10 minutes.
    - Error: Can indicate that an error condition occurred during a deployment or upgrade of an agent.
    - Deployed: A Deployed status for an extended period of time might indicate that although the deployment of the agent was successful, the agent was either unable to start, or it cannot communicate with the SQL Server to update its status to Running.

- If an error status occurs during deployment or upgrade, check the deployment log file.
- Is the machine running?
- Is the service running? Try to start it. If the service account and password combination are incorrect, you will receive an error message. Fix the account or password and try again.

Agent cannot communicate with the database

- A Deployed status for an extended period of time likely indicates that although the deployment of the agent was successful, the agent was either unable to start/run, or it cannot communicate with the SQL Server (to update its status to Running).
- Agents send a heartbeat (the last update time column) to the database every 10 minutes. If the last heartbeat is longer than 10 minutes, this can indicate the agent is either offline or has lost connectivity with the database.

Troubleshooting communication issues with the SQL Server can be complicated, as there are multiple factors. High-level factors include:

- Does the agent machine have connectivity to the database server? (firewall issues, DNS, routing, etc.)
- Does the agent computer account have the correct permissions to the database?

You can right-click on agents and choose the Restart option. This may be helpful if your agent doesn't appear to be running properly or if a change has been made to SQL Server. Also note that the Update option will upgrade all systems with agents. You can select one or more DCs when using the Update option.

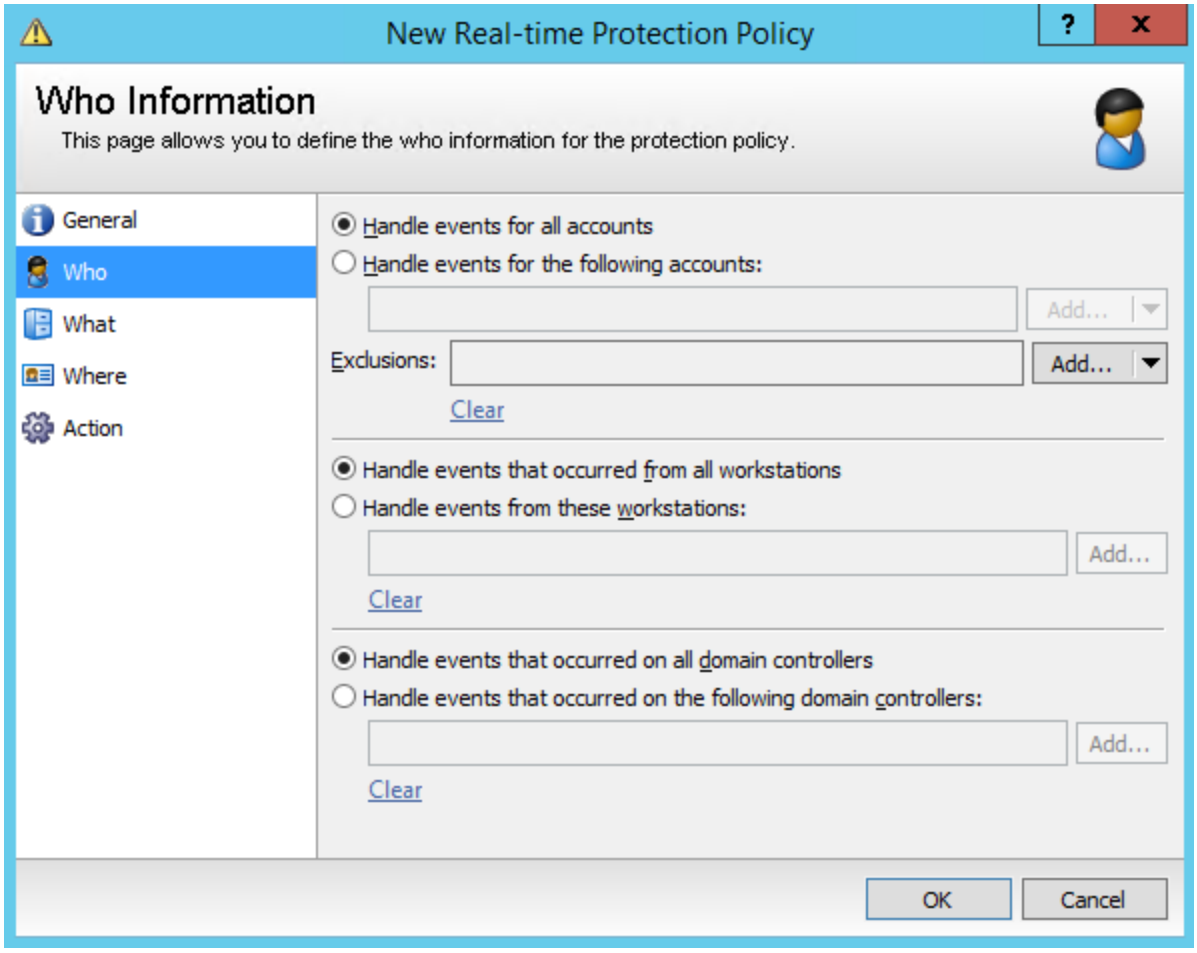
Agent Status

Status	Description
Deploying	Written to the database by the Auditor server service. It is attempting to copy agent files to the DC and setup/start the service.
Deployed	Written to the database by the Auditor server service. Files were copied and service work has been done on the DC.
Updating	Written to the database by the Auditor server service. It is attempting to copy the new files to the DC and setup/start the service.
Updated	Written to the database during the upgrade by the server. The file copy and service changes were successful on the DC.
Running	Written to the database by the agent. The service has started properly and has successfully contacted the SQL database.

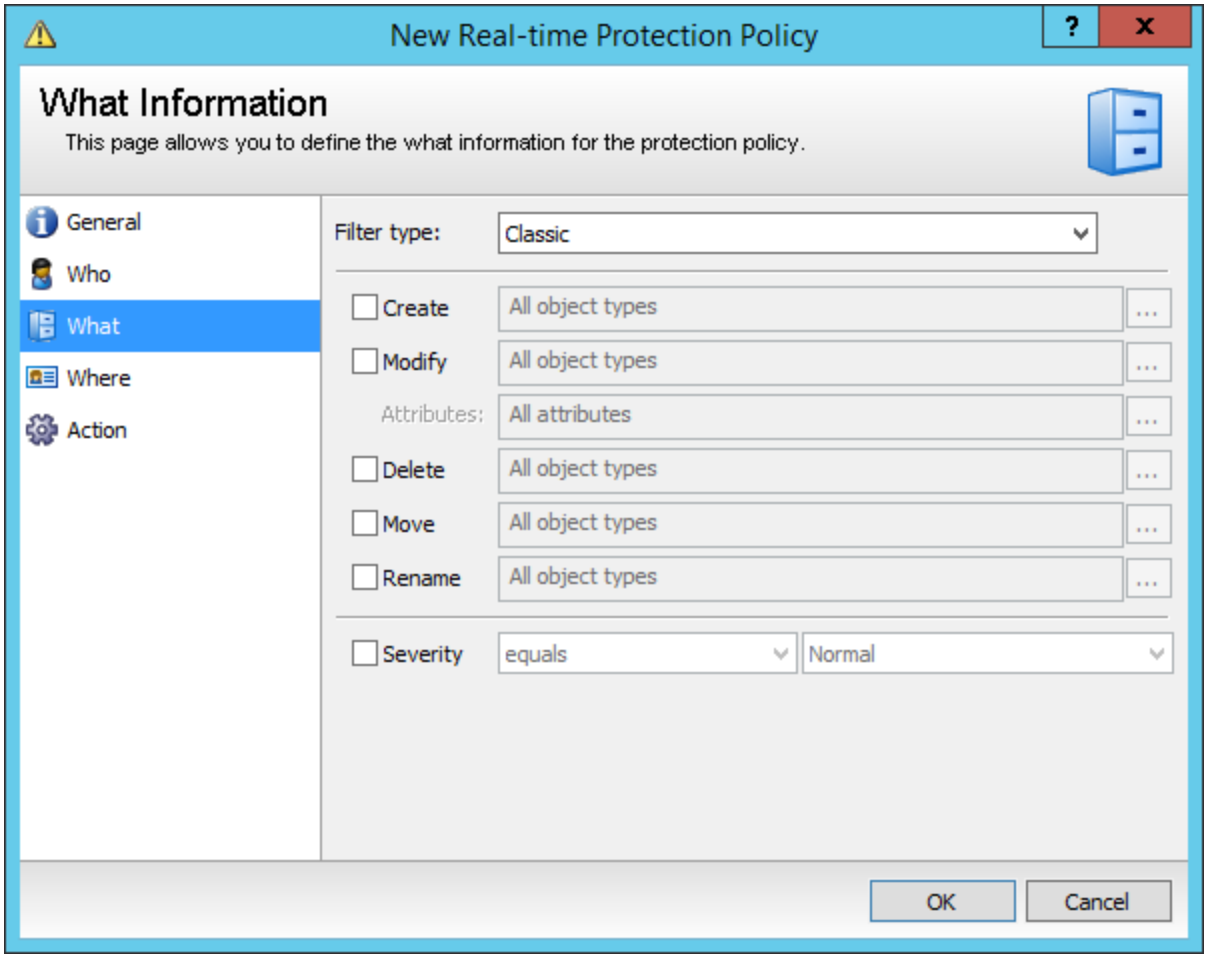
Status	Description
Offline	Written to the database by the Auditor server service. It has noticed the agent has not updated its heartbeat in 10-15 minutes.
Error	Written to the database by the Auditor server service. This status will appear if it can not complete the task of deploying, updating, or removing an agent. If you see a status of Error, check both the event logs and the Auditor logs on the Auditor server and Domain Controller.
Running, with Queue	Written to the database by the Auditor server service. This status will appear if the agent is queuing events due to SQL connectivity issues.

Create a Real-time Policy

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Select the Active Directory node.
4. Right-click **Real-time Protection** and then select **New > Real-time Protection Policy**.
5. On the General page, provide a name and description for the policy.
6. By default all policies are enabled. Click the check box to disable the policy.

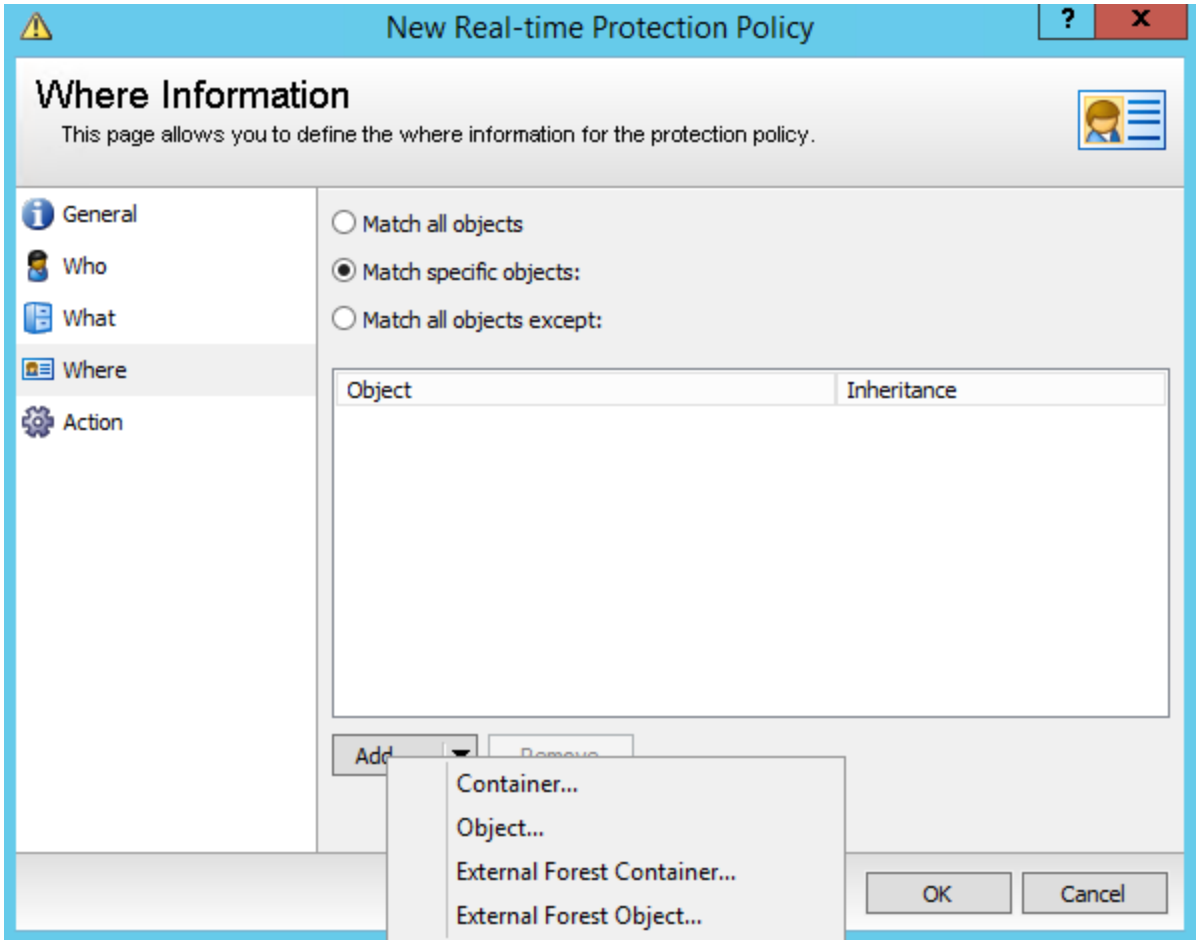


7. On the Who page, select the accounts, workstations, and domain controllers where you want to audit changes as they occur. You can do this by choosing all items or using the Add buttons in each section.
8. On the What page, select a filter type from the menu or modify existing filter types. You can choose from Password Never Expires, Account is Disabled, No Password Required, and Bad password Count.
    - If you select an existing filter, you must then set the value in the New Value list as True to enable it.

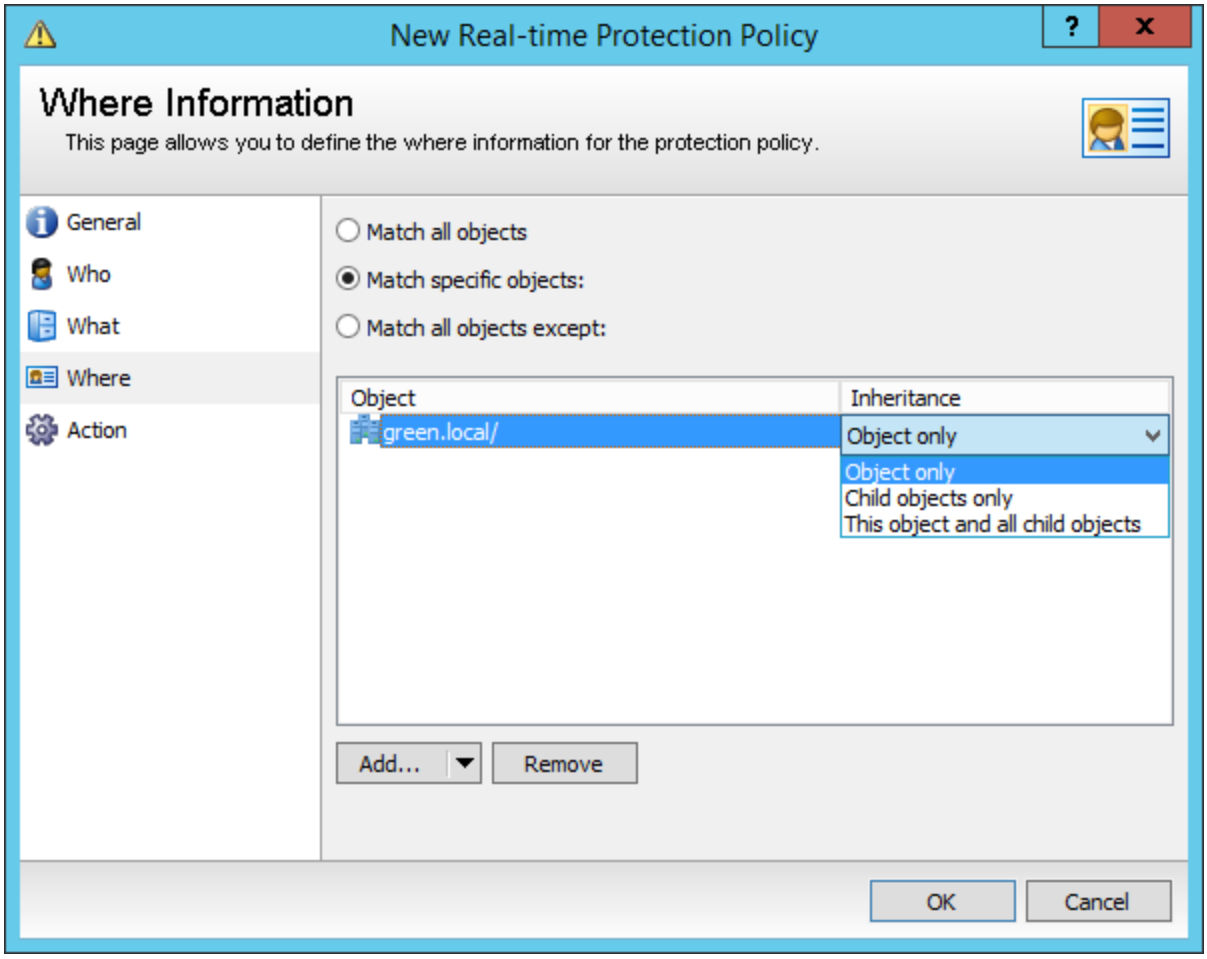


9. Select the Classic filter type, and then select the following actions to alert on. You can select more than one action type.
   - Create: Alerts when objects are created. If you do not want reporting data on all objects, click browse and select the objects to monitor.

     For example, select the User check box to be notified every time a user account is created.
   - Modify: Alerts every time an object is modified. If you do not want reporting data on all objects or attributes, click browse to select the objects and attributes to alert on.
   - Delete: Alerts when an object is deleted. If you do not want reporting data on all objects, click browse to select the objects to alert on.
   - Move: Alerts every time an object is moved. If you do not want reporting data on all objects, click browse and select the objects to monitor.
   - Rename: Alerts every time an object is renamed. If you do not want reporting data on all objects, click browse and select the objects to monitor.
   - Severity: Select to set the severity parameters: Critical, High, Normal, Low.



10. On the Where page, click Add to select a container or an object. Multiple containers and objects can be added to the list.
    - Match all objects: Monitors actions on every object detected by the domain controller. Actions are selected on the What page.
    - Match Specific object: Select a particular container or object to narrow the scope of the monitoring.
    - Match all objects except: Select this option to make exclusions to the criteria. This is useful when creating a real-time policy to alert when a new user is created that is NOT in a designated OU.



11. After an object or container is selected, click the cell under Inheritance and select one of the following:
    - Object only: Monitor the object only.
    - Child objects only: Monitors only children of the selected object.
    - This object and all child objects: Monitors the object and all children.
12. On the Actions page, select **Prevent the operation from being committed** so audited changes are not saved to Active Directory.

Note: This policy can only be applied to Groups, OUs, Containers, Printers and Shared Folders.

13. Select from the following alert types:
    - Send an email: Select the check box and a template. For more information, please see Email Templates.

- Write to event log: Writes an event to the event log on the machine the component is running on. Protector for AD event log alert is written to the event log on the domain controller.
- Send SNMP message: Protector for AD sends a network message with the alert details, and any SNMP monitoring application receives it.
- Send to SIEM receiver: Forwards events to external Security Information and Event Management (SIEM) servers. You can select more than one SIEM server. Browse to add SIEM servers. Provide Connection Name, Destination Server, and Port (UDP). Click Test to ensure the connection to the SIEM server works.
- Enable smart filtering: Provides more control over how often alerts are sent out. See Smart Filtering below.

14. Click **OK**.

Smart Filtering

Enabling Smart Filtering allows you to have more control over how often alerts are received. This allows for auditing ease by only being alerted on events you have defined as critical or important. Rather than receiving an alert every time one user matches the criteria configured in the rule for example, you can choose to receive one alert when a the number of times the rule has been triggered reaches the threshold you specified.

An example Use Case would be a situation where there is simultaneous lockout of several different users. This could indicate an issue with a script or worse, perhaps an intrusion attempt. Setting the match count to 3 and changing the time window to 5 minutes means that there would have to be 3 or more lockouts that would have to occur within a 5-minute window to trigger an alert.

The following options can also be enabled by checking the box:

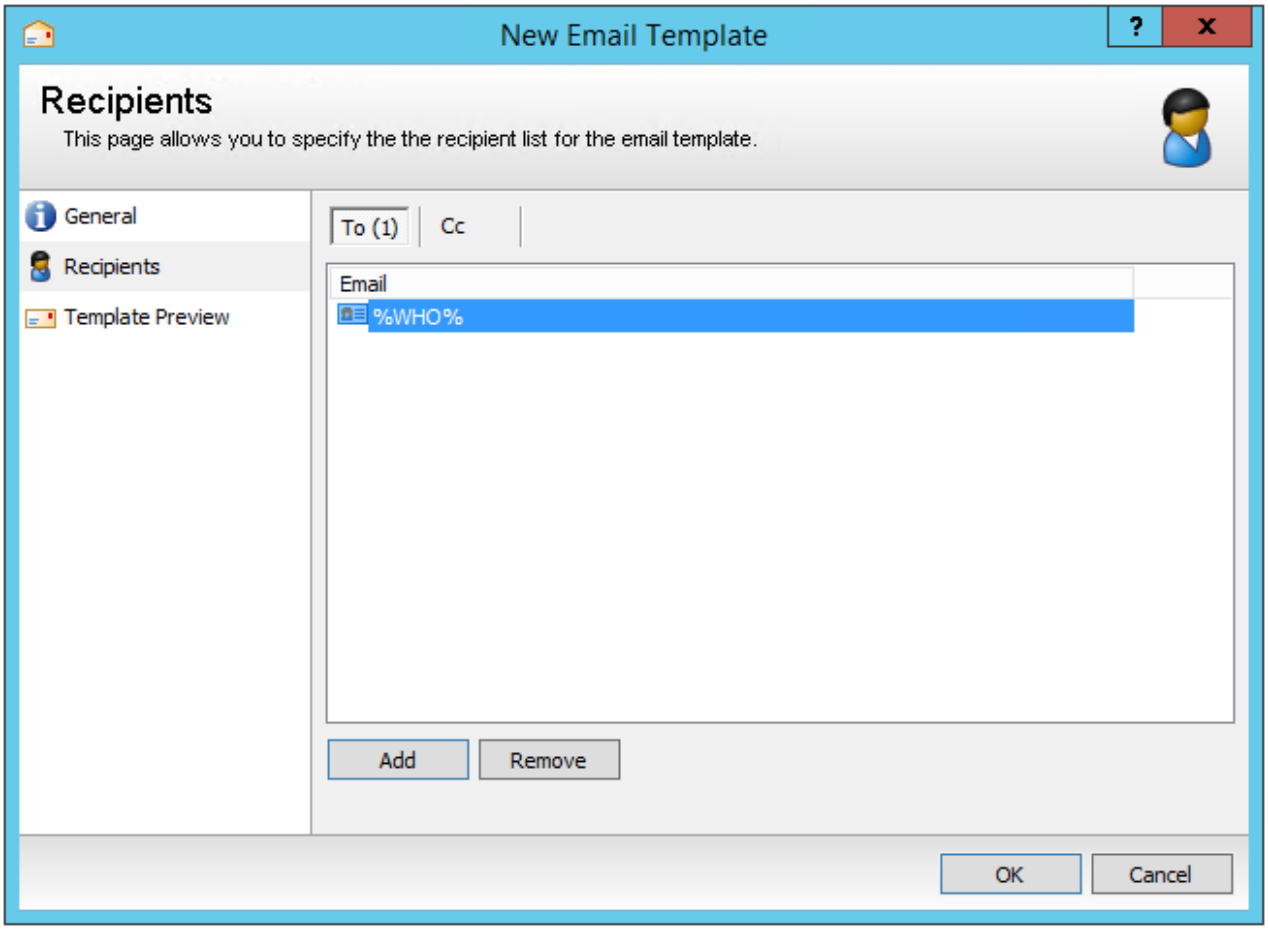
- Make this smart alert per user: The alert only triggers if the rule is triggered the correct number of times and the user who triggered the event is the same each time.
- Make this smart alert per object: The alert only triggers if the rule is triggered the correct number of times and the AD Object that caused the event is the same each time.
- Reset smart alert when triggered: The agent ignores the events already used in this rule to trigger it.

Email Templates

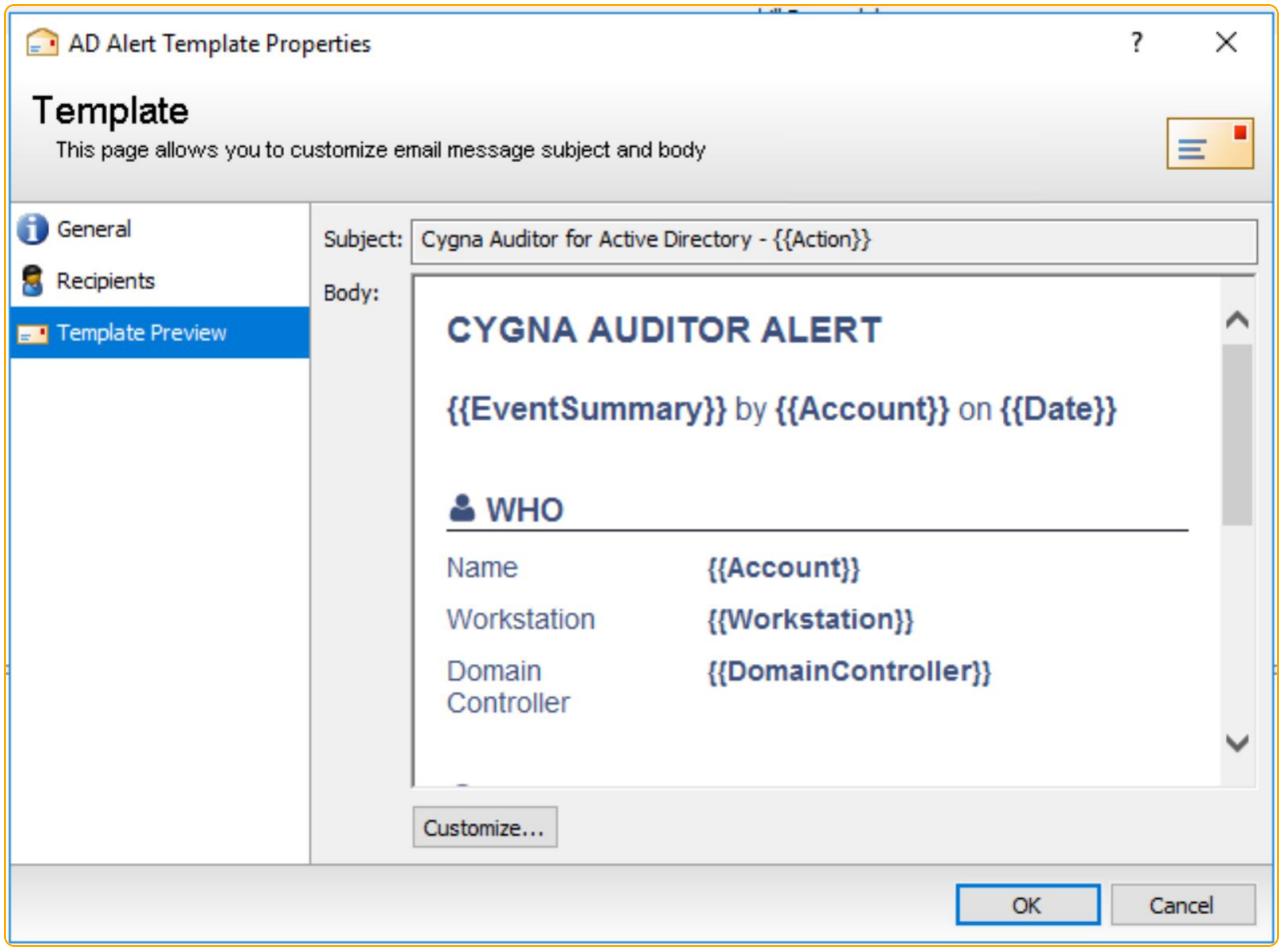
On the Actions page when creating a real-time policy, select the Send an email Alert option and then click the browse button to choose or create an email template.

When creating an email template, you create a unique name, add recipients, and customize the email templates (optional).

1. In the console, expand Configuration > Email Templates.
2. Right-click the node for the module you want to create the template for. For example, Active directory Alerts or File System Alerts.
3. Provide a name and description for the template.
4. Select the Recipients tab, and then click Add to enter recipients.



Administrators can enter the %WHO% wildcard to send an email to a user that exists in Active Directory. This email notifies the user of the changes they made.



5. Select Template Preview.
6. Click Customize to change the template.
7. On the HTML tab, you can modify the text in the window or you can click Source to modify the HTML code. You can also import and export .html files. The Import and Export buttons are enabled when you click Source.
8. Click OK.
9. After you finish configuring the template, click OK.

Modify a Real-time Protection Policy

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Select the Active Directory node.
4. Select the **Real-time Protection** node.
5. To change the name of the policy, right-click the policy, and then select **Rename**.
6. Enter a new name and press **Enter**.
7. To change more options for a policy, right-click the policy, and then select Properties.
8. Change the options, and then click **OK**.

For more information about the options, please see Create a Real-time Policy .

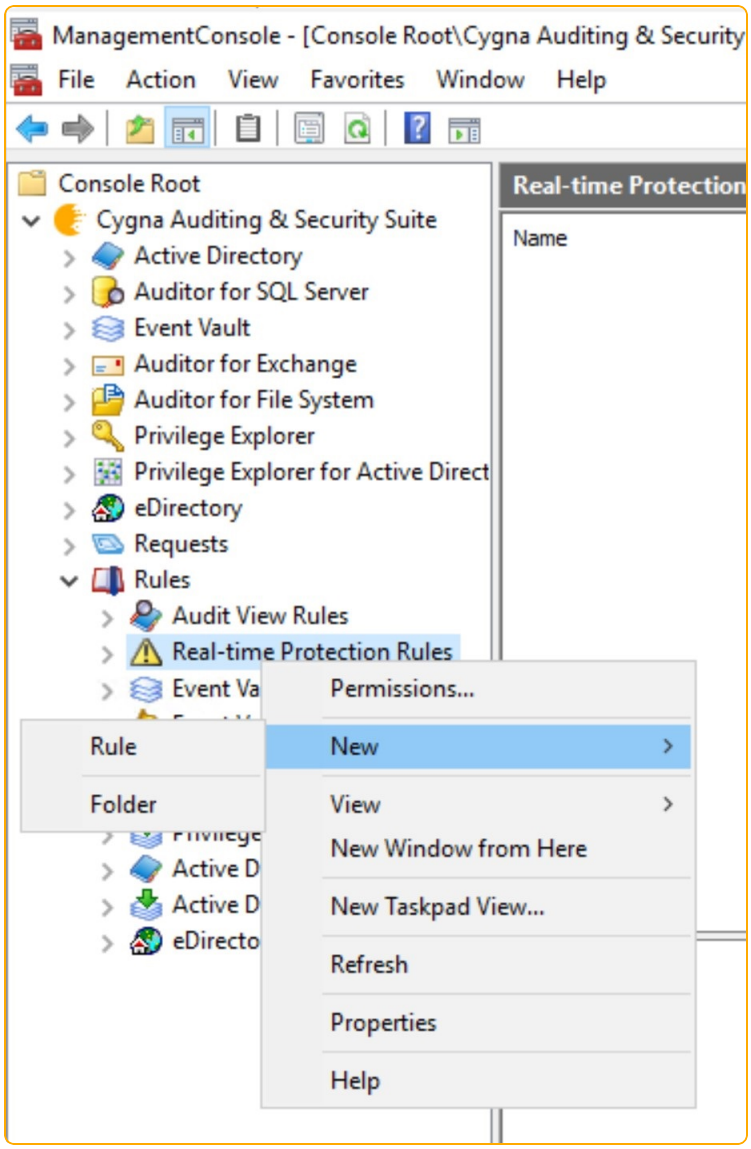
Delete a Real-time Protection Policy

1. Start the console.
2. Expand Cygna Auditing & Security Suite.
3. Expand Active Directory.
4. Select the Real-time Protection node.
5. Right-click the policy that you want to delete, and then select Delete.
6. Click Yes to confirm the delete.

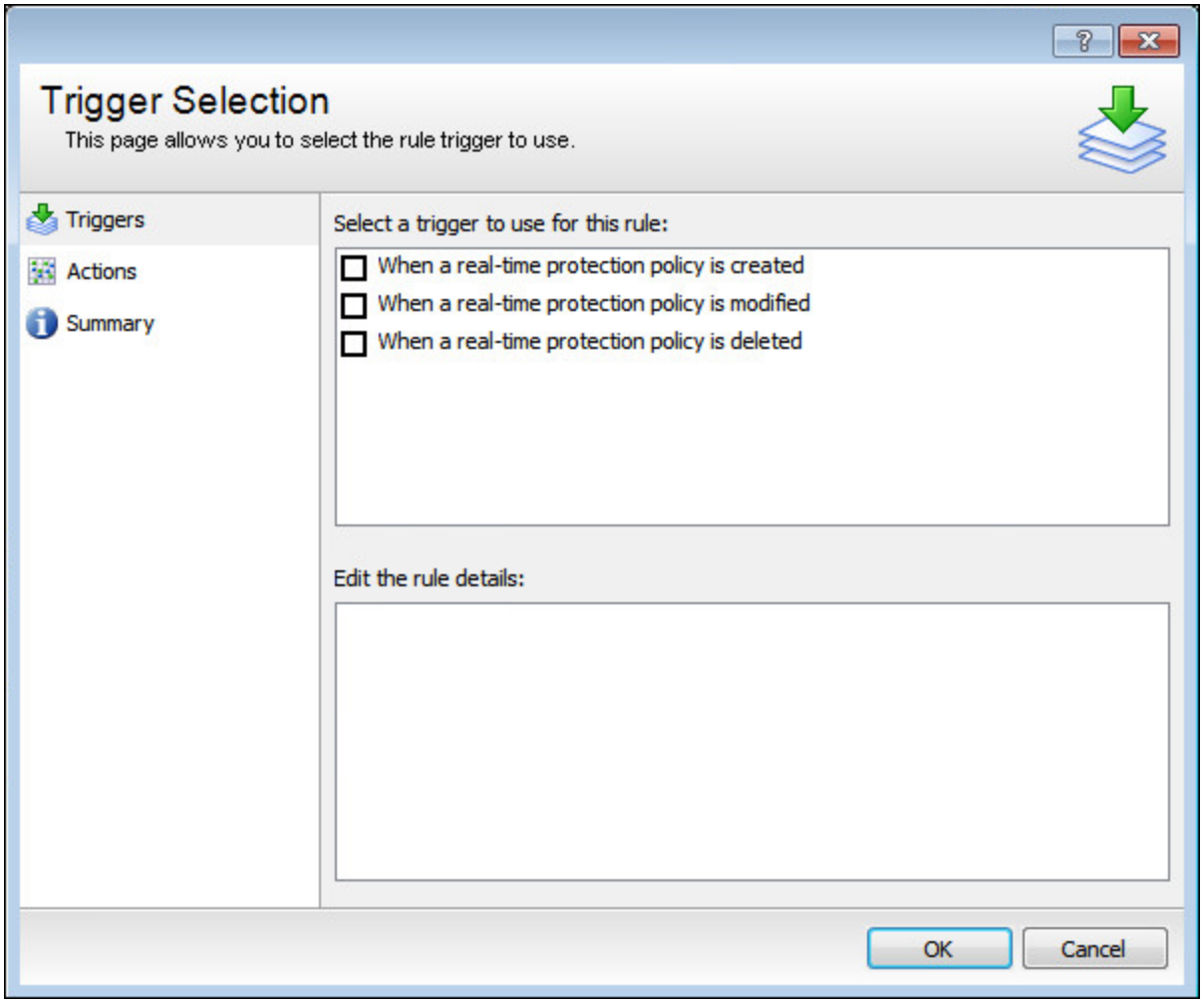
Add Rules to Real-time Protection Policies

Note: Overuse of rules will impact Domain Controller performance.

1. Start the console.
2. Expand Cygna Auditing & Security Suite.
3. Expand Rules.

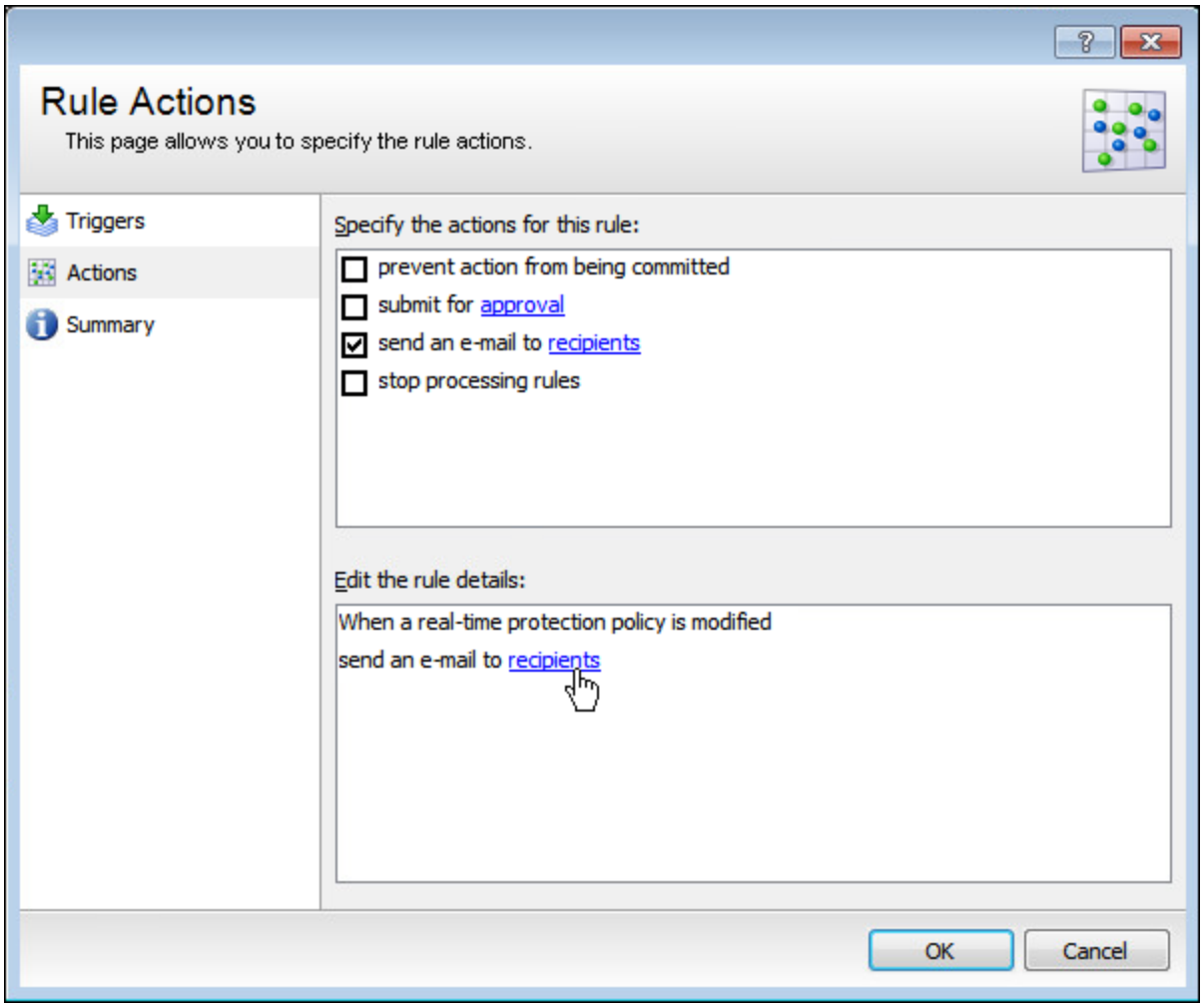


4. Right-click Real-time Protection Rules, and then select New > Rule.

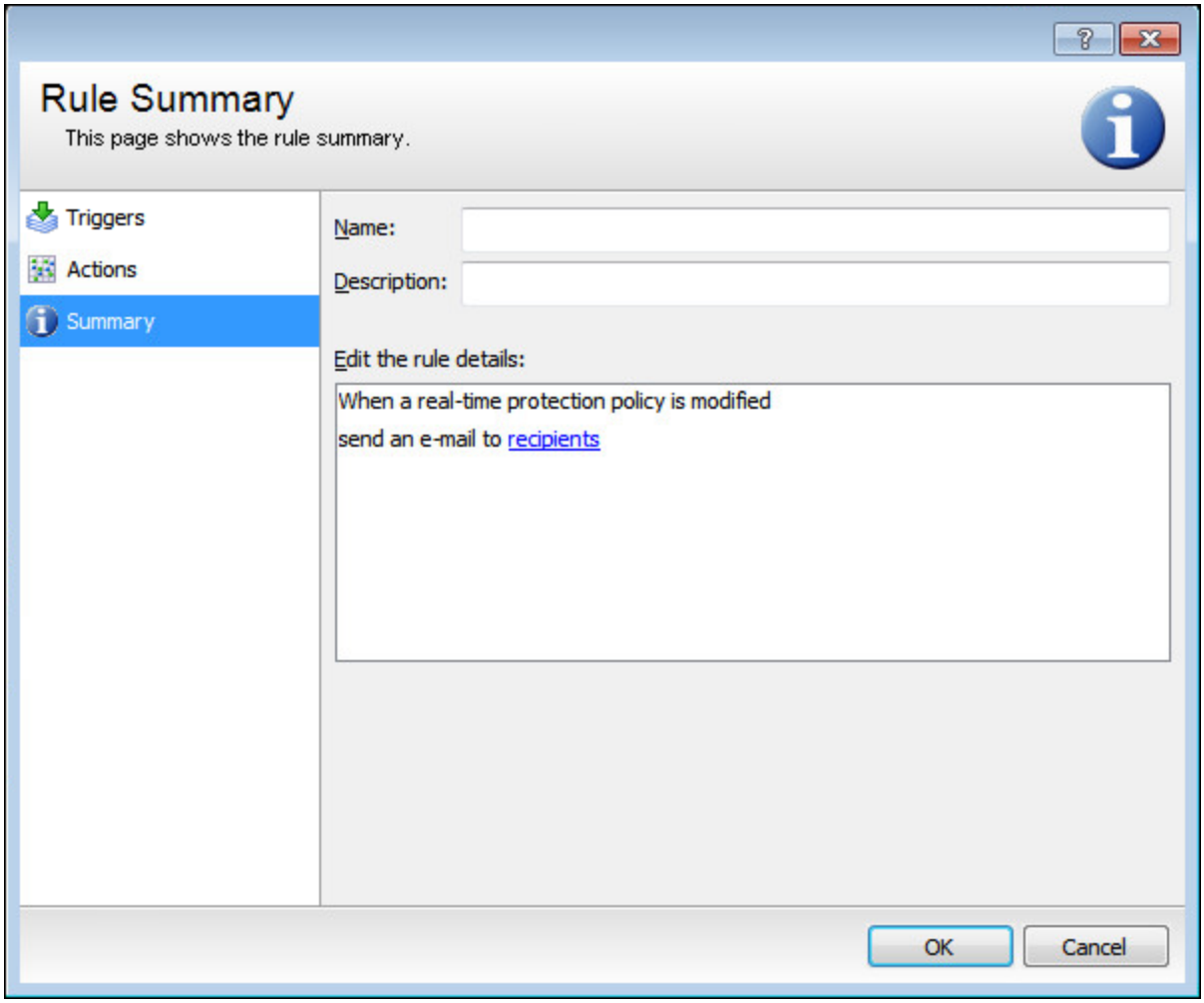


5. On the Triggers page, select the trigger to use for the rule and click OK.

6. Select Actions, and then select the action you want to take.



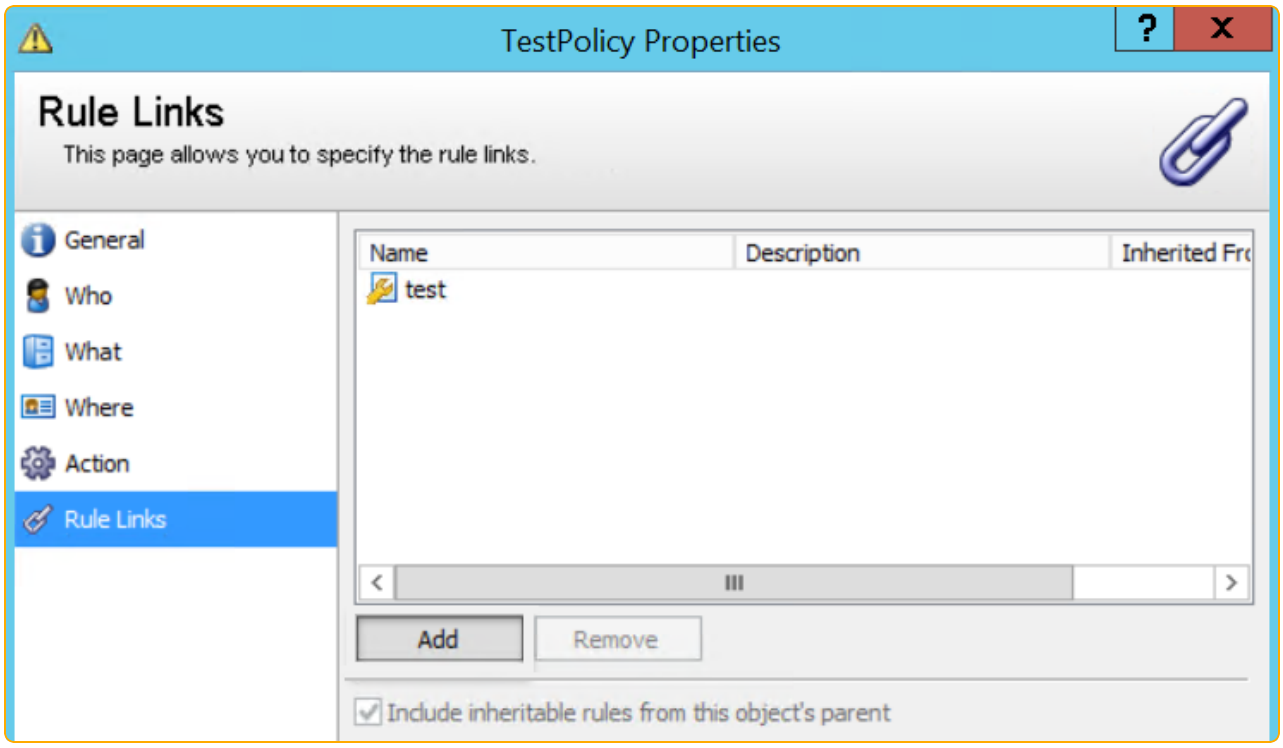
For example, if you want to receive an email notifying you of the change, select the send an email option and then click on the recipients link to enter an email address.



7. Select Summary and add a name and description for the rule.
8. Click OK to commit your changes.

Link a Rule to a Real-time Protection Policy

1. Start the console.
2. Expand Cygna Auditing & Security Suite.
3. Expand Active Directory.
4. Select the Real-time Protection Policy node.
5. Right-click the policy you want to link to a rule and then select Properties.



6. Click Rule Links and then click Add.
7. Select the rule to link to the policy and then click OK.
8. Click OK to commit your changes.

Create an Audit View from a Real-time Policy

You can create an audit view from any real-time policy by right-clicking the policy and selecting Create Audit View from the menu. You will see the New Audit View dialog box. Provide all of the information for each page: General, Who, What, Where, and Schedule to create the new audit view.

For more information about creating and using audit views, please see the Cygna Auditor for Active Directory User Guide.

Note that applicable settings from the source Real-time Policy will be automatically preset in the new Audit View.

Set Up Email Notification

To send email alerts, you must configure the SMTP settings for Auditor.

1. Start the console.
2. Expand Cygna Auditing & Security Suite.
3. Expand Configuration.
4. Select the General Settings node.
5. The Email Settings are blank until they are configured. Click Edit to configure each section.
6. When the Email Settings dialog box opens, enter a name in the Display Name box.
7. Type an email address in the Email Address box.
8. Type the name or the IP address of the SMTP server. If necessary, select the Use logon information box and enter credentials for the SMTP server. Security Protocol:
   - None: Creates an unencrypted connection on the specified port (default 25).
   - SSL: Creates a secure connection using SSL (Secure Sockets Layer) encryption on the specified port (default 465). Requires SSL, otherwise the connection fails. SSL and TLS connections require credentials.
   - TLS: Creates a secure connection using TLS (Transport Layer Security) encryption on the specified port (default 587). Requires TLS, otherwise the connection fails.
   - Check for server certificate revocation: If selected, enforces a server certificate revocation check before sending email alerts. This requires internet access for the machines where AS Server, MMC, and agents are deployed; otherwise checks fail and no email alerts are sent.
9. After you enter this information, click Test to ensure the settings are working correctly. A test message is sent to the email address provided.
10. Click Save.
11. After you save your configuration, the information appears when you select the General Settings node.

To turn off email notifications, clear Enable email settings and click Save.

Troubleshoot Email Notifications

If you have trouble receiving your email notifications, please note the following:

- Both DCs and the Management Server need permission to send.
- DCs must be on the allowed list for the SMTP server to accept an email from them.
- The DC must be able to communicate with the SQL Server to pick up SMTP settings.
- The DC must be able to communicate with the SMTP server to send the notification.
- On the Email Configuration page, ensure you test the settings.