ZSCALER AND CIMCOR DEPLOYMENT GUIDE

SEPTEMBER 2024, VERSION 3.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see **Zscaler's website**.

Cimcor Overview

Cimcor develops innovative, next-generation compliance and system integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real time while providing detailed forensic information about all changes. CimTrak helps reduce configuration drift and ensure that systems are in a secure and hardened state. Securing your infrastructure with CimTrak helps you get compliant and stay that way. To learn more, refer to **Cimcor's website**.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- **Zscaler Resources**
- **Cimcor Resources**
- **Appendix A: Requesting CimTrak Support**
- **Appendix B: Requesting Zscaler Support**

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact **partner-doc-support@zscaler.com** to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact **z-bd-sa@zscaler.com** to reach the team that validated and authored the integrations in this document.

Zscaler and Cimcor Introduction

Overviews of the Zscaler and Cimcor applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

CimTrak Overview

CimTrak is an integrity assurance and compliance solution that detects changes (additions, modifications, or deletions) in real time to files, directories, configurations, registries, ports, users, groups, and other critical system components across a variety of application use cases, including servers, network devices, hypervisors, containers, cloud configurations, database schemas, active directory, and more. CimTrak can then determine if those changes are good or bad.

- CimTrak's rollback capability enables it to revert to a previously trusted state in the event of malicious or circumvented changes. This functionality is coupled with CimTrak's ability to deny change(s) from occurring entirely.
- CimTrak also leverages the best practices of both DISA STIGs and CIS Benchmarks to determine if a system, device, application, or operating system is in a trusted and hardened state. When integrity drift is detected by CimTrak, it provides the description, assessment, rationale, impact, and remediation capability to ensure trust and resiliency throughout the enterprise.
- CimTrak supports regulatory compliance with continuous detailed reporting and auditing features and integrates seamlessly with other security and management systems, including Zscaler.
- CimTrak is the only solution that can fully meet Zero Trust Tenet #5's expectations and objectives as defined by NIST SP 800-207.

Cimcor Resources

The following table contains links to Cimcor support resources.

Name	Definition
CimTrak/Zscaler Info	Information and videos on CimTrak and Zscaler integration.
Submit a CimTrak Support Ticket	CimTrak Support ticket entry form.
CimTrak ReadMe Docs	CimTrak user documentation for install, configuration, and deployment.
CimTrak Support Portal	CimTrak Knowledge Base and Support ticket management.
PDF Download Link	White paper for CimTrak and ZPA.
PDF Download Link	White paper for CimTrak and ZIA.

Integrations Summary

The following table shows a summary of the Zscaler and Cimcor integrations.

Integration Name	Description of Integration	License Considerations
ZPA Integrity Monitoring	Allows users to monitor, baseline, alert, and roll back ZPA configuration changes.	Monitoring the integrity of ZPA requires a separate license.
ZPA Compliance Trigger	Allows users to automate enabling and disabling Zscaler policies based on CimTrak Compliance/Benchmark scan failures.	Based on the number of endpoints under management.
ZPA Integrity Trigger	Allows users to automate enabling and disabling Zscaler policies based on CimTrak's detection of integrity violations.	Based on the number of endpoints under management.
ZIA Integrity Monitoring	Allows users to monitor, baseline, alert, and roll back ZIA configuration changes.	Monitoring the integrity of ZIA requires a separate license.
ZIA Compliance Trigger	Allows users to automate isolating systems via Zscaler Device Postures based on CimTrak Compliance/ Benchmark scan failures.	Based on the number of endpoints under management.
ZIA Integrity Trigger	Allows users to automate isolating systems via Zscaler Device Postures based on CimTrak's detection of integrity violations.	Based on the number of endpoints under management.

Prerequisites

The following sections list the prerequisites for the Zscaler and Cimcor integration.

CimTrak Prerequisites

To integrate CimTrak with Zscaler, make sure the following prerequisites are met:

- CimTrak Repository v4.1.42 or later installed
- CimTrak AppServer v4.1.42 or later installed
- CimTrak Collector v4.1.42 or later installed
- CimTrak Agent v4.1.42 or later installed
- CimTrak Administrator Web Console access
- CimTrak Server needs Internet access or a valid route to ZIA or ZPA services

ZPA Prerequisites

To integrate ZPA with CimTrak, make sure the following prerequisites are met:

- ZPA Endpoint URL
- ZPA Customer ID
- ZPA Client ID
- ZPA Client Secret

Finding ZPA Endpoint URL

To find the ZPA endpoint URL:

1. Log in to the ZPA Admin Portal.
2. Take note of the URL used to login.

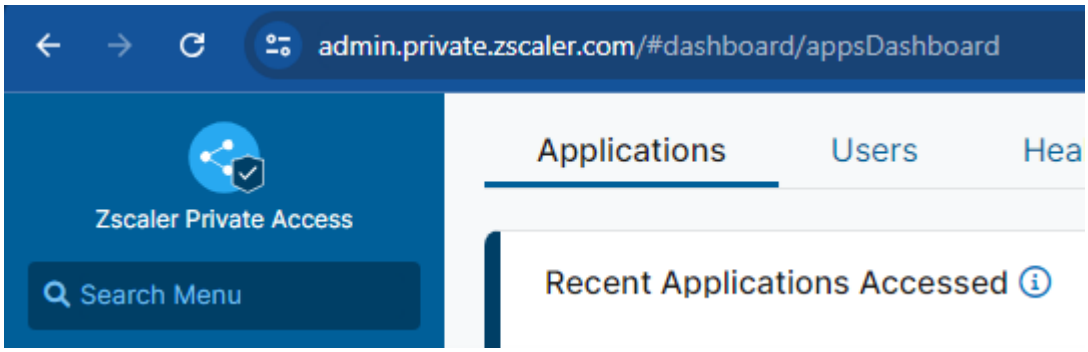

Figure 1. ZPA Admin Portal

Use this URL, but point it to the API subdomain. For example:

```
https://config.private.zscaler.com
```


Finding ZPA Customer ID

To find the ZPA customer ID:

1. Log in to the ZPA Admin Portal and go to **Configuration & Control** > **Administration Control** > **Company**. The **Company Profile** window is displayed.

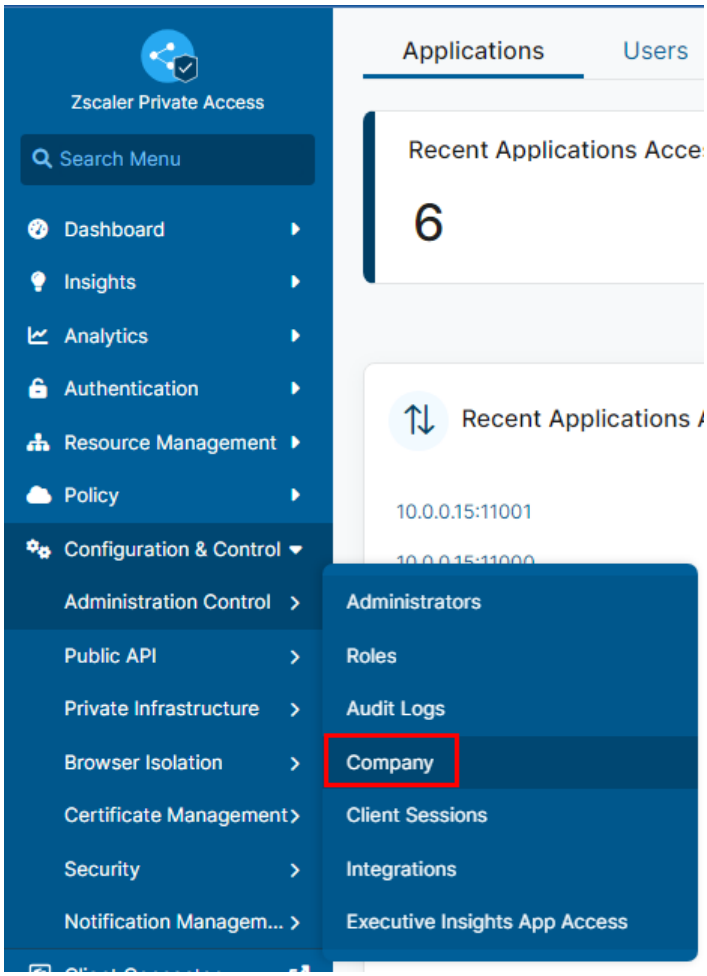

Figure 2. Company

2. In the **Company** window, find the **ZPA Tenant ID**. Copy the **ZPA Tenant ID**.

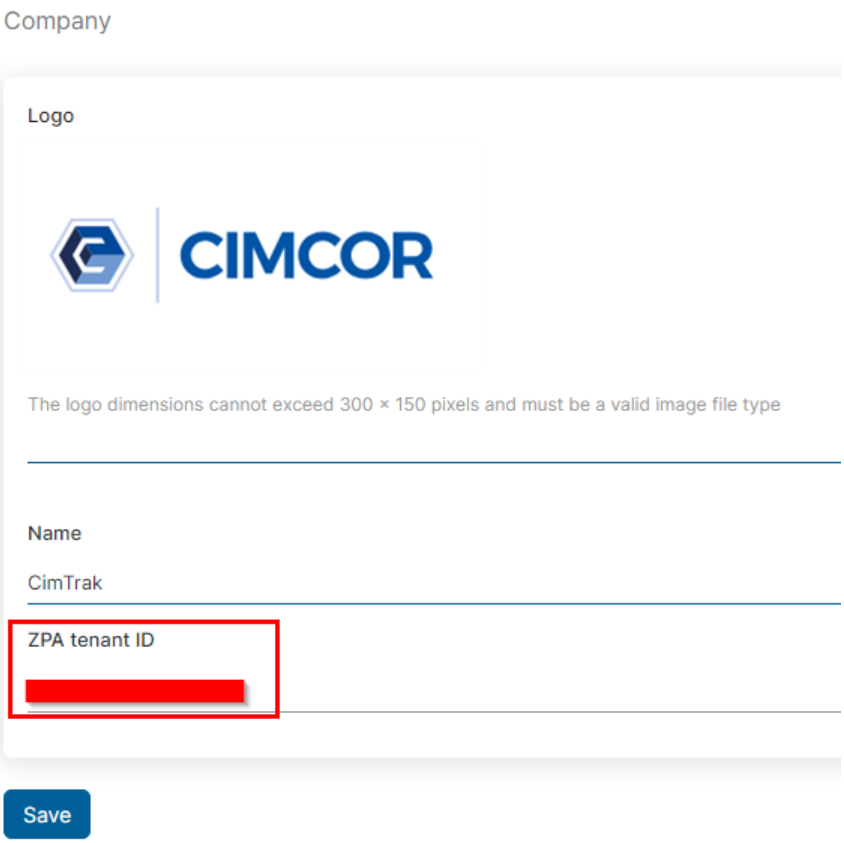

Figure 3. ZPA Tenant ID

Generating ZPA Client ID / Client Secret

To learn more about generating a API Client ID and Client Secret, see **About API Keys** (government agencies, see **About API Keys**).

ZIA Prerequisites

To integrate ZIA with CimTrak, you must gather the following:

- ZIA Endpoint URL
- ZIA Administrator Username
- ZIA Administrator Password
- ZIA API Key

Finding ZIA Endpoint URL

To find the ZIA endpoint URL:

1. Log in to the ZIA Admin Portal.
2. View the URL you used to login.

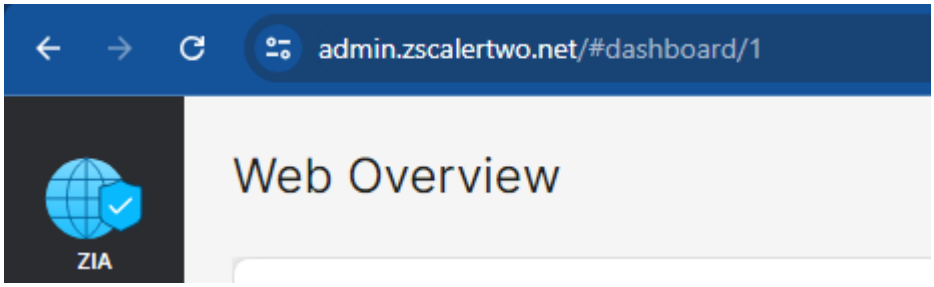

Figure 4. ZIA Admin Portal URL

Use the ZIA Admin Portal URL, but point to the API subdomain. For example:

`https://zsapi.zscalertwo.net`

Username/Password

Use an Administrator user's credentials.

Generating API Key

To generate an API key from the ZIA Admin Portal:

1. Go to **Administration** > **Cloud Service API Security**.
2. Click **Add API Key.**

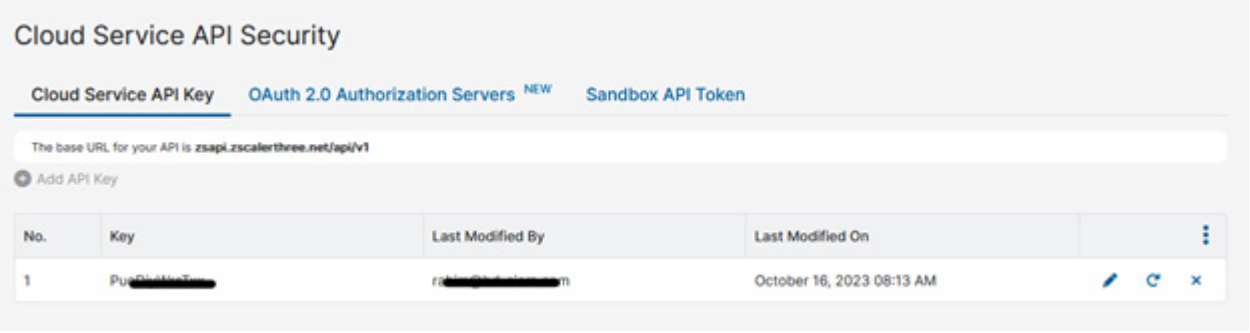

Figure 5. Cloud Service API Security

Creating a Role

Use an Administrator user's credentials. To create a role:

1. Go to **Administration** > **Role Management**.
2. Click **Add API Role**. The **Add API Role** window is displayed.

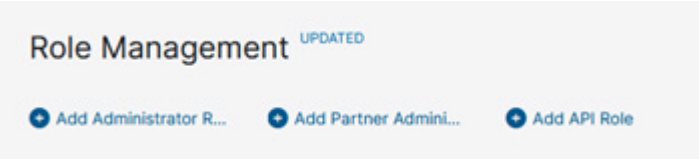

Figure 6. Role Management

3. Create the **API Role** by configuring the fields as shown in the image.

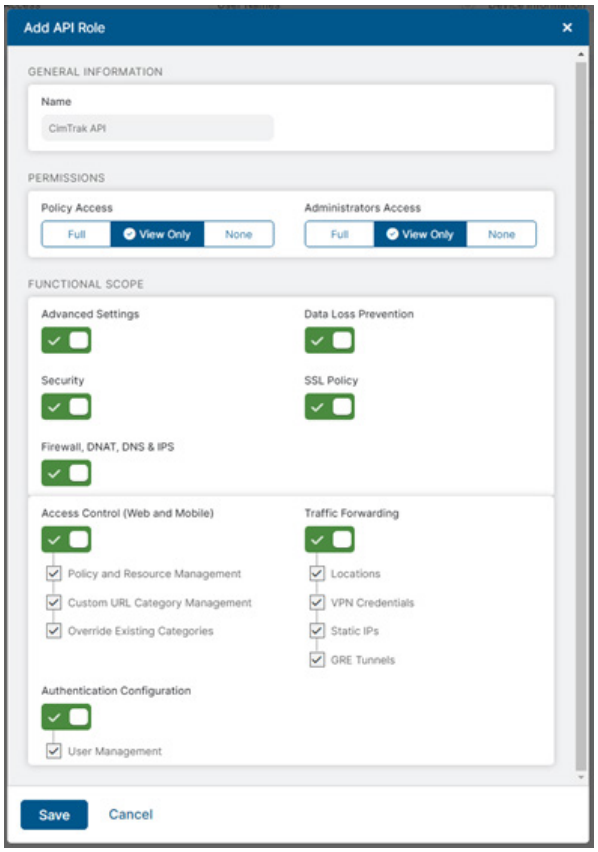

Figure 7. Add API Role

Creating an API User

To create an API user:

1. Go to **Administration** > **Administrator Management**.
2. Click **Add Administrator** and assign the created Role.
3. Enter the **Login ID** and **Password**.
4. Click **Save**.

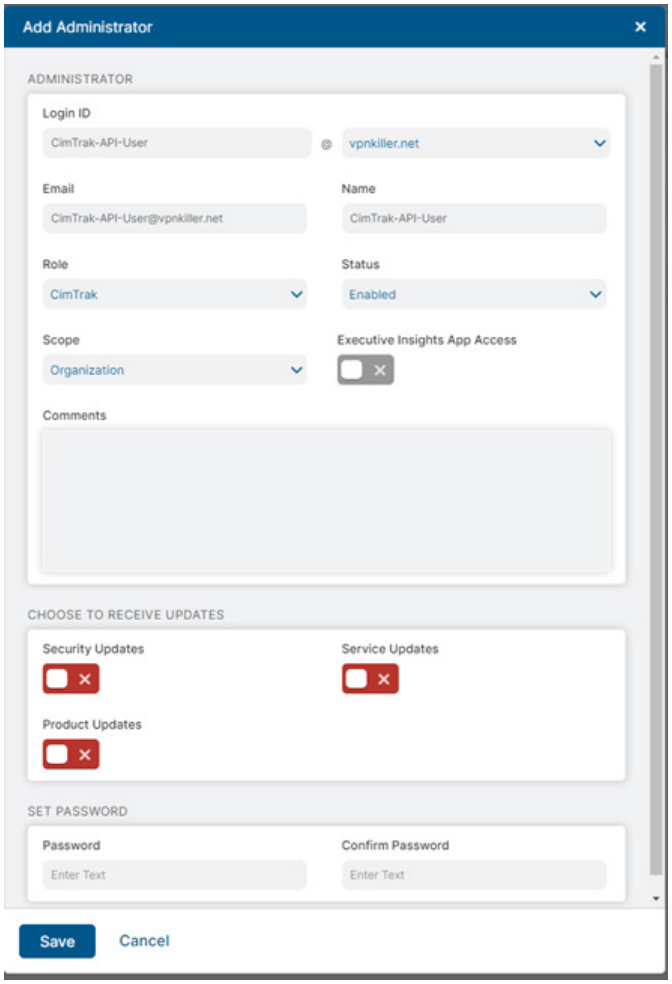

Figure 8. Add Administrator

Configuring ZPA and CimTrak

This section of the deployment guide helps you configure CimTrak to integrate with Zscaler and deploy the monitoring capabilities or triggers to automate Zscaler policies.

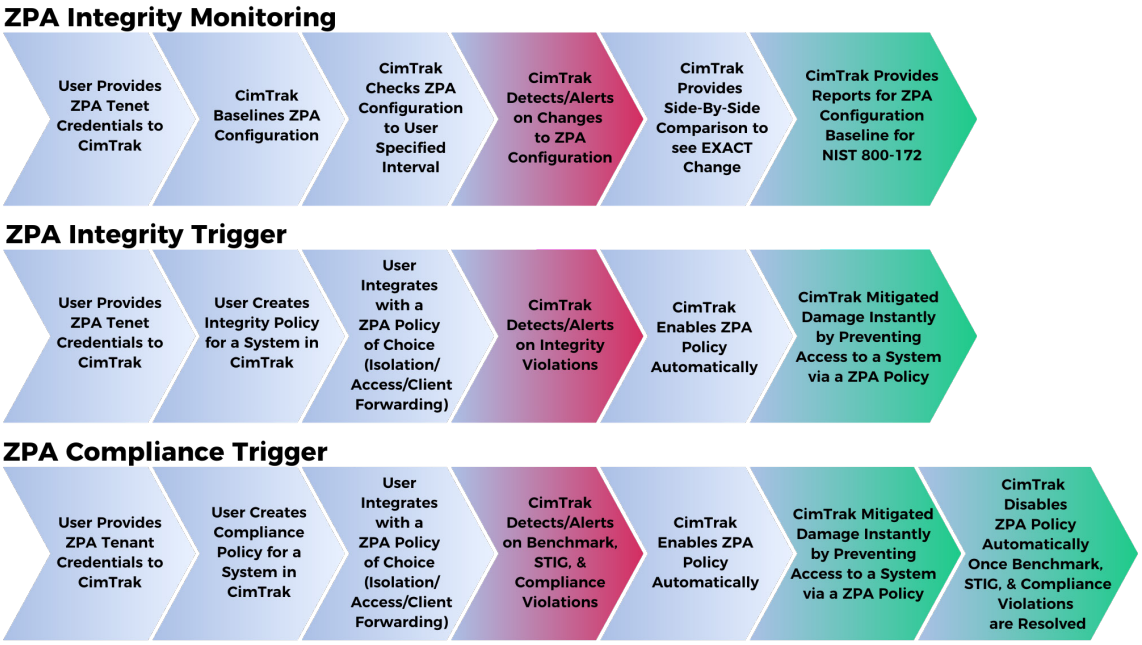

Figure 9. ZPA and CimTrak monitoring flow

Monitoring ZPA

To set up monitoring ZPA for configuration changes, review the following sections.

Log In to Your CimTrak Console

Go to your CimTrak Web Console in your environment and log in as a CimTrak Administrator. Refer to the following for example links:

- *https://CimTrak-Server/cmc*
- *https://192.168.4.15/cmc*

Figure 10. CimTrak log in

Creating CimTrak Integrity Policy

After logging in to the dashboard:

1. Right-click the **CimTrak Repository** in the **Tree View**.
2. Go to **New** > **Device and Policy**.

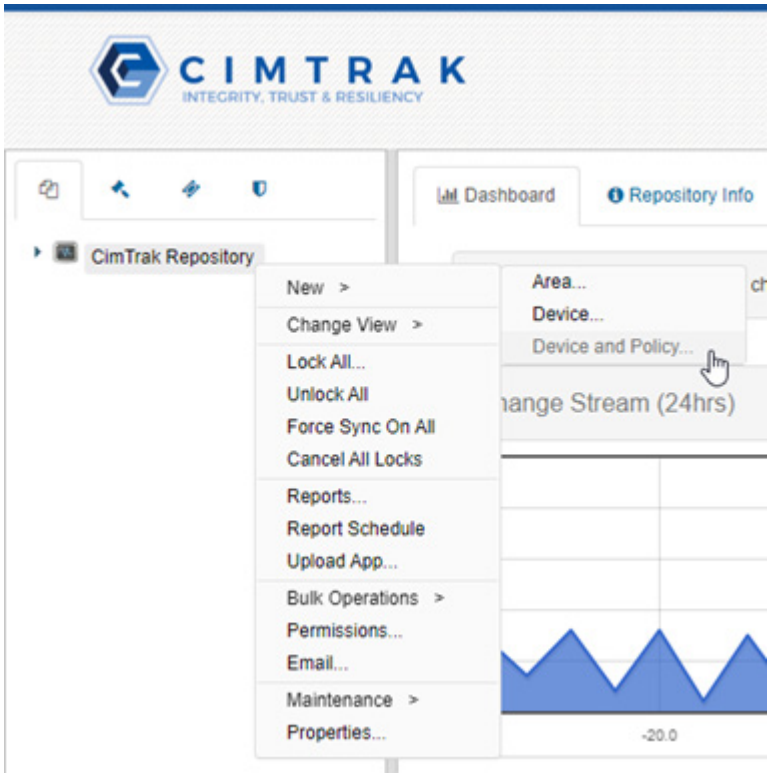

Figure 11. Device and Policy

3. In the **New Device and Policy** window, select the **Integrity Monitoring (Agentless)** option. The **Plugin Properties** window is displayed.

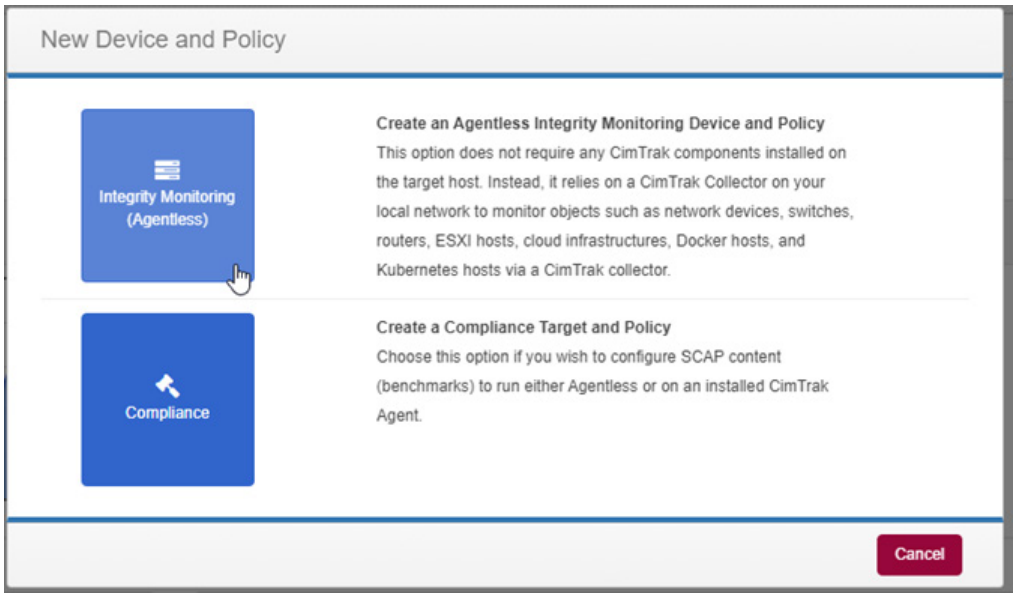

Figure 12. New Device and Policy

4. In the **Plugin Properties** window:
   a. For **Device Type**, select **Zscaler**.
   b. For **Zscaler Product,** select **ZPA**.
   c. Enter the **ZPA Endpoint/Customer ID/Client ID/Client Secret** previously gathered.
   d. Choose your **Output Format** (Zscaler recommends **Properties Format**).
   e. Click **OK**.

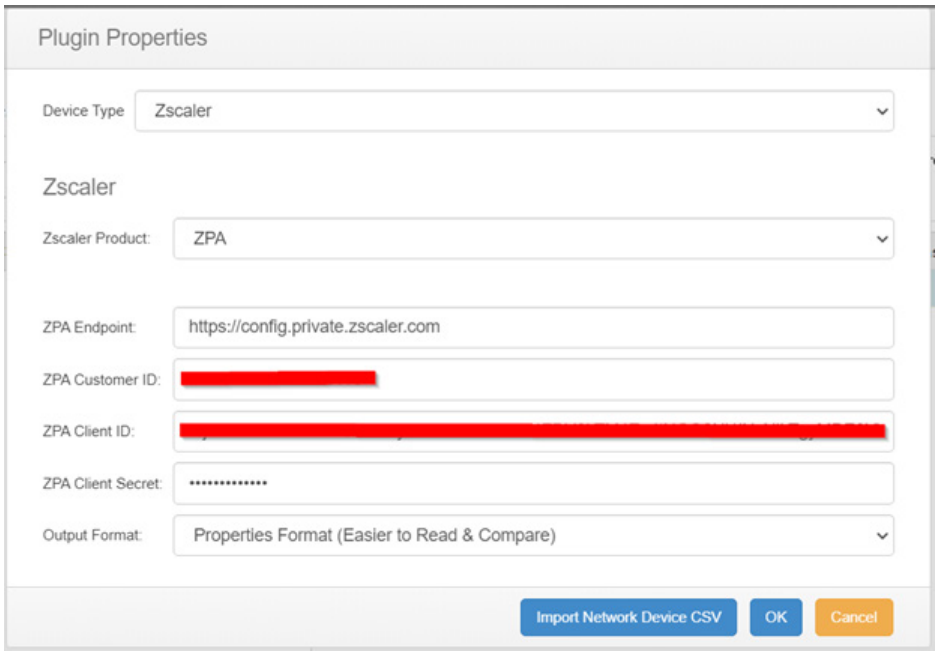

Figure 13. Plugin Properties

   f. Click the **Arrow** next to /DeviceRoot. This shows you what is available to monitor. Zscaler recommends that you select the top checkbox next to /DeviceRoot to monitor all ZPA configurations.
   g. Deselect the configurations you want to exclude.

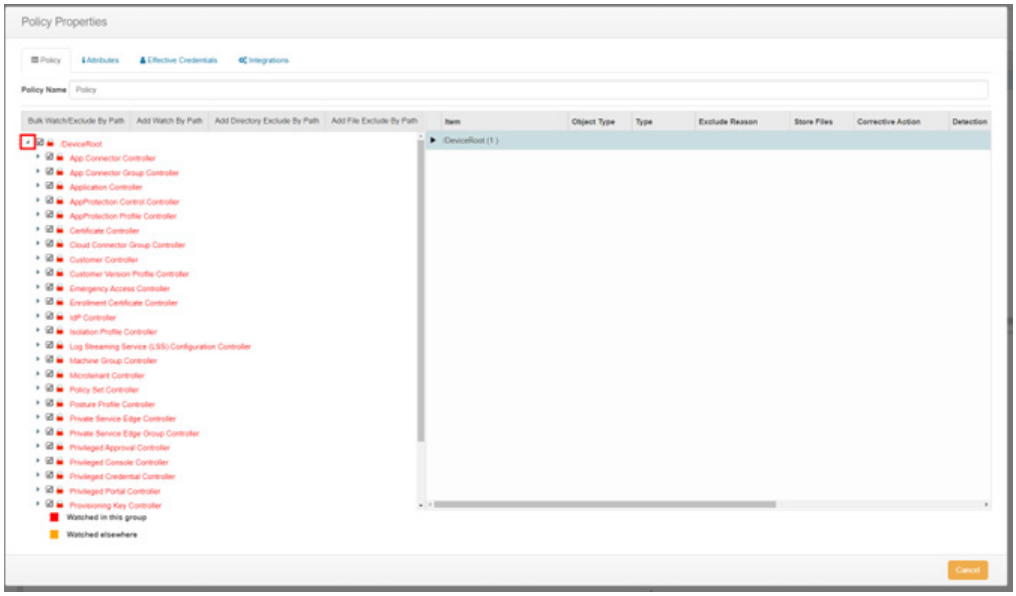

Figure 14. Policy Properties

5. After selecting the checkbox, configure the **Watch Properties**. CimTrak recommends choosing **Log** mode.
6. Change the **Poll Detection (interval)** to have CimTrak check for an interval of your choice for Zscaler. The default is every two hours (02 hours and 00 minutes).
7. Leave all other default settings as they are not relevant for this integration.
8. Click **OK**.

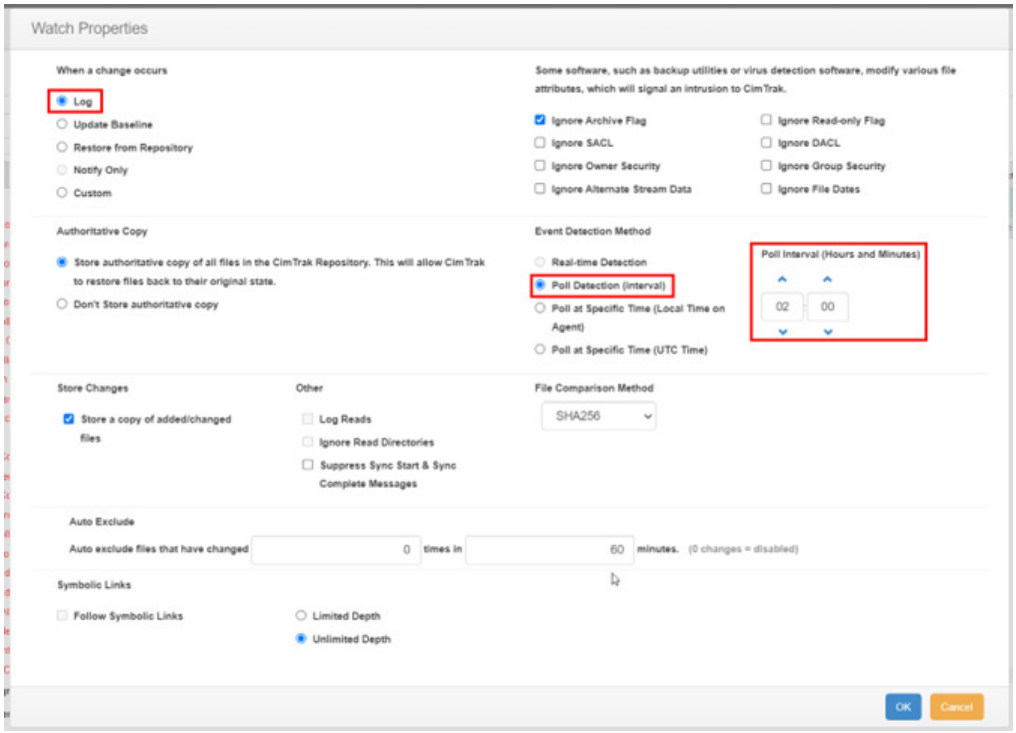

Figure 15. Watch Properties

9. Enter a **Device Name** (e.g., `Zscaler ZPA`).

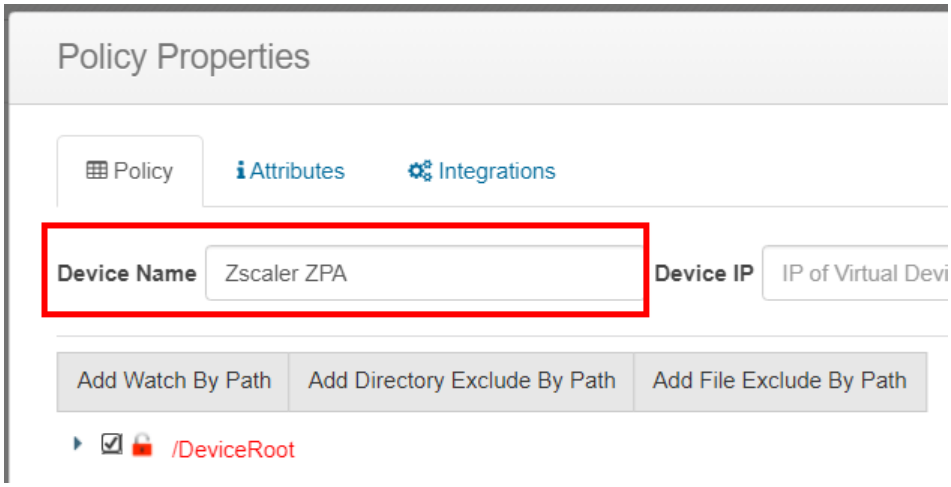

Figure 16. Device Name

10. Click **OK**.

Enabling CimTrak Integrity Policy

After the policy is created, it is not yet being monitored. To enable policy monitoring intervals:

1. Right-click the policy name and select **Lock and Digitally Sign**. Monitoring starts by taking an initial baseline and then reports on any deviations since this baseline.

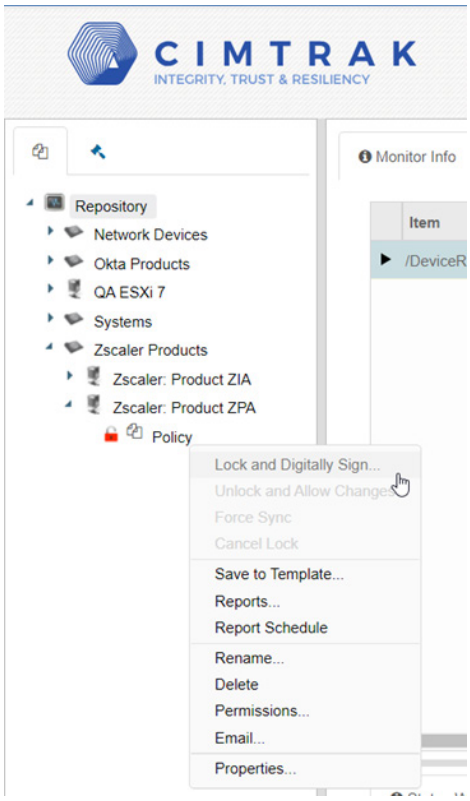

Figure 17. Repository

This process can take some time, and you can see the progress in the **Status Window**.

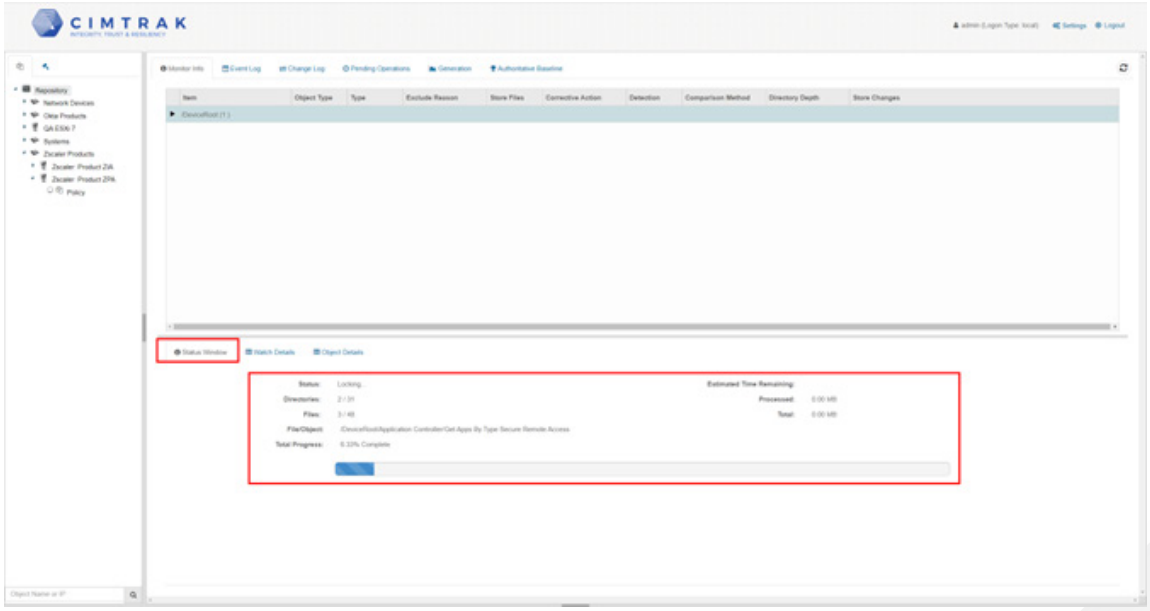

Figure 18. Status window

2. After it is complete, the policy changes from a red **Unlock** icon to a blue **Lock** icon. The policy continues to check on your specified interval. You see the **Sync Start** message in the **Event** Log.

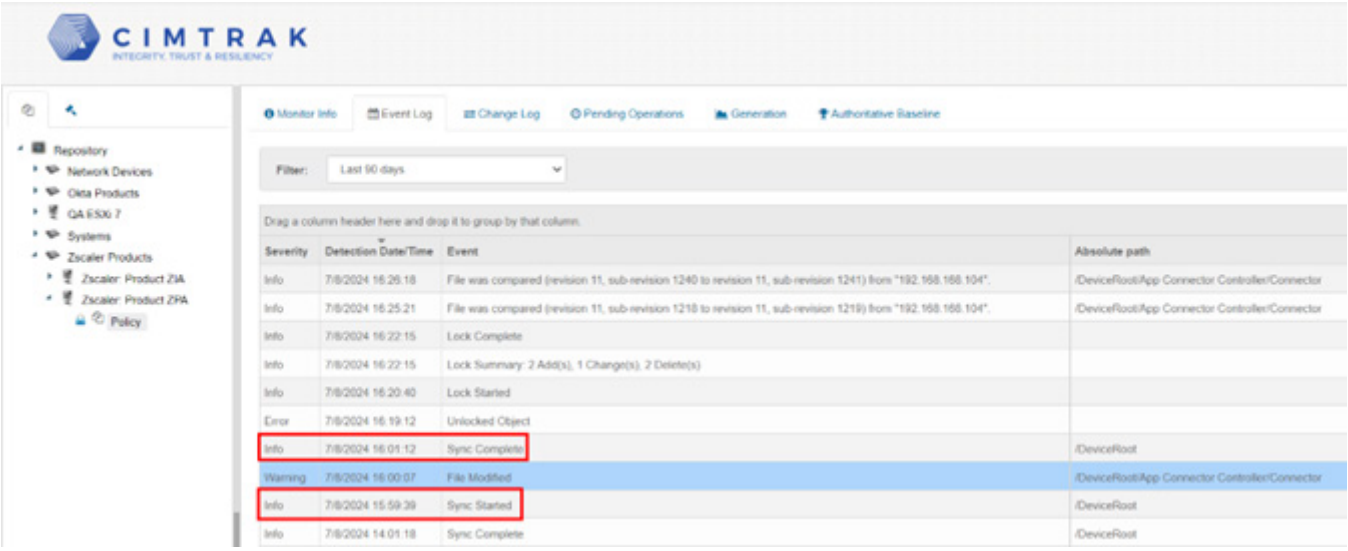

Figure 19. Event Log

Reviewing the Change Log

After CimTrak starts detecting changes, it is reported in the Change Log.

In the following images, you can see the time CimTrak detected the change, and the absolute path that indicates what changed.

These are the same categories of ZPA configurations you saw when creating the integrity policy initially.

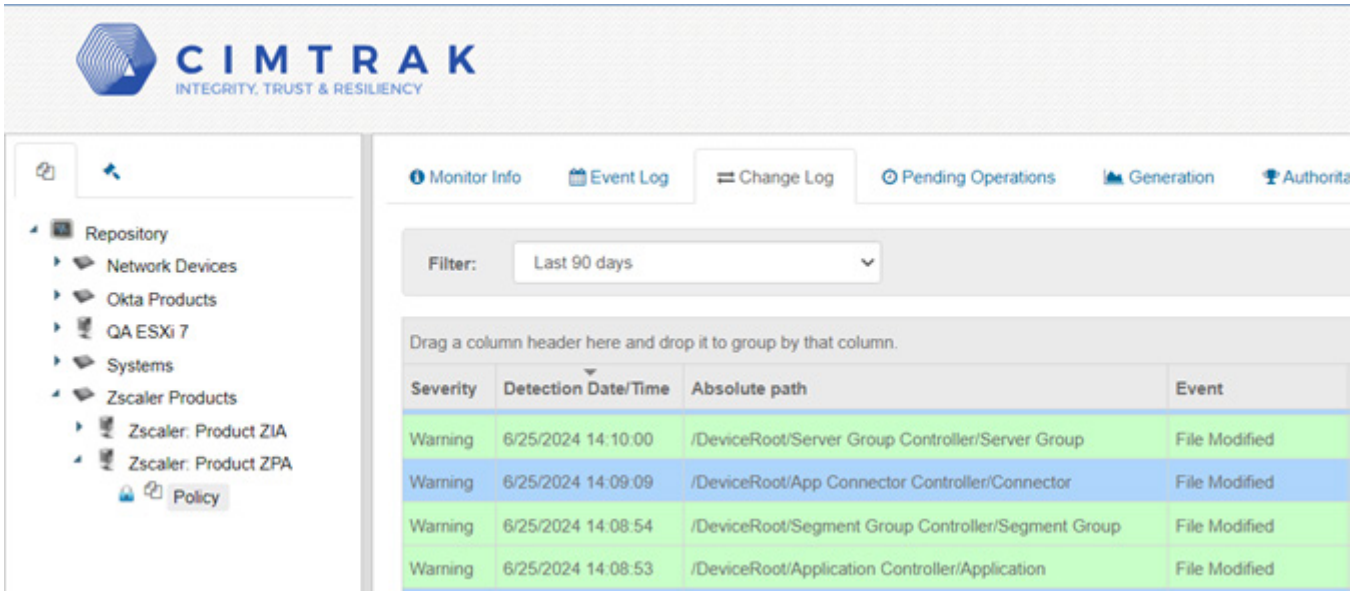

Figure 20. Policy Change Log

You can right-click an event and click **Compare Against Previous State On Agent** to see a side-by-side comparison to see exactly what has changed.

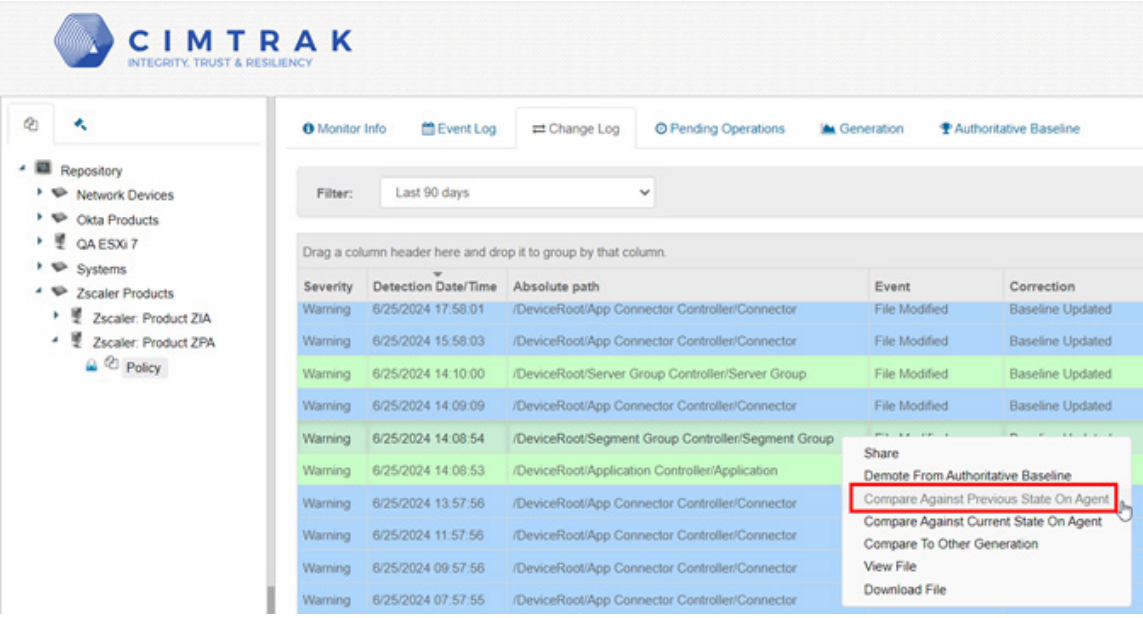

Figure 21. Compare Against Previous State On Agent

The following is the side-by-side comparison window.

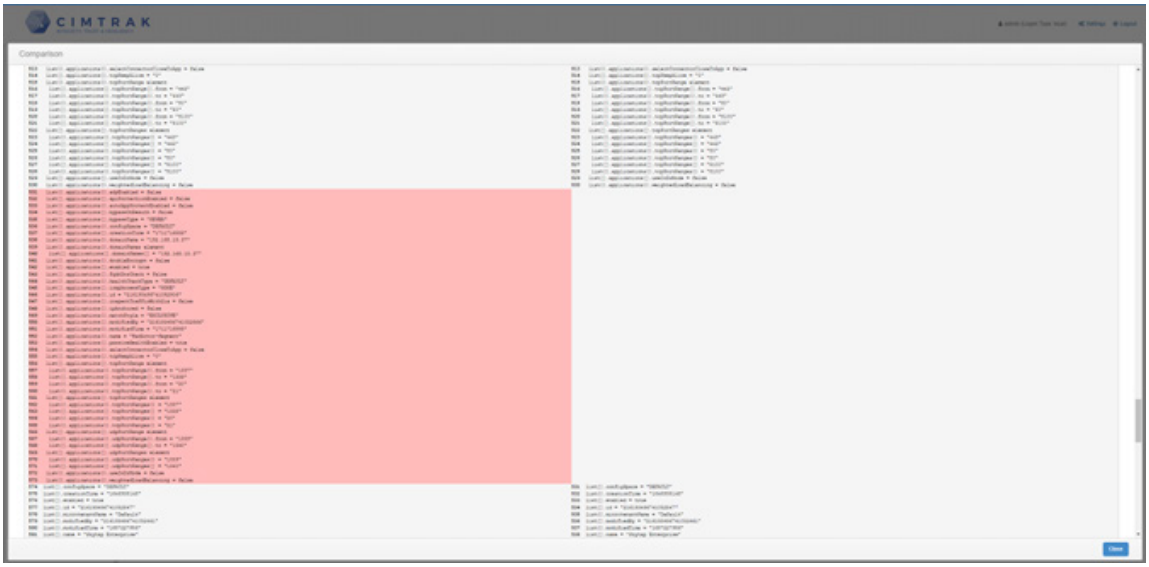

Figure 22. Compare Against Previous State

ZPA Integrity Triggers

The following sections detail how to configure ZPA integrity triggers.

Log In to Your CimTrak Console

Go to your CimTrak Web Console in your environment and log in as a CimTrak Administrator. For example:

- `https://CimTrak-Server/cmc`
- `https://192.168.4.15/cmc`

Figure 23. CimTrak Admin

Integrating Zscaler Tenant

To integrate the Zscaler tenant:

1. Right-click **Repository** in the **Tree View** on the left.
2. Select **Properties**.

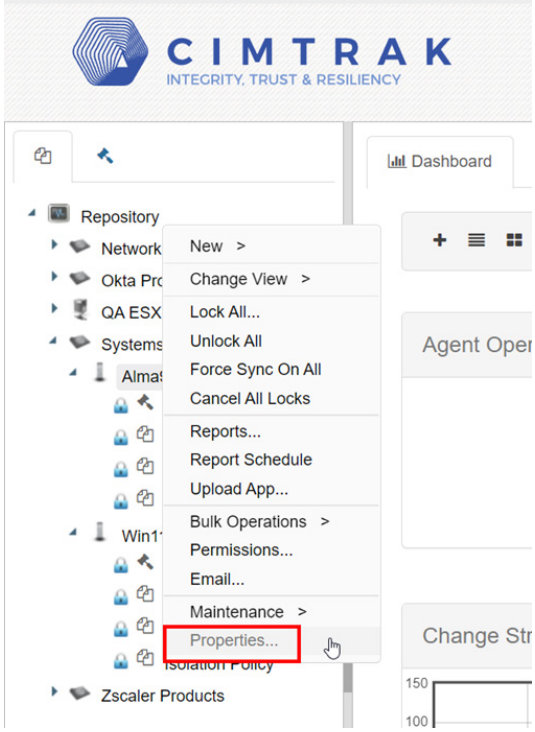

Figure 24. Properties

3. Click the **Integrations** tab.

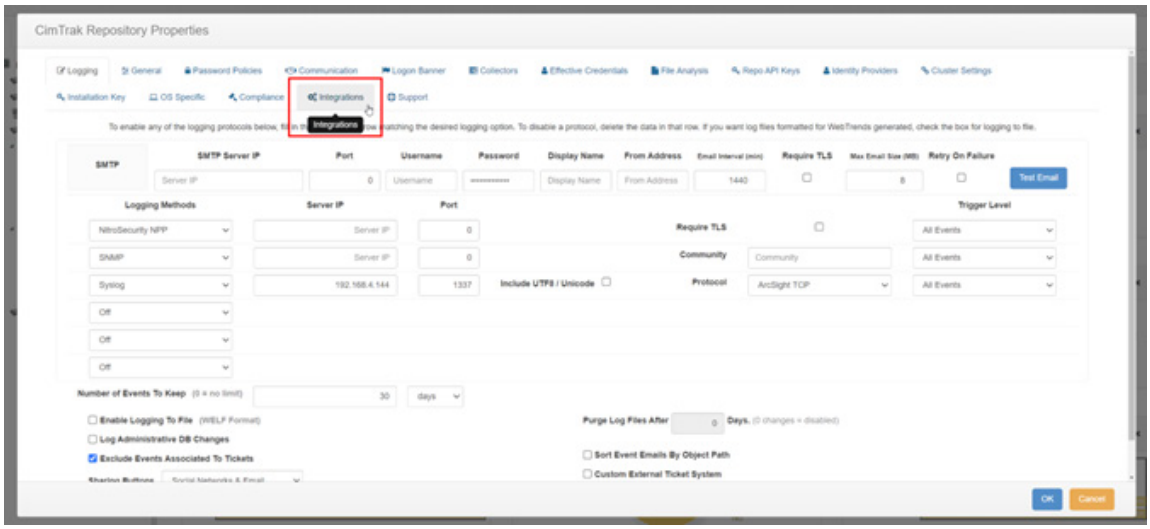

Figure 25. Integrations

4. Enter your ZPA Credentials:
   - **Endpoint**: the endpoint URL.
   - **Client Id**: the ZPA client ID.
   - **API Key**: the ZPA API key.
   - **Customer Id**: the ZPA customer ID.

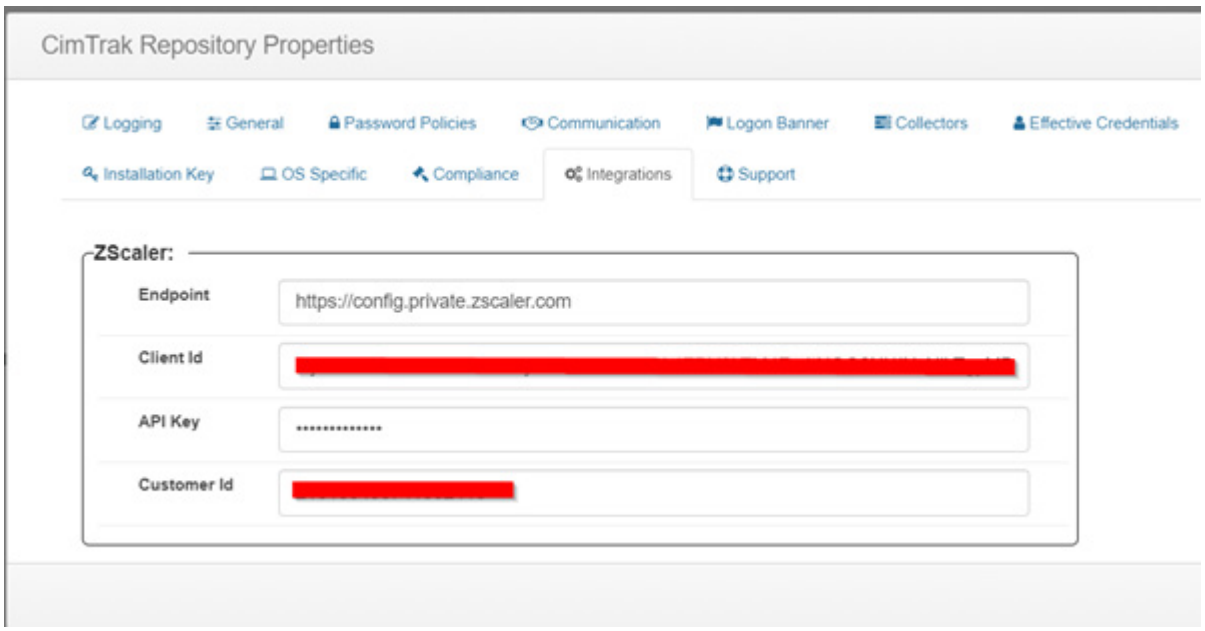

Figure 26. ZPA credentials

Creating CimTrak Integrity Policy

To create a CimTrak integrity policy:

1. In the left-side **Tree View**, find the system in question for which you want to create a policy.
2. Right-click the <agent name>, and select **New** > **Policy.**

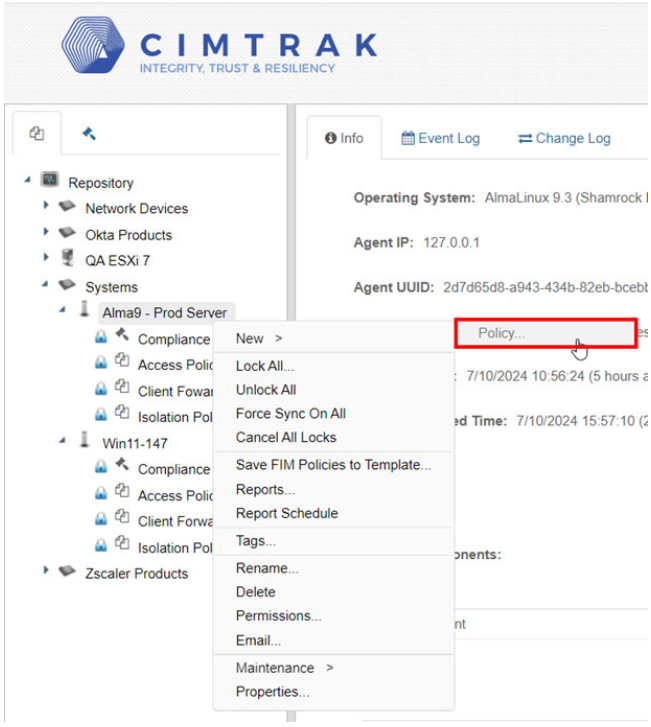

Figure 27. CimTrak policy

3. Select **Integrity Monitoring (Agent Based)**.

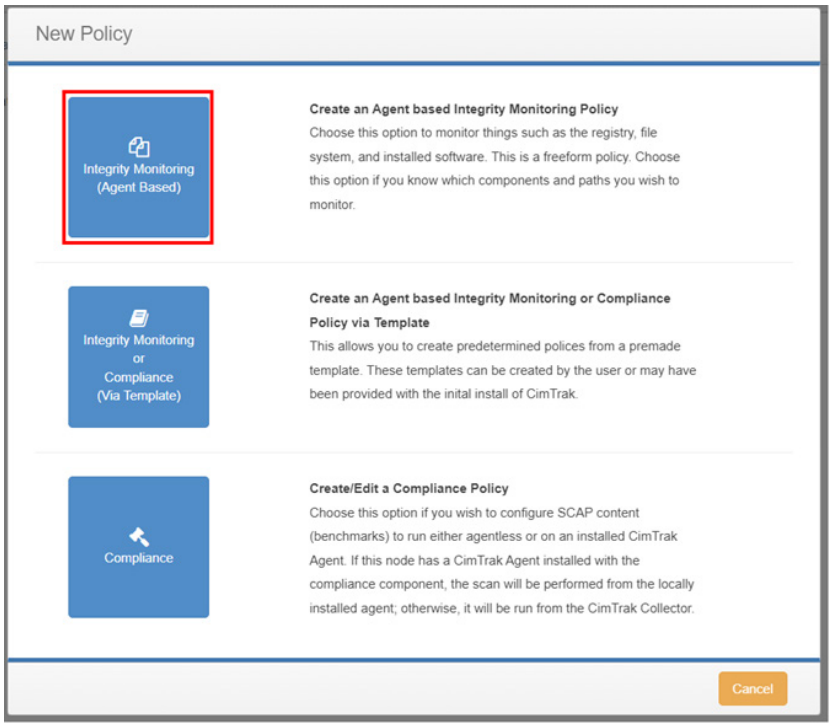

Figure 28. New Policy

4. Select the folder or object that you want to monitor. In this case, it is a folder on a Linux system.

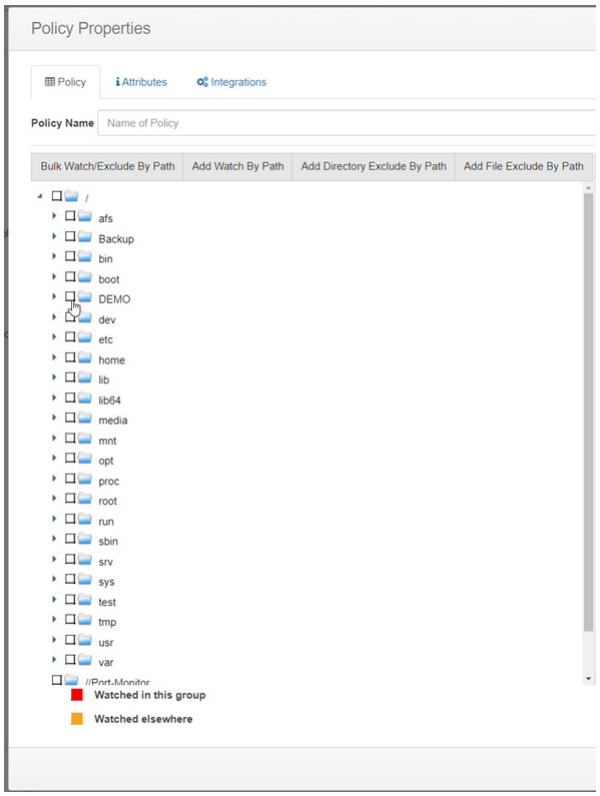

Figure 29. Policy Properties

5. In the window that displays, select the monitoring options you would like to use. For this example, **Log** mode is selected and everything else remains as default.
6. Click **OK**.

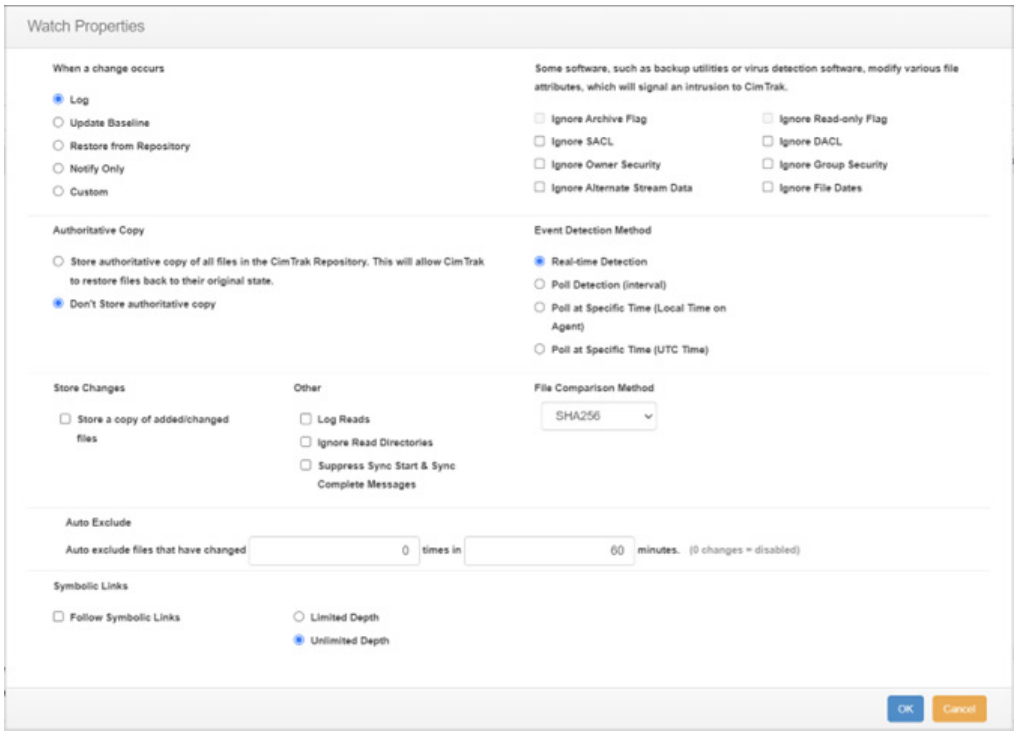

Figure 30. Watch Properties

7. Enter a name for the **Policy Name**.
8. Do not click **OK** and proceed to **Configuring Zscaler Integration**, next.

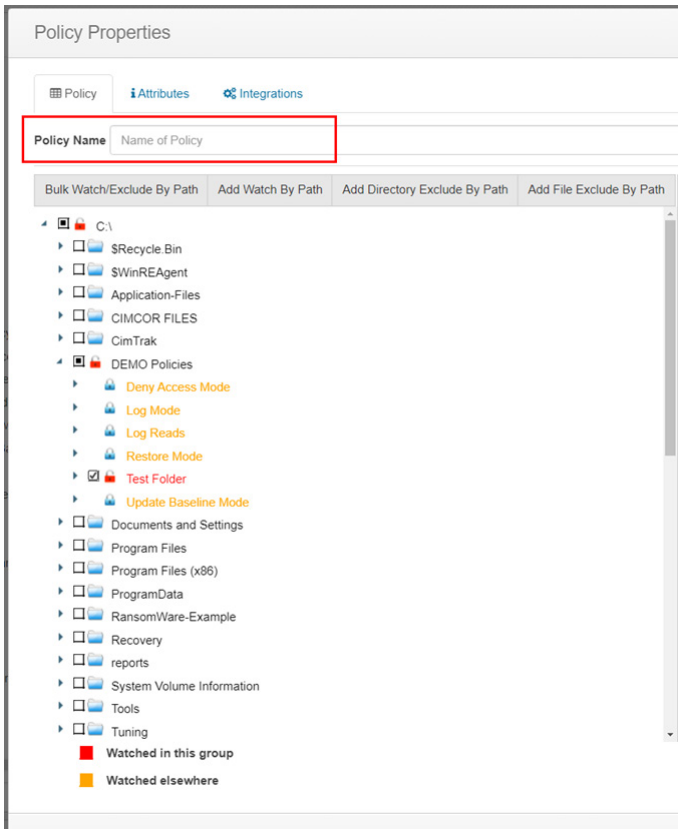

Figure 31. Policy Name

Configuring Zscaler Integration

To configure the Zscaler integration:

1. Click the **Integrations** tab.

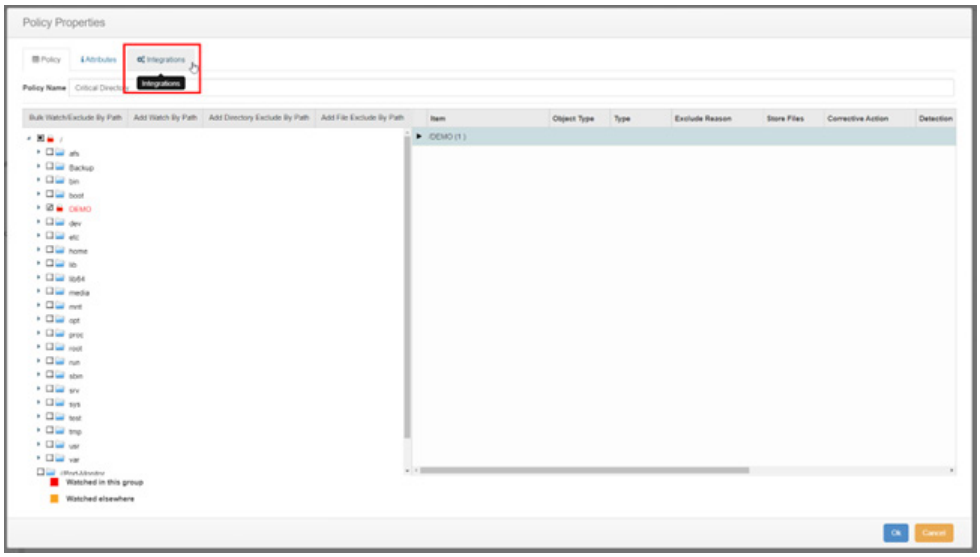

Figure 32. Integrations tab

2. Choose the ZPA Policy type to integrate:
   - **Access Policy.** See **Integrating with Access Policies**.
   - **Client Forwarding Policy**. See **Integrating with Client Forwarding Policies**.
   - **Isolation Policy**. See **Integrating with Isolation Policies**.

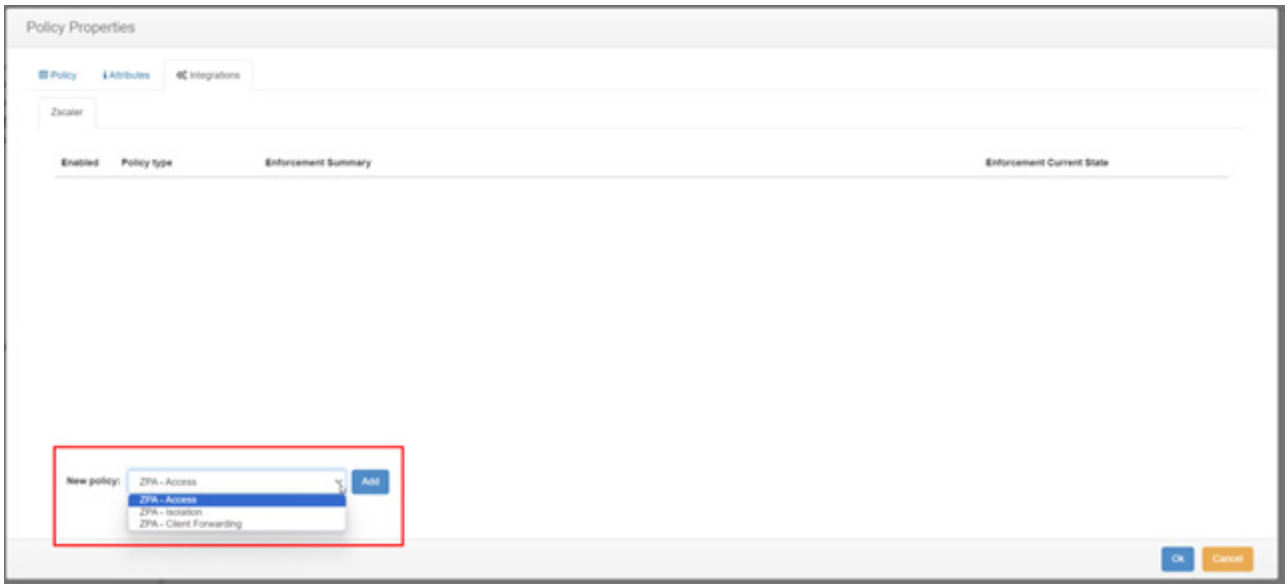

Figure 33. Policy Types

Integrating with Access Policies

To integrate access policies:

1. Select **ZPA – Access** and click **Add**.

Figure 34. New Policy

2. A window displays for you to configure how you want this integration to interact with your policy. It is a logic statement that you can configure and change with a drop-down menu, as follows:

   If an <INTEGRITY TRIGGER> occurs, then trigger Zscaler rule <ZSCALER ACCESS POLICY> in <MODE> mode, otherwise leave the policy in <MODE> mode.

Figure 35. Access Integrity Trigger

The following sections define the parameters:

- **INTEGRITY TRIGGERS**: The CimTrak Integrity options to trigger the policy you configure.
  - **Change**: If any change that deviates the baseline.
  - **Denied List Item Found**: If any change was a matching hash in the CimTrak Deny List (denylist).
  - **Not in allowed list**: If any change was NOT a matching hash in the CimTrak Allow List (allowlist).
- **ZSCALER ACCESS POLICY**: This drop-down menu populates the available Access Policy found in your ZPA environment:
  - **Access Policy 1**
  - **Access Policy 2**
  - **Access Policy N**

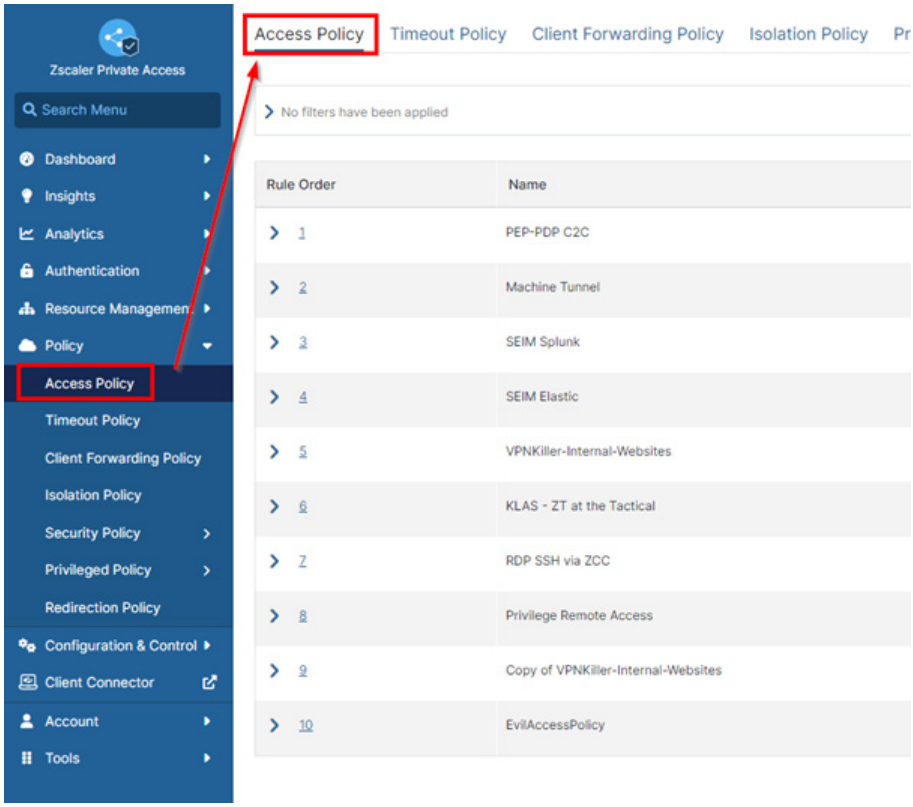

Figure 36. Access Policy

- **MODE**: The Access Policy Rule Actions:
  - **Allow Access**
  - **Require Approval**
  - **Block Access**

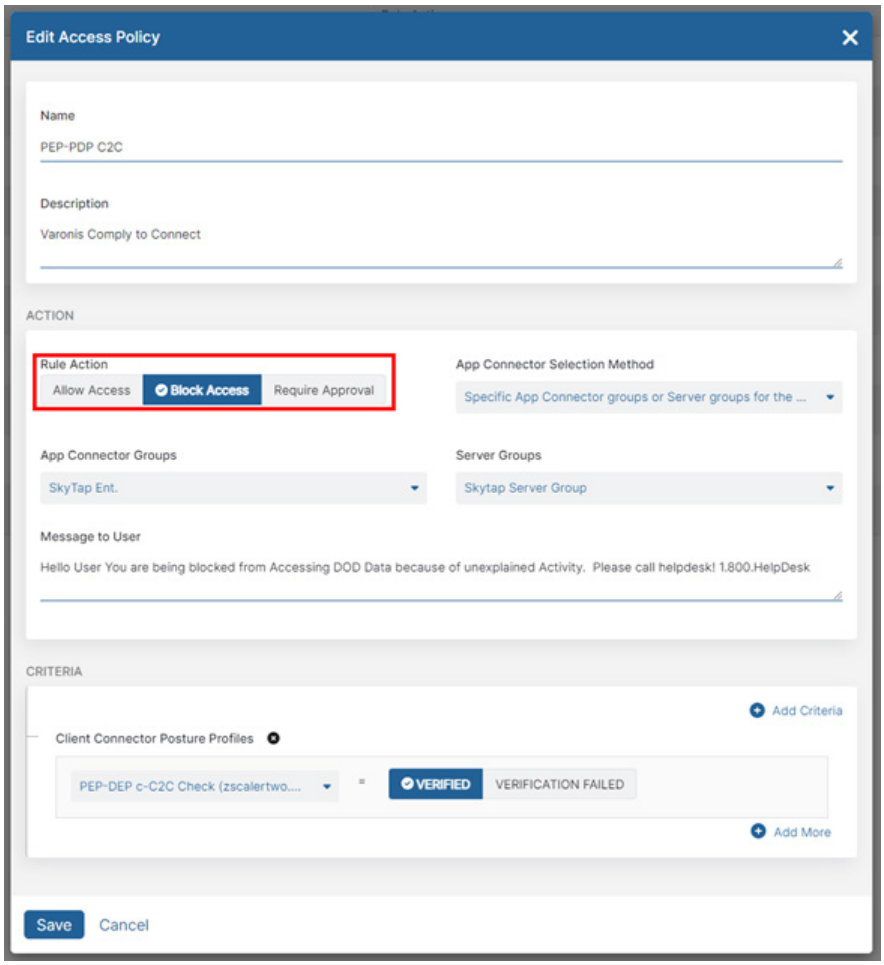

Figure 37. Rule Actions

3. Click **Save**. The final logic statement created for the policy trigger is displayed.

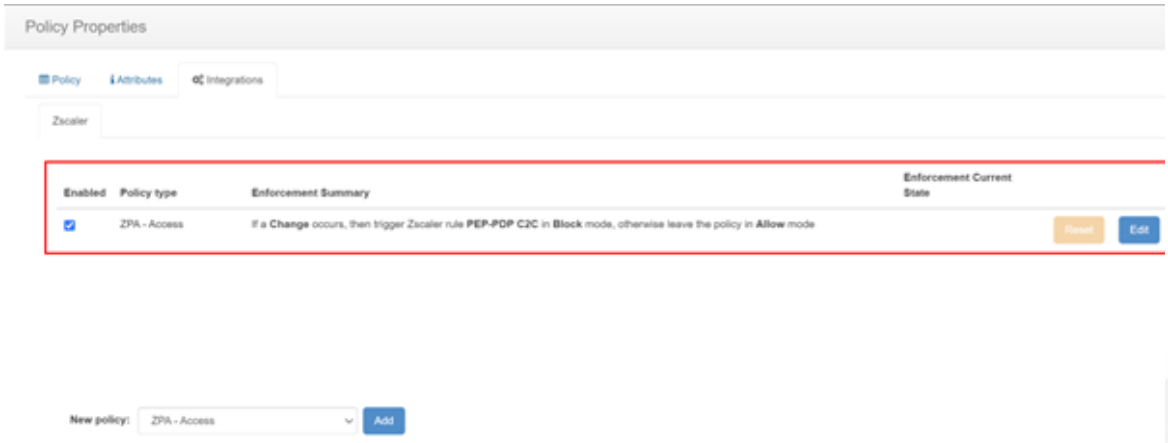

Figure 38. Final logic statement

4. Click **OK** to save the policy.

Figure 39. Save the policy

5. Find your new policy under the **Agent**. It was created with a red **Unlocked** icon because it is disabled. To enable it, right-click and select **Lock and Digitally Sign**.

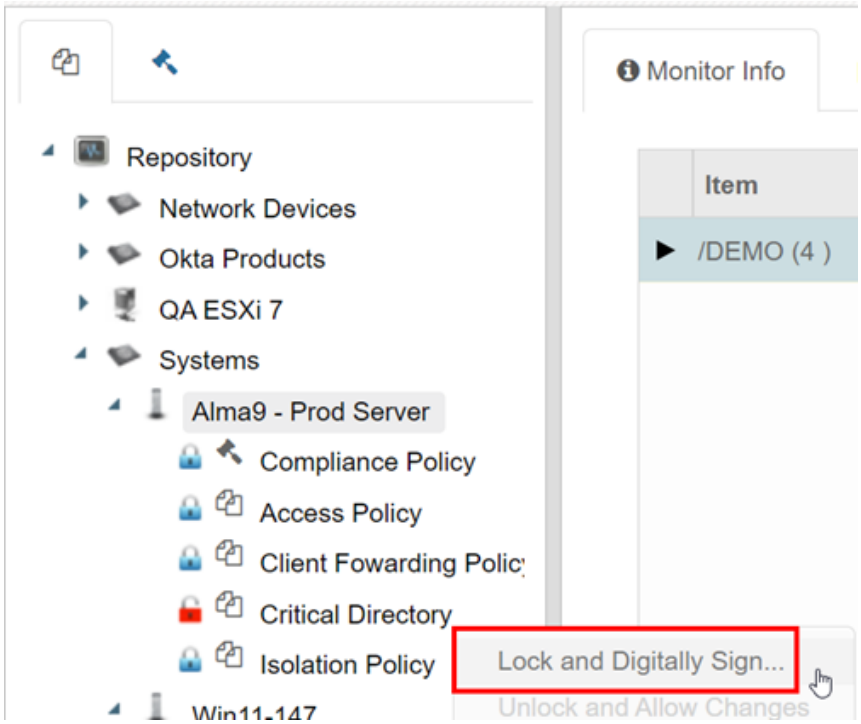

Figure 40. Lock and Digitally Sign

It takes a baseline of the objects you configured to monitor to get the current state. When complete, it has a blue Locked icon, which means it is enabled.

Testing the Integration

Now it is time to test your rules.

In the following example, a policy was set up to monitor the directory /DEMO. The trigger is CHANGE, which enables the Access Policy that is in ALLOW mode.

1. Check the directory. The following shows the current state of the directory.

```
[root@alma9-50 DEMO]# pwd
/DEMO
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 41. Current directory state

2. If a file is added that does not match any hash in the CimTrak Authoritative Baseline, it triggers the access policy.

```
[root@alma9-50 DEMO]# touch nefarious-file
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root      0 Jul 10 15:58 nefarious-file
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 42. Triggered Access Policy

3. From the CimTrak Web Console, go to the **Policy Event Log**.

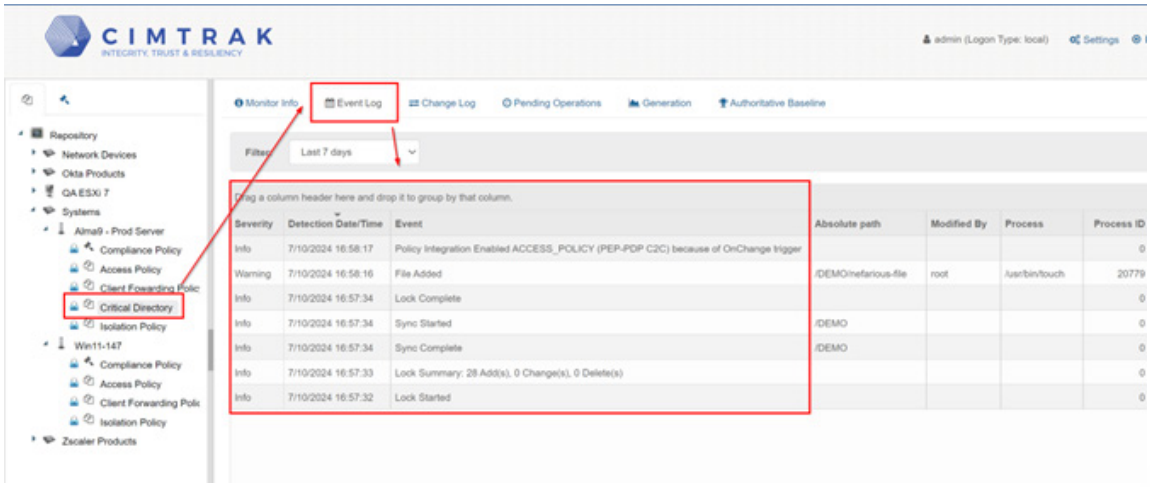

Figure 43. Policy Event Log

4. In the **Event Log**, you can see that the new file was detected with other forensic details. You can also see one second later the access policy was triggered.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event	Absolute path	Modified By	Process	Process ID
Info	7/10/2024 16:58:17	Policy Integration Enabled ACCESS_POLICY (PEP-PDP C2C) because of OnChange trigger				0
Warning	7/10/2024 16:58:16	File Added	/DEMO/nefarious-file	root	/usr/bin/touch	20779
Info	7/10/2024 16:57:34	Lock Complete				0
Info	7/10/2024 16:57:34	Sync Started	/DEMO			0
Info	7/10/2024 16:57:34	Sync Complete	/DEMO			0
Info	7/10/2024 16:57:33	Lock Summary: 28 Add(s), 0 Change(s), 0 Delete(s)				0
Info	7/10/2024 16:57:32	Lock Started				0

Figure 44. Triggered Access Policy

5. Go to ZPA **Edit Access Policy**. The Access Policy is in Block Access mode.

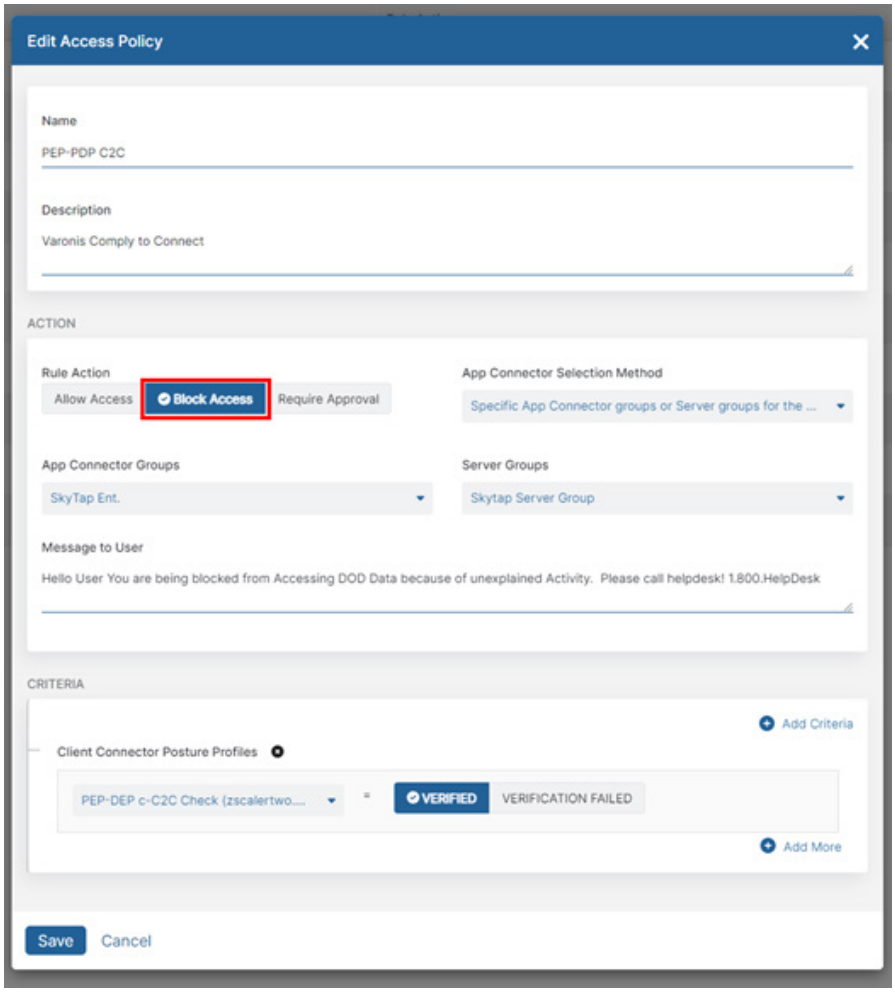

Figure 45. Edit Access Policy

Resetting the Integration

While you can change the Rule Action status within ZPA, there is also an option to do it from the CimTrak Web Console:

1. Right-click **Repository**, then select **Properties**.

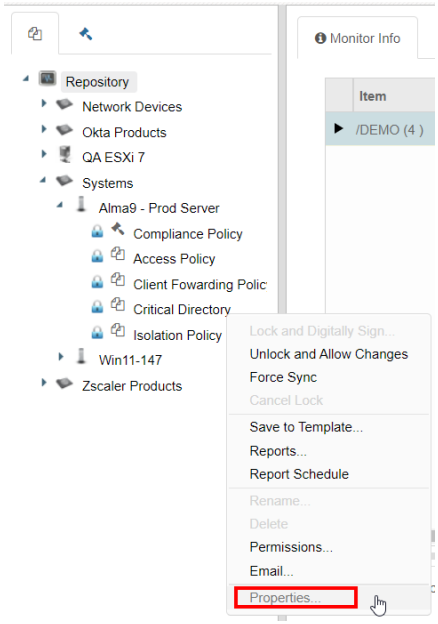

Figure 46. Policy Properties

2. Click the **Integrations** tabs. You can see the current ZPA policy status.

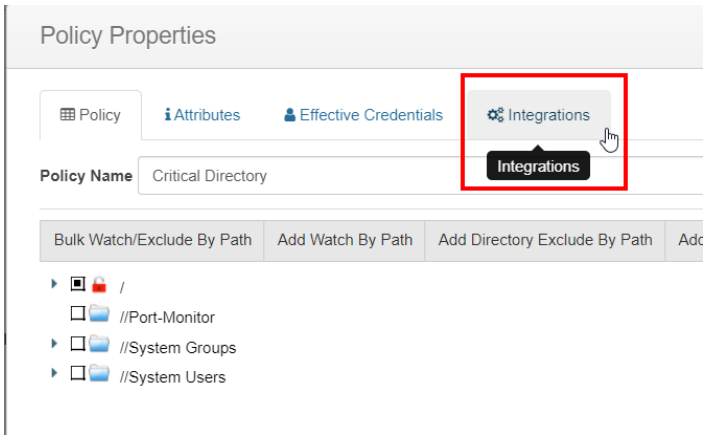

Figure 47. CimTrak Integrations

3. Click **Reset** to undo the action.

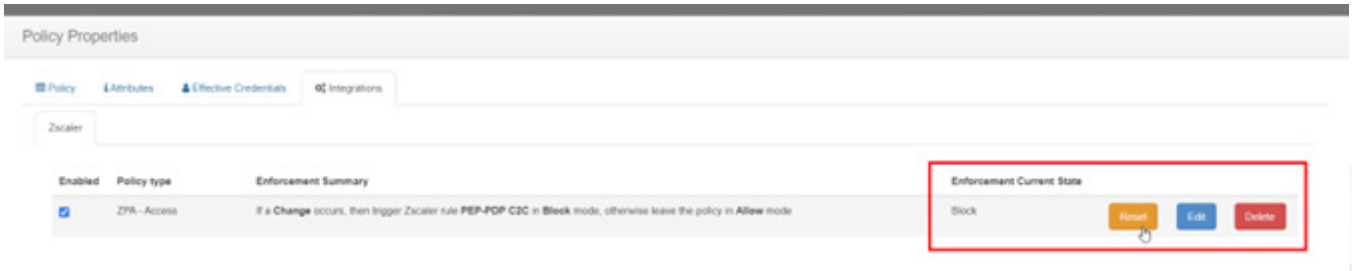

Figure 48. Reset button

Integrating with Client Forwarding Policies

To integrate with client forwarding policies:

1. Select **ZPA – Client Forwarding** and click **Add**.

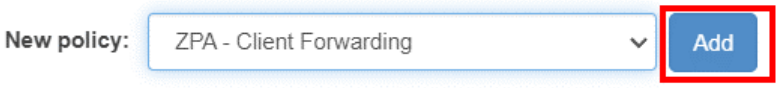

Figure 49. ZPA Client Forwarding

2. In the **Client Forwarding Policy** window, configure how you want this integration to interact with your policy.

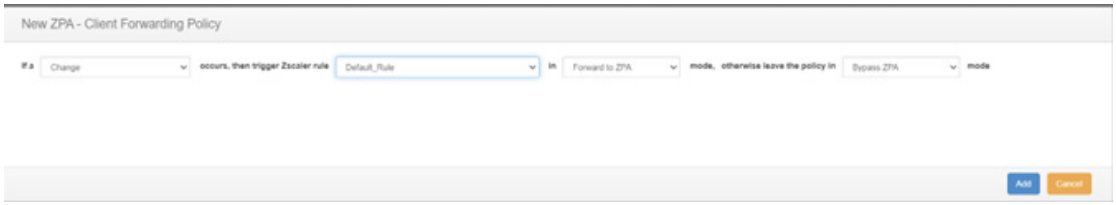

Figure 50. Client Forwarding Policy

This is a logic statement that you can configure and change with a drop-down menu, as follows:

If an <INTEGRITY TRIGGER> occurs, then trigger Zscaler rule <ZSCALER CLIENT FORWARDING POLICY> in <MODE> mode, otherwise leave the policy in <MODE> mode.

These variables are defined as follows:

- **INTEGRITY TRIGGERS**: The CimTrak Integrity options to trigger the policy you configure.
  - **Change**: If any change that deviates the baseline.
  - **Denied List Item Found**: If any change was a matching hash in the CimTrak Deny List (denylist).
  - **Not in allowed list**: If any change was NOT a matching hash in the CimTrak Allow List (allowlist).
- **ZSCALER CLIENT FORWARDING POLICY**: This drop-down menu populates the available Access Policy found in your ZPA environment:
  - **Client Forwarding Policy 1**
  - **Client Forwarding Policy 2**
  - **Client Forwarding Policy N**

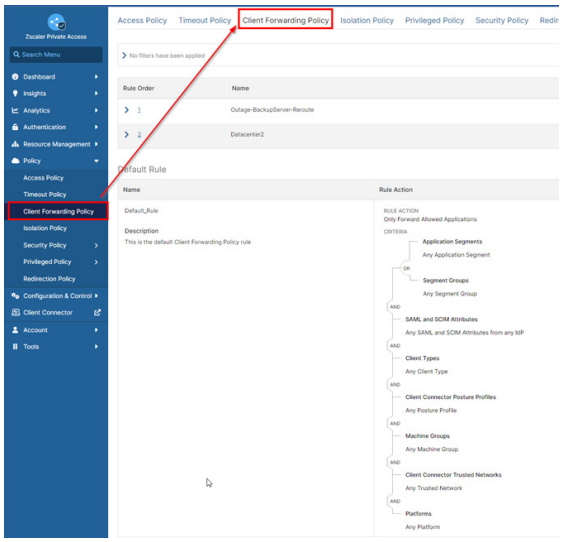

Figure 51. ZPA Client Forwarding Policy

- **MODE**: The Client Forwarding Policy Rule Actions:
  - **Forward to ZPA**
  - **Only Forward Allowed Applications**
  - **Bypass ZPA**

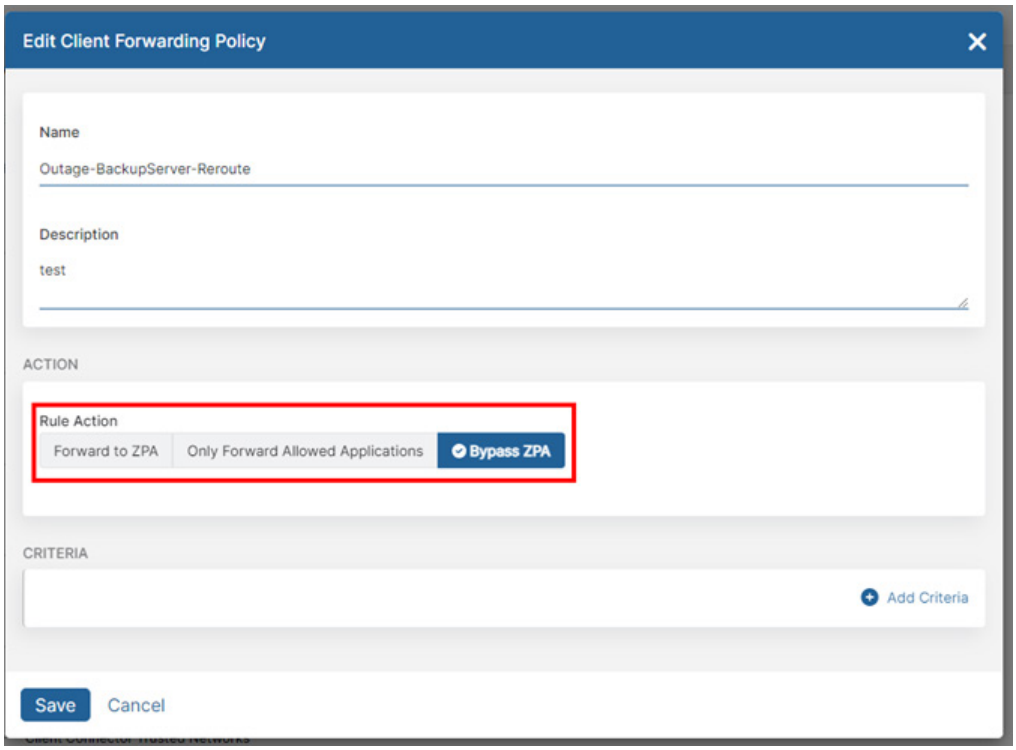

Figure 52. Edit Client Forwarding Policy

3. Click **Save**. The final logic statement is created for the policy trigger.

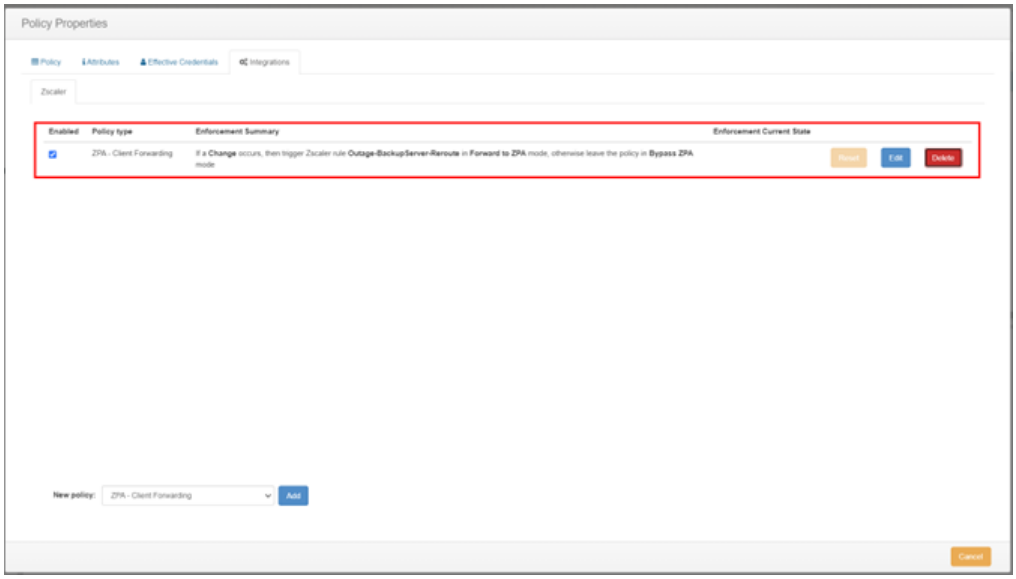

Figure 53. Logic statement

4. Click **OK** to save the policy.

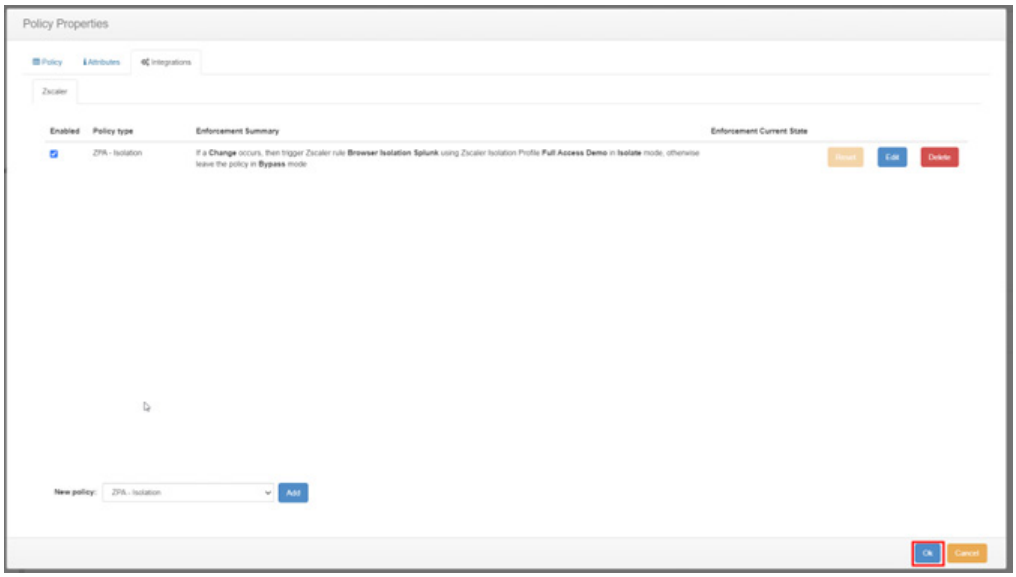

Figure 54. Save the Policy

5. Find your new policy under the Agent. It was created with a red **Unlocked** icon. This means it is disabled. To turn it on, right-click and select **Lock and Digitally Sign**.

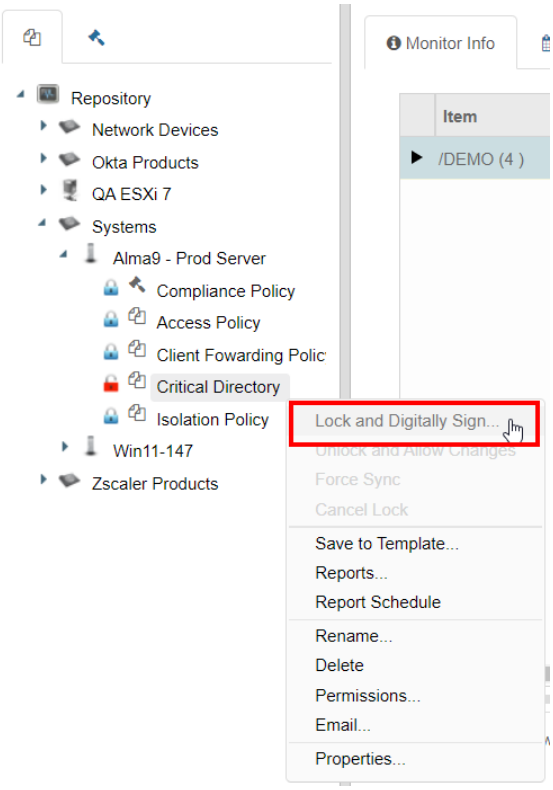

Figure 55. Lock and Digitally Sign

It takes a baseline of the objects you configured to monitor to get the current state. After it is enabled, it has a blue **Locked** icon.

Testing the Integration

Now you can test the integration rules. In the following example, a policy was set up to monitor the directory /DEMO. The trigger is CHANGE, which enables the Client Forwarding Policy (currently in Bypass ZPA mode).

This is the current state of the directory:

```
[root@alma9-50 DEMO]# pwd
/DEMO
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 56. Current directory

When you add a new file that does not match any hash in the CimTrak Authoritative Baseline, it triggers the Access Policy.

```
[root@alma9-50 DEMO]# touch nefarious-file
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root      0 Jul 10 15:58 nefarious-file
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 57. Access policy triggered

In the CimTrak Web Console, go to the Policy Event Log. In the Event Log, you can see that the new file was detected with other forensic details.

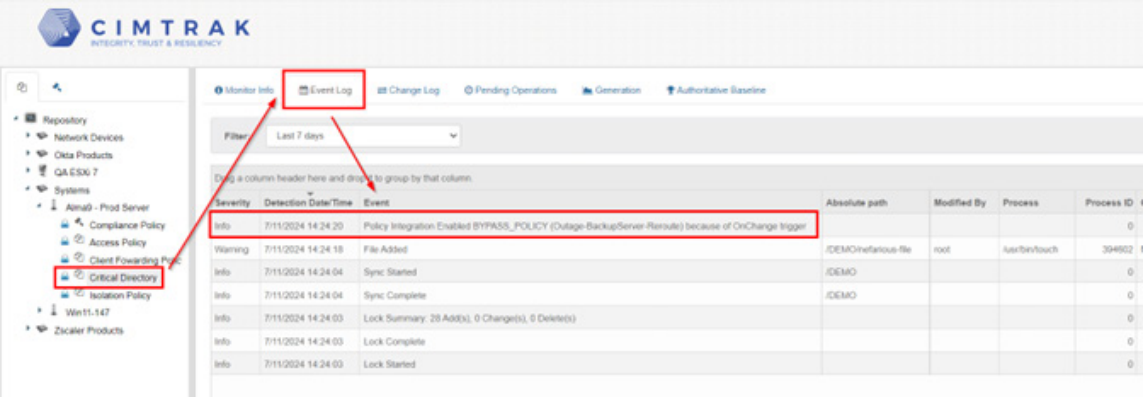

Figure 58. Policy Event Log

You can also see 1 second later the Access Policy in question was triggered.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event	Absolute path	Modified By	Process	Process ID
Info	7/11/2024 14:24:20	Policy Integration Enabled BYPASS_POLICY (Outage-BackupServer-Reroute) because of OnChange trigger				0
Warning	7/11/2024 14:24:18	File Added	/DEMO/nefarious-file	root	/usr/bin/touch	394602
Info	7/11/2024 14:24:04	Sync Started	/DEMO			0
Info	7/11/2024 14:24:04	Sync Complete	/DEMO			0
Info	7/11/2024 14:24:03	Lock Summary: 28 Add(s), 0 Change(s), 0 Delete(s)				0
Info	7/11/2024 14:24:03	Lock Complete				0
Info	7/11/2024 14:24:03	Lock Started				0

Figure 59. Access policy triggered

The ZPA Client Forwarding Policy is in Forward to ZPA mode.

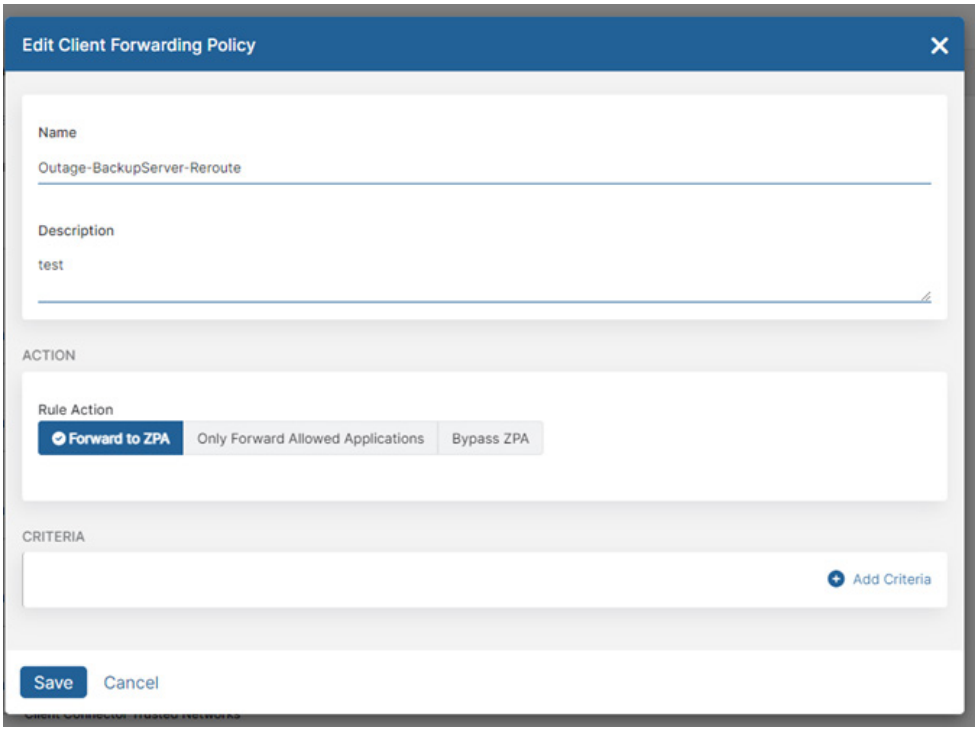

Figure 60. Edit Client Forwarding Policy

Resetting the Integration

While you can change the Rule Action status in ZPA, there is also an option to do it from the CimTrak Web Console.

1. Right-click **Repository**, then select **Properties**.

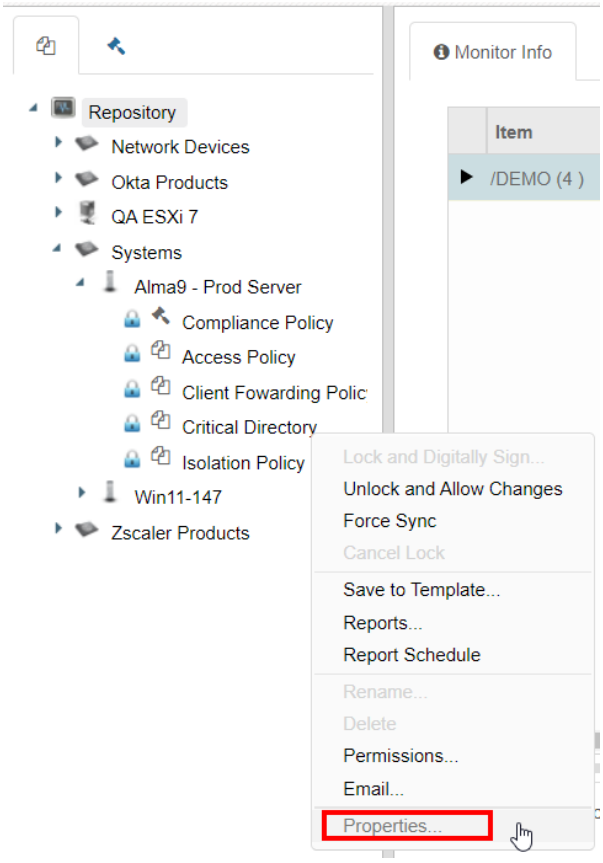

Figure 61. Properties

2. Click the **Integrations** tab.

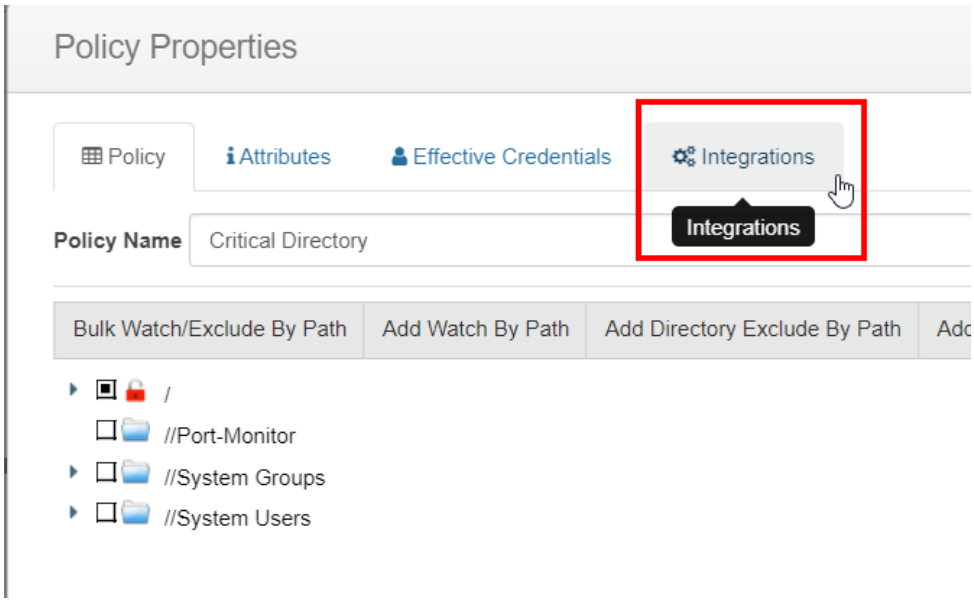

Figure 62. Integrations

You can see the current ZPA Policy status. Click **Reset** to undo the action.

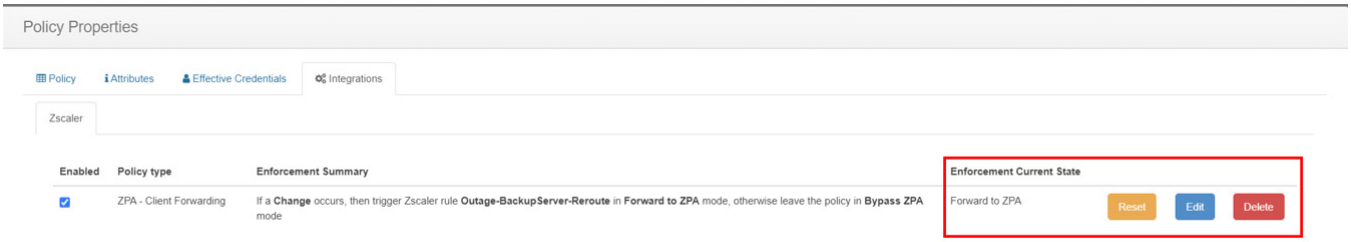

Figure 63. Reset the action

Integrating with Isolation Policies

To integrate with isolation policies:

1. Select **ZPA–Isolation** and click **Add**.

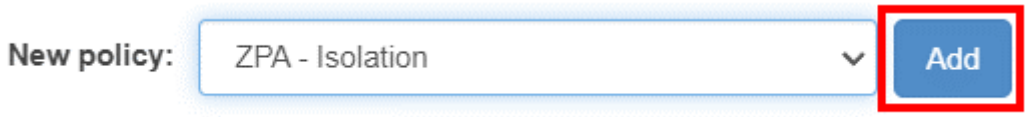

Figure 64. ZPA–Isolation

2. The following dialog displays. Configure how you want this integration to interact with your policy.

Figure 65. Isolation policy configuration

This is a logic statement that you can configure and change with a drop-down menu, as follows:

If an <INTEGRITY TRIGGER> occurs, then trigger Zscaler rule <ZSCALER ISOLATION POLICY> using Zscaler Isolation Profile <ZSCALER ISOLATION PROFILE> in <MODE> mode, otherwise leave the policy in <MODE> mode.

These variables are defined as follows:

- **INTEGRITY TRIGGERS**. The following are the CimTrak integrity options to trigger the configured policy:
  - **Change**: If any change that deviates the baseline.
  - **Denied List Item Found**: If any change was a matching hash in the CimTrak Deny List (denylist).
  - **Not in allowed list**: If any change was NOT a matching hash in the CimTrak Allow List (allowlist).
- **ZSCALER ISOLATION POLICY**: This drop-down menu populates the available access policy found in your ZPA environment:
  - **Isolation Policy 1**
  - **Isolation Policy 2**
  - **Isolation Policy N**

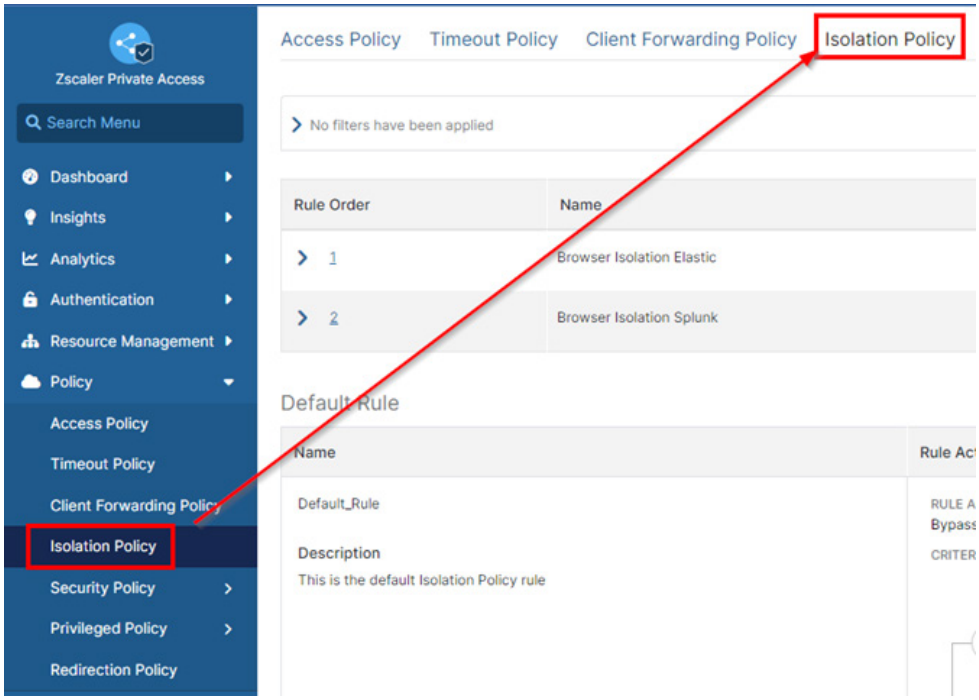

Figure 66. Isolation Policy

- **ZSCALER ISOLATION PROFILE**:
  - **Isolation Profile 1**
  - **Isolation Profile 2**
  - **Isolation Profile N**
- **MODE**: This refers to the isolation policy Rule Actions:
  - **Allow Isolation**
  - **Bypass Isolation**

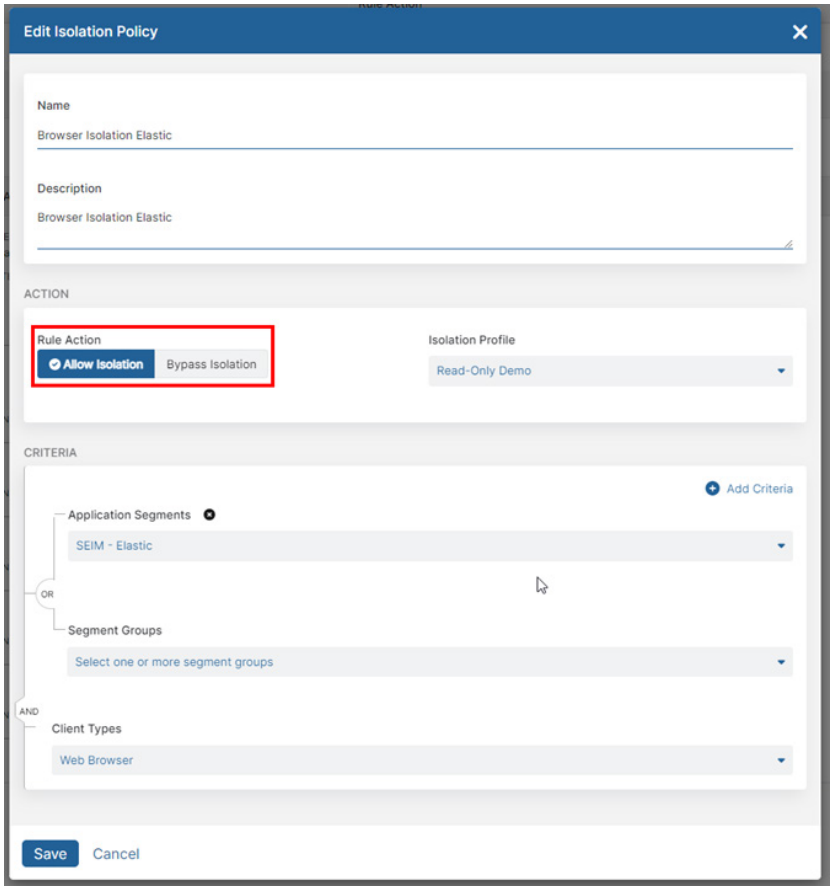

Figure 67. Rule Actions

3. After clicking **Add**, the final logic statement is created for the policy trigger.

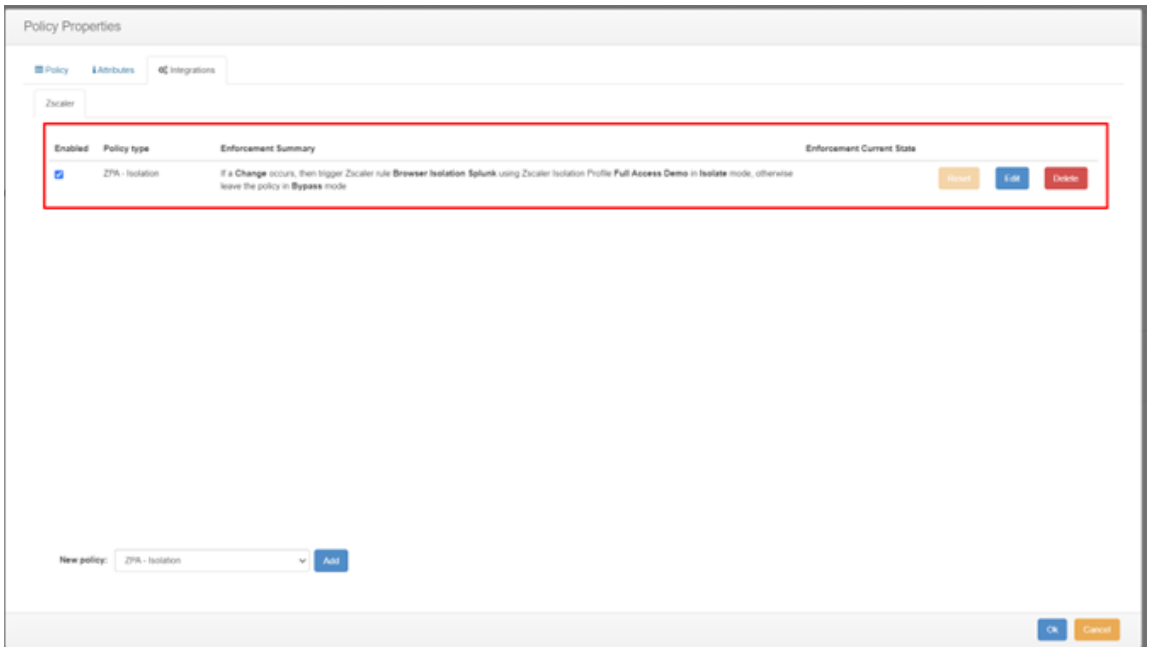

Figure 68. Logic statement

4. Click **OK**.

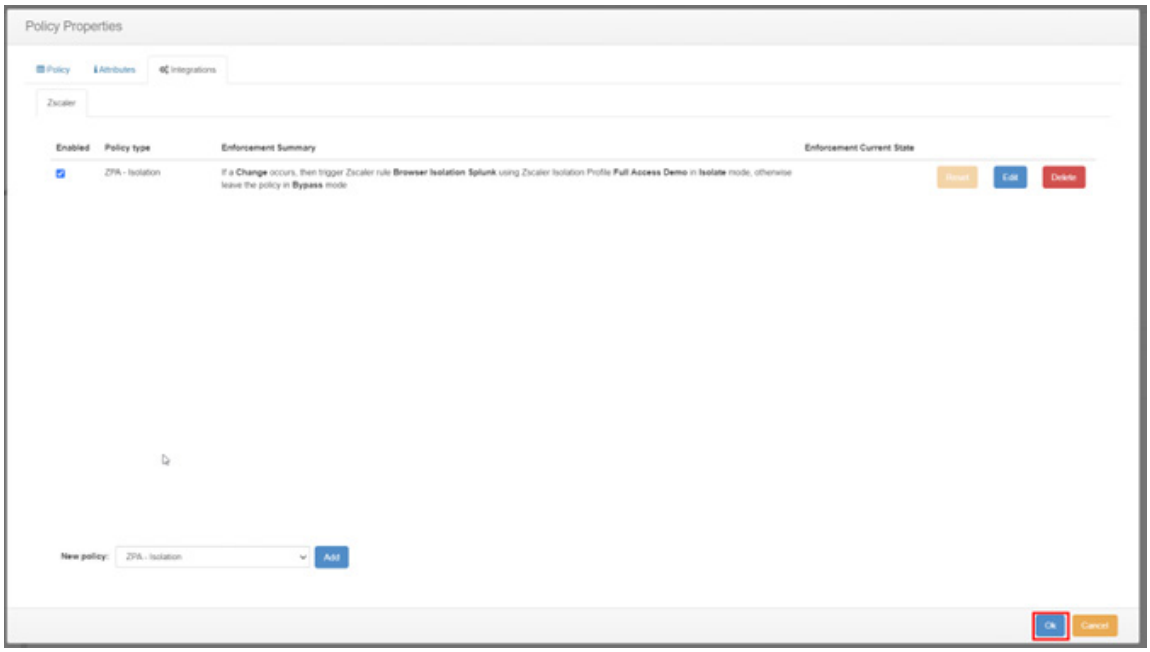

Figure 69. Save the policy

5. The new policy is under the **Agent** and is created with a red **Unlocked** icon. This means it is disabled. To turn it on, right-click and select **Lock and Digitally Sign**.

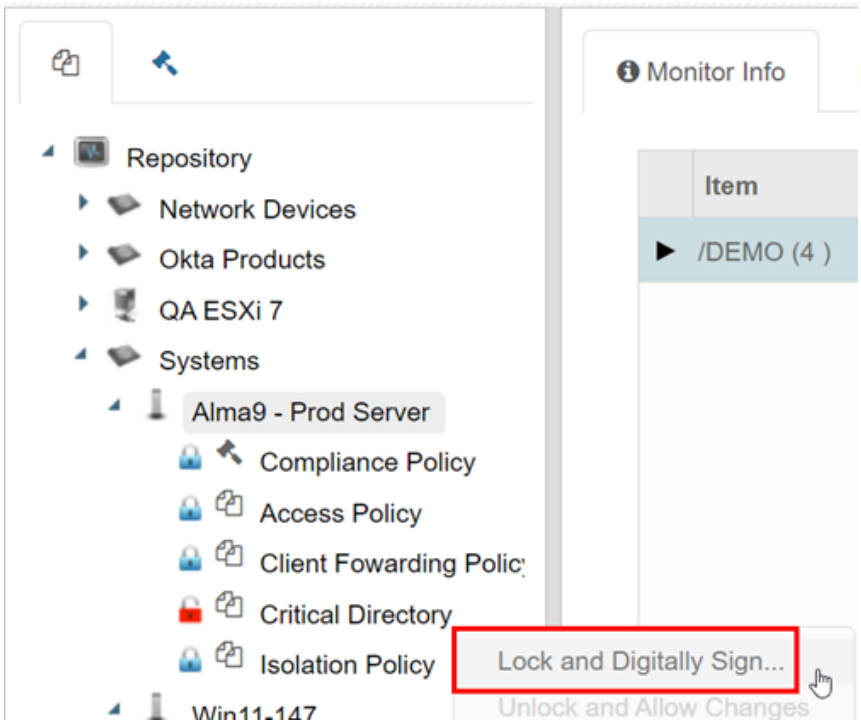

Figure 70. Lock and Digitally Sign

It takes a baseline of the objects you configured to monitor to get to the current state. After that is completed, it has a blue **Locked** icon, which means it is enabled.

Testing the Integration

Now you can test your rules. The following example is a policy set up to monitor the directory /DEMO. The trigger is CHANGE, which enables the Isolation Policy in Bypass Isolation mode.

The following is the current state of the directory:

```
[root@alma9-50 DEMO]# pwd
/DEMO
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 71. Directory state

When you add a new file that does not match any hash in the CimTrak Authoritative Baseline, it triggers the Access Policy.

```
[root@alma9-50 DEMO]# touch nefarious-file
[root@alma9-50 DEMO]# ls -l
total 848
-rw-r--r--. 1 root root      0 Jul 10 15:57 file1
-rw-r--r--. 1 root root      0 Jul 10 15:57 file2
-rw-r--r--. 1 root root      0 Jul 10 15:57 file3
-rw-r--r--. 1 root root    605 Jul 10 15:56 fstab
-rw-r--r--. 1 root root      0 Jul 10 15:58 nefarious-file
-rw-r--r--. 1 root root     12 Jul 10 15:56 nginx.conf
-rwxr-xr-x. 1 root root 859488 Jul 10 15:56 ssh
drwxr-xr-x. 5 root root     83 Jul 10 15:55 test-folder
[root@alma9-50 DEMO]#
```

Figure 72. Triggered Access Policy

From the CimTrak Web Console, go to the Policy Event Log.

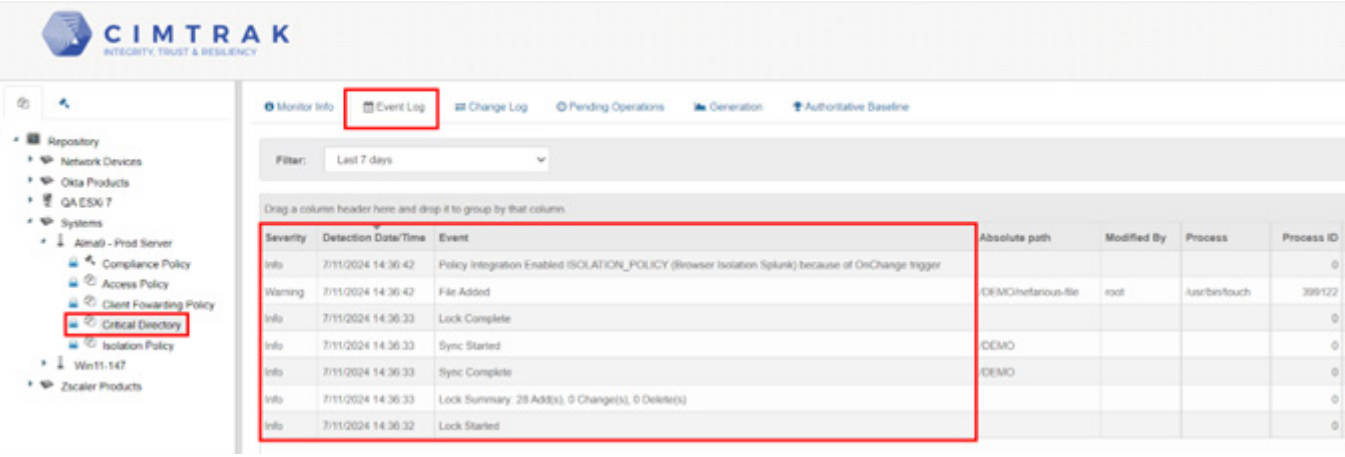

Figure 73. CimTrak Web Console

In the Event Log, you can see that the new file was detected with other forensic details. You can also see one second later the Access Policy in question was triggered.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event	Absolute path	Modified By	Process	Process ID
Info	7/11/2024 14:36:42	Policy Integration Enabled ISOLATION_POLICY (Browser Isolation Splunk) because of OnChange trigger				0
Warning	7/11/2024 14:36:42	File Added	/DEMO/nefarious-file	root	/usr/bin/touch	399122
Info	7/11/2024 14:36:33	Lock Complete				0
Info	7/11/2024 14:36:33	Sync Started	/DEMO			0
Info	7/11/2024 14:36:33	Sync Complete	/DEMO			0
Info	7/11/2024 14:36:33	Lock Summary: 28 Add(s), 0 Change(s), 0 Delete(s)				0
Info	7/11/2024 14:36:32	Lock Started				0

Figure 74. Event Log

The ZPA Isolation Policy is now in Allow Isolation mode.

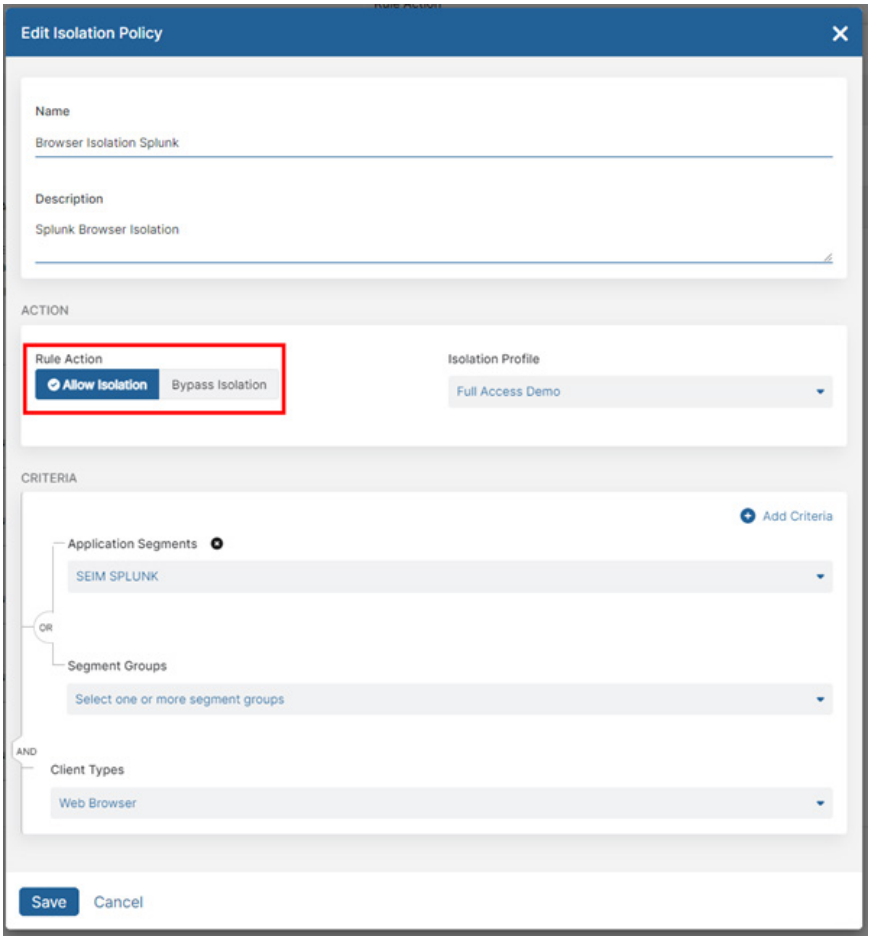

Figure 75. ZPA isolation policy in Allow Isolation mode

Resetting the Integration

While you can change the Rule Action status within ZPA, there is also an option to change it from the CimTrak Web Console.

1. Right-click **Repository**, then select **Properties**.

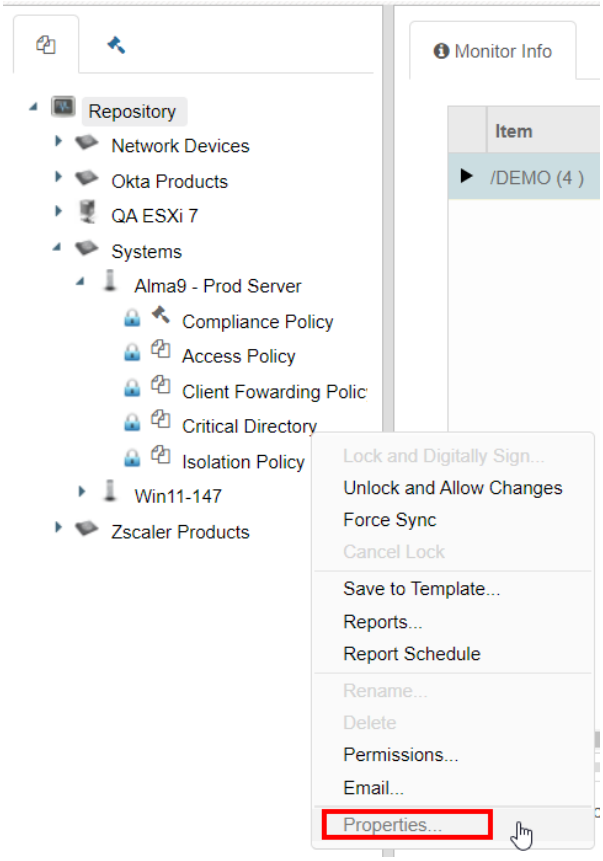

Figure 76. Properties

2. Click the **Integrations** tab. You can see the current ZPA Policy status.

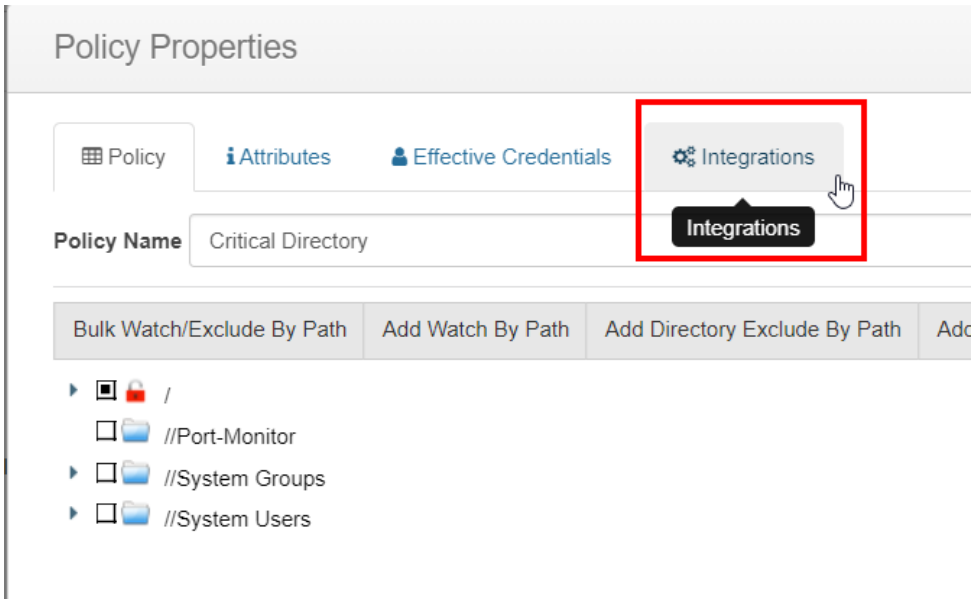

Figure 77. Integrations

3. Click **Reset** to undo the action.

Figure 78. ZPA Policy Status

ZPA Compliance Triggers

The following sections describe how to configure ZPA compliance triggers.

Log In to Your CimTrak Console

Go to your CimTrak Web Console in your environment and log in as a CimTrak Administrator. For example:

- `https://CimTrak-Server/cmc`
- `https://192.168.4.15/cmc`

Figure 79. CimTrak console

Integrating Zscaler Tenant

To integrate the Zscaler tenant:

1. Right-click **Repository**, then select **Properties**.

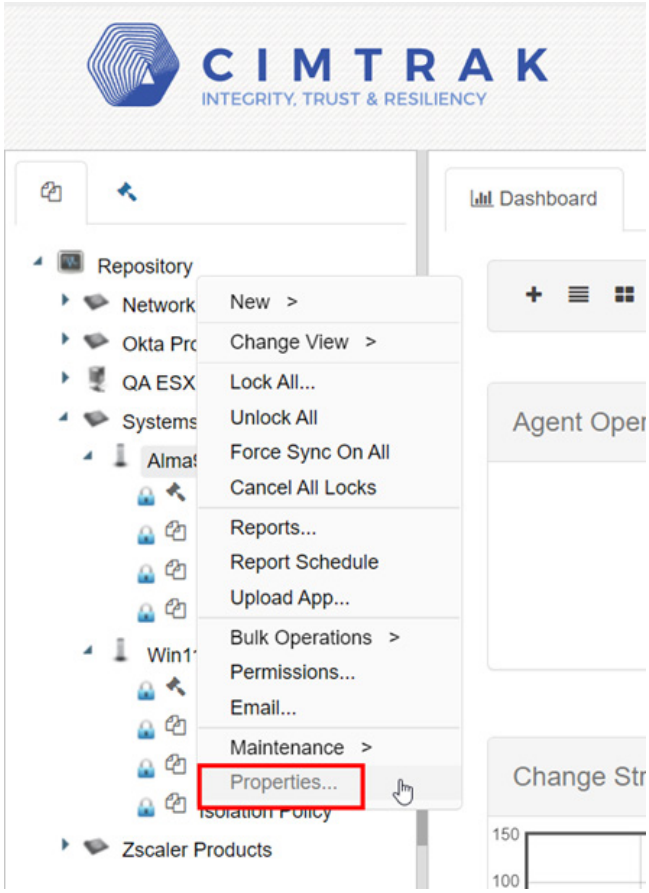

Figure 80. CimTrak properties

2. Click the **Integrations** tab.

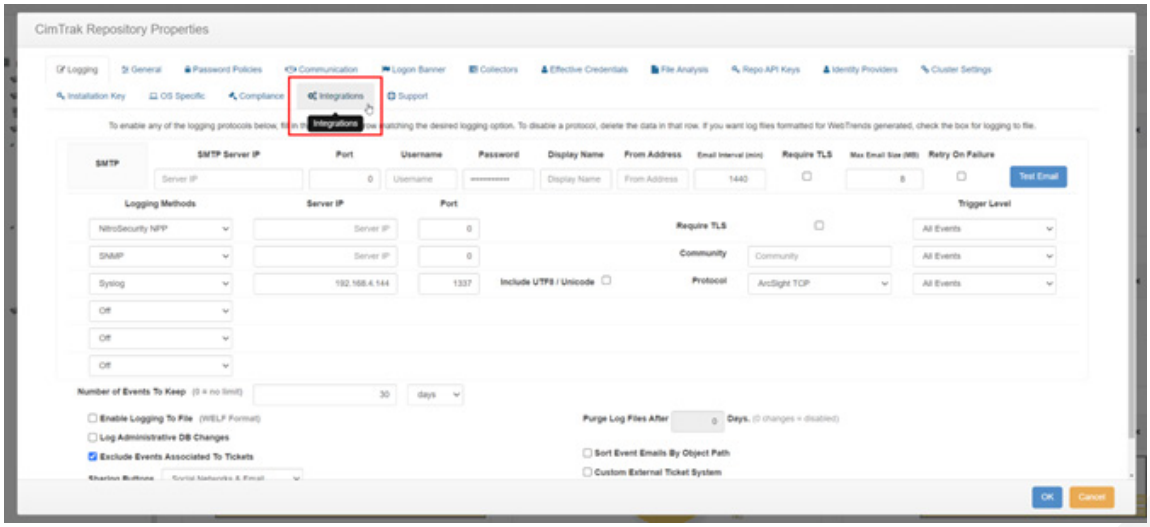

Figure 81. Integrations tab

3. Enter your ZPA Credentials:
   - **ZPA Endpoint URL**
   - **ZPA Client ID**
   - **ZPA API Key**
   - **ZPA Customer ID**

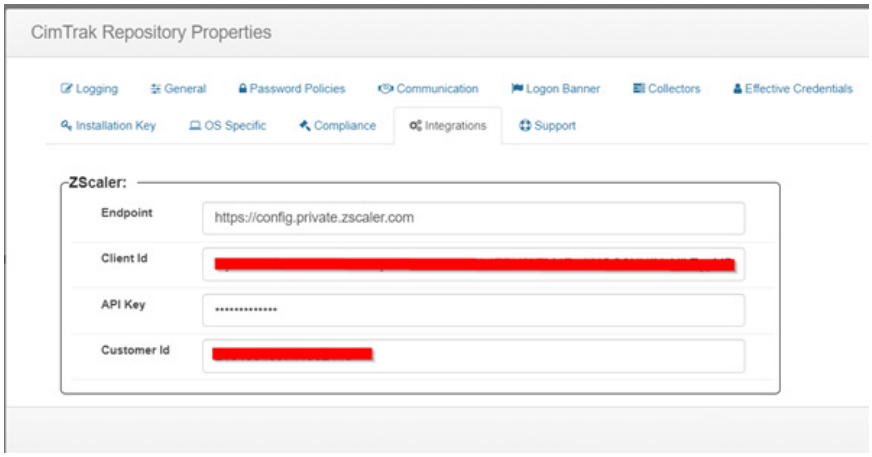

Figure 82. ZPA Credentials

Creating CimTrak Compliance Policy

To create a CimTrak compliance policy:

1. In the left-side **Tree View**, find the system for which you want to create a policy.
2. Right-click <Agent name>, select **New** and then **Policy**.

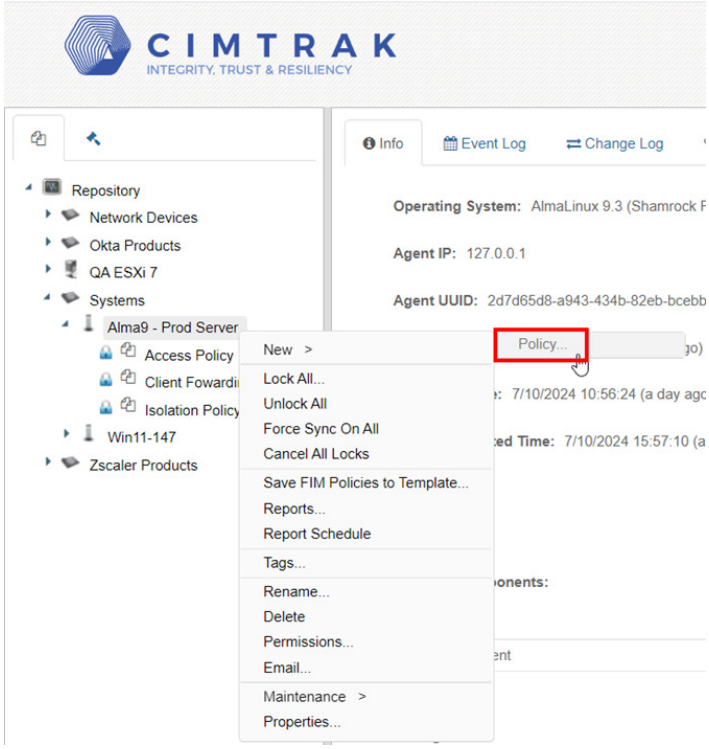

Figure 83. Policy

3. Click **Compliance Policy**.

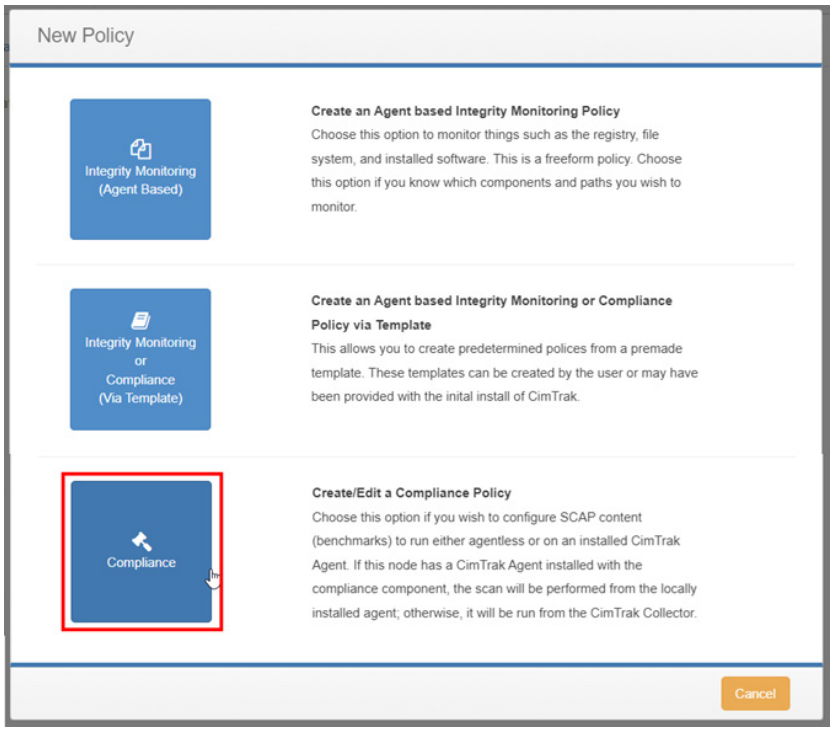

Figure 84. Compliance

4. Expand the **Mappings** node.

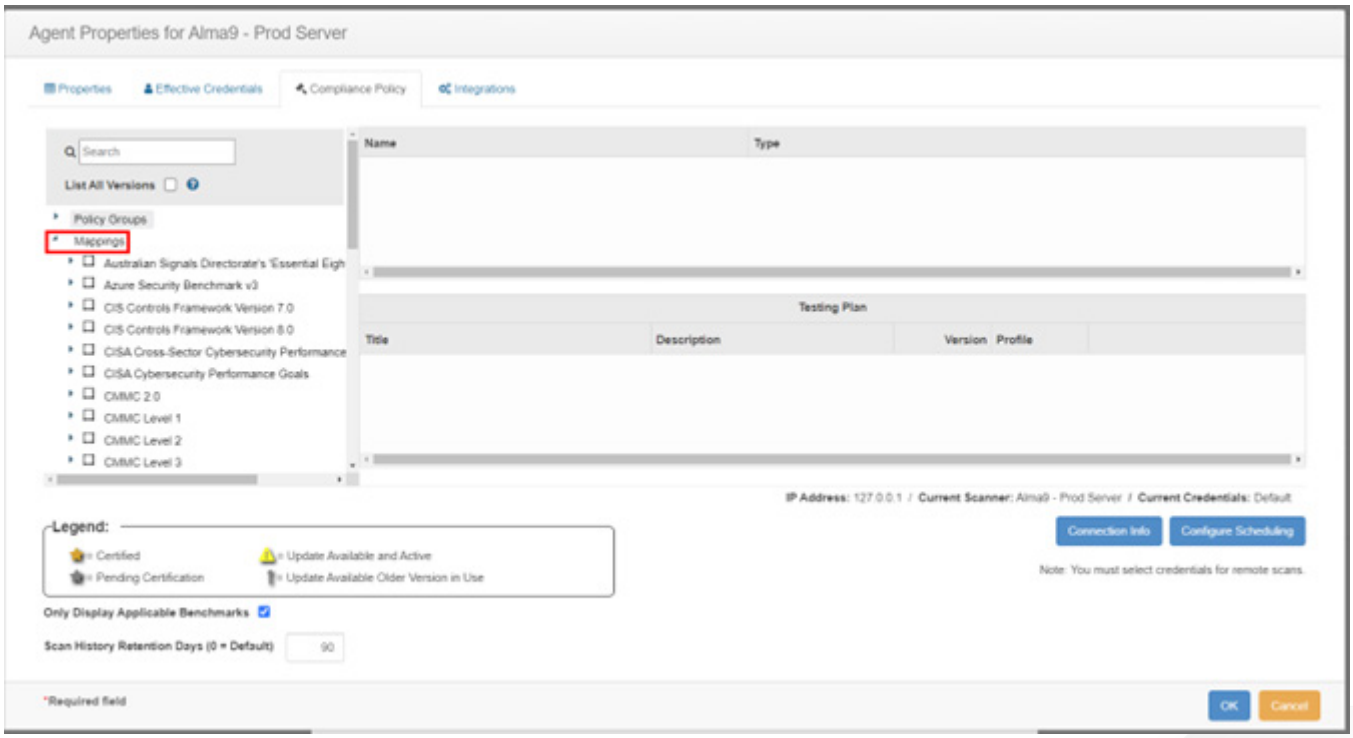

Figure 85. Mappings node

5. Select any **Compliance Frameworks** you are tracking on this system. It automatically chooses the CIS Benchmark you must run to track that Compliance Framework. You can choose multiple if required.
6. Select the **Profile** for the benchmark that is applicable for the system (i.e., **Workstation**/**Server**/**Domain Controller**).

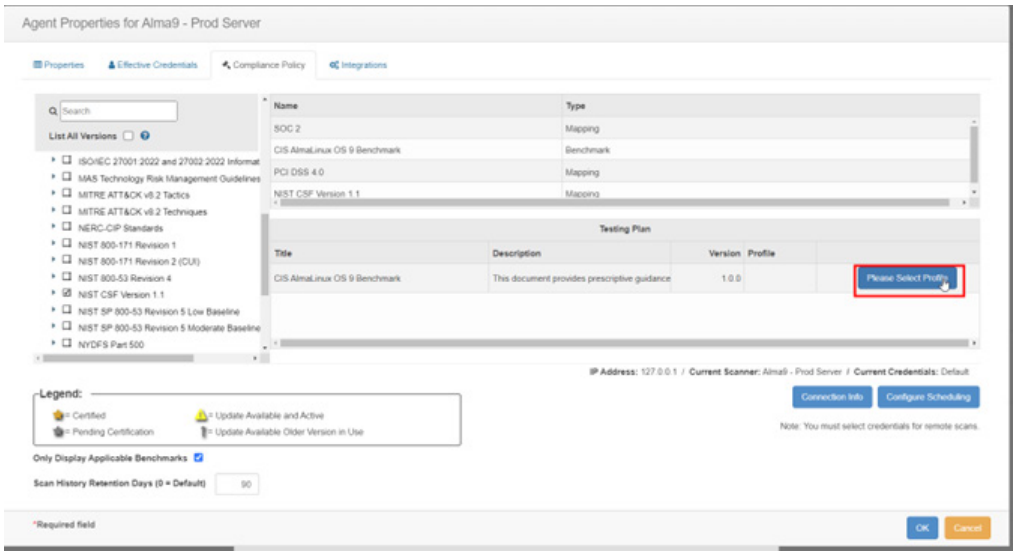

Figure 86. Select Profile

The following image shows the profile type.

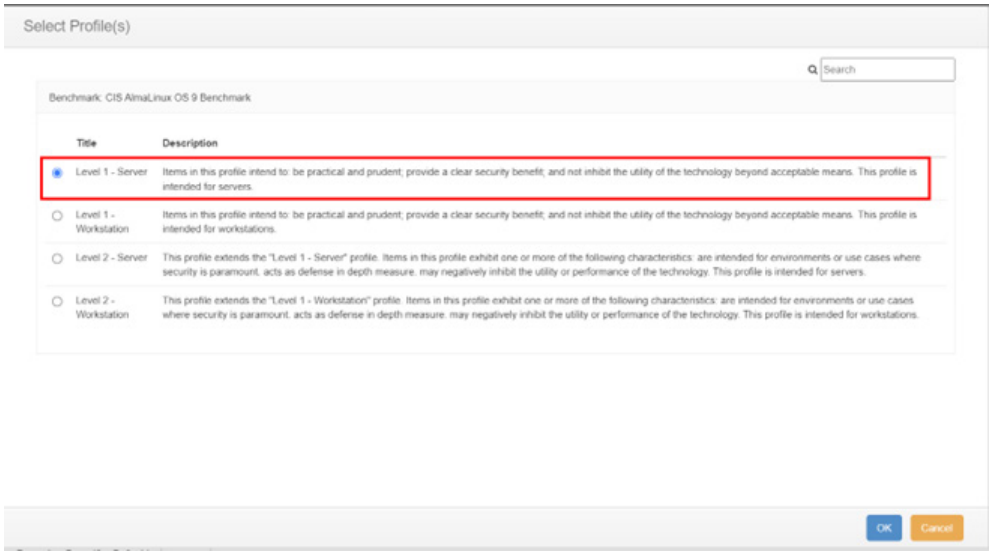

Figure 87. Select Profile Type

7. Select **Configure Schedule** to determine when you want CimTrak to run the benchmark scans.

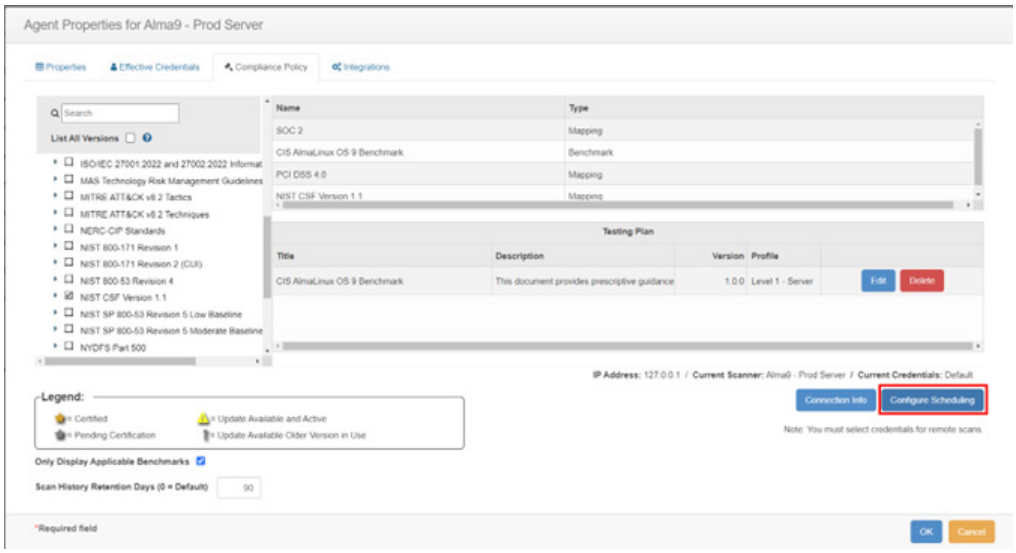

Figure 88. Configure Scheduling

The default is **Every Day at Midnight Server Time**.

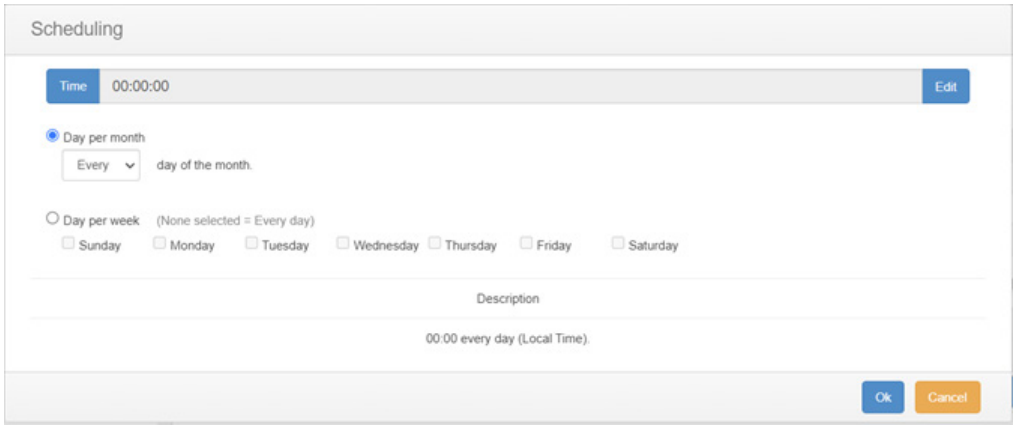

Figure 89. Set schedule

Configuring Zscaler Integration

To configure Zscaler integration, click the **Integrations** tab.

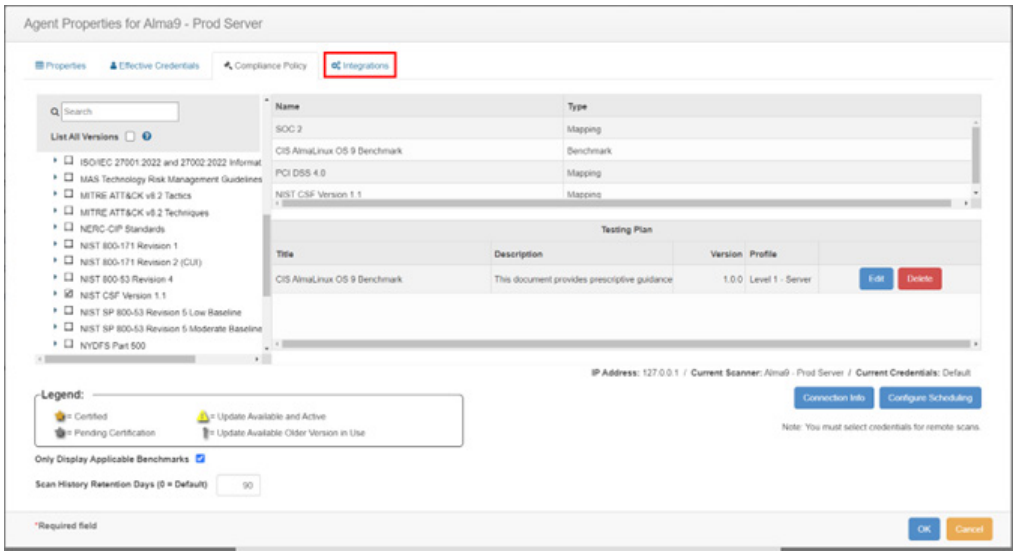

Figure 90. Integrations

Integrating with Access Policies

To integrate with access policies:

1. Select **ZPA–Access** and click **Add**.

Figure 91. Add ZPA Access

2. Configure how you want this integration to interact with your policy.

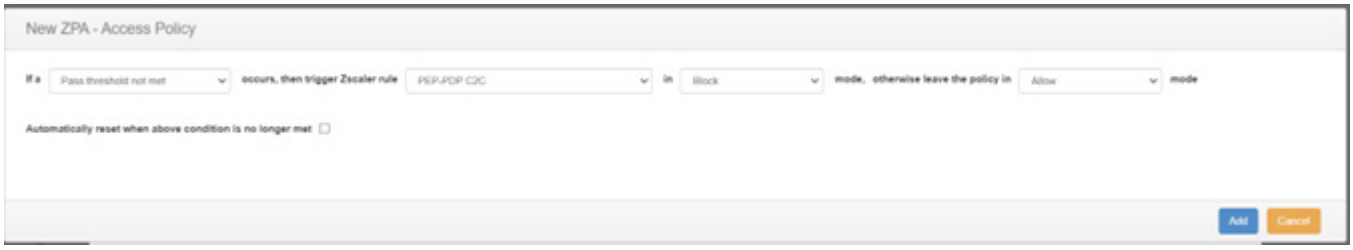

Figure 92. Configure Access Policy

3. This is a logic statement that you can configure using a drop-down menu, as follows:

   If a <COMPLIANCE TRIGGER> occurs, then trigger Zscaler rule <ZSCALER ACCESS POLICY> in <MODE> mode, otherwise leave the policy in <MODE> mode.

   - **Automatically reset when above condition is no longer met**. This setting disables the ZPA Policy if the system is in a PASSING state for the configured Compliance Policy.

These variables are defined as follows:

- **COMPLIANCE TRIGGERS**: There is only one Compliance Trigger:
  - **Pass threshold not met**: This means if the Compliance/Benchmark scores do not meet the configured threshold in CimTrak, the ZPA Policy triggers. You can configure this threshold in the Repository Properties. Right-click **Repository** in the **Tree View** on the left, then select **Properties**.

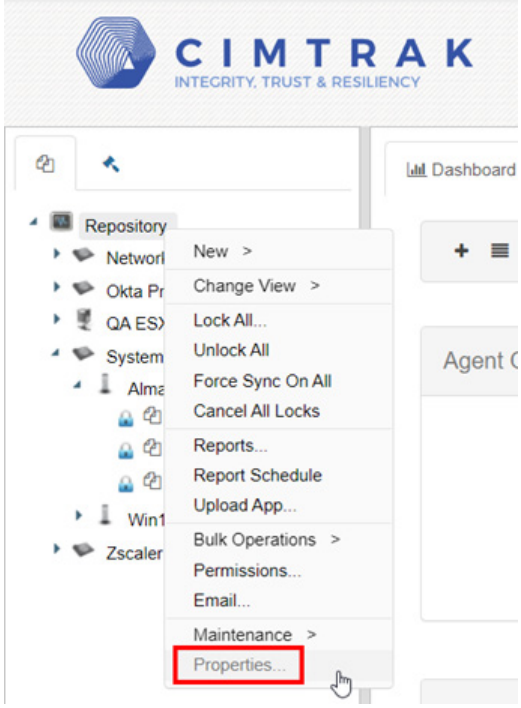

Figure 93. Properties

4. Click the **Compliance** tab.

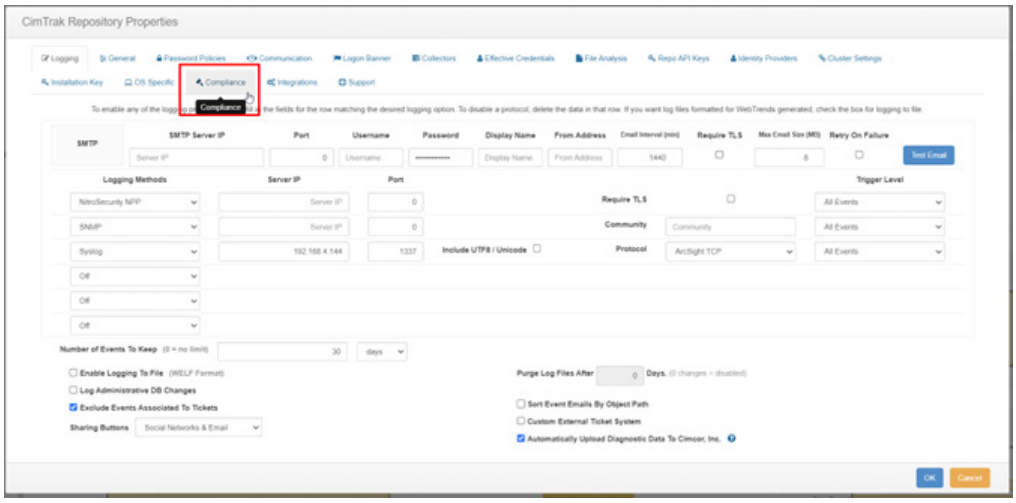

Figure 94. Compliance tab

5. Configure what test percentages equate to a PASS value. The default is 100%.

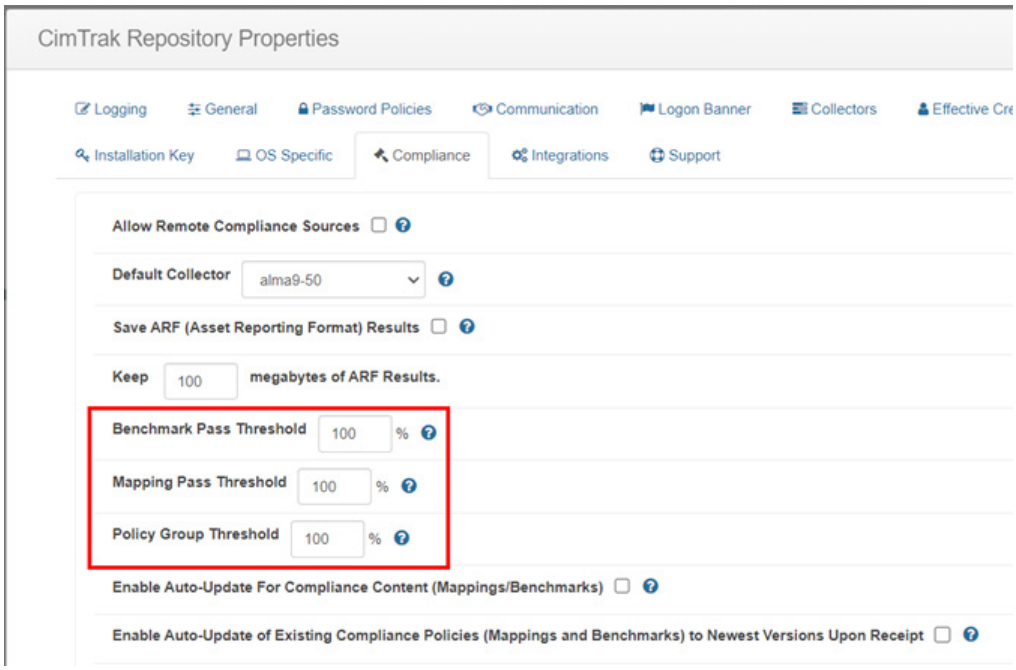

Figure 95. Repository Properties

- **ZSCALER ACCESS POLICY**: This drop-down menu populates the available Access Policy found in your ZPA environment:
  - **Access Policy 1**
  - **Access Policy 2**
  - **Access Policy N**

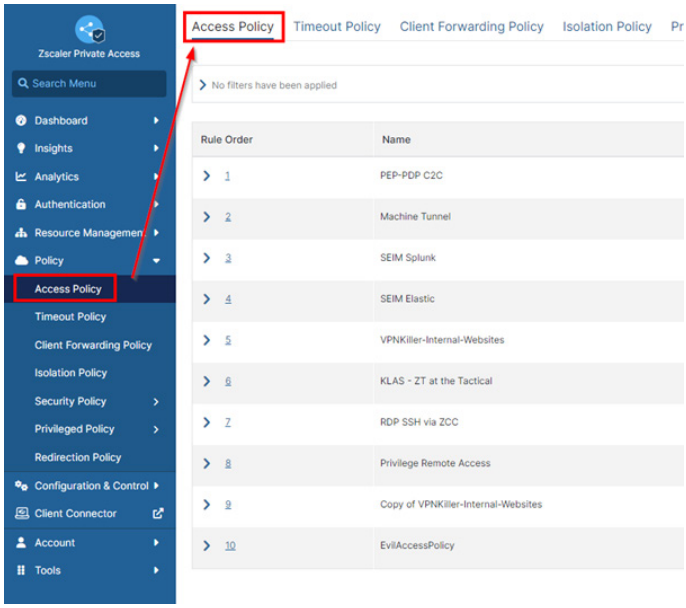

Figure 96. Access Policy

- **MODE**: This refers to the Access Policy Rule Actions:
  - **Allow Access**
  - **Block Access**
  - **Require Approval**

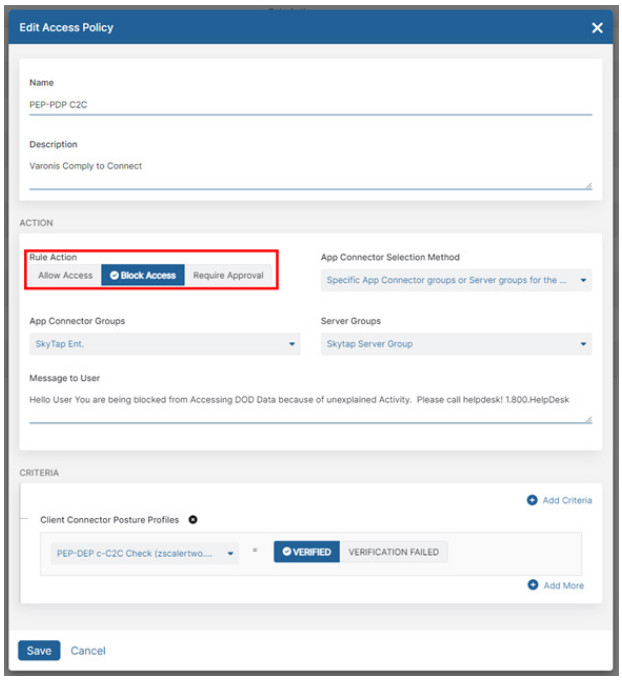

Figure 97. Rule Action

6. After clicking **Save**, you see the final logic statement created for the policy trigger.

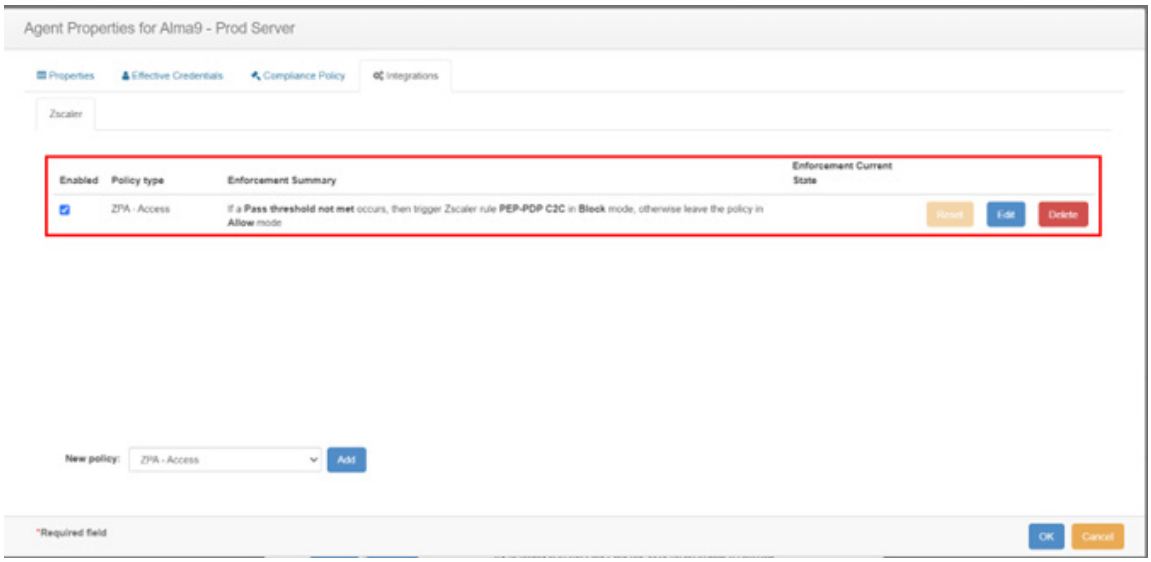

Figure 98. Policy Trigger

7. Click **OK** to save the policy.

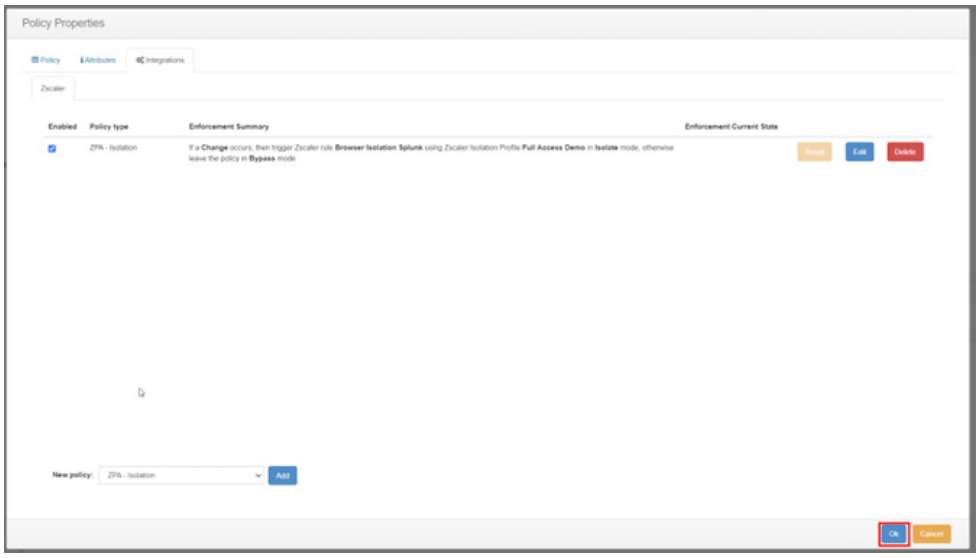

Figure 99. Save Policy

8. The new policy is created under the Agent with a red **Unlocked** icon. This means it is disabled. To turn it on, right-click and select **Lock**.

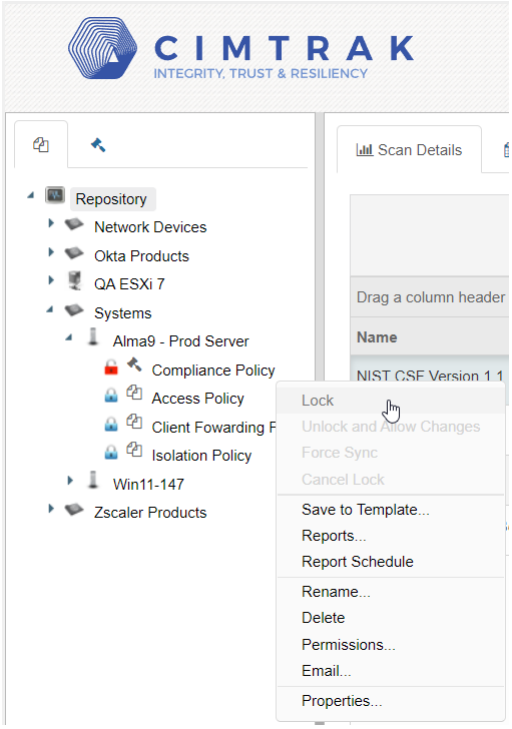

Figure 100. Lock

CimTrak initiates the scan and completes the Benchmark/Compliance tests. After completion, you receive the Compliance Scan Completed event in the Event Log.

Find the score in the **Scan Details** tab.

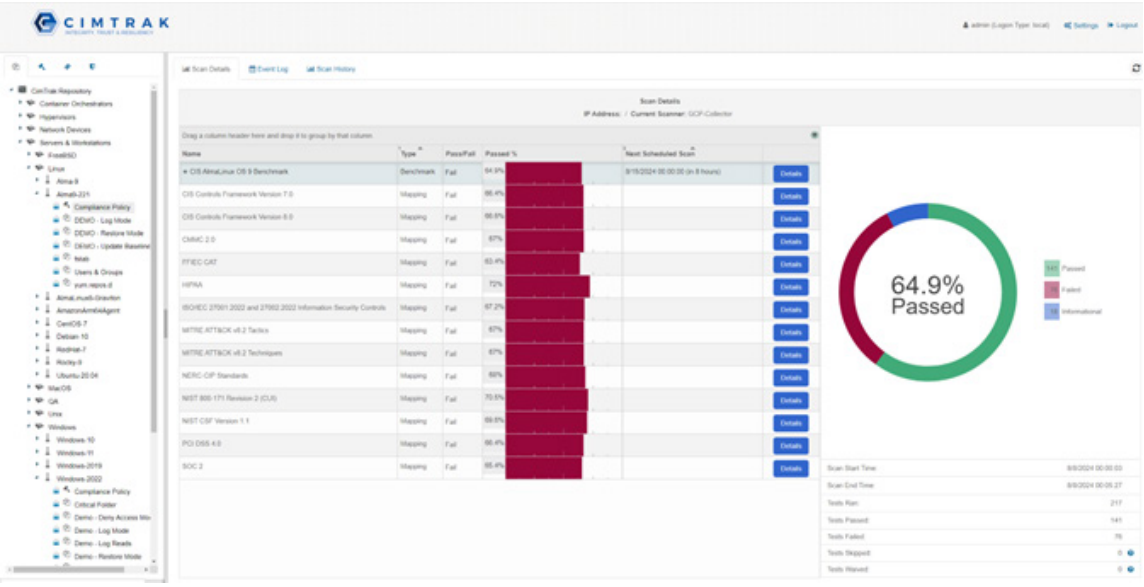

Figure 101. Scan details

Testing the Integration

Now you can test the rules.

The following example is a policy that expects a 100% PASSING score, or the ZPA Access policy triggers to Block Access mode.

The following image shows the completed scan.

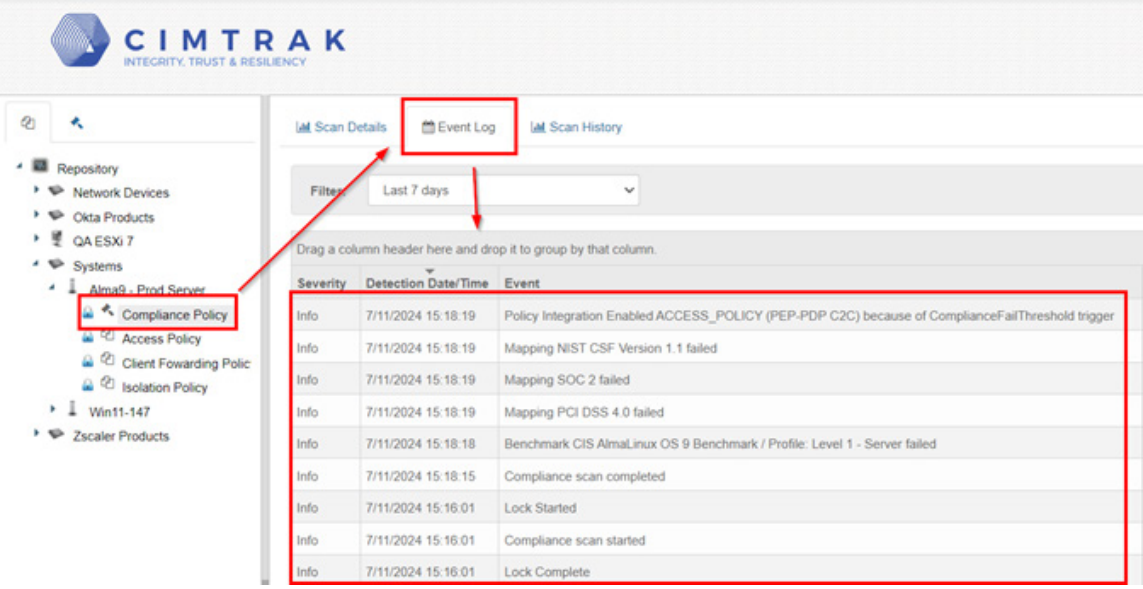

Figure 102. Completed scan

This shows a score of 65.3% (this does not meet the 100% pass standard).

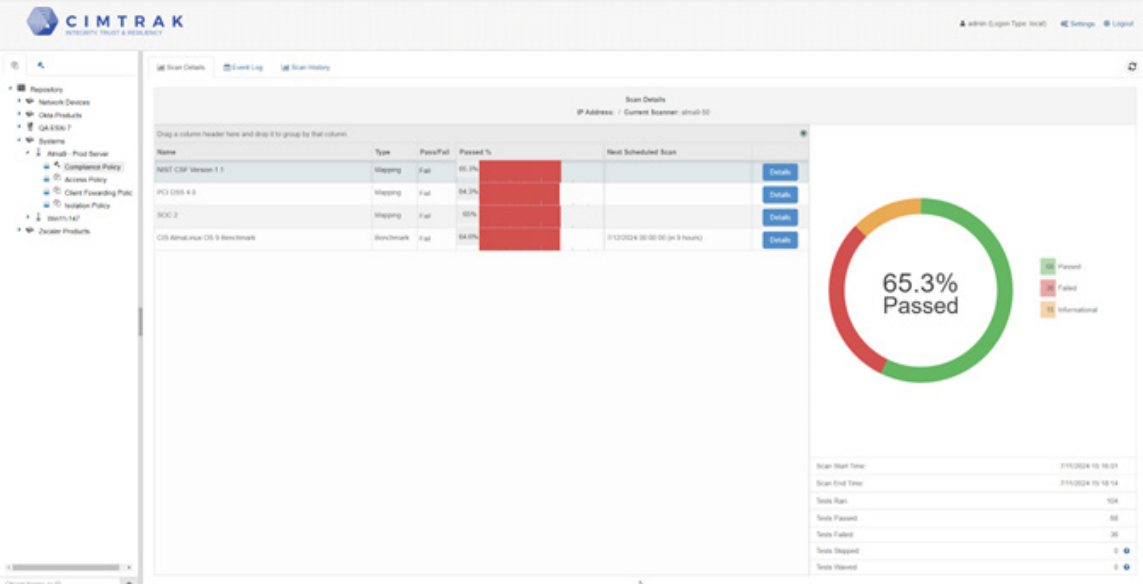

Figure 103. Scan score

The following image shows the triggered CimTrak ZPA Policy.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event
Info	7/11/2024 15:18:19	Policy Integration Enabled ACCESS_POLICY (PEP-PDP C2C) because of ComplianceFailThreshold trigger
Info	7/11/2024 15:18:19	Mapping NIST CSF Version 1.1 failed
Info	7/11/2024 15:18:19	Mapping SOC 2 failed
Info	7/11/2024 15:18:19	Mapping PCI DSS 4.0 failed
Info	7/11/2024 15:18:18	Benchmark CIS AlmaLinux OS 9 Benchmark / Profile: Level 1 - Server failed
Info	7/11/2024 15:18:15	Compliance scan completed
Info	7/11/2024 15:16:01	Lock Started
Info	7/11/2024 15:16:01	Compliance scan started
Info	7/11/2024 15:16:01	Lock Complete

Figure 104. Triggered CimTrak ZPA Policy

In the ZPA console, the Policy has switched to **Block Access** mode.

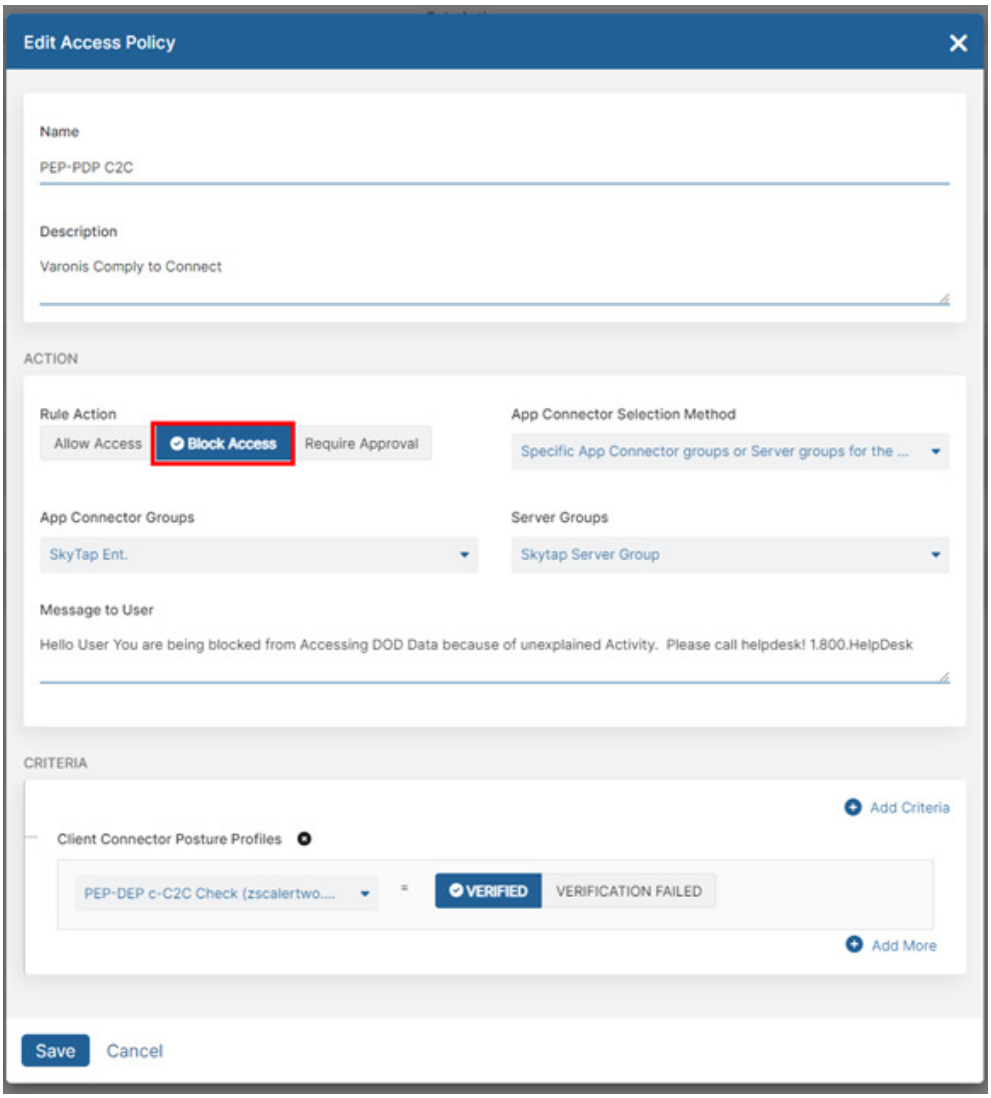

Figure 105. Block Access mode

Resetting the Integration

While you can change the Rule Action status within ZPA, there is also an option to do it in the CimTrak Web Console.

1. Right-click **Repository**, then select **Compliance Policy** and **Properties**.

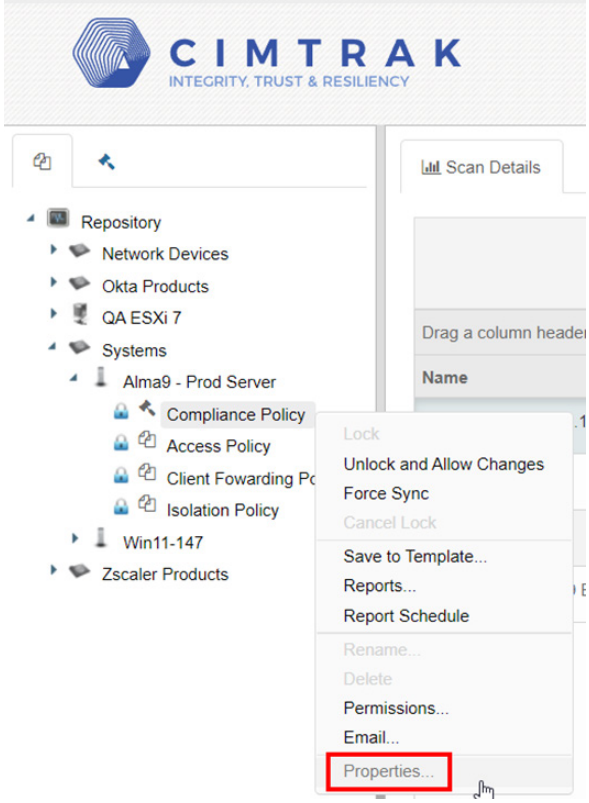

Figure 106. Properties

2. Click the **Integrations** tab.

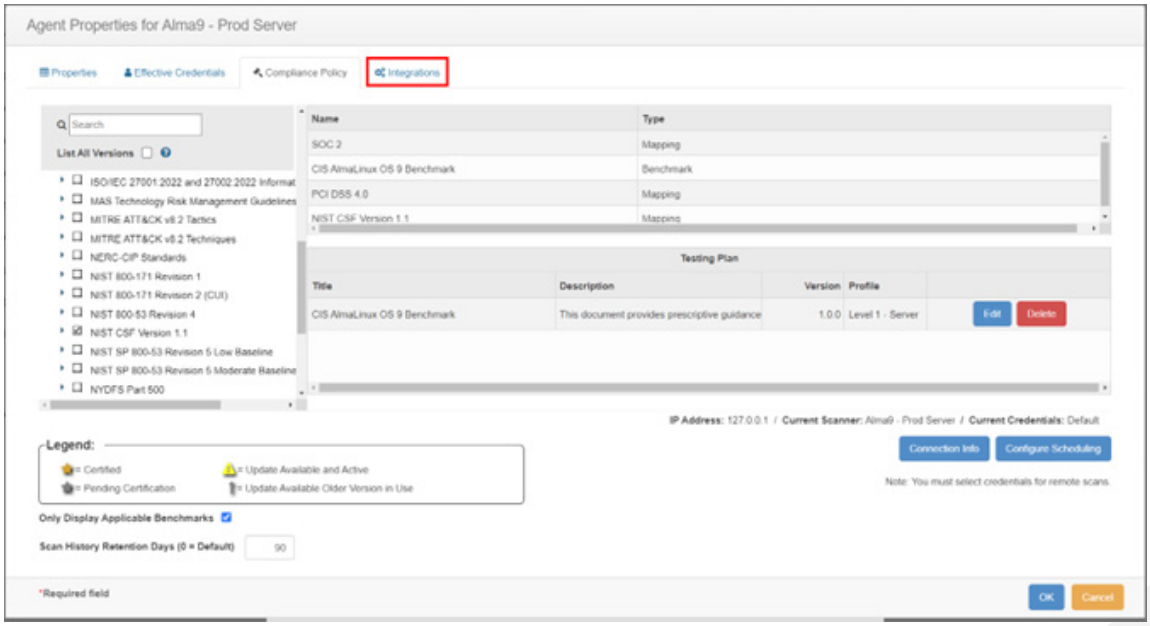

Figure 107. Integrations

3. View the current ZPA Policy status. Click **Reset** to undo the action.

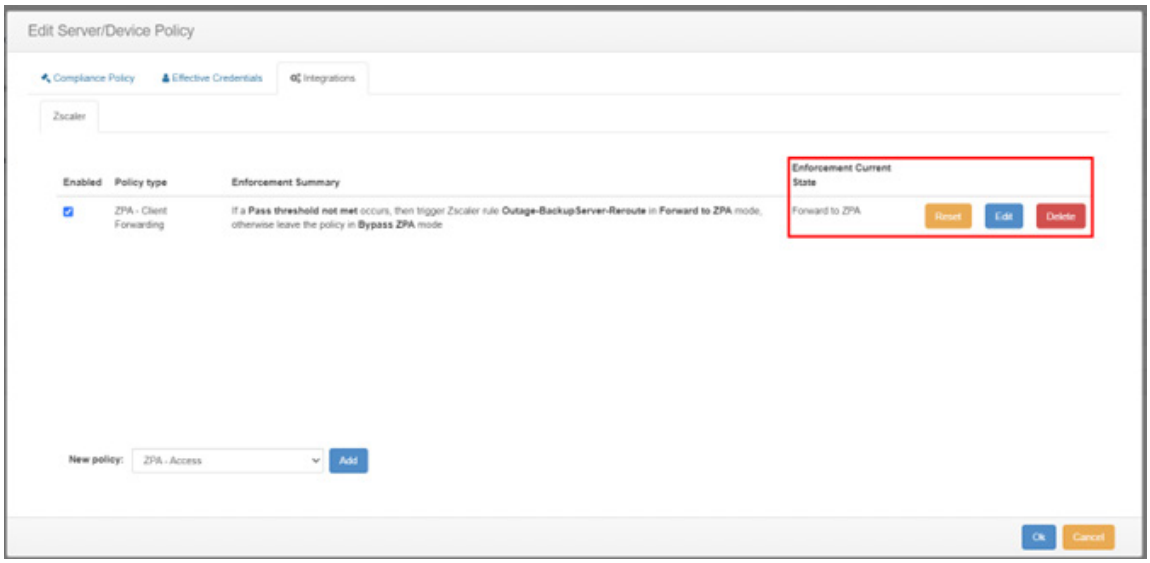

Figure 108. Reset

Integrating with Client Forwarding Policies

To integrate with client forwarding policies:

1. Select **ZPA–Client Forwarding** and click **Add**.

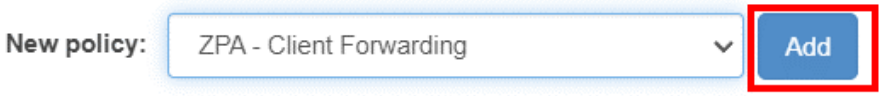

Figure 109. Add ZPA–Client Forwarding

2. The following dialog displays. Configure how you want this integration to interact with your policy.

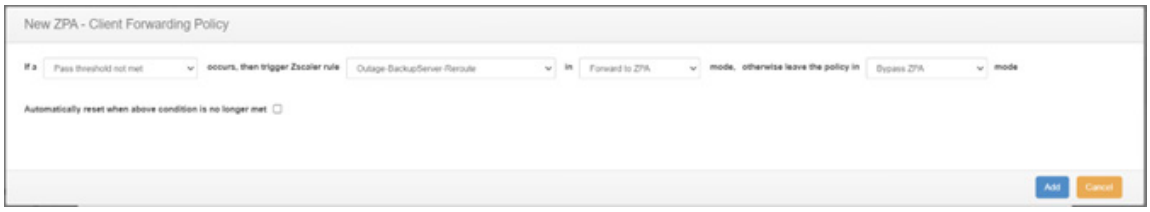

Figure 110. Client Forwarding Policy

The configuration uses a logic statement that you can configure and change with a drop-down menu, as follows.

If a <COMPLIANCE TRIGGER> occurs, then trigger Zscaler rule <ZSCALER CLIENT FORWARDING POLICY> in <MODE> mode, otherwise leave the policy in <MODE> mode.

- **Automatically reset when above condition is no longer met**: This setting disables the ZPA policy if the system is in a PASSING state for the configured compliance policy.

These variables are defined as follows:

- **COMPLIANCE TRIGGERS**: There is only one Compliance Trigger:
  - **Pass threshold not met**: This means the Compliance/Benchmark scores do not meet the configured threshold in CimTrak, and triggers the ZPA Policy. You can configure this threshold in the Repository Properties.

3. Right-click **Repository** in the **Tree View** on the left , then select **Compliance Policy** and **Properties**.

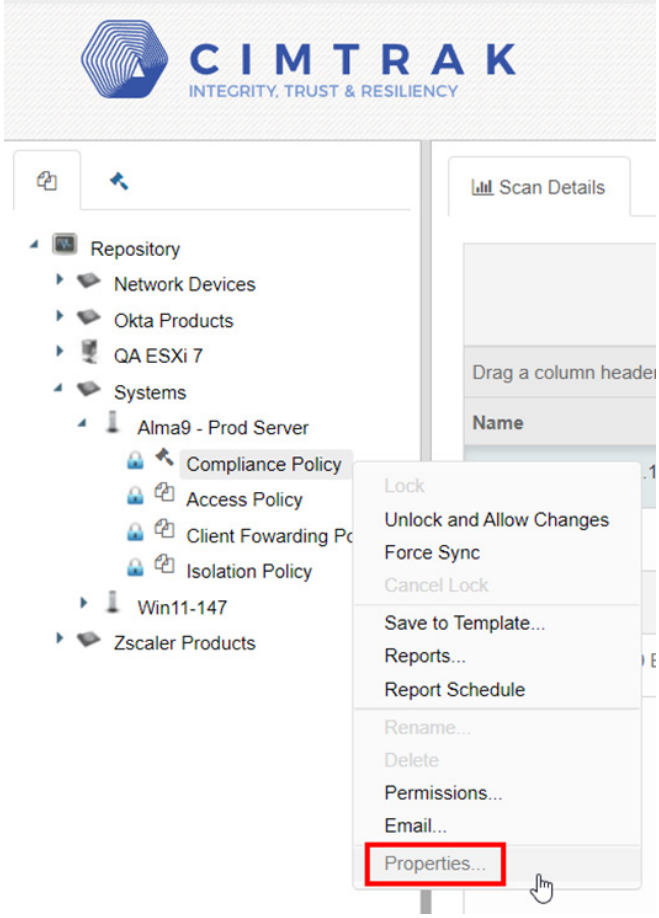

Figure 111. Properties

4. Click the **Compliance** tab.

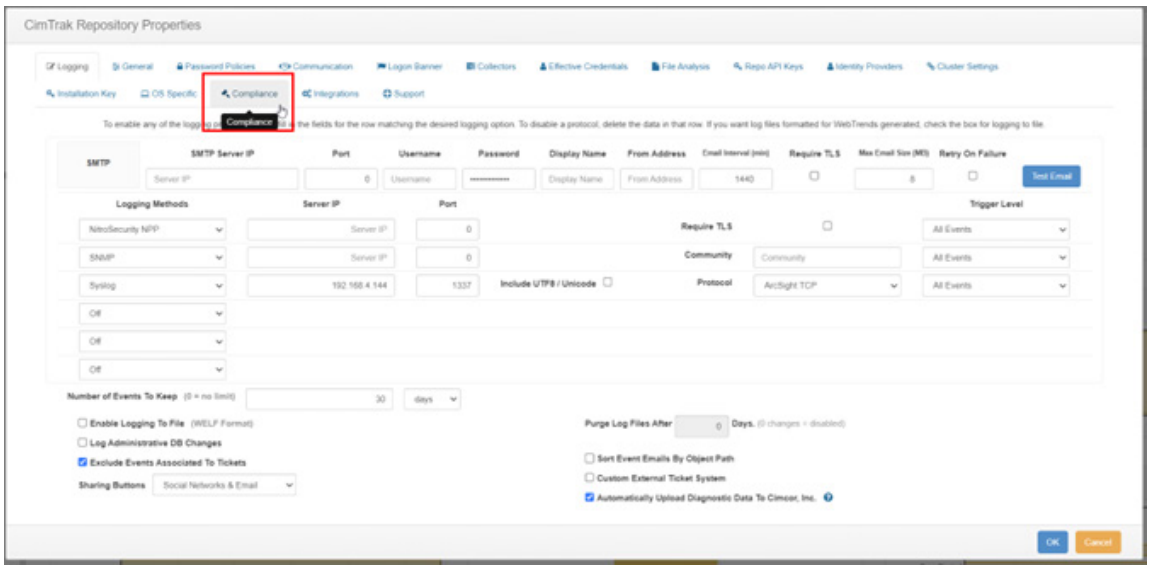

Figure 112. Compliance tab

5. Configure what test percentages equate to a PASS value. The default is 100%.

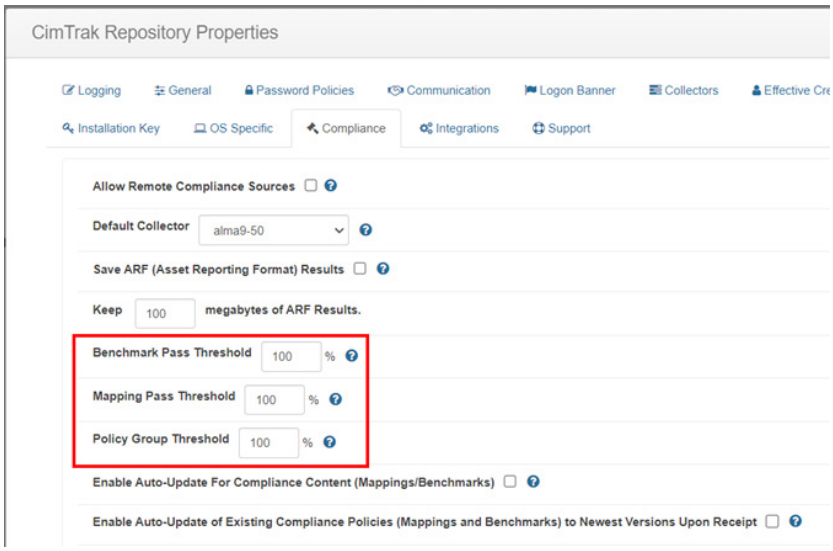

Figure 113. Pass thresholds

- **ZSCALER CLIENT FORWARDING POLICY**: This drop-down menu populates the available access policy found in your ZPA environment:
  - **Client Forwarding Policy 1**
  - **Client Forwarding Policy 2**
  - **Client Forwarding Policy N**

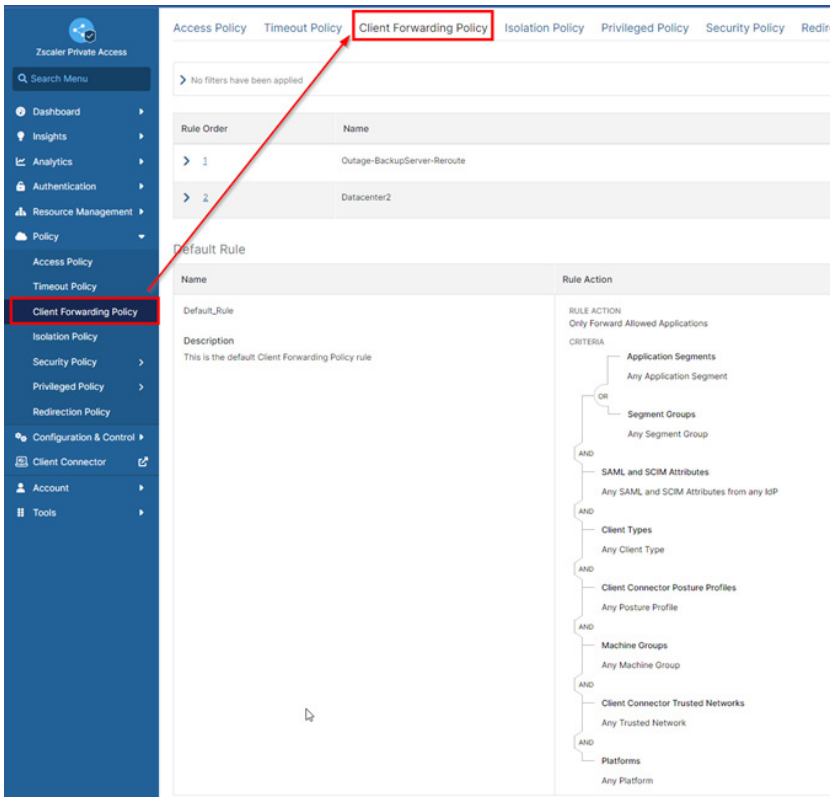

Figure 114. Client Forwarding Policy

- **MODE**: This refers to the client forwarding policy rule actions:
  - **Forward to ZPA**
  - **Only Forward Allowed Applications**
  - **Bypass ZPA**

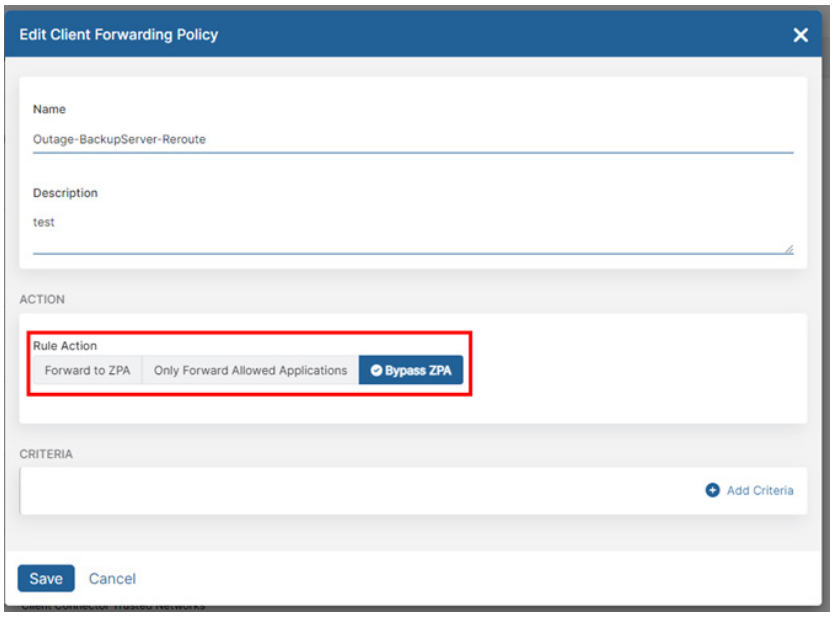

Figure 115. Edit Client Forwarding Policy

6. After clicking **Save**, the final logic statement is created for the policy trigger.

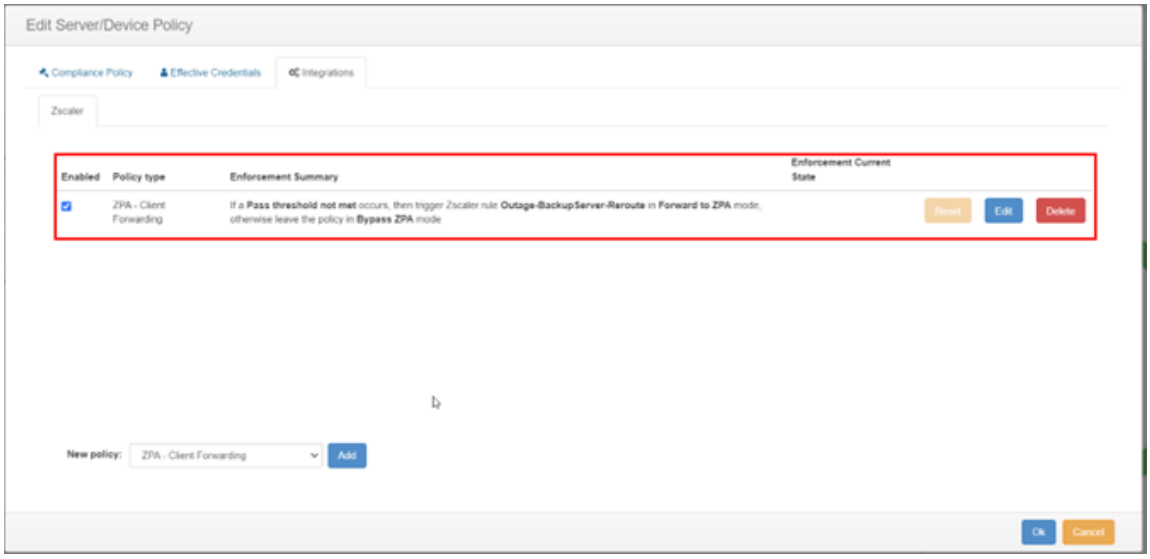

Figure 116. Policy trigger

7. Click **OK** to save the policy.

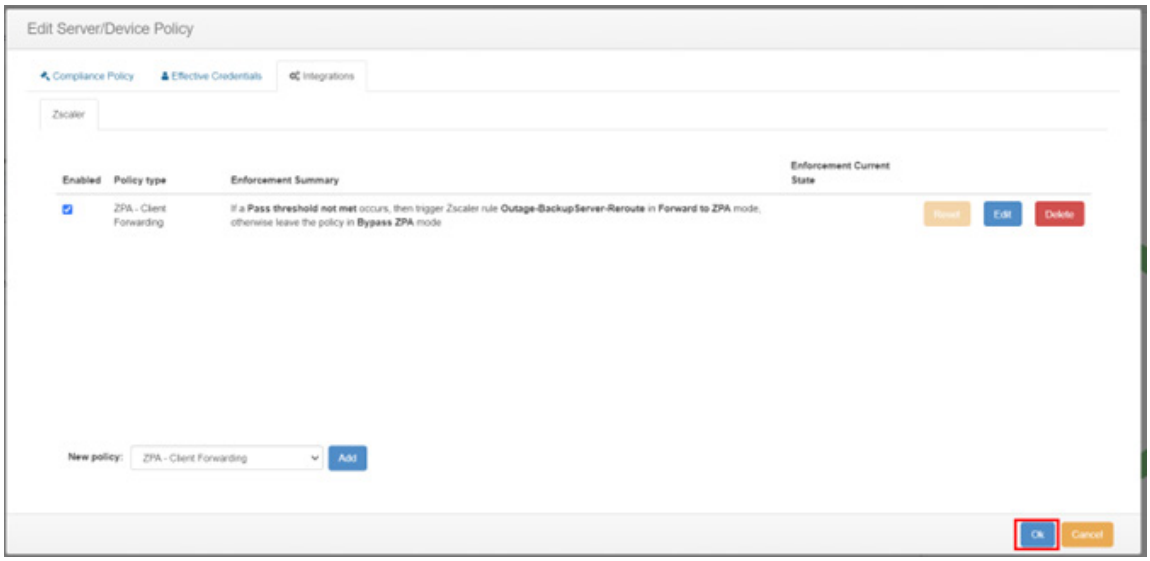

Figure 117. Save the policy

8. The new policy is created under the **Agent** with a red **Unlocked** icon. This means it is disabled. To turn it on, right-click and select **Lock**.

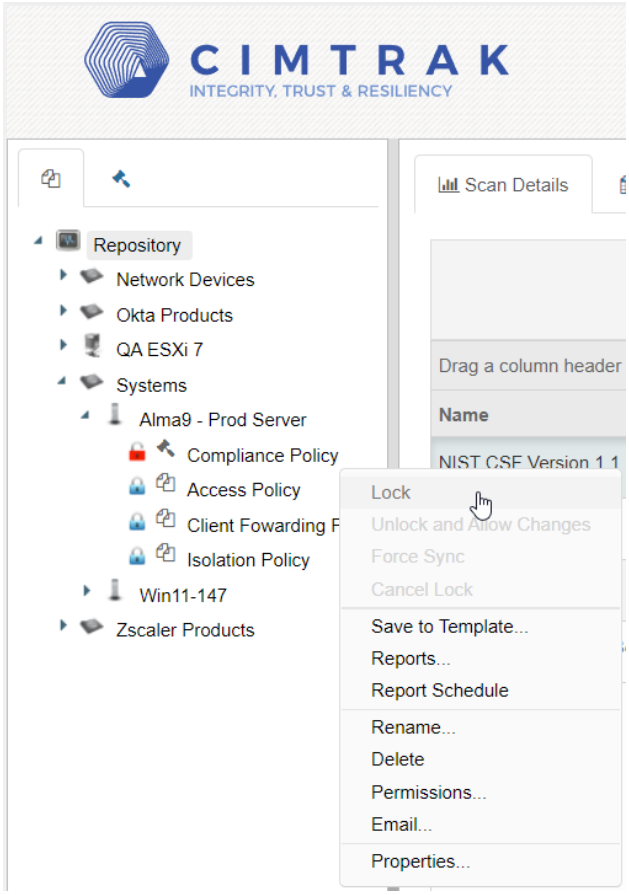

Figure 118. Lock

CimTrak initiates the scan and completes the Benchmark/Compliance tests.

After it is complete, you receive the Compliance Scan Completed event in the Event Log.

Find the score in the **Scan Details** tab.

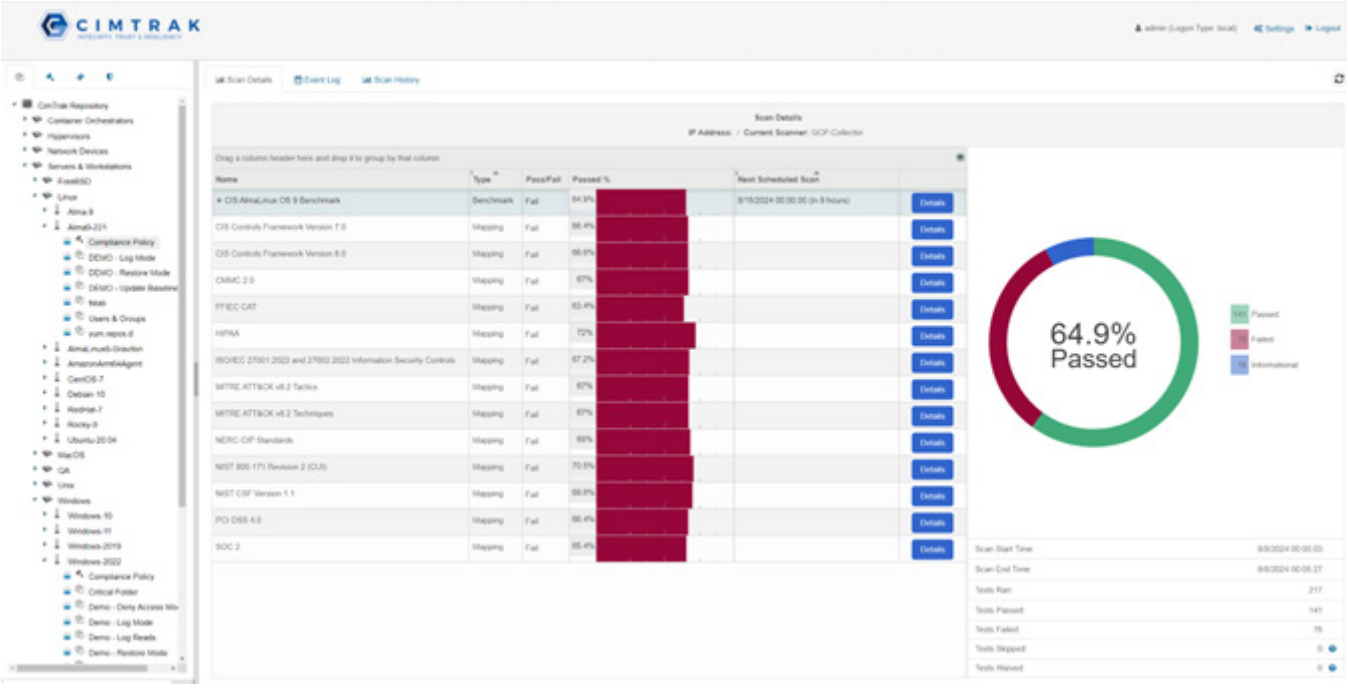

Figure 119. Scan details tab

Testing the Integration

You can test the rule. The following example uses a policy that expects a 100% PASSING score, otherwise the ZPA Client Forwarding policy triggers **Forward to ZPA** mode.

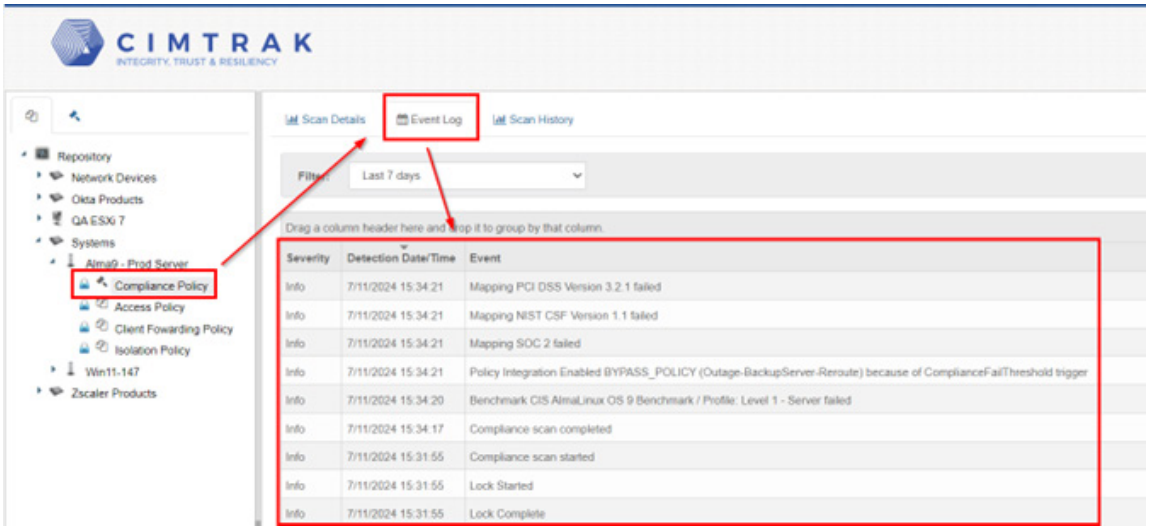

Figure 120. Policy trigger

The scan shows the score is 65.3% (this does not meet the 100% criteria).

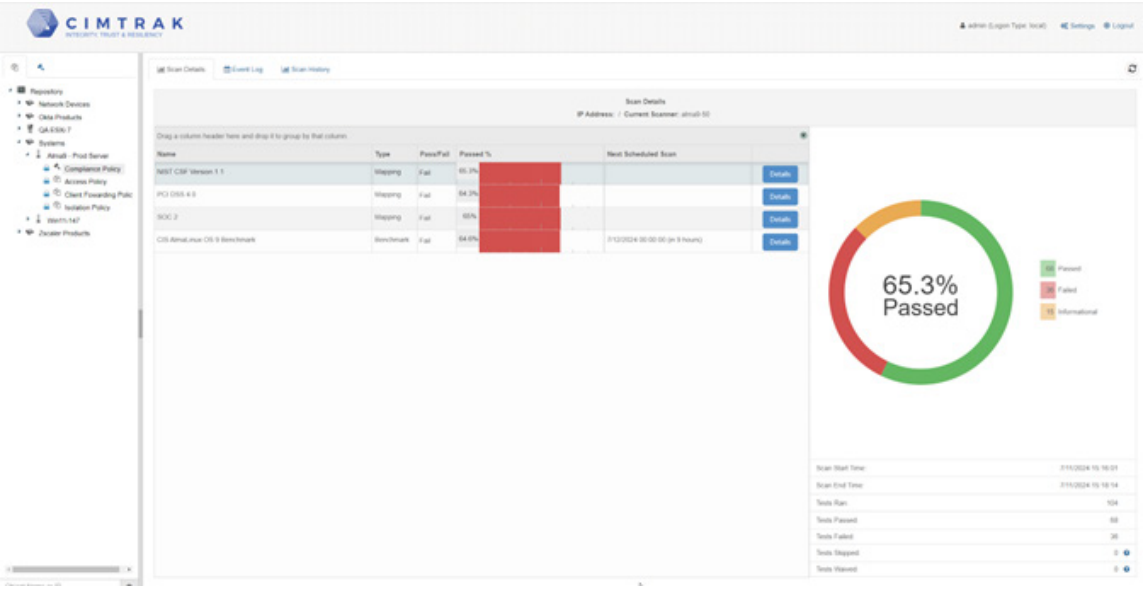

Figure 121. Scan score

You can see CimTrak triggered the ZPA Policy.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event
Info	7/11/2024 15:34:21	Mapping PCI DSS Version 3.2.1 failed
Info	7/11/2024 15:34:21	Mapping NIST CSF Version 1.1 failed
Info	7/11/2024 15:34:21	Mapping SOC 2 failed
Info	7/11/2024 15:34:21	Policy Integration Enabled BYPASS_POLICY (Outage-BackupServer-Reroute) because of ComplianceFailThreshold trigger
Info	7/11/2024 15:34:20	Benchmark CIS AlmaLinux OS 9 Benchmark / Profile: Level 1 - Server failed
Info	7/11/2024 15:34:17	Compliance scan completed
Info	7/11/2024 15:31:55	Compliance scan started
Info	7/11/2024 15:31:55	Lock Started
Info	7/11/2024 15:31:55	Lock Complete

Figure 122. Policy triggered

In the ZPA Admin Portal, the policy has switched to **Forward to ZPA** mode.

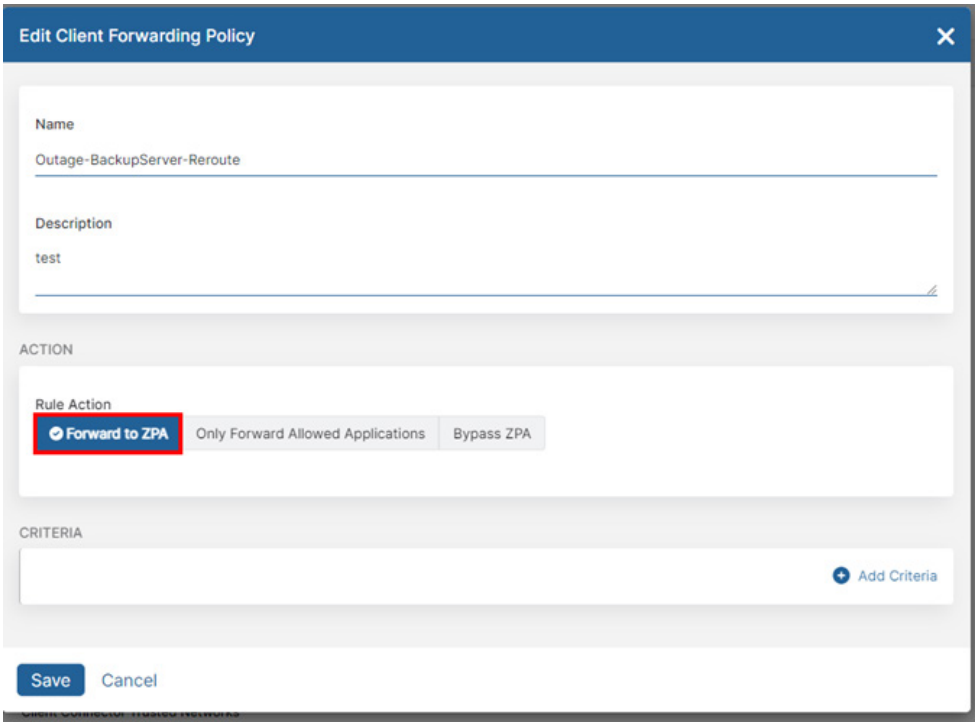

Figure 123. Forward to ZPA

Resetting the Integration

While you can change the Rule Action status in ZPA, there is also an option to do it from the CimTrak Web Console.

1. Right-click **Repository**, then select **Compliance Policy** and **Properties**.

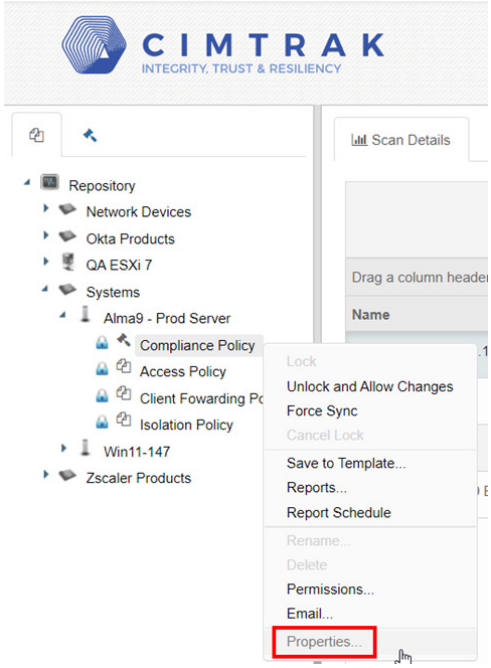

Figure 124. Properties

2. Click the **Integrations** tab.

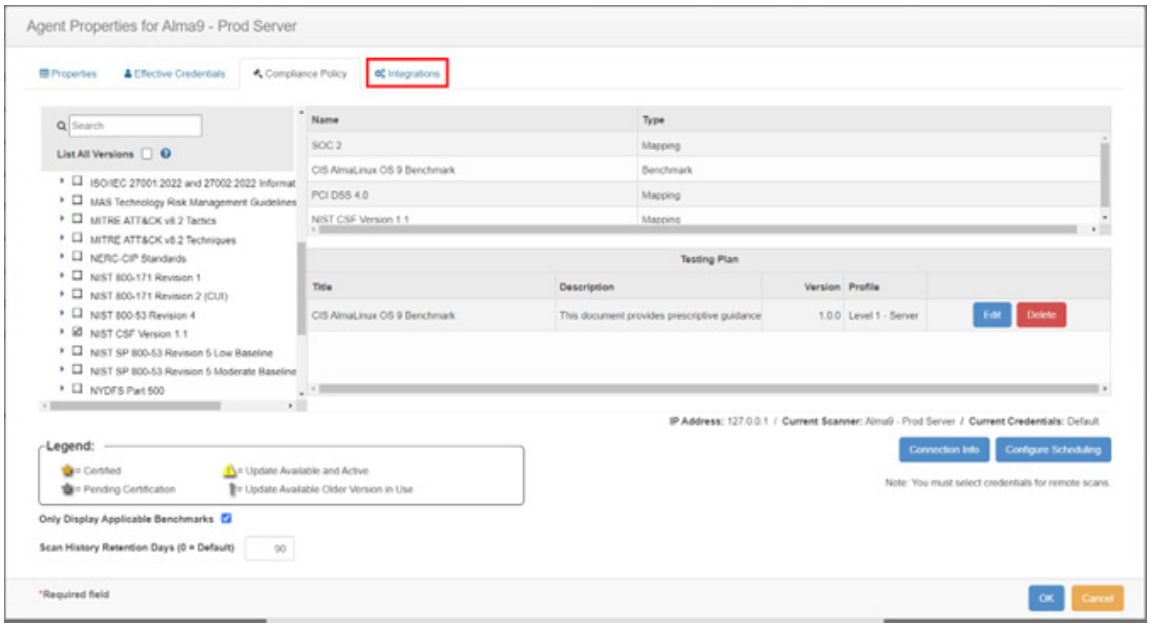

Figure 125. Integrations

3. The following shows the current ZPA Policy status. Click **Reset** to undo the action.

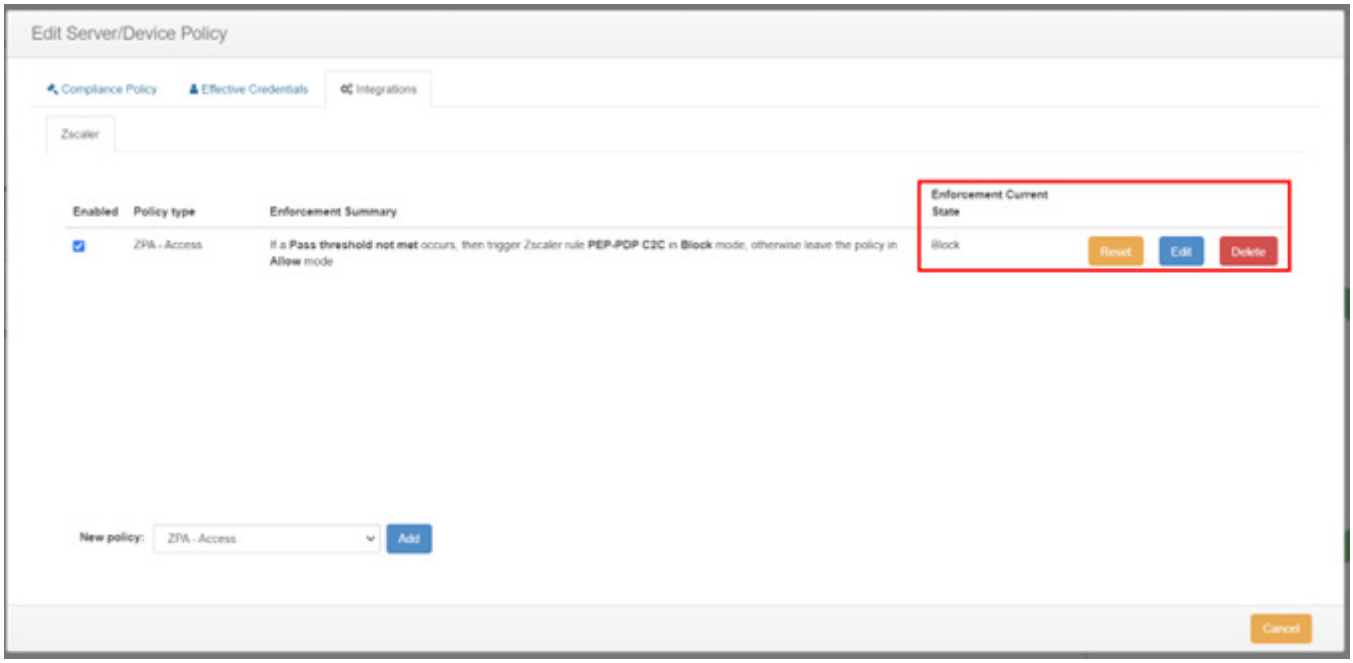

Figure 126. Reset

Integrating with Isolation Policies

To integrate with isolation policies:

1. Select **ZPA–Isolation** and click **Add**.

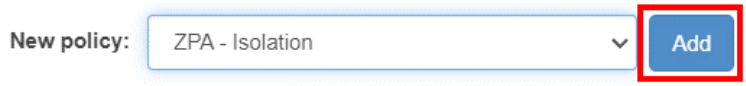

Figure 127. ZPA–Isolation

2. Configure how you want this integration to interact with your policy.

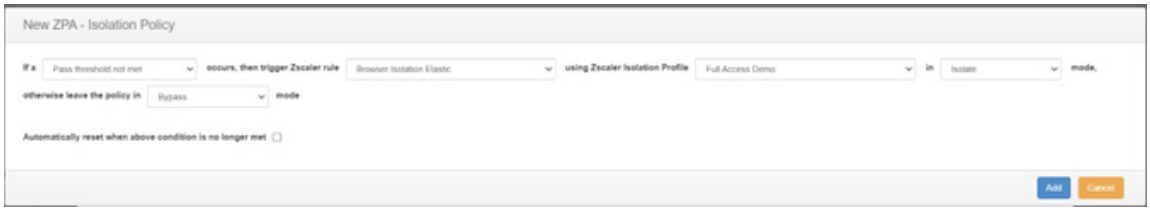

Figure 128. Configure integration

This is a logic statement that you can easily configure and change with a drop-down menu, as follows:

If a <COMPLIANCE TRIGGER> occurs, then trigger Zscaler rule <ZSCALER ISOLATION POLICY> in <MODE> mode, otherwise leave the policy in <MODE> mode.

- **Automatically reset when above condition is no longer met**. This setting disables this ZPA Policy if the system is in a PASSING state for the configured compliance policy

The variables are defined as follows:

- **COMPLIANCE TRIGGERS**: There is only one Compliance Trigger:
  - **Pass threshold not met**: This means that not meeting the Compliance/Benchmark scores of the configured threshold in CimTrak triggers the ZPA policy.

    Configure this threshold in the Repository Properties. Right-click **Repository** in the left-side **Tree View** and select **Properties**.

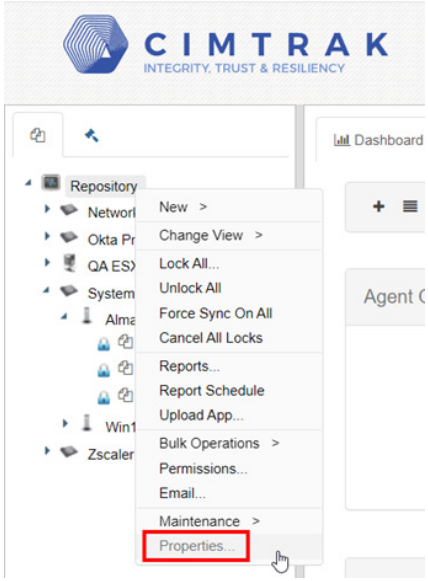

Figure 129. Properties

3. Click the **Compliance** tab.

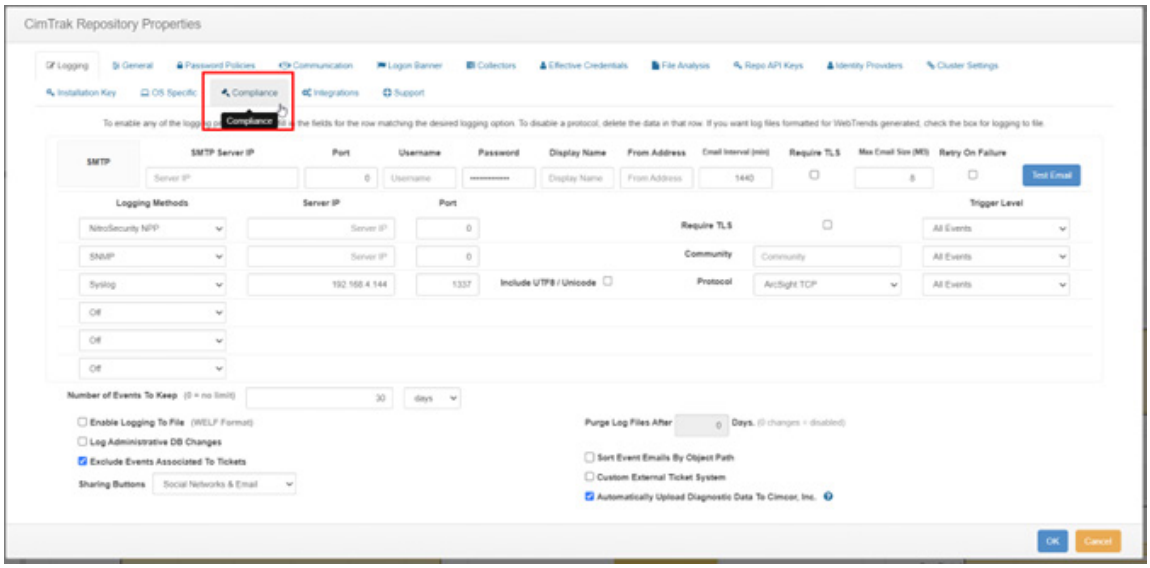

Figure 130. Compliance

4. Configure what test percentages equate to a PASS value. The default is 100%.

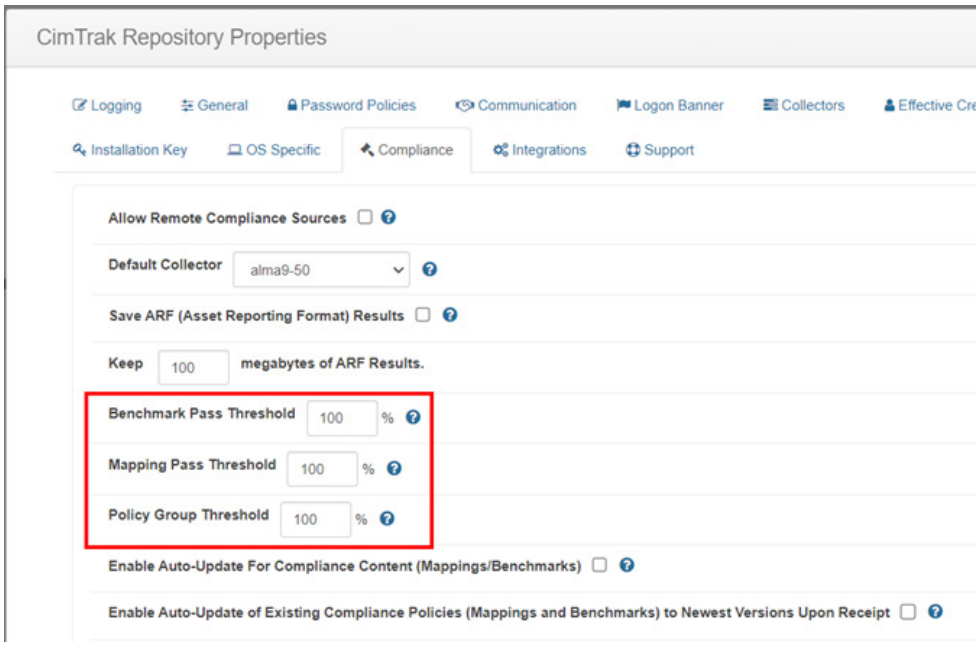

Figure 131. Compliance values

- **ZSCALER ISOLATION POLICY**: This drop-down menu populates the available access policy found in your ZPA environment:
  - **Isolation Policy 1**
  - **Isolation Policy 2**
  - **Isolation Policy N**

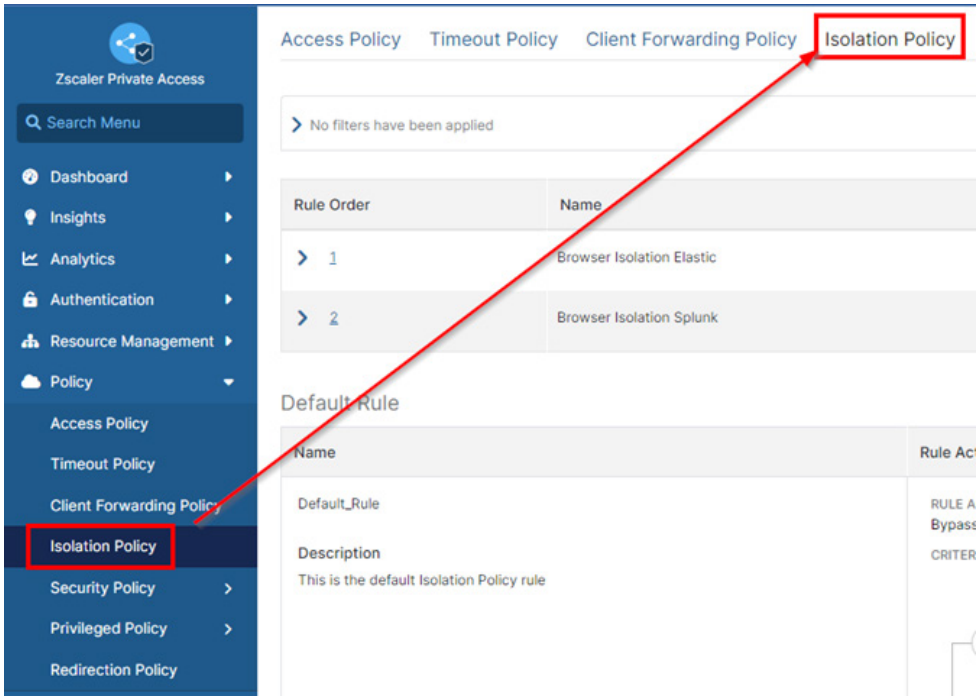

Figure 132. Isolation Policy

- **MODE**: This refers to the isolation policy Rule Actions:
  - **Allow Isolation**
  - **Bypass Isolation**

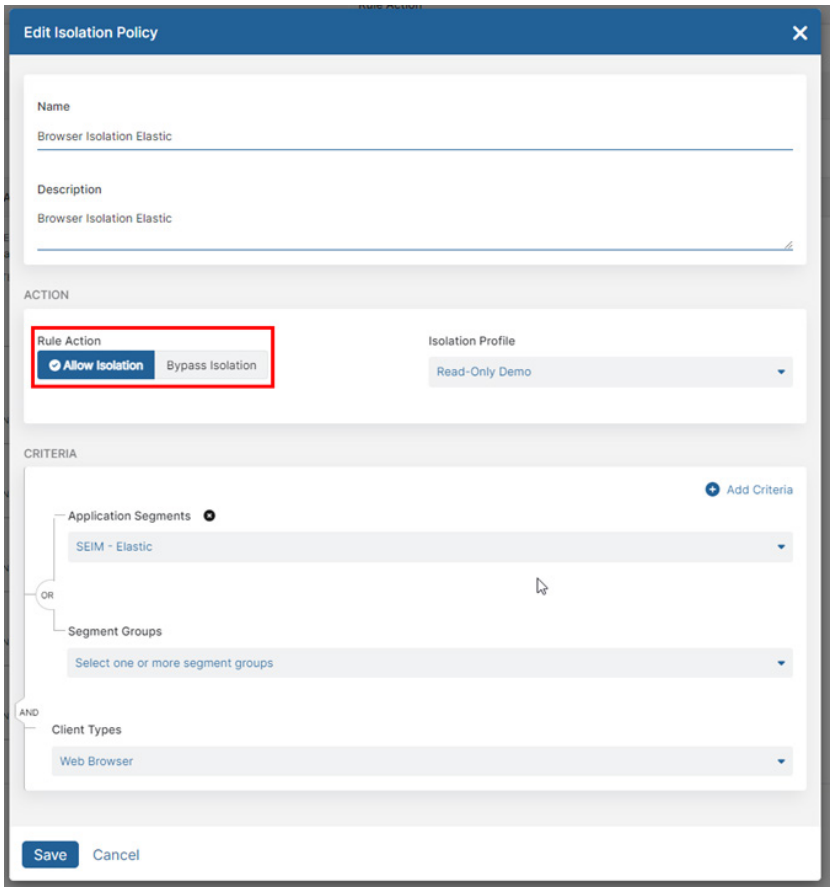

Figure 133. Isolation policy rule actions

5. Click **Save** to show the final logic statement created for the policy trigger.

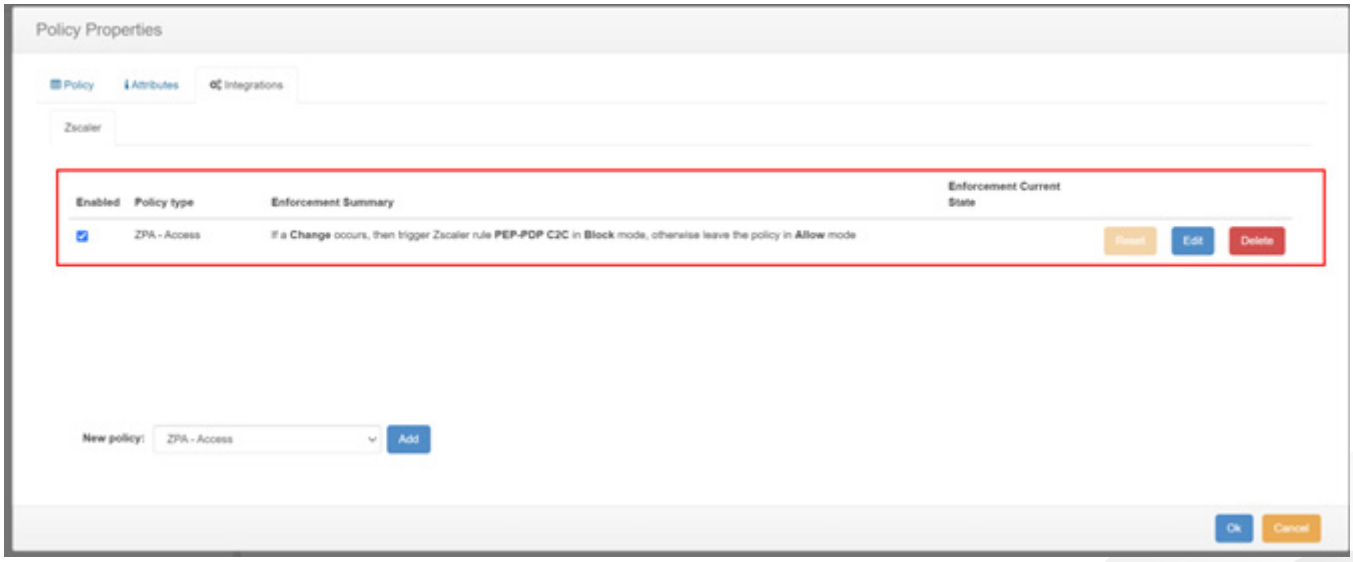

Figure 134. Final logic statement

6. Click **OK** to save the policy.

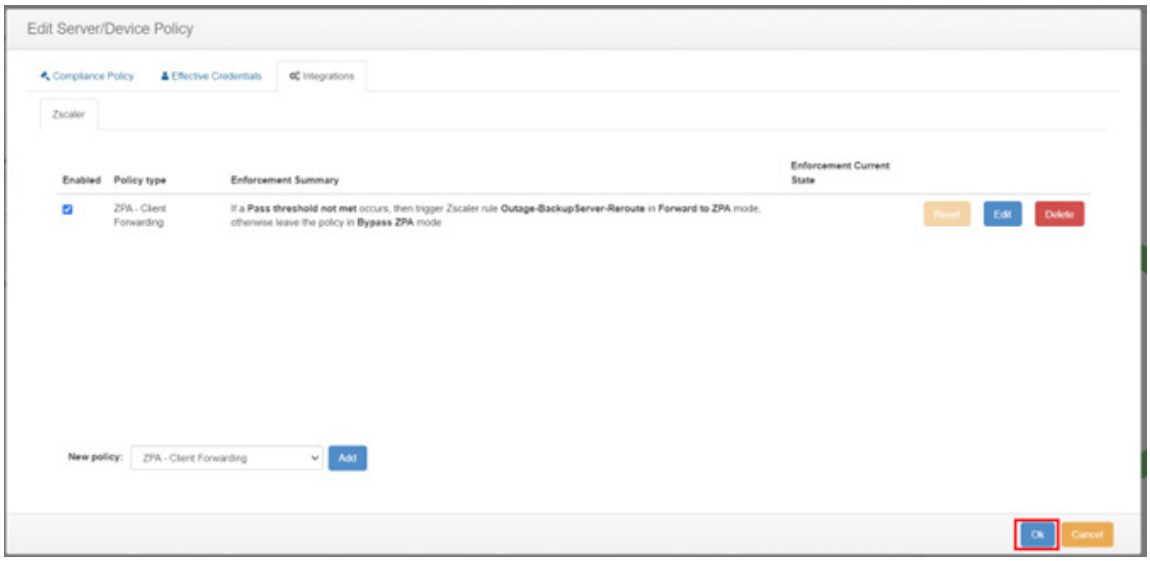

Figure 135. Save the policy

7. The new policy is created under the **Agent** with a red **Unlocked** icon. This means it is disabled. To turn it on, right-click and select **Lock**.

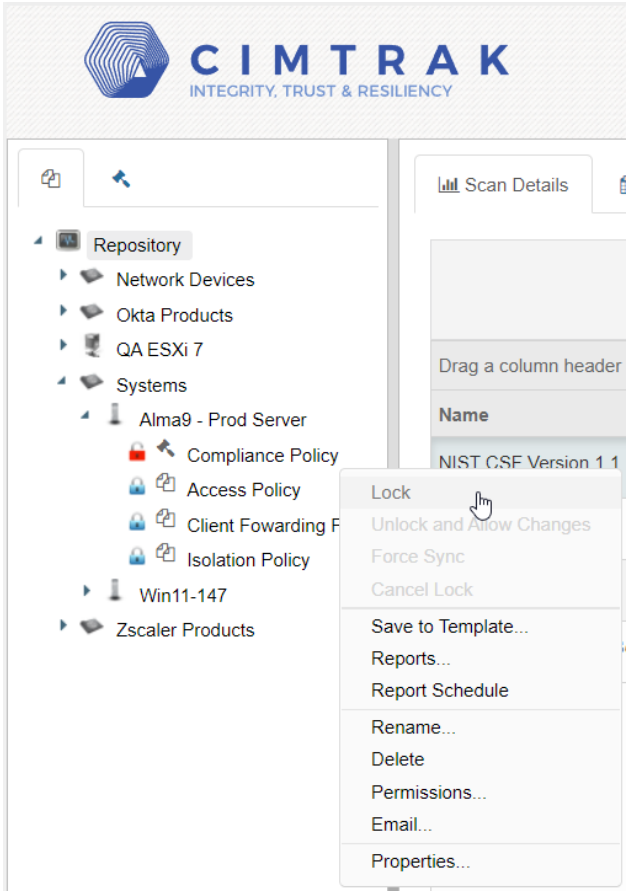

Figure 136. Lock

8. CimTrak initiates the scan and completes the Benchmark/Compliance tests. After completion, you receive the Compliance Scan Completed event in the Event Log. The score is found in the Scan Details tab.

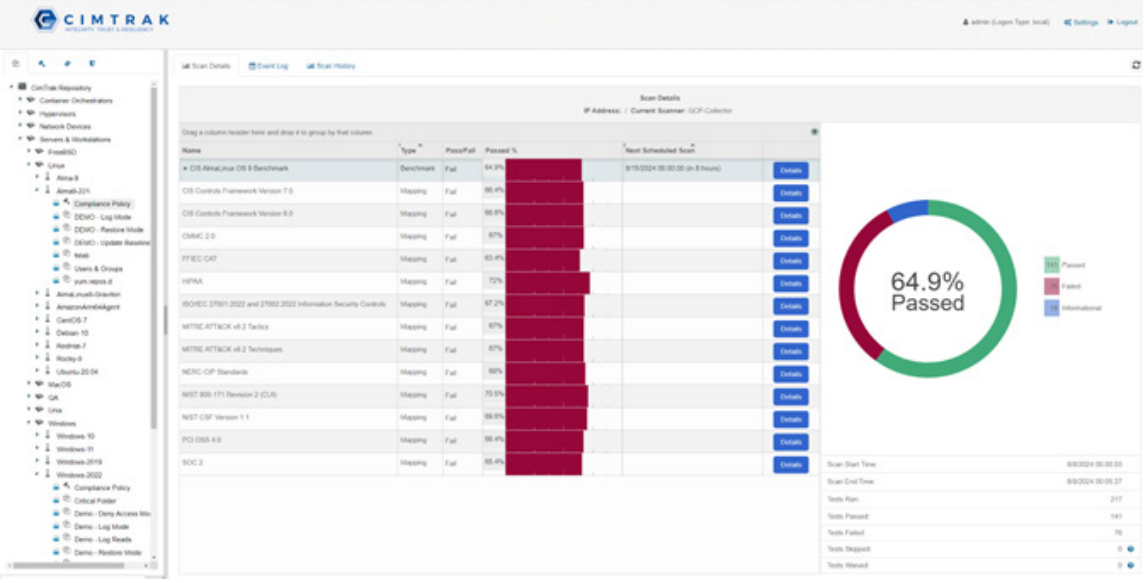

Figure 137. Completed scan

Testing the Integration

You can test the rules.

The following example uses a policy that expects a 100% PASSING score, otherwise the ZPA Isolation policy is triggered to **Allow Isolation** mode.

The following image shows the completed scan.

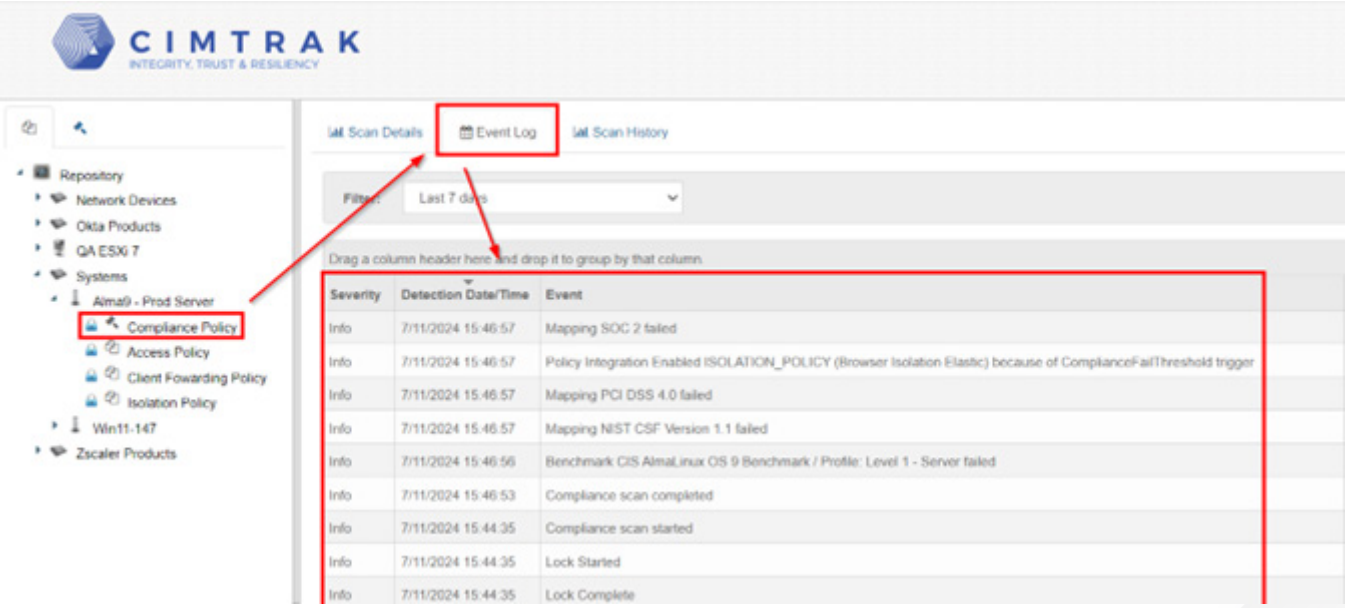

Figure 138. Completed scan

The score is 65.3% (this does not meet the 100% criteria).

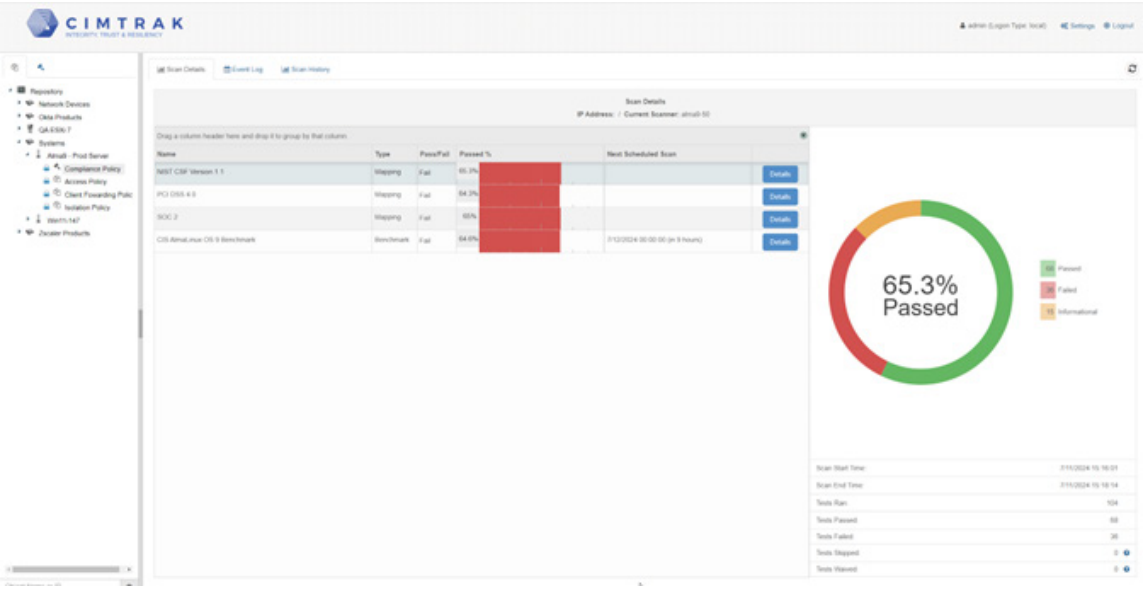

Figure 139. Scan score

You can see CimTrak triggered the ZPA Policy.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event
Info	7/11/2024 15:46:57	Mapping SOC 2 failed
Info	7/11/2024 15:46:57	Policy Integration Enabled ISOLATION_POLICY (Browser Isolation Elastic) because of ComplianceFailThreshold trigger
Info	7/11/2024 15:46:57	Mapping PCI DSS 4.0 failed
Info	7/11/2024 15:46:57	Mapping NIST CSF Version 1.1 failed
Info	7/11/2024 15:46:56	Benchmark CIS AlmaLinux OS 9 Benchmark / Profile: Level 1 - Server failed
Info	7/11/2024 15:46:53	Compliance scan completed
Info	7/11/2024 15:44:35	Compliance scan started
Info	7/11/2024 15:44:35	Lock Started
Info	7/11/2024 15:44:35	Lock Complete

Figure 140. Triggered ZPA policy

In the ZPA Admin Portal, you can see the Policy has switched to **Allow Isolation** mode.

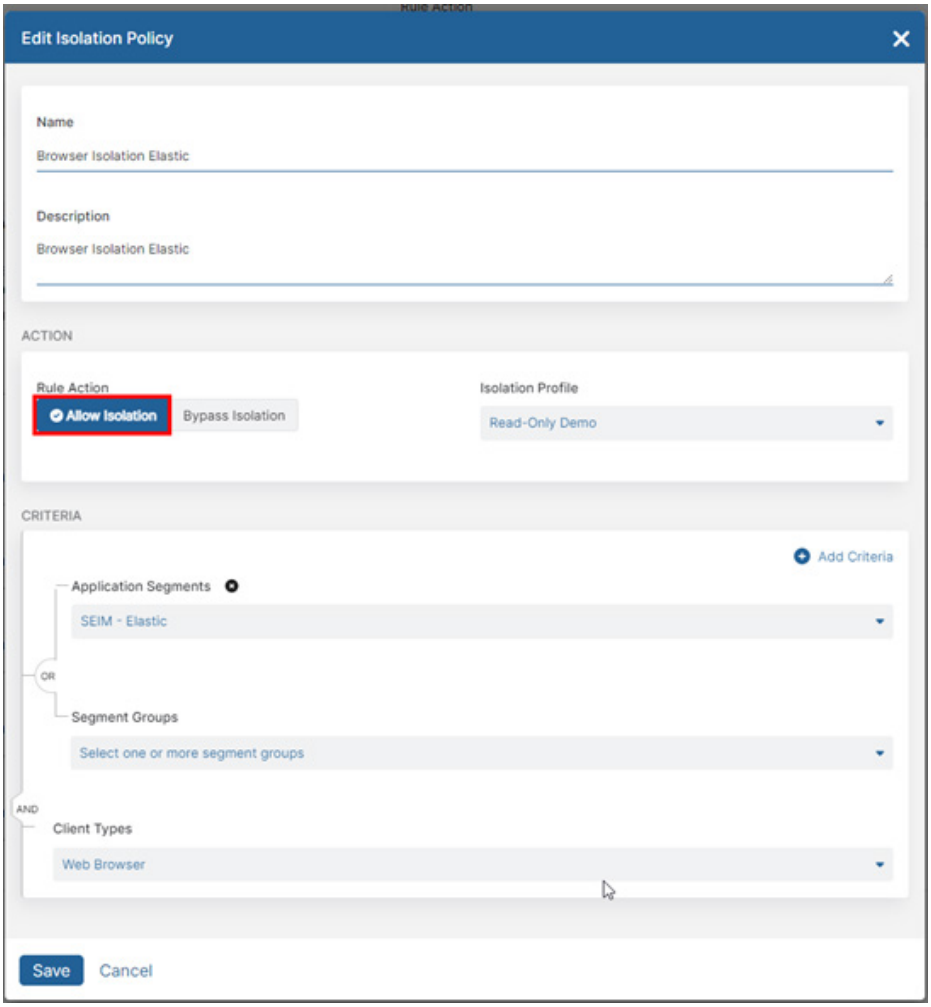

Figure 141. Allow Isolation mode

Resetting the Integration

While you can change the Rule Action status within ZPA, there is also an option to do it from the CimTrak Web Console.

1. Right-click **Repository**, then select **Compliance Policy** and **Properties**.

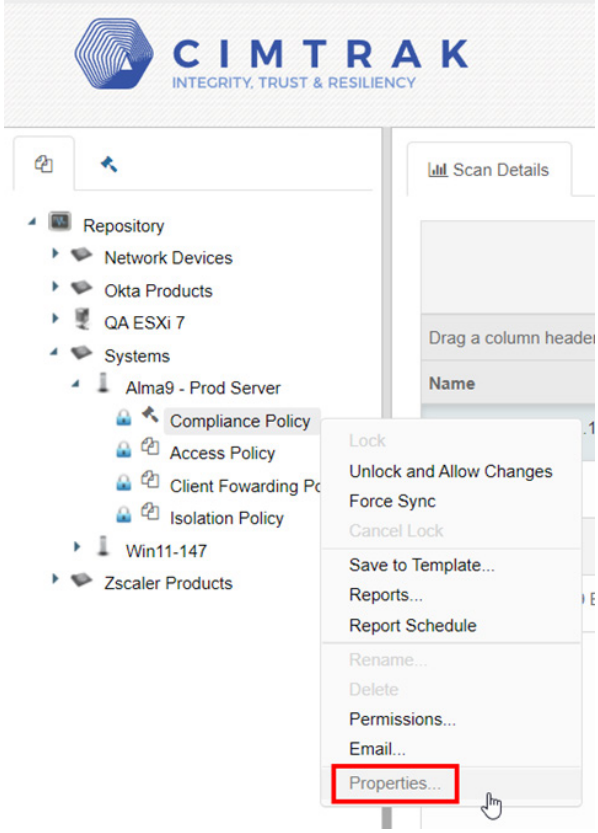

Figure 142. Properties

2. Click the **Integrations** tab.

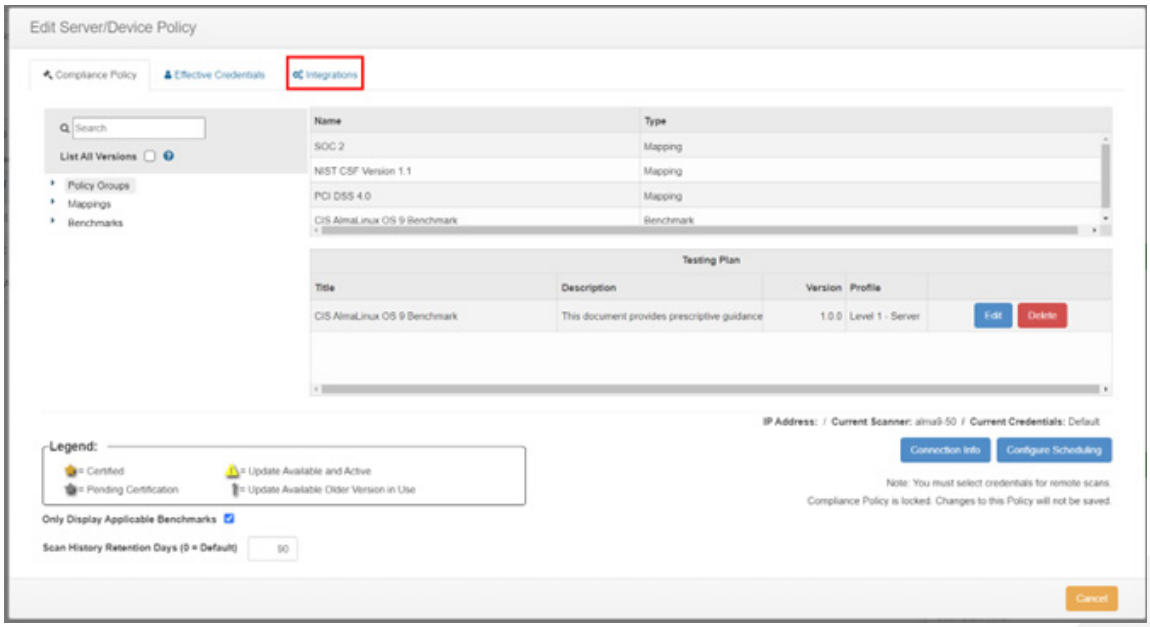

Figure 143. Integrations

3. You can see the current ZPA Policy status. Click the **Reset** button to undo the action.

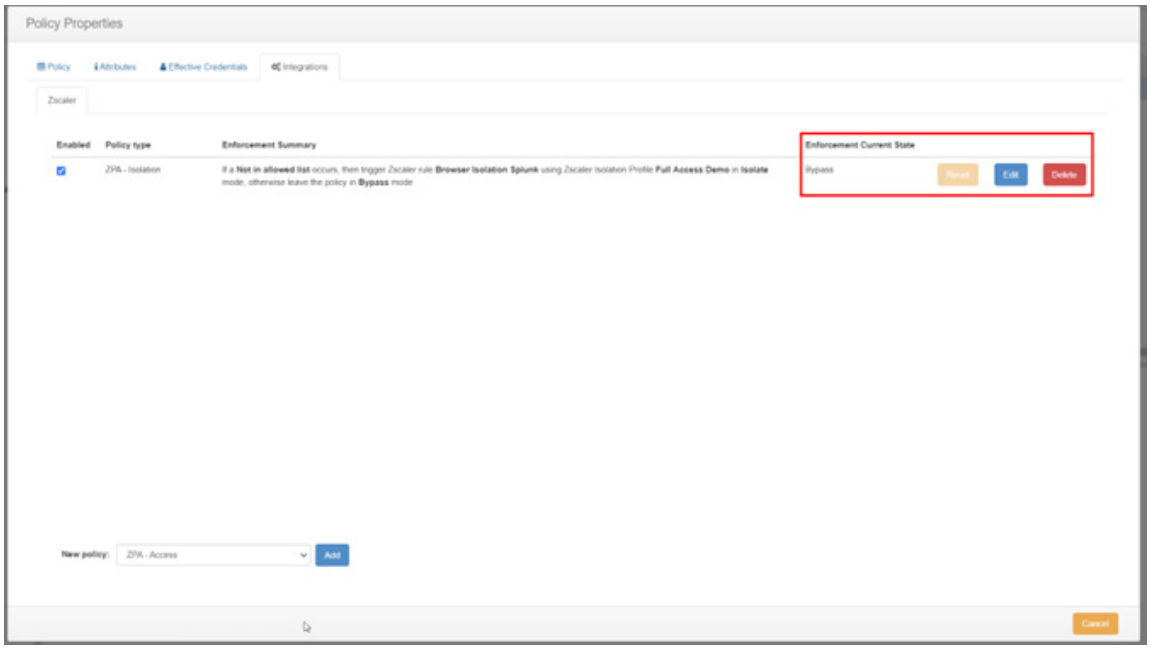

Figure 144. Reset status

Configuring ZIA and CimTrak

The following sections describe how to configure ZIA and CimTrak.

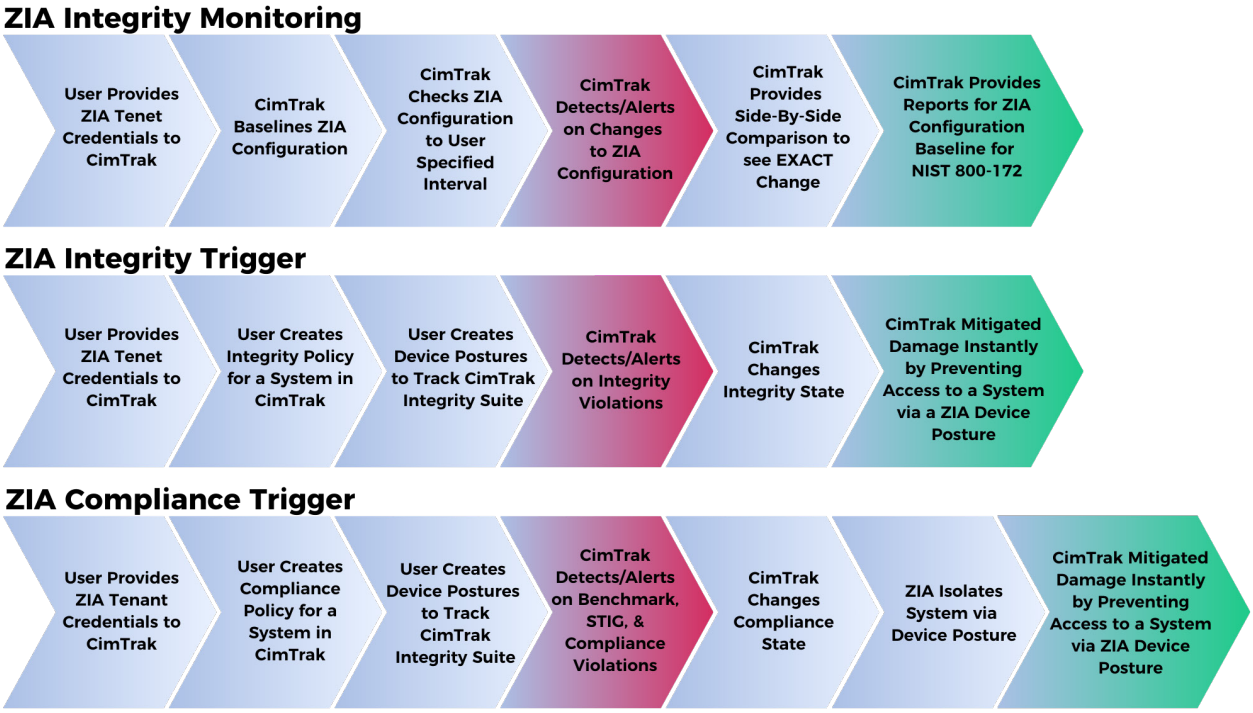

Figure 145. ZIA and CimTrak monitoring flow

Monitoring ZIA

The following sections describe how to monitor ZIA.

Login CimTrak Console

Go to the CimTrak Web Console for your environment and log in as a CimTrak Administrator. For example:

- `https://CimTrak-Server/cmc`
- `https://192.168.4.15/cmc`

Figure 146. CimTrak Web Console

Creating CimTrak Integrity Policy

After logging in to the dashboard:

1. Right-click **Repository** in the **Tree View** and select **New** > **Device & Policy**.
2. Click **Integrity Monitoring (Agentless)**.

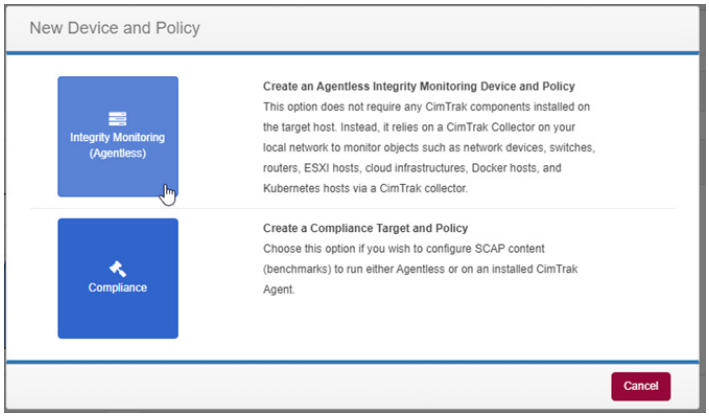

Figure 147. New Device and Policy

3. For **Device Type**, select **Zscaler**.
4. For **Zscaler Product**, select **ZIA**.
5. Input the **ZIA Endpoint**/**Username**/**Password**/**API Key** previously gathered.
6. Choose the **Output Format** (Zscaler recommends **Properties Format**).
7. Click **OK**.

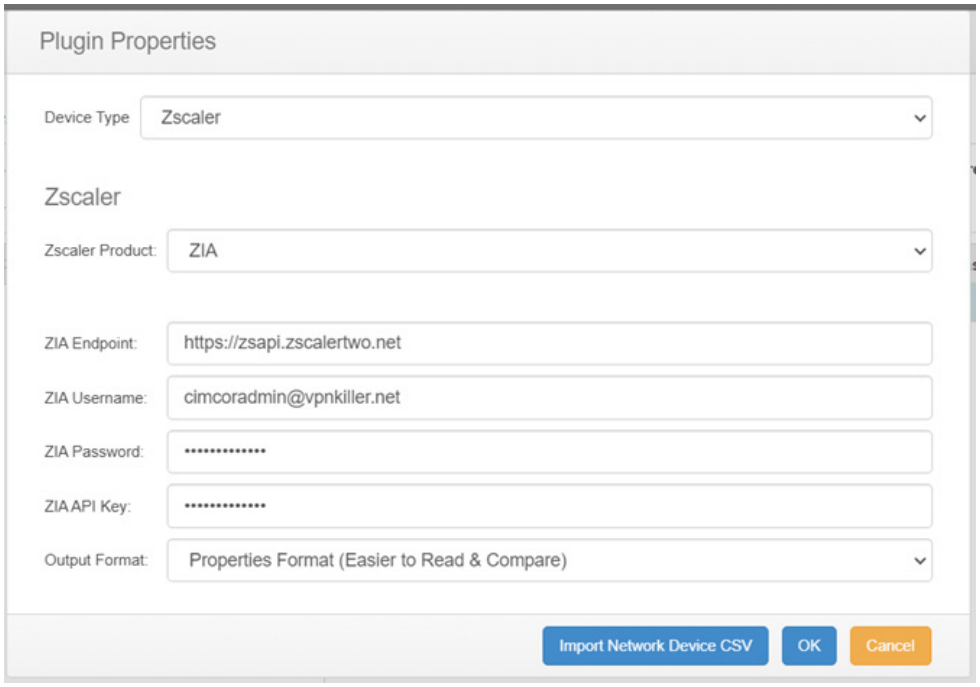

Figure 148. Plugin Properties

8. Click the **Arrow** next to **/DeviceRoot**. This shows what is available to monitor. Zscaler recommends selecting the top checkbox next to **/DeviceRoot** to monitor all ZIA configurations.
9. Deselect **Configurations** for anything you want to exclude.

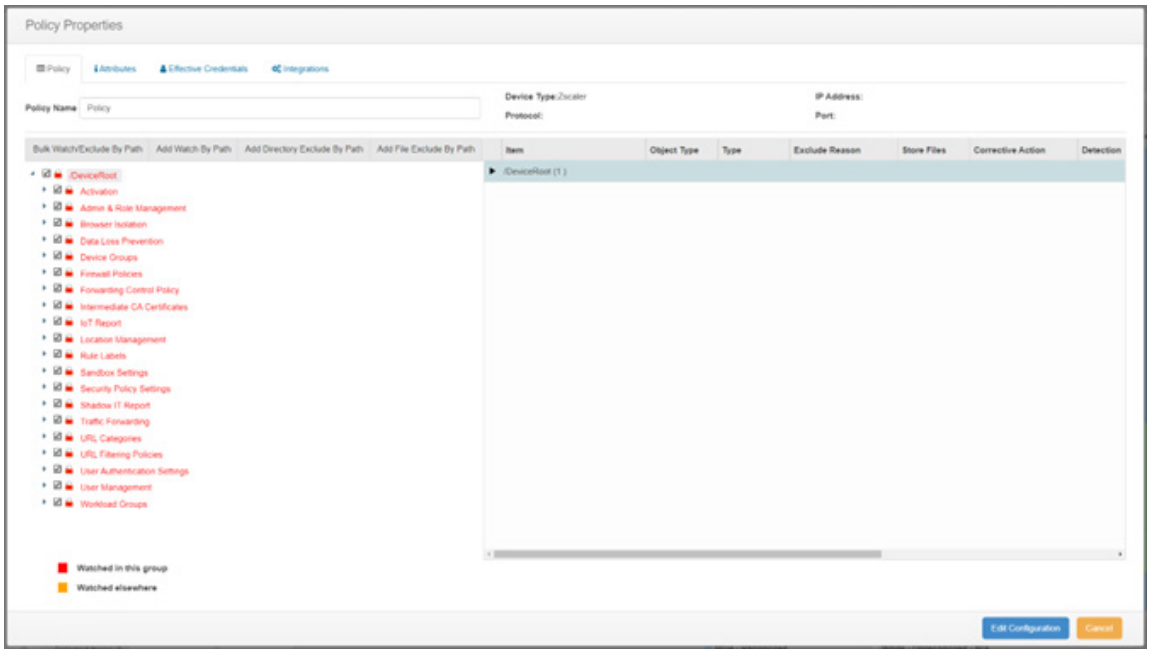

Figure 149. Policy Properties

10. Upon selecting the checkbox, you must configure the **Watch Properties**. Zscaler recommends choosing **Log** mode.
11. Change the **Poll Detection (interval)** to have CimTrak check for Zscaler changed to an interval of your choice. The default is every two hours (02 hours and 00 minutes).
12. Leave all other default settings, as they are not relevant for this integration.
13. Click **OK**.

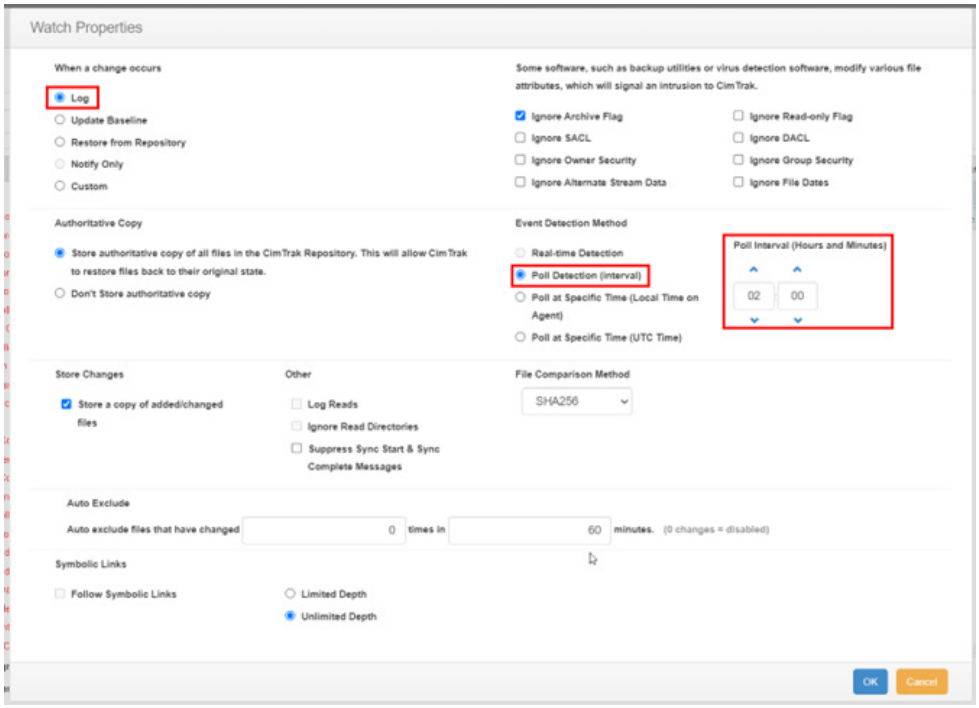

Figure 150. Watch Properties

14. Give the **Device** a name (e.g., `Zscaler ZIA`).

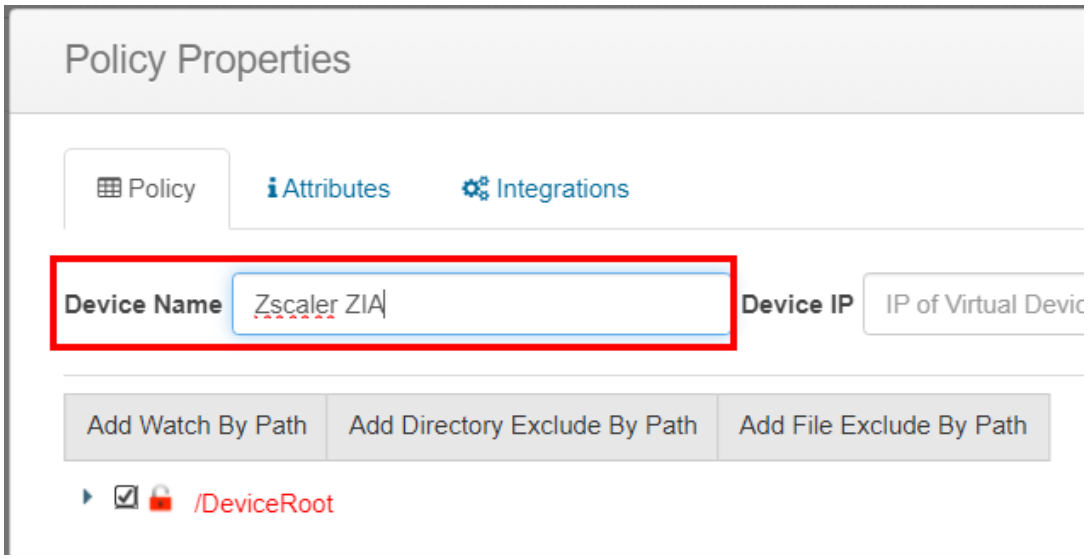

Figure 151. Device Name

15. Click **OK**.

Enabling CimTrak Integrity Policy

The policy must be monitored. To enable the policy to start its monitoring intervals:

1. Right-click the policy name and select **Lock and Digitally Sign**. It takes an initial baseline and then monitors on the configured schedule and reports on any deviations since the baseline.

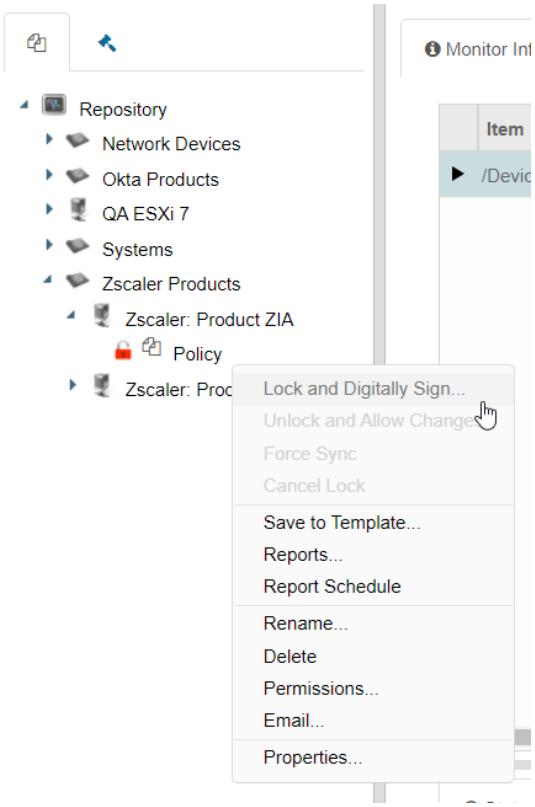

Figure 152. Lock and Digitally Sign

2. Watch the progress in the **Status Window** for completion.

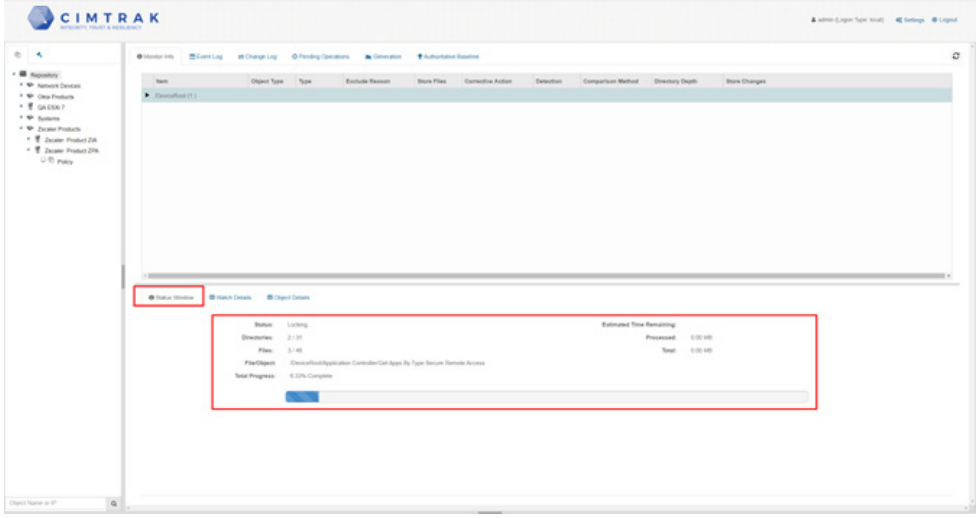

Figure 153. Status window

3. When complete, you see the policy change from a red **Unlock** icon to a blue **Lock** icon. It continues to check on your specified interval. You see the **Sync Start** message in the **Event Log** to indicate progress.

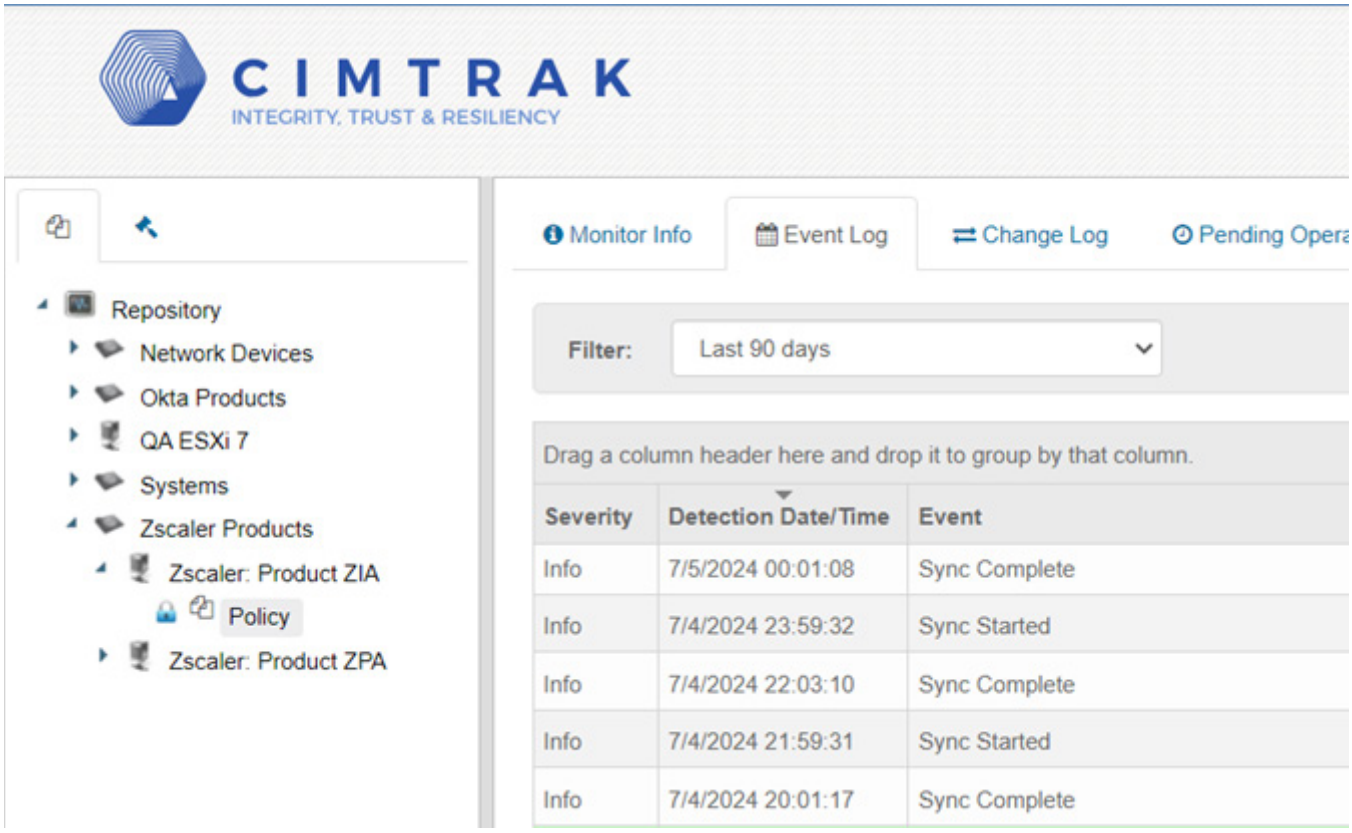

Figure 154. Complete Sync

Reviewing the Change Log

After CimTrak starts detecting changes, they are reported in the Change Log.

The following image shows the time CimTrak detected the change, and the Absolute Path indicates what changed. These are the same categories of ZIA configurations you saw when creating the Integrity Policy initially.

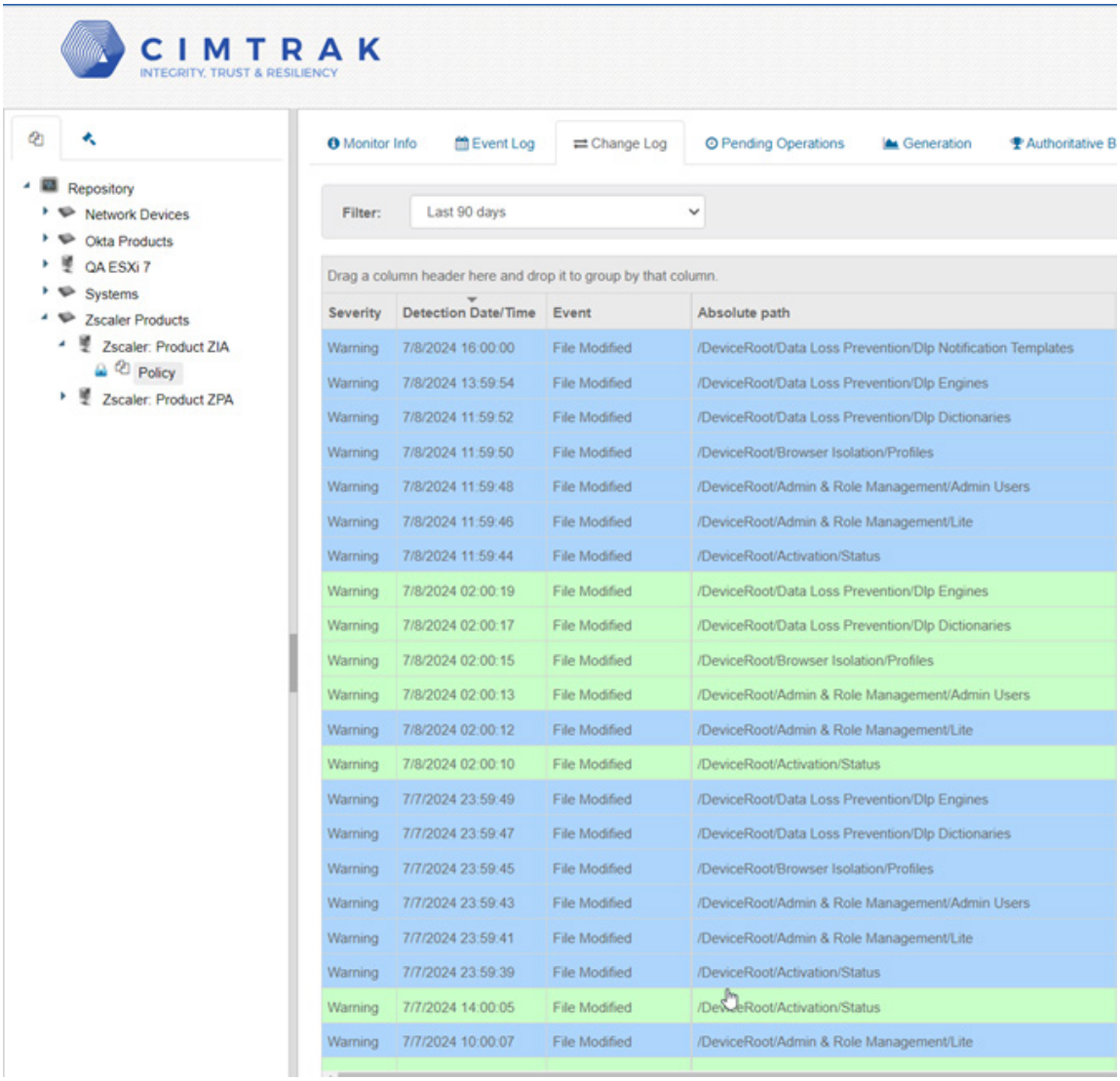

Figure 155. Change log

Right-click an event and select **Compare Against Previous State on Agent** to see a side-by-side comparison of exactly what changed.

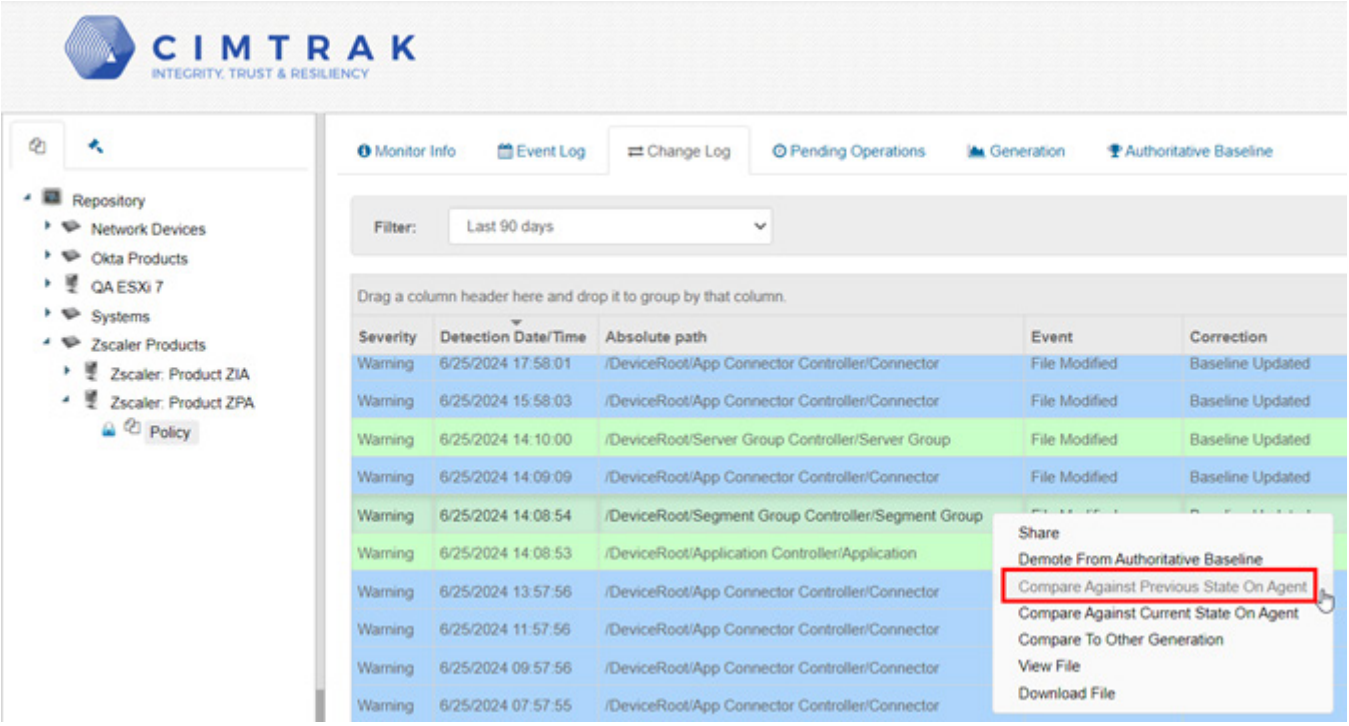

Figure 156. Compare Against Previous State On Agent

The following image shows the side-by-side comparison window.

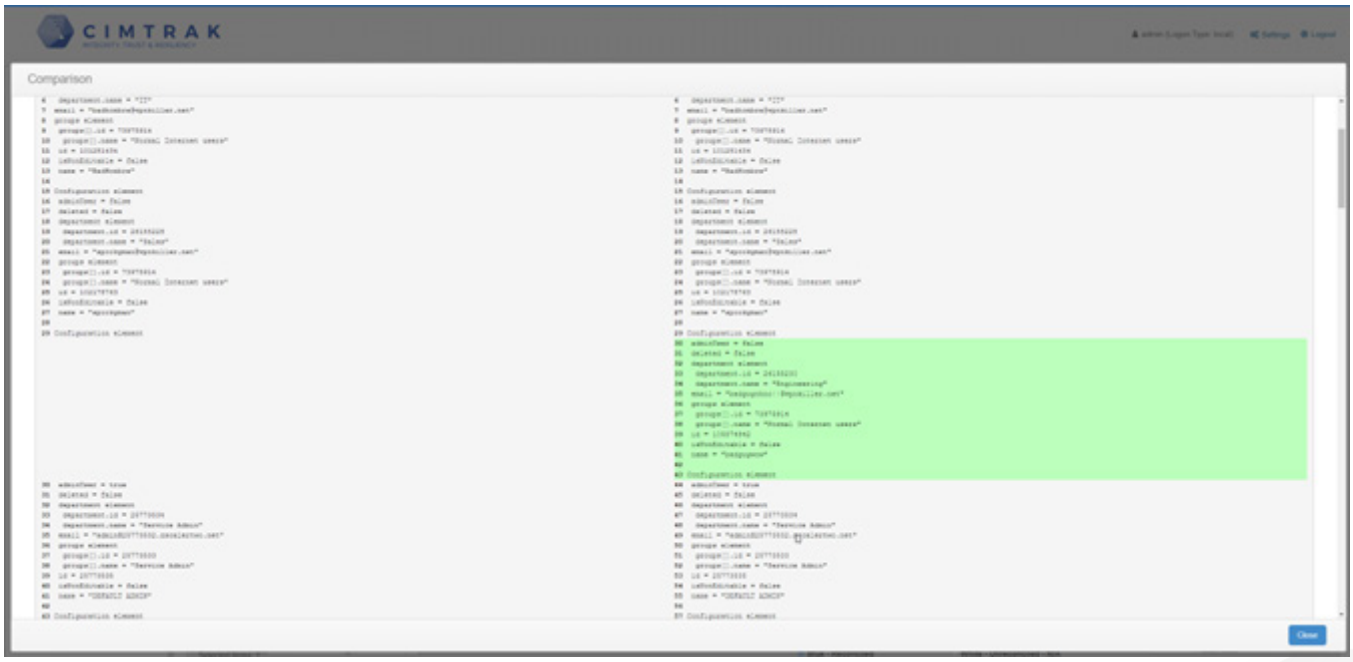

Figure 157. State changes

ZIA Integrity Triggers

The following sections describe how to configure ZIA integrity triggers.

This feature is for Windows Agents only.

Log in to the CimTrak Console

Go to your CimTrak Web Console in your environment and log in as a CimTrak Administrator. For example:

- `https://CimTrak-Server/cmc`
- `https://192.168.4.15/cmc`

Figure 158. CimTrak Web Console

Creating CimTrak Integrity Policy

In the left-side Tree View, find the system in question that you want to create a policy for.

1. Right-click the <agent name>, and then select **New** > **Policy**.

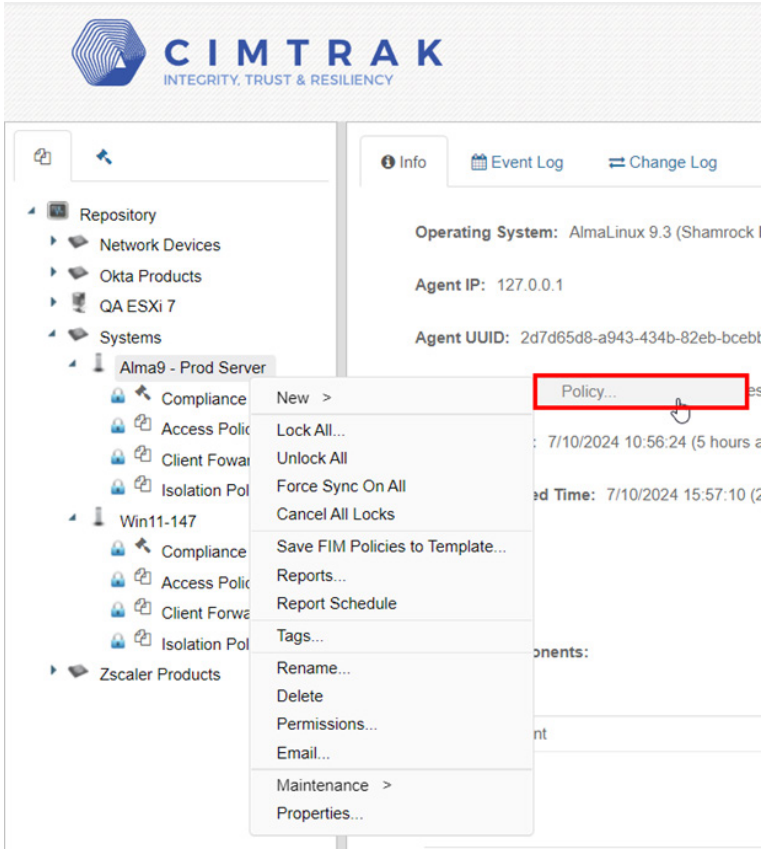

Figure 159. Policy

2. Click **Integrity Monitoring (Agent Based)**.

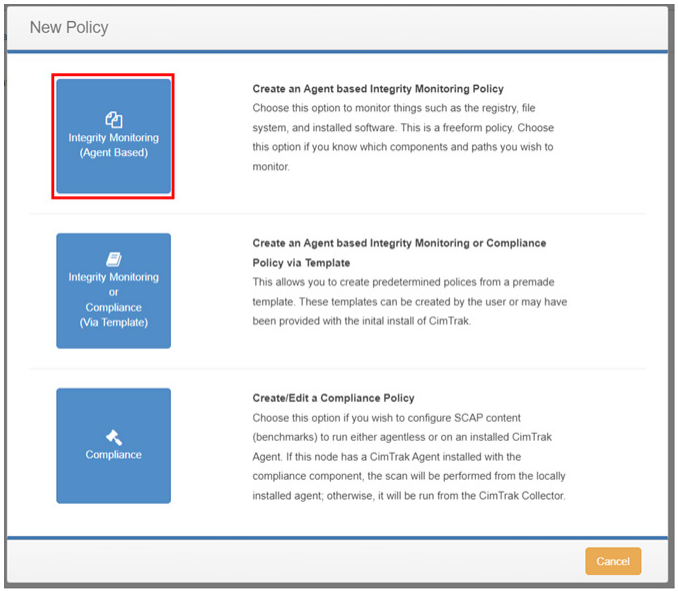

Figure 160. Integrity Monitoring (Agent Based)

3. Select the folder or object that you want to monitor. In this case, it is a folder on a Windows system.

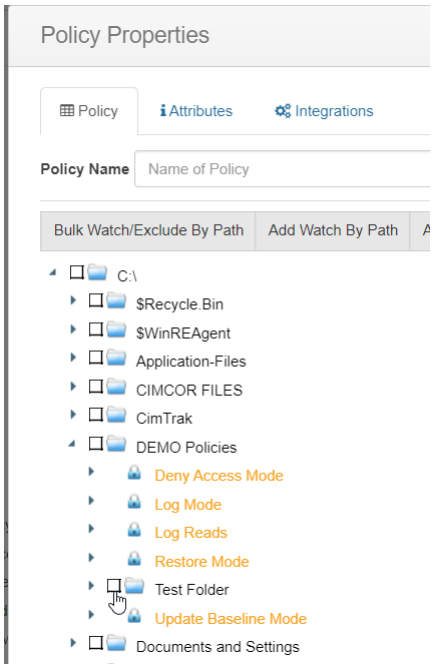

Figure 161. Policy Properties

4. In the **Watch Properties** dialog, select the monitoring options. For this example, select **Log** mode and leave the other field defaults.
5. Click **OK**.

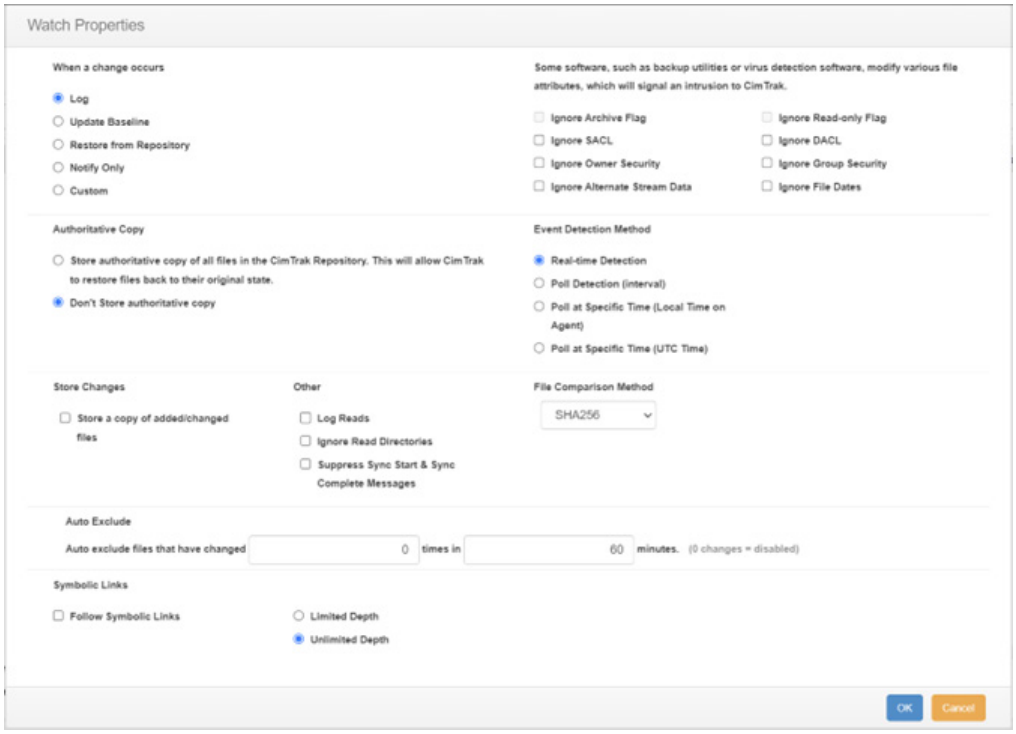

Figure 162. Watch properties

6. Enter a **Policy Name**. Don't click **OK**.

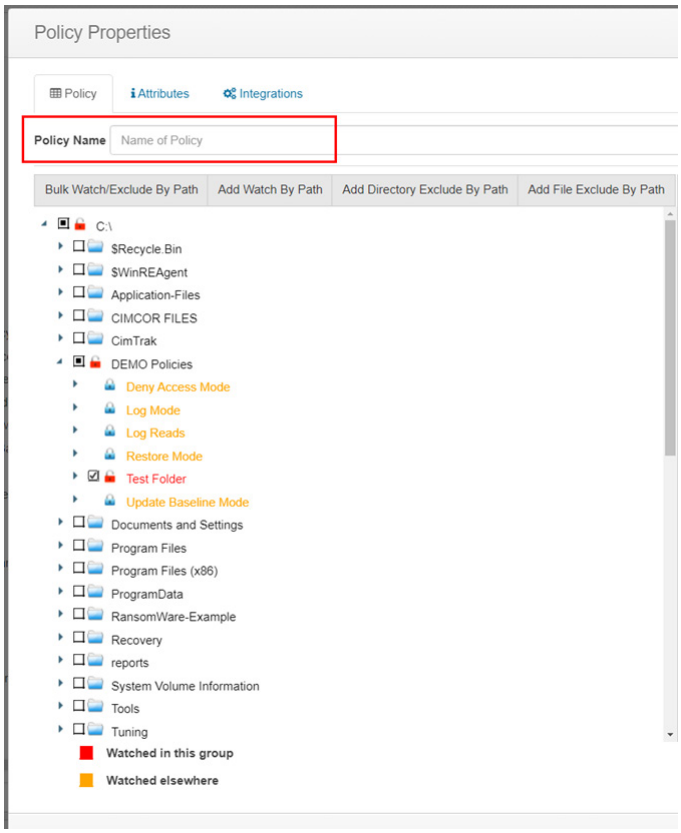

Figure 163. Policy name

Configuring Zscaler Integration

To configure the Zscaler integration:

1. Click the **Integrations** tab.

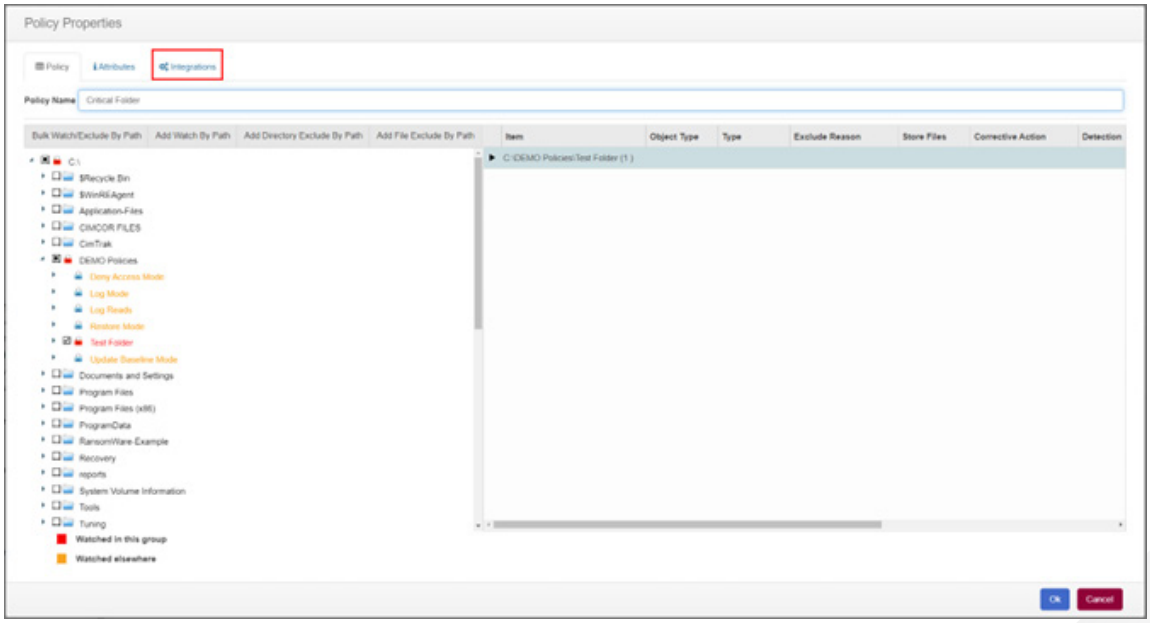

Figure 164. Integrations tab

2. Choose **ZIA – Registry Key Set** and click **Add**.

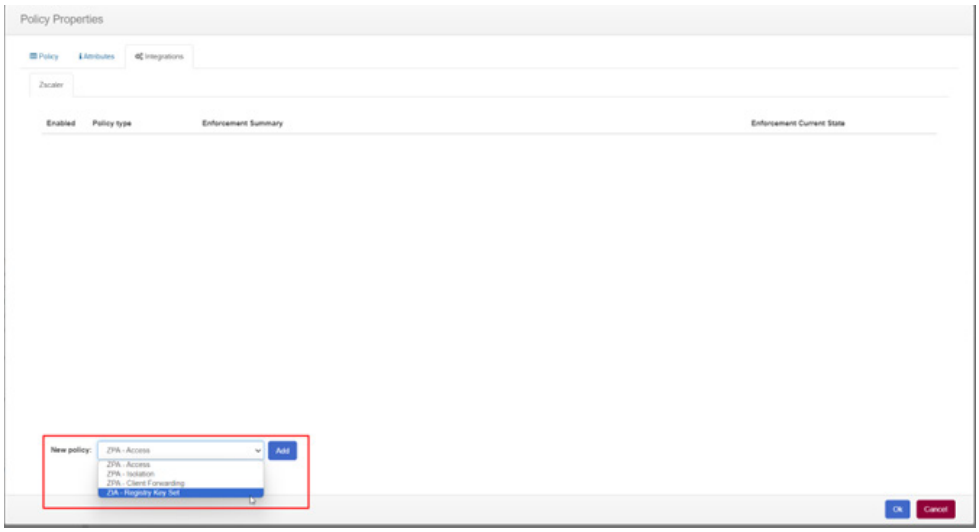

Figure 165. ZIA – Registry Key Set

3. The following window is displayed. Configure how you want this integration to interact with your policy.

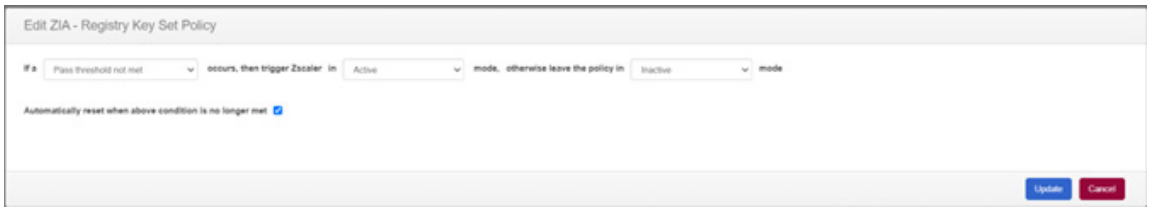

Figure 166. Set Policy

This is a logic statement that you can configure and change with a drop-down menu, as follows:

If an <INTEGRITY TRIGGER> occurs, then trigger Zscaler in Active mode, otherwise leave the policy in Inactive mode.

These variables are defined as follows:

- I**NTEGRITY TRIGGERS**: These are the CimTrak Integrity options to trigger the policy.
  - **Change**: If any change that deviates the baseline
  - **Denied List Item Found**: If any change was a matching hash in the CimTrak Deny List (denylist).
  - **Not in allowed list**: If any change was NOT a matching hash in the CimTrak Allow List (allowlist).

Integrating with ZIA Device Posture

Use the CimTrak Agent to automatically create and manage a Registry Key to represent the Integrity and Compliance states. These values are then tracked via ZIA Device Postures to isolate machines based on the CimTrak states provided. These keys are automatically created and changed based on the state of Integrity and Compliance it detects when the policies are locked.

Registry Key Path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cimcor\CimTrak\CimTrakAgent
```


ZIA DWORD Values:

- **Agent Running**: Either 0 or 1 (0 = shutdown, 1 = started)
- **Configuration Assessment Score**: Either 0 or 1 (0 = compliant, 1 = noncompliant)
- **Integrity Score**: Either 0 or 1 (0 = no violations, 1 = integrity violation)

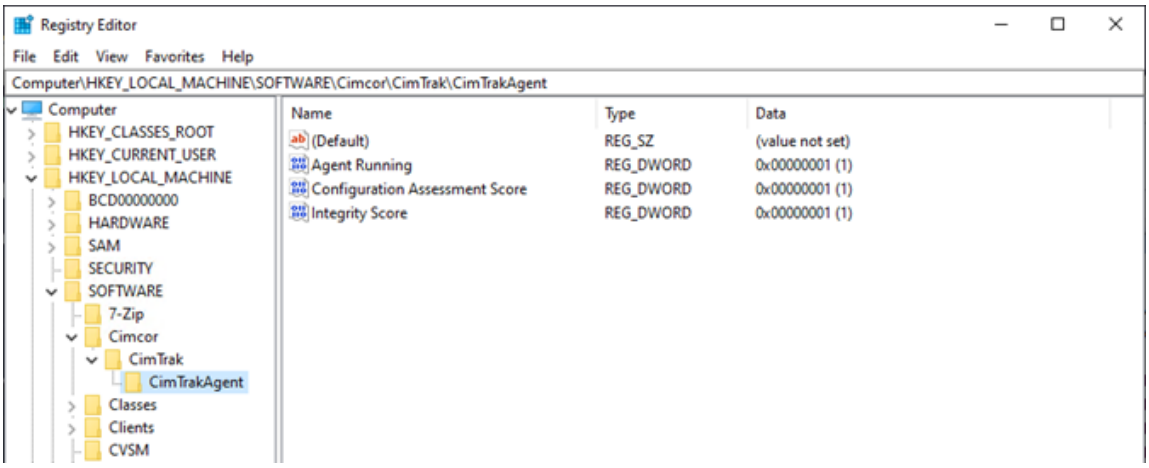

Figure 167. Registry Editor

ZIA Device Postures

To set ZIA device postures:

1. From the ZIA Client Connector Portal, select **Device Posture**.
2. Click **Add Device Posture**.

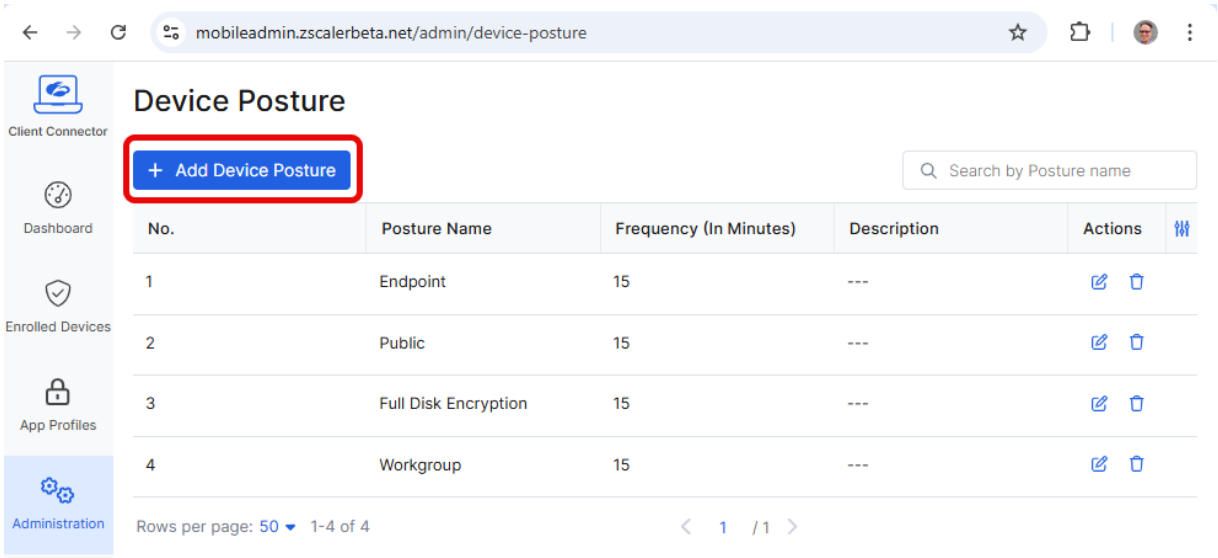

Figure 168. Add Device Posture

3. Create a Posture for the Integrity Registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cimcor\CimTrak\CimTrakAgent\Integrity Score`

   You must create a Device Posture Check for each state (1 and 0). Use the following nomenclature, or customize it for your needs:

   - CimTrak Integrity Verified – GOOD state – Registry key value of 0
   - CimTrak Integrity Violation – BAD state - Registry key value of 1

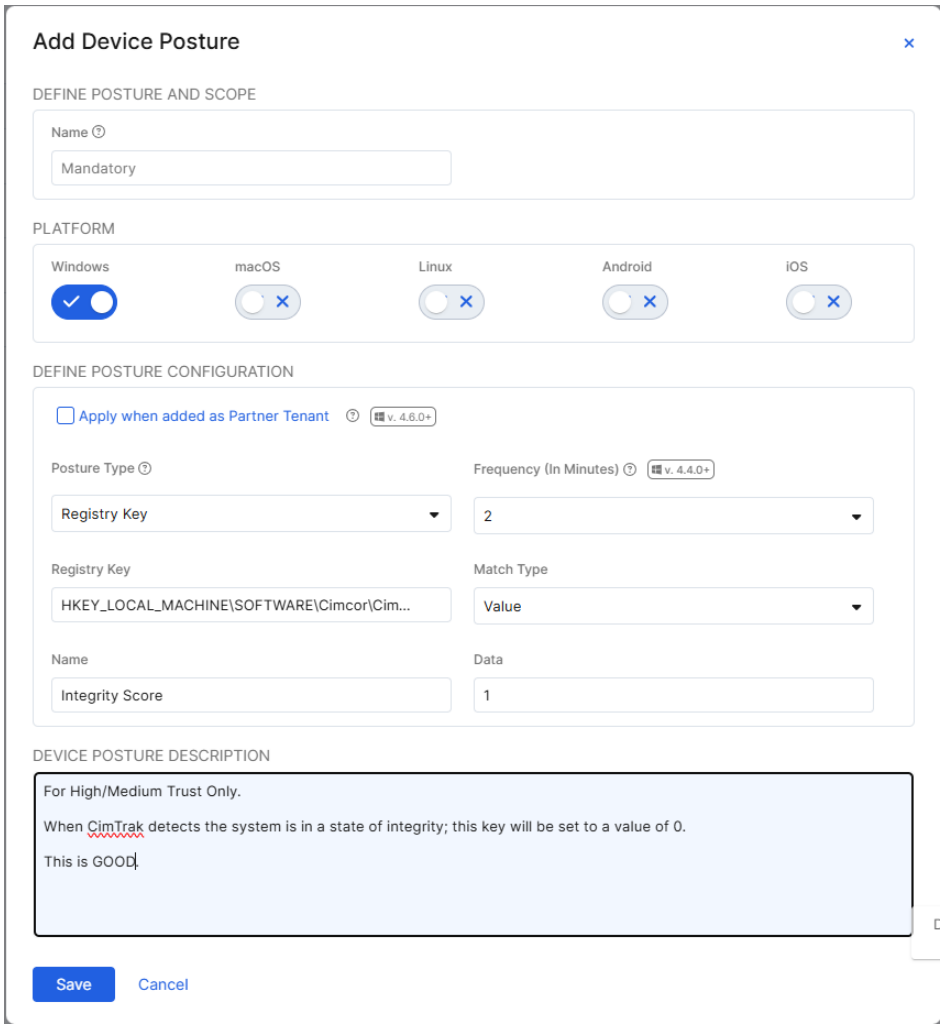

Figure 169. Add Device Posture

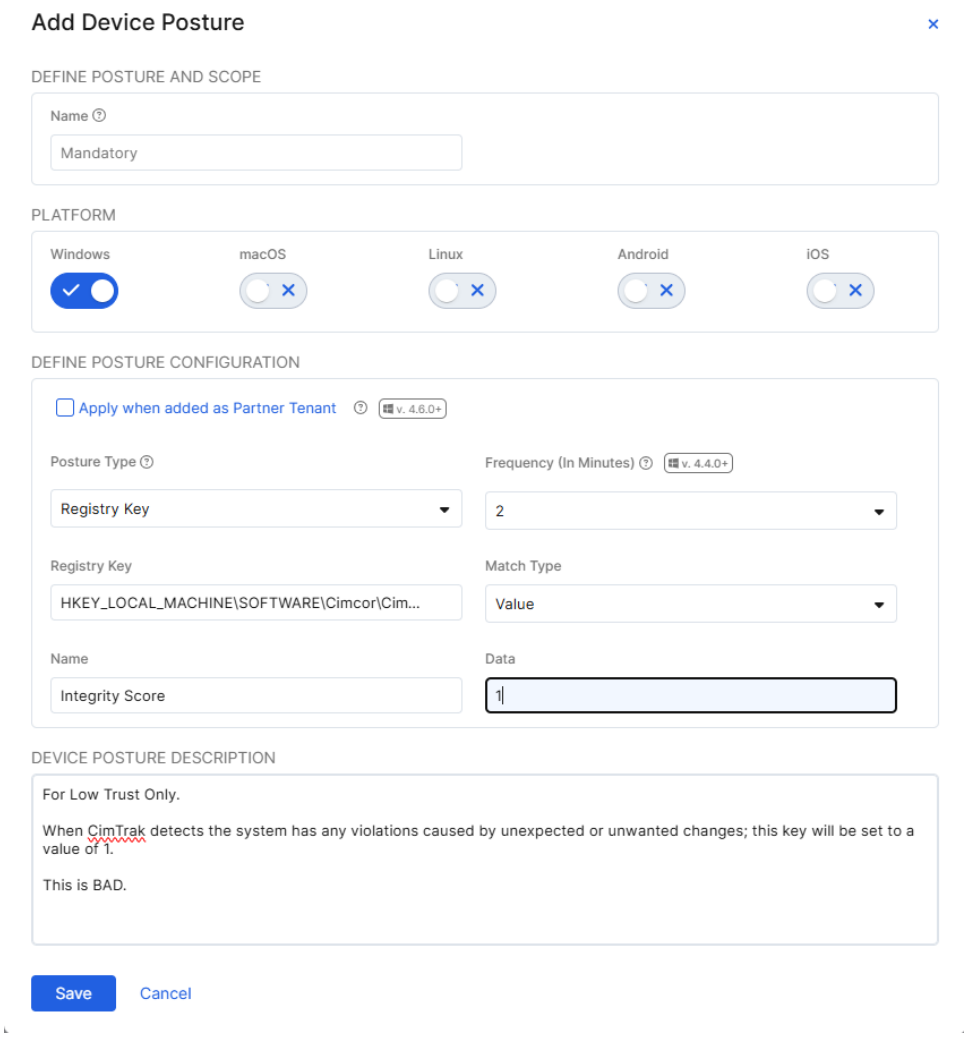

Figure 170. Add Device Posture

You can take advantage of this Device Posture in ZIA. A common example is if CimTrak detects an Integrity or Compliance violation, cut off access to all cloud apps, all internet, or certain networks based on CimTrak's findings. In this example, CimTrak monitors the user's endpoint (workstations or laptop). When that endpoint is in a compromised state, cut off access in any way you specify in ZIA using this Device Posture as the trigger. The possibilities are customizable on the ZIA side to handle what access to give or revoke based on the CimTrak triggers.

While you can use Device Posture in ZPA, that is not needed here, and Zscaler recommends you use the other ZPA integrations in this guide.

ZIA Posture Profile

After the Device Postures are set, create a profile to set levels of trust for systems that pass or fail these CimTrak Integrity or Compliance checks.

In the Zscaler Client Connector Portal:

1. Go to **Administration** > **ZIA Posture Profile** > **Windows**.
2. Click **Add ZIA Posture**.

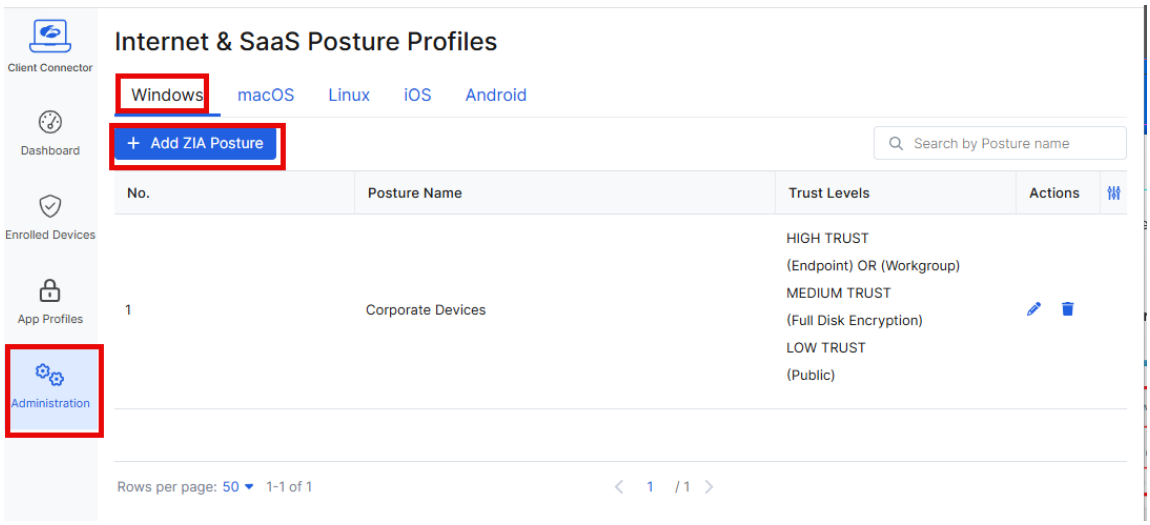

Figure 171. Add ZIA Posture Profile

3. Enter a **Posture Name** (e.g., `CimTrak Posture Profile`).

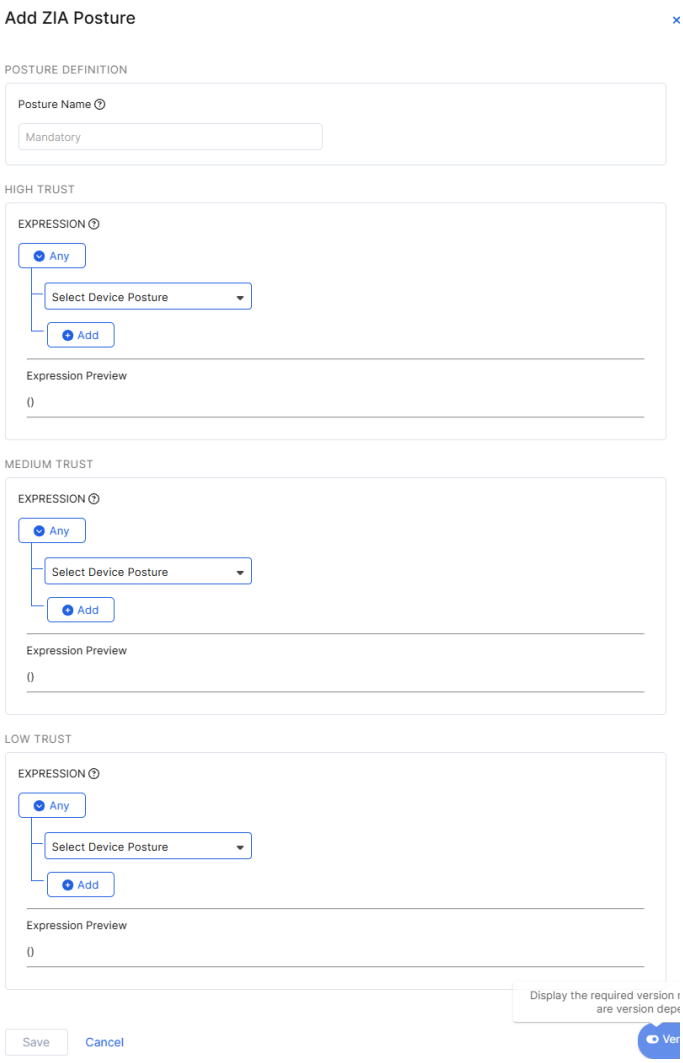

Figure 172. Add ZIA Posture

There are three levels of trust in this profile, as defined in the following list:

- **High Trust**: Passes both Integrity AND Compliance checks.
- **Medium Trust**: Passes Integrity OR Compliance checks.
- **Low Trust**: Passes NEITHER check.

If you only have CimTrak Integrity features, Zscaler recommends you apply the Integrity Posture check High Trust and leave blank Medium Trust and Low Trust.

4. For High Trust, click **Add** and select both **CimTrak Compliance Verified** and **CimTrak Integrity Verified**.

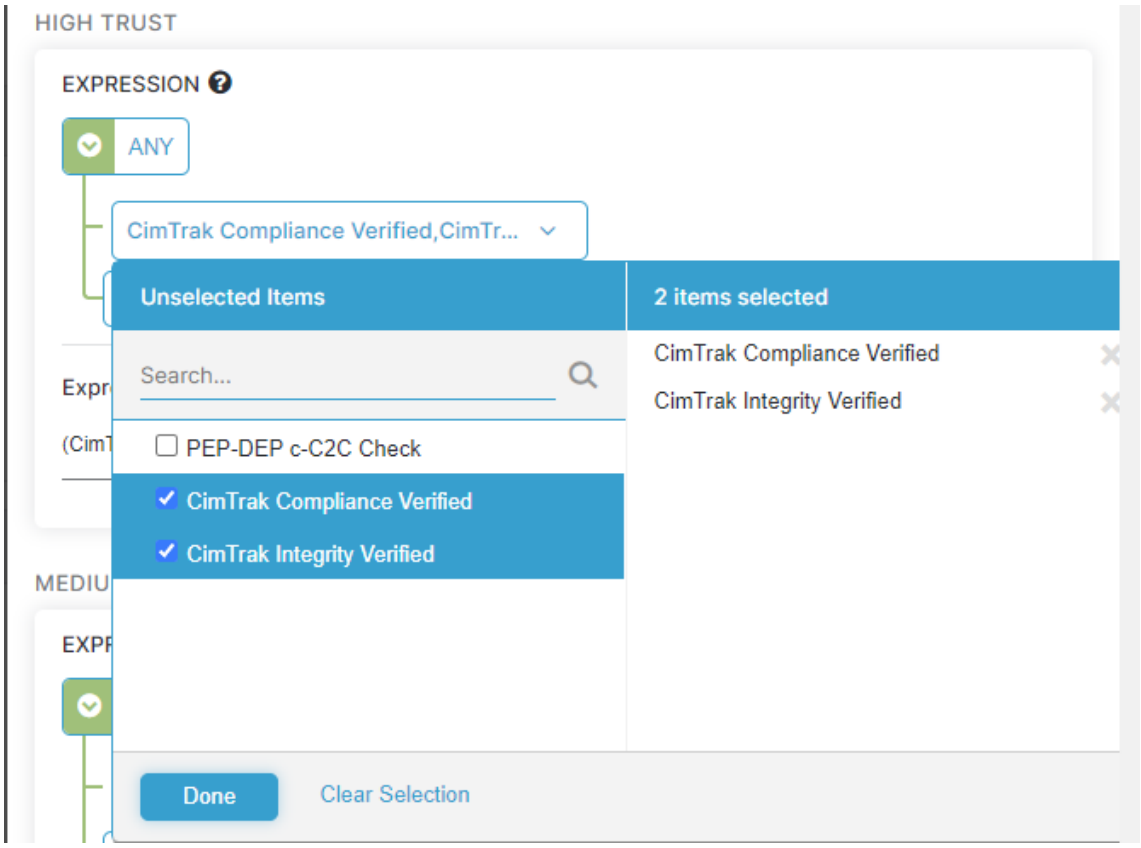

Figure 173. High Trust

5. For Medium Trust, click **Add** twice, once for each posture check changing the logic to OR.

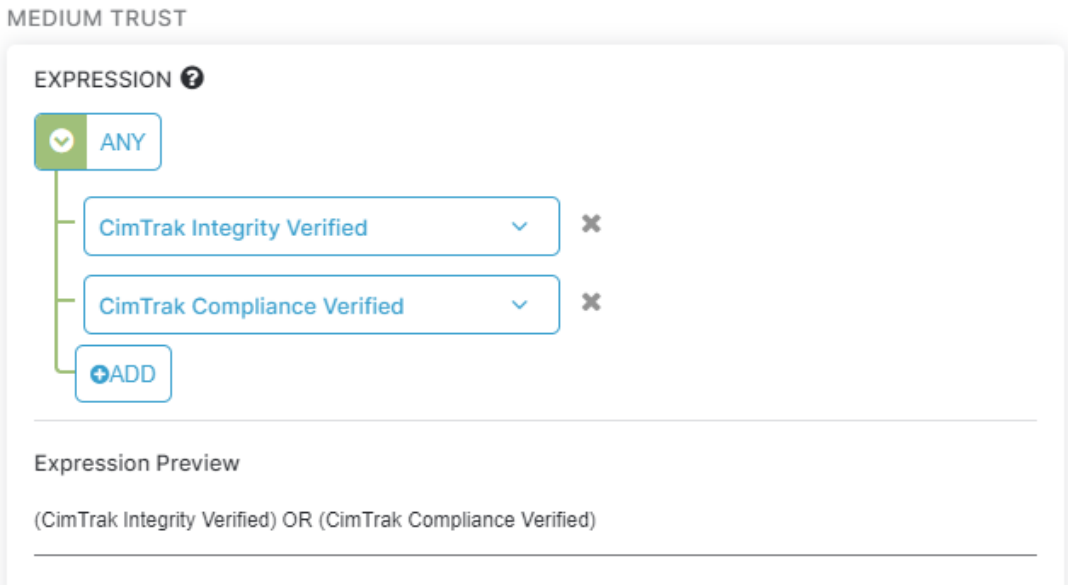

Figure 174. Medium Trust

6. For Low Trust click **Add** once, and then select both **CimTrak Compliance Violation** and **CimTrak Integrity Violation**.

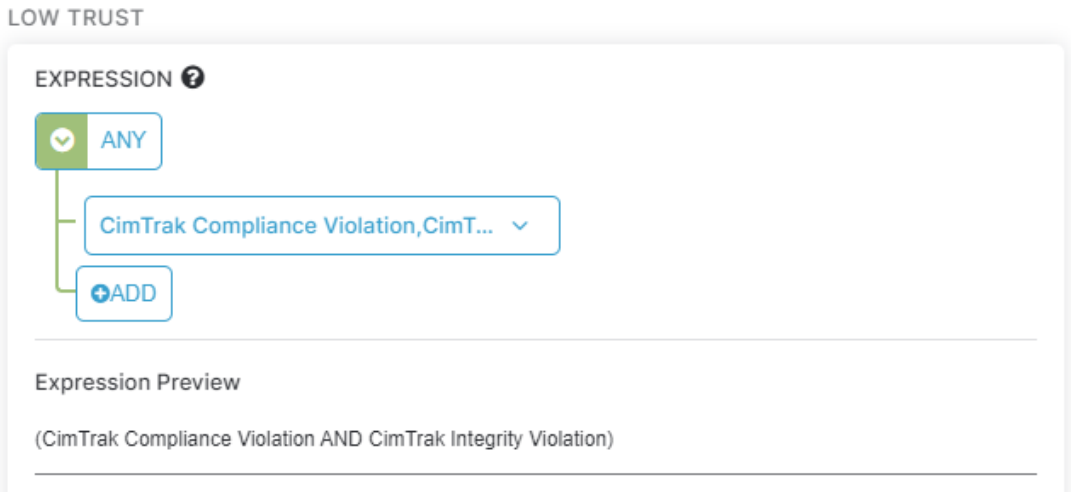

Figure 175. Low Trust

ZIA Isolation Profile

An Isolation profile must be configured to use an option to react to a CimTrak violation.

1. Go to the ZIA Admin Portal.
2. Go to **Administration** > **Browser Isolation**.

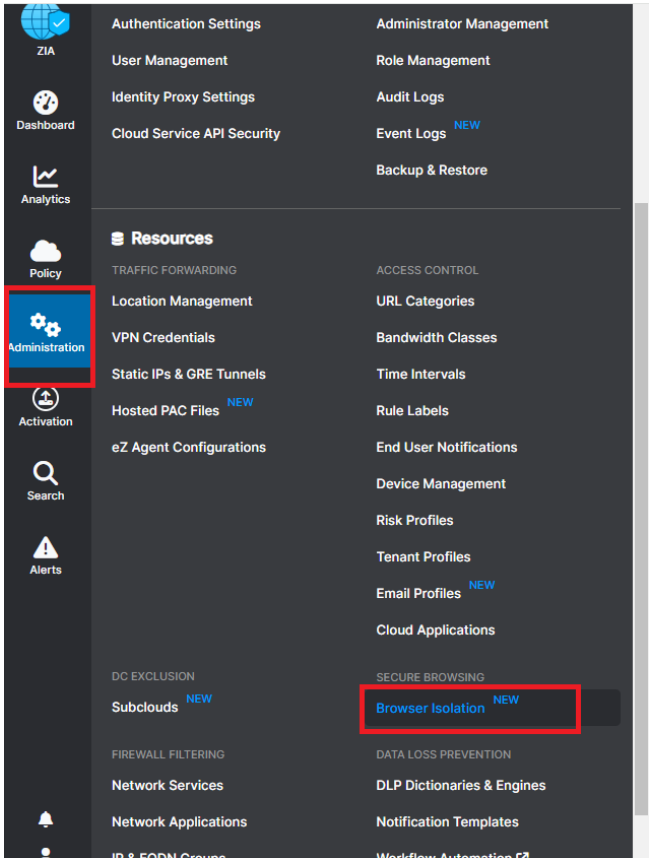

Figure 176. Browser Isolation

3. Click **Add Profile**.

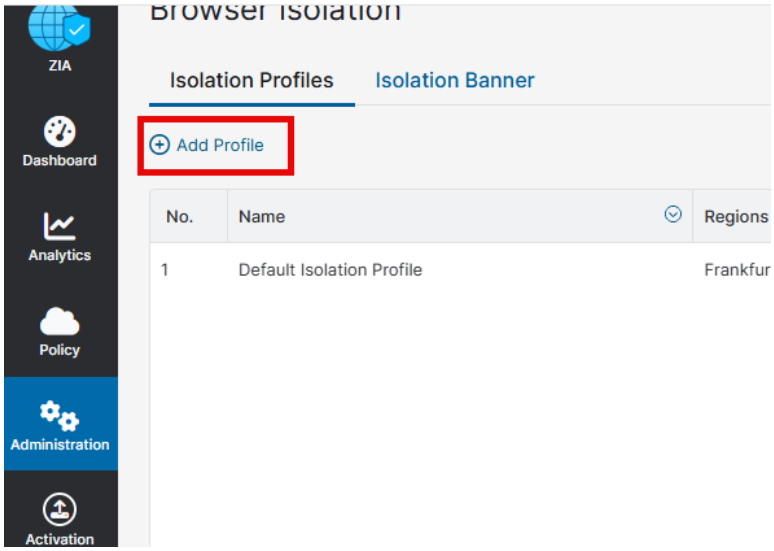

Figure 177. Add Profile

4. Enter a **Name** and **Description**.
5. Keep **Turbo Mode** disabled.
6. Click **Next**.

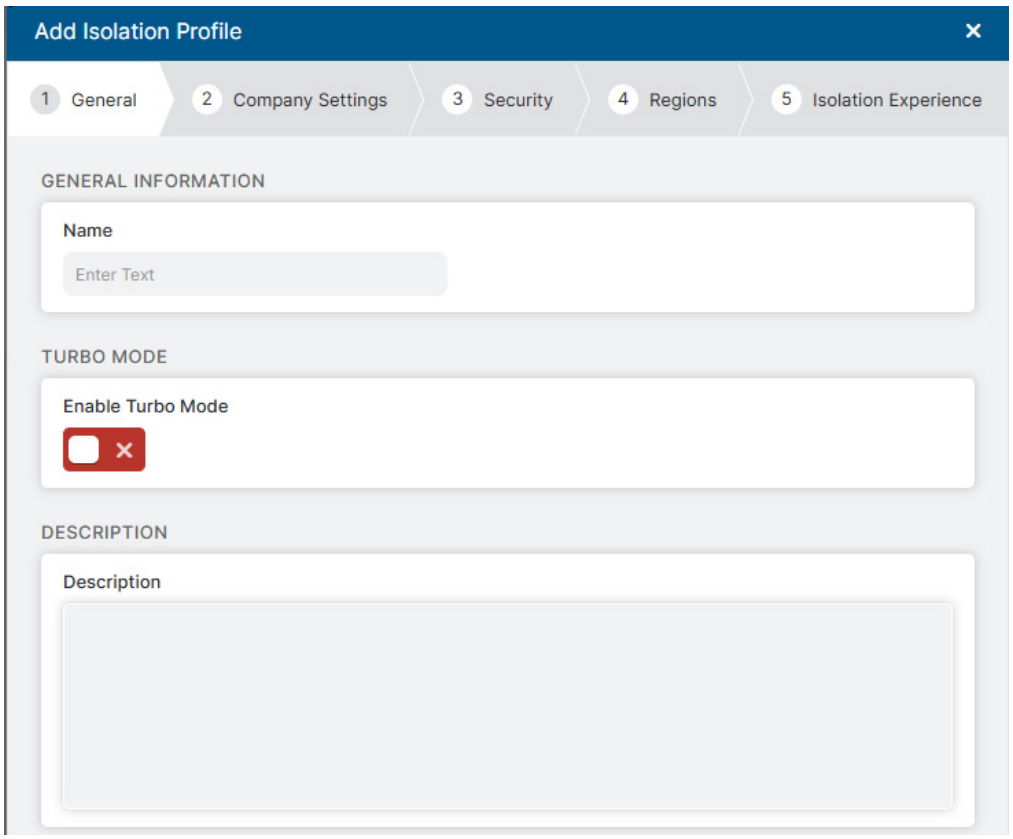

Figure 178. Add Isolation Profile

7. On the **Company Settings** tab, click **Next**.

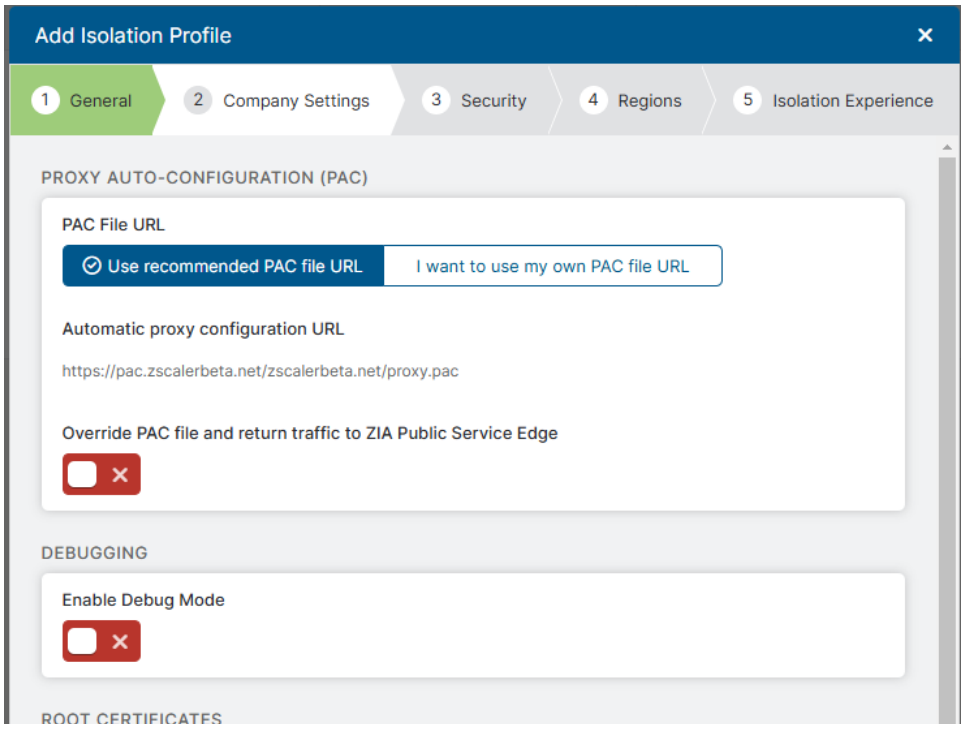

Figure 179. Company Settings

8. Under **Security**, enable **Read-Only Isolation**.
9. Click **Next**.

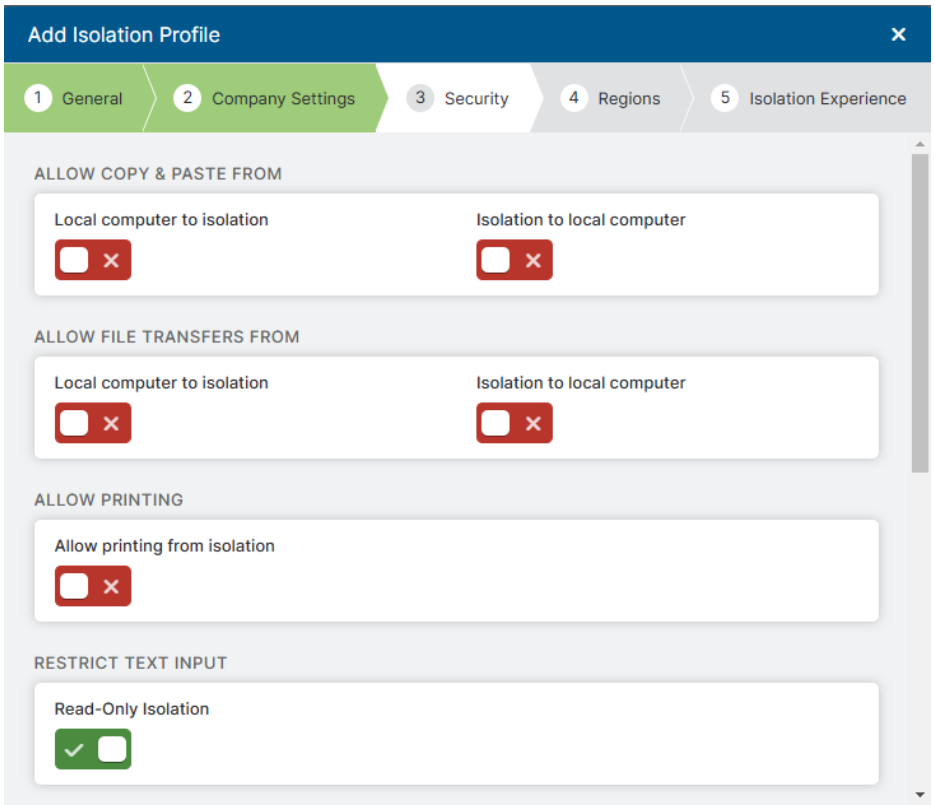

Figure 180. Security

10. Enable at least two **Regions** the isolation profile should be available in.

11. Click **Next**.

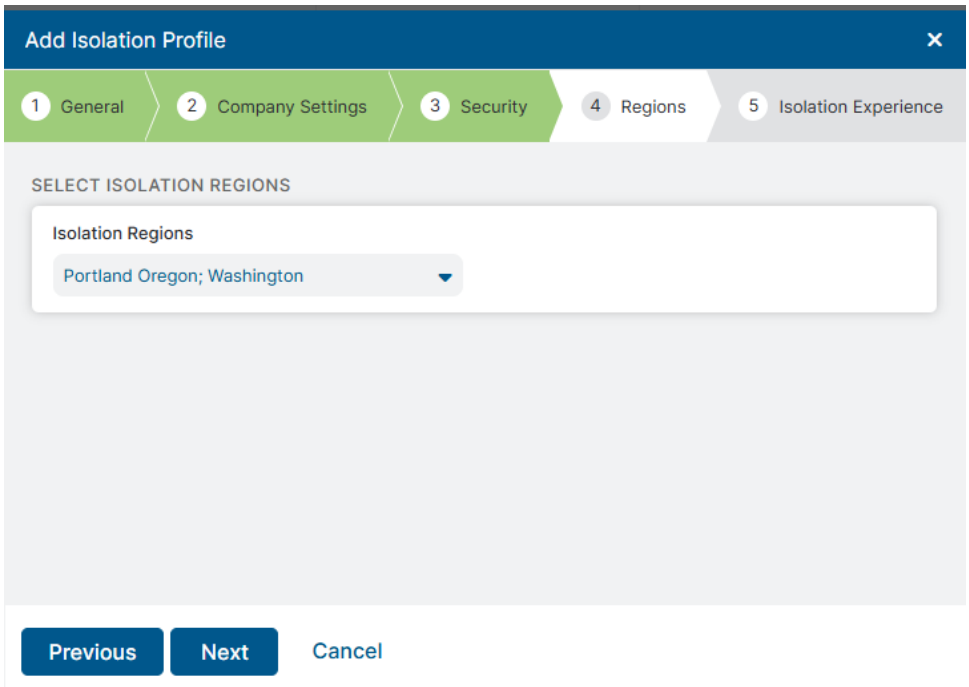

Figure 181. Regions

12. Select the **End User Notification** options for the end user's experience in isolation.
13. Click **Save**.

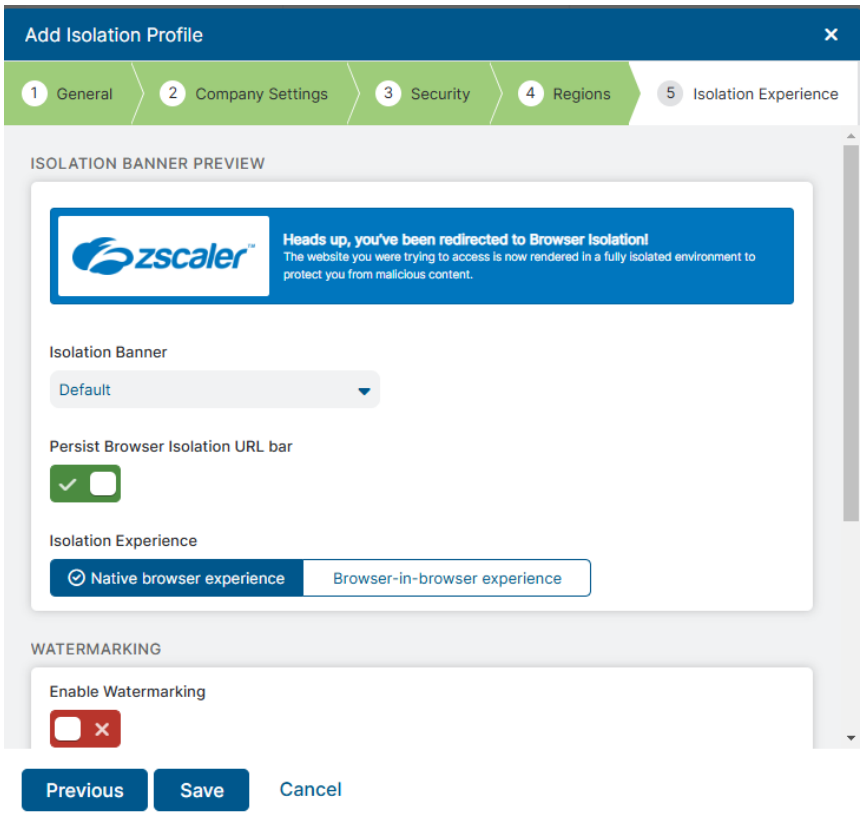

Figure 182. End User Notification

ZIA URL and Cloud App Control

To set up ZIA URL and Cloud App Control:

1. From the ZIA Admin Portal, go to **Access Control** > **URL & Cloud App Control**.

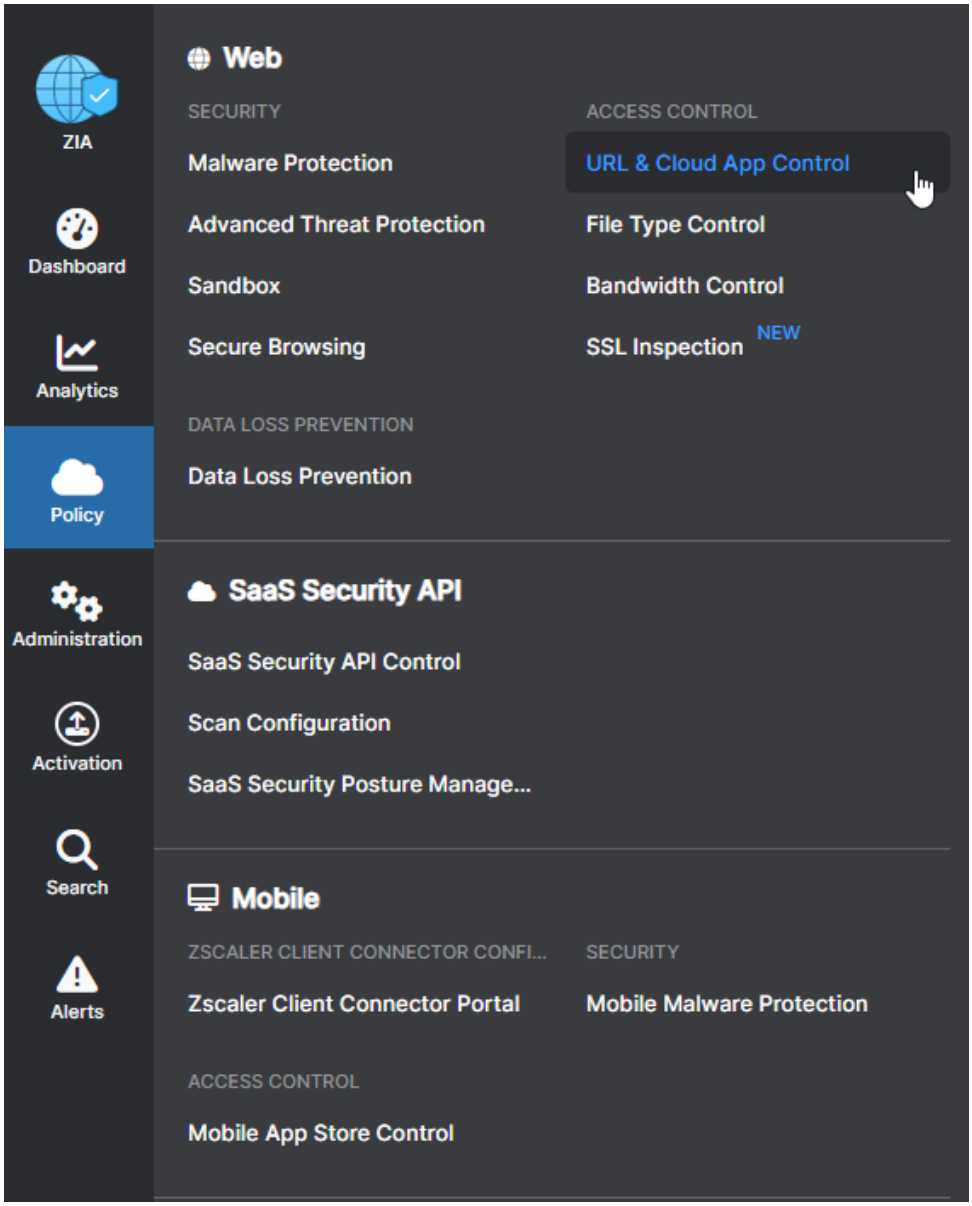

Figure 183. URL & Cloud App Control

2. Take advantage of those and create policies to automate security access:
   - If system is Low Trust (or Unknown), Block all network protocols.
   - If system is Medium Trust, set the Browser Isolate to Read Only mode for all HTTP/HTTPS.
   - If system is in High Trust, do nothing. It's in a good state of Integrity and Compliant.

When that the Posture Profiles are assigned to the appropriate Trust level, you can trigger off of those within the Cloud App Control Policies.

Create a Cloud App Control Policy for each Category. They should always be Rule Order 1 in most scenarios per Category. For each category you can do a Low Trust and Medium Trust rule, as follows:

> It doesn't matter if each category has different criteria, since the goal is to select any or all in every option, and to set the Device Trust Level to Low or Medium and the access to Block or Isolate.

For any category that uses User Agent, select ALL except Other.

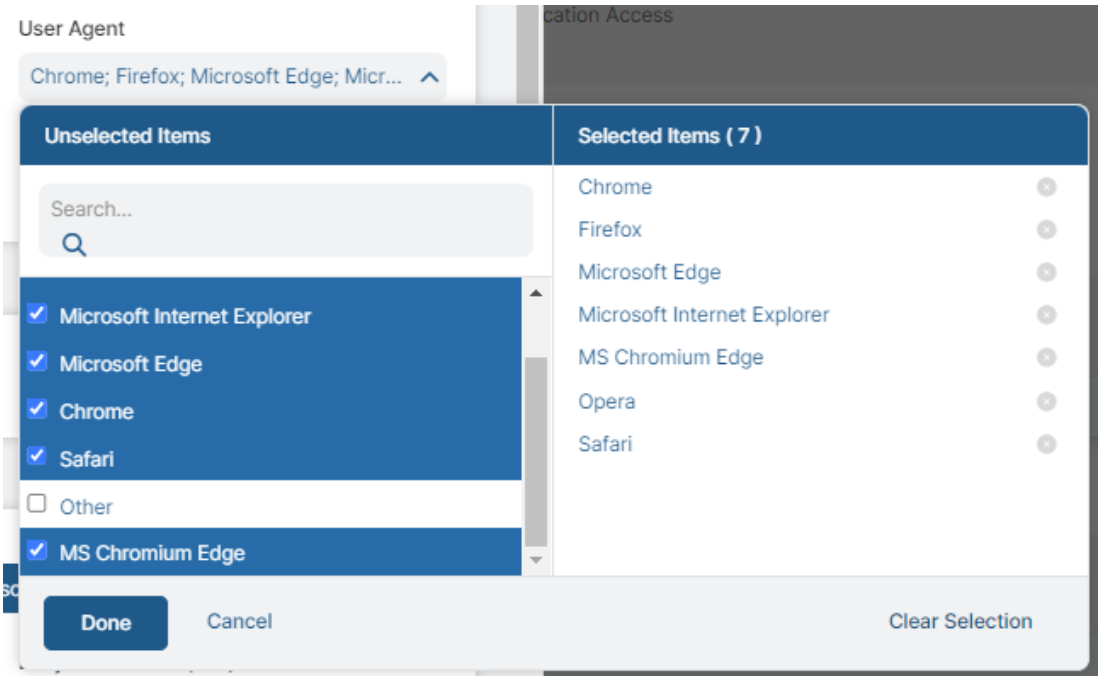

Figure 184. User Agent

You can see the configuration in the following figure.

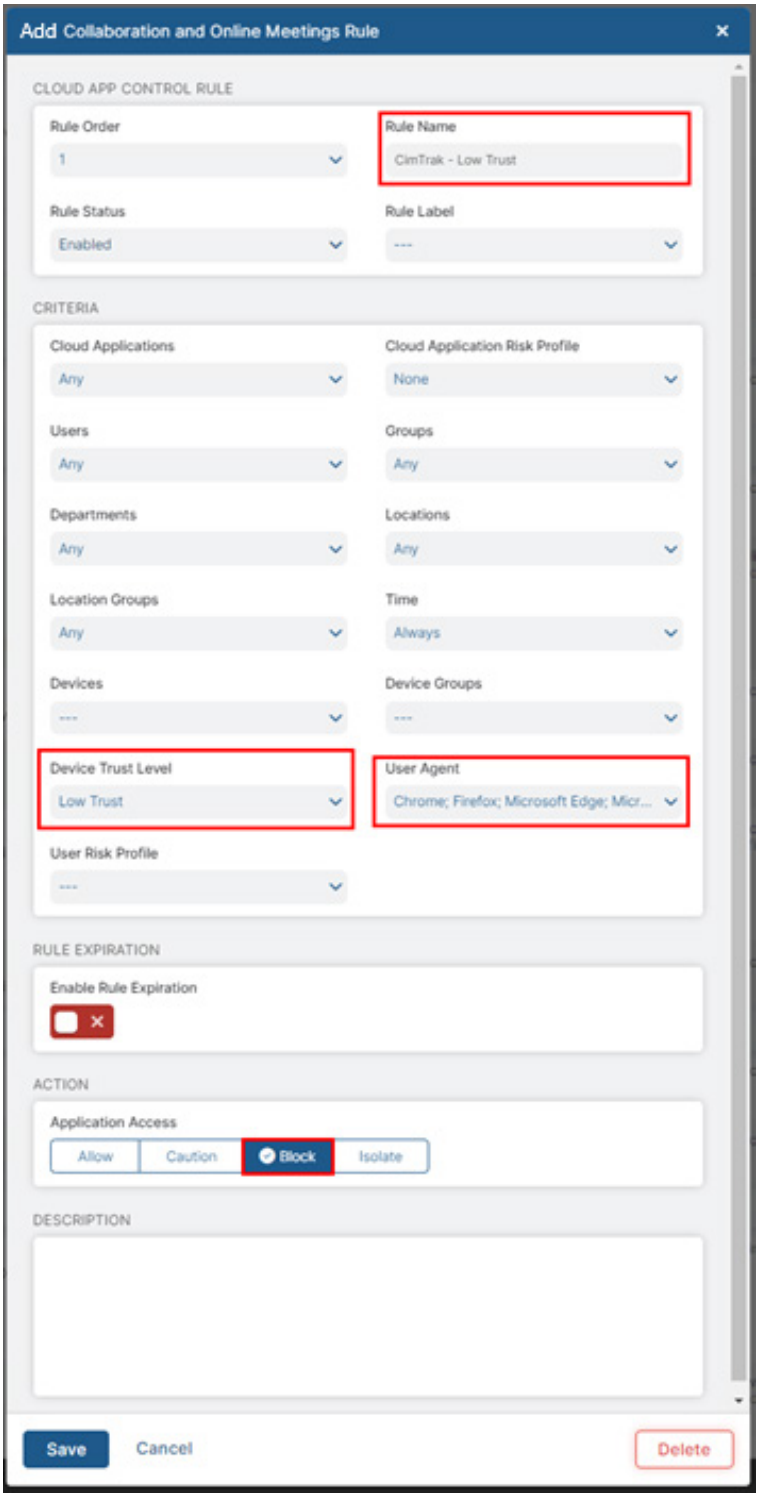

Figure 185. Add Collaboration and Online Meeting Rule

You can see the configuration in the following figure.

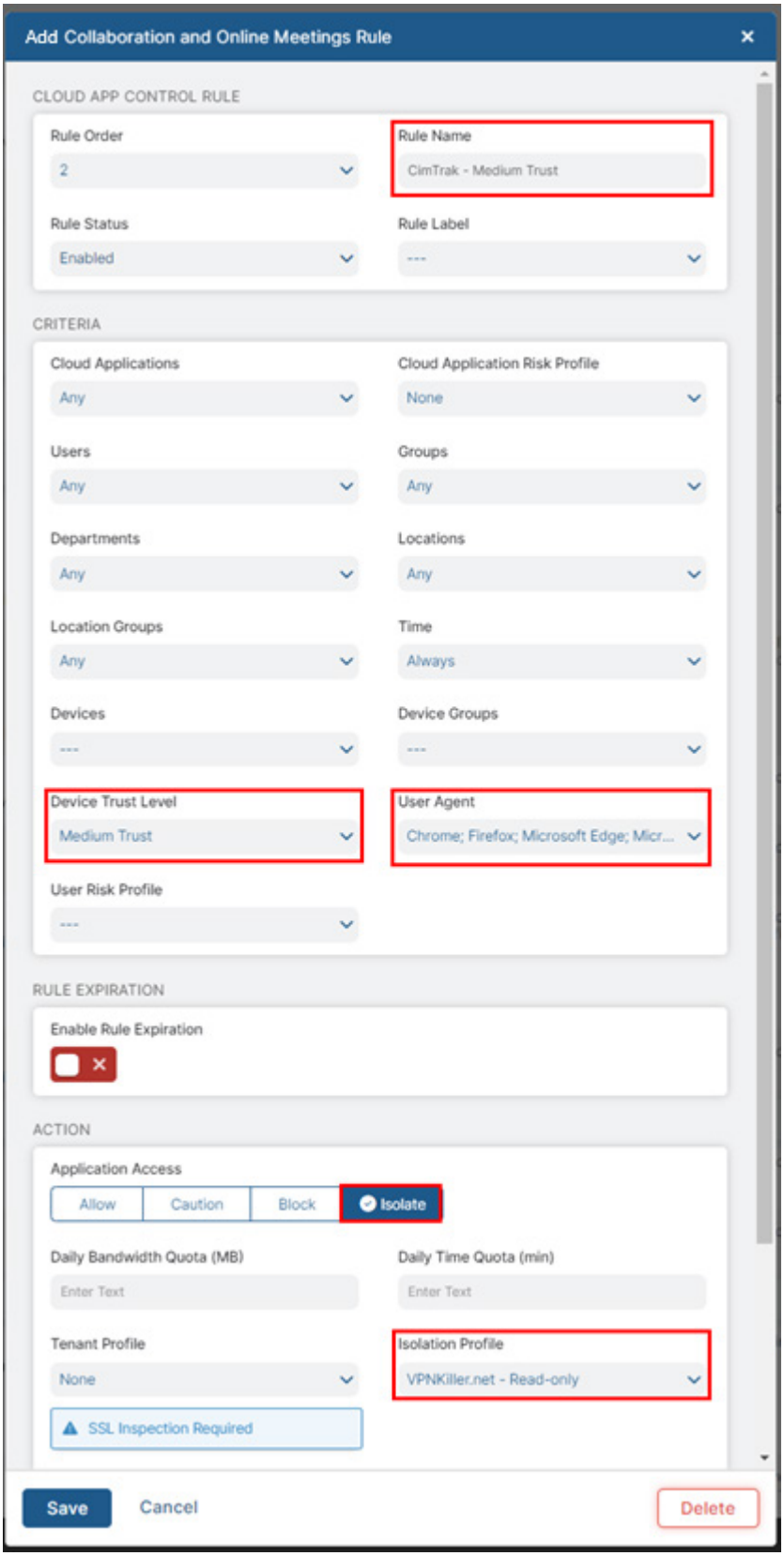

Figure 186. Add Collaboration and Online Meeting Rule

Log In to Zscaler Client Connector

On any endpoint where you want to enforce these rules:

1. Login to Zscaler Client Connector.

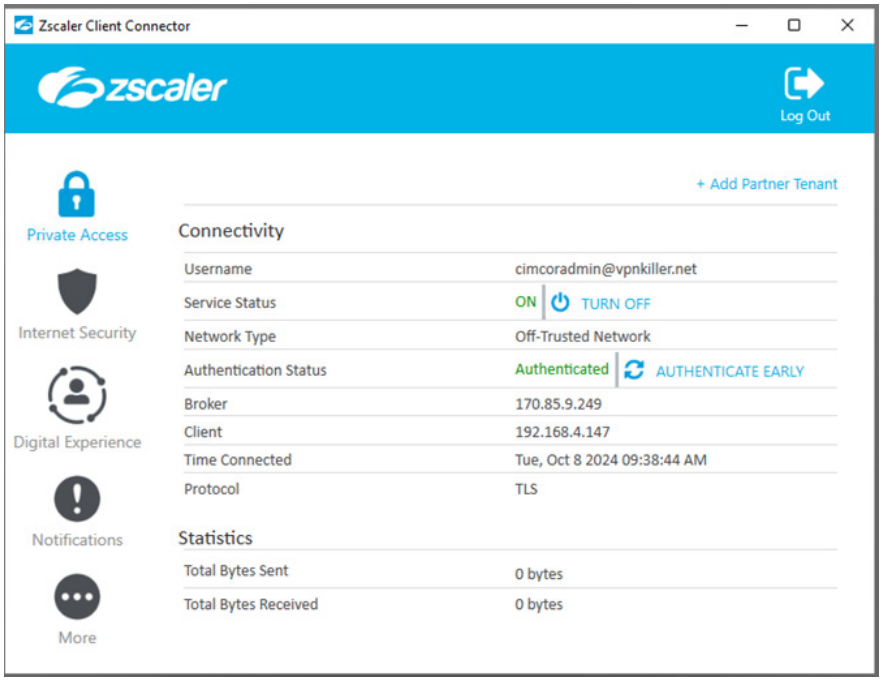

Figure 187. Zscaler Client Connector

2. Click **More**
3. In the **About** section, select **Update Policy**.

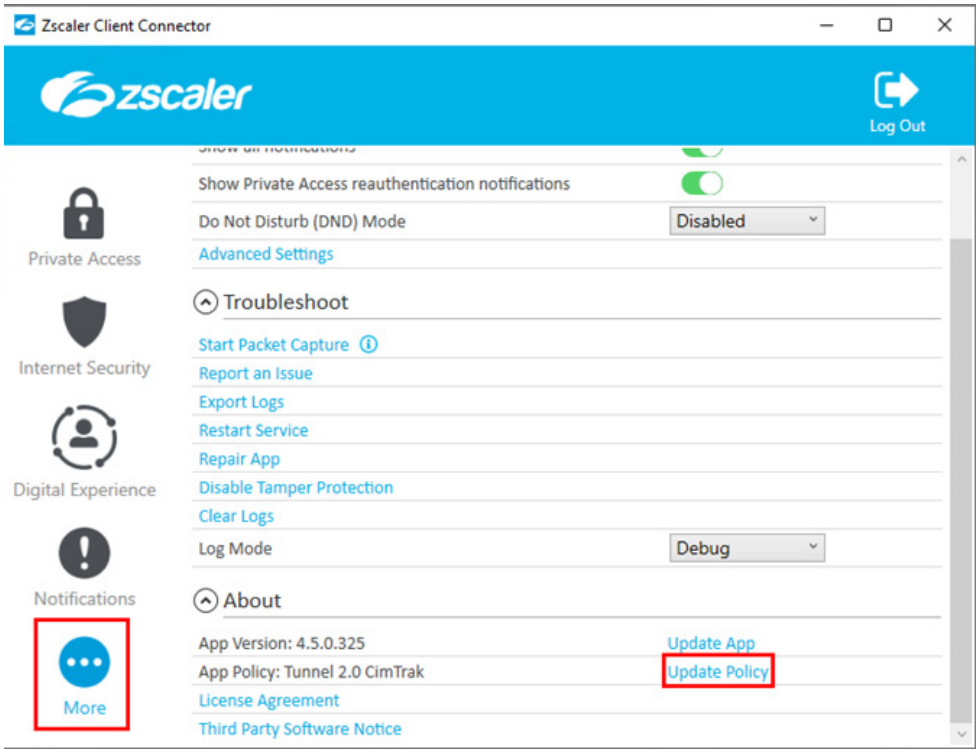

Figure 188. Update Policy

Enabling CimTrak Integrity Policy

After creating the policy, it must be monitored.

To enable the policy to start its monitoring intervals, right-click the policy name and select **Lock and Digitally Sign**. This starts an initial baseline and then monitors on the configured scheduled and reports on any deviations since this baseline.

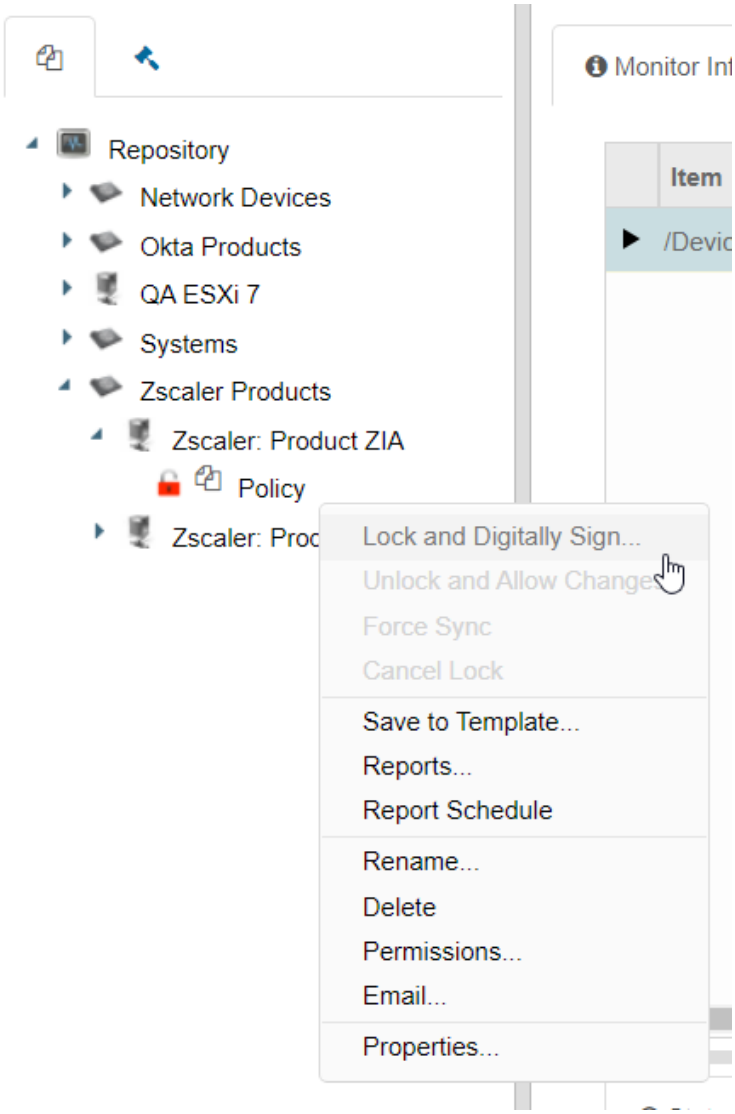

Figure 189. Lock and Digitally Sign

Testing the Integration

Test the integration. In this example, a policy was set up to monitor the directory C:\DEMO Policies\Test Folder. The trigger is CHANGE, which sets ZIA Device Posture to ACTIVE.

This is the current state of the directory:

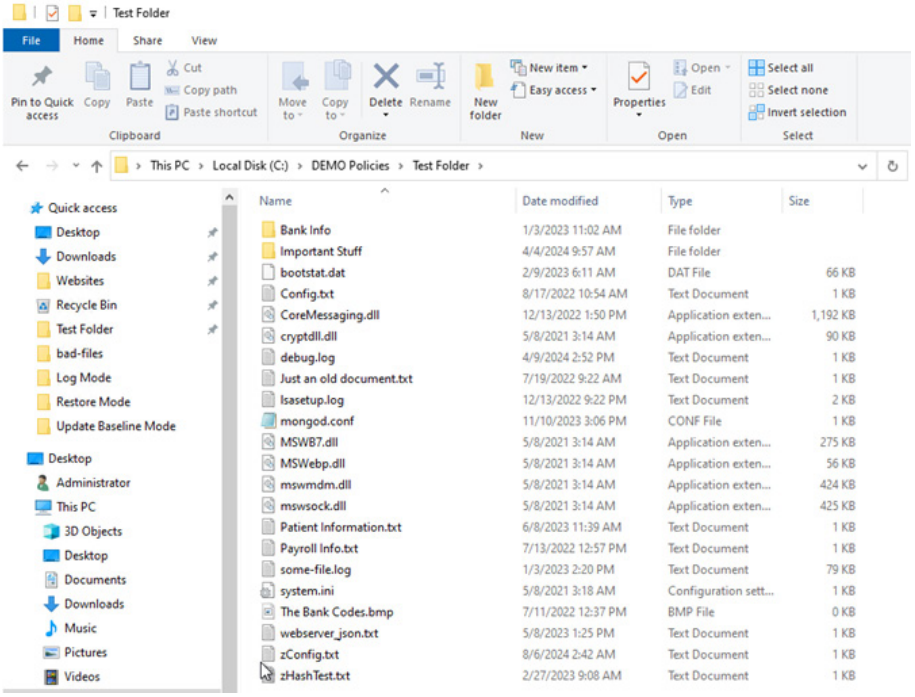

Figure 190. Current directory state

If a new file is added that does not match any hash in the CimTrak Authoritative Baseline, it triggers the access policy.

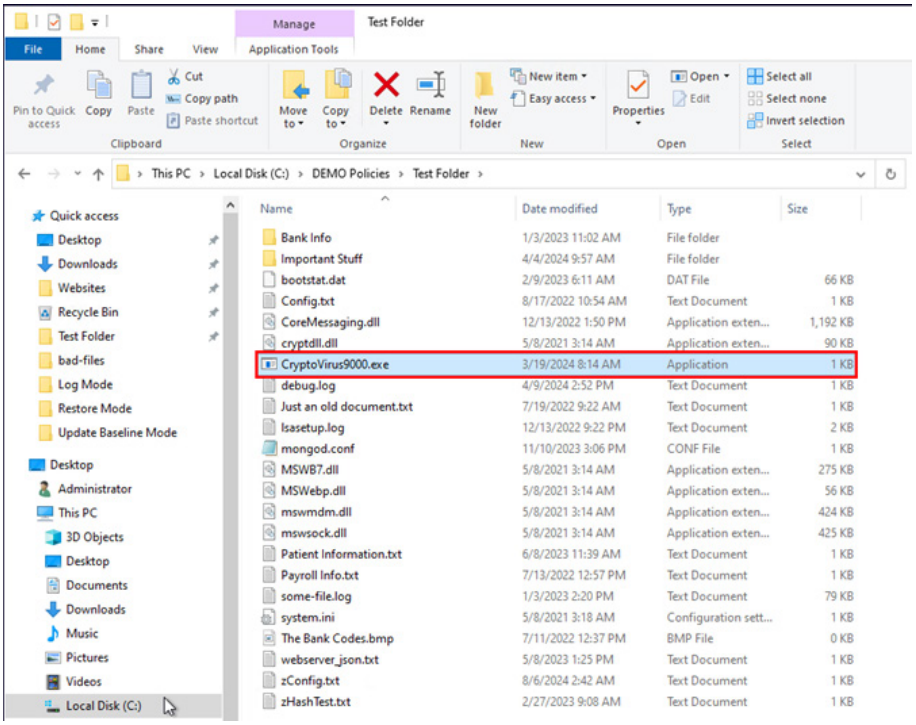

Figure 191. New file

Return to the CimTrak Web Console, and go to the Policy Event Log.

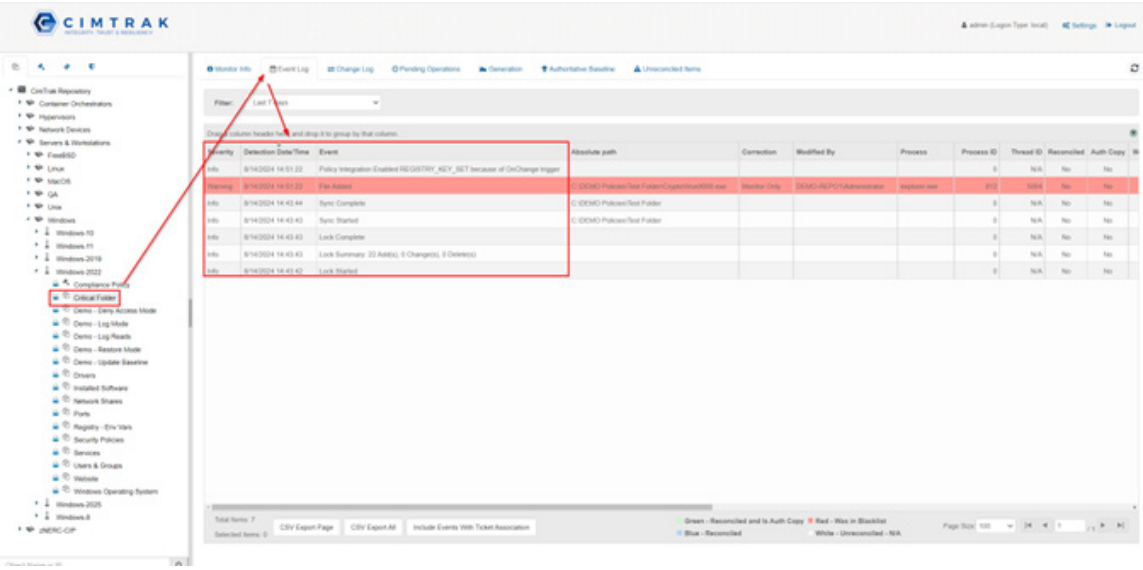

Figure 192. Policy Event log

In the Event Log, you can see that the new file was detected with other forensic details.

You can also see one second later the Registry Key Set was changed due to the new invalid state of Integrity.

Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event
Info	8/14/2024 14:51:23	Policy Integration Enabled REGISTRY_KEY_SET because of OnChange trigger
Warning	8/14/2024 14:51:22	File Added
Info	8/14/2024 14:43:44	Sync Complete
Info	8/14/2024 14:43:43	Sync Started
Info	8/14/2024 14:43:43	Lock Complete
Info	8/14/2024 14:43:43	Lock Summary: 22 Add(s), 0 Change(s), 0 Delete(s)
Info	8/14/2024 14:43:42	Lock Started

Figure 193. Changed registry key

ZIA isolates that system automatically based on this integrity violation detected by CimTrak in real time.

When Set to Block

ZIA blocks all the categories of external sources a user might try to access, based on where these rules are applied.

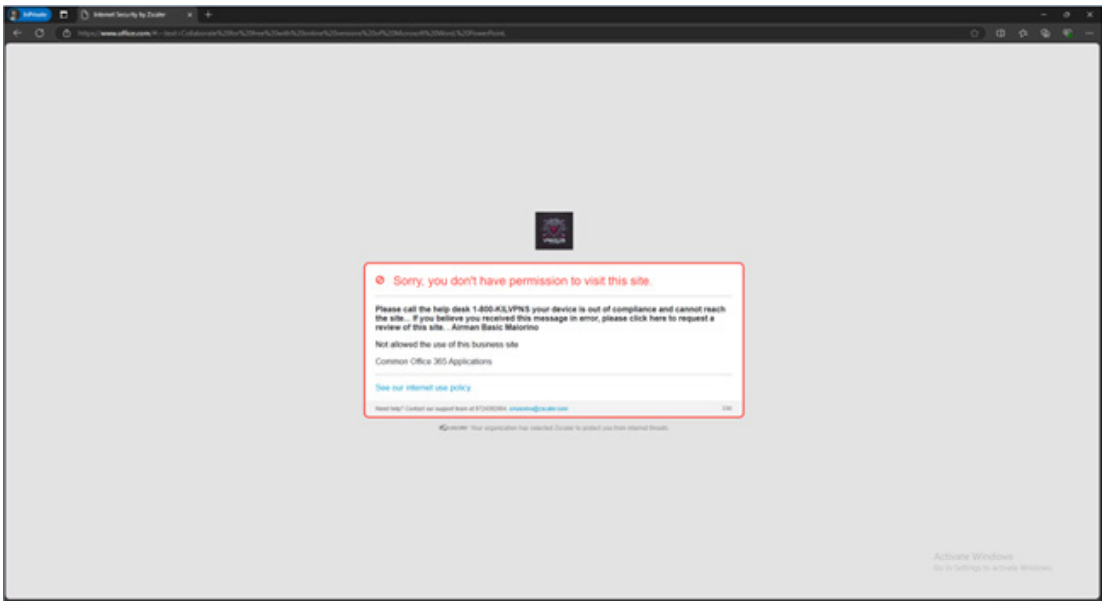

Figure 194. Set to Block

When Set to Isolate

ZIA isolates all the categories of external sources a user might try to access, based on where these rules are applied, and isolates that system automatically based on this Integrity violation detected by CimTrak in real time.

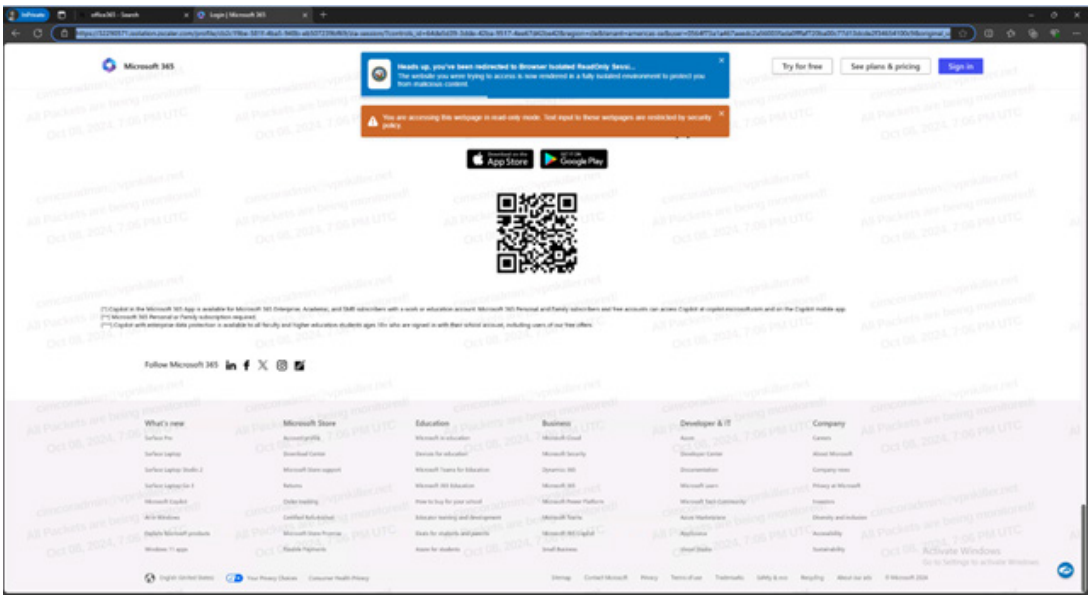

Figure 195. Set to Isolate

Resetting the Integration

Unlock the system (as it is back in a good state of integrity) by resetting the Policy Properties.

1. Right-click **Compliance Policy** and select **Properties**.

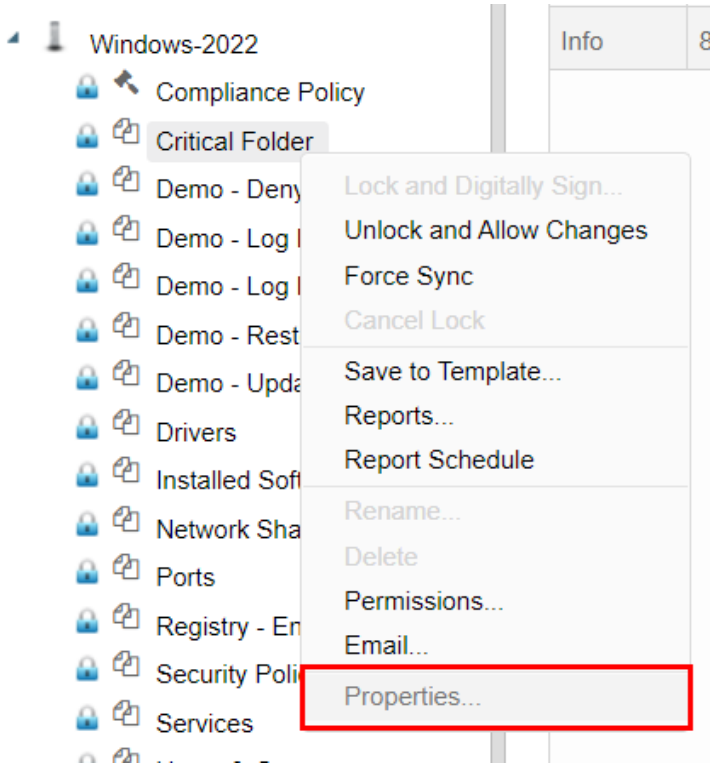

Figure 196. Properties

2. Click the **Integrations** tab and note the **Enforcement Status**. Click **Reset** to reset the Integrity State and disable ZIA Device Posture for this system.

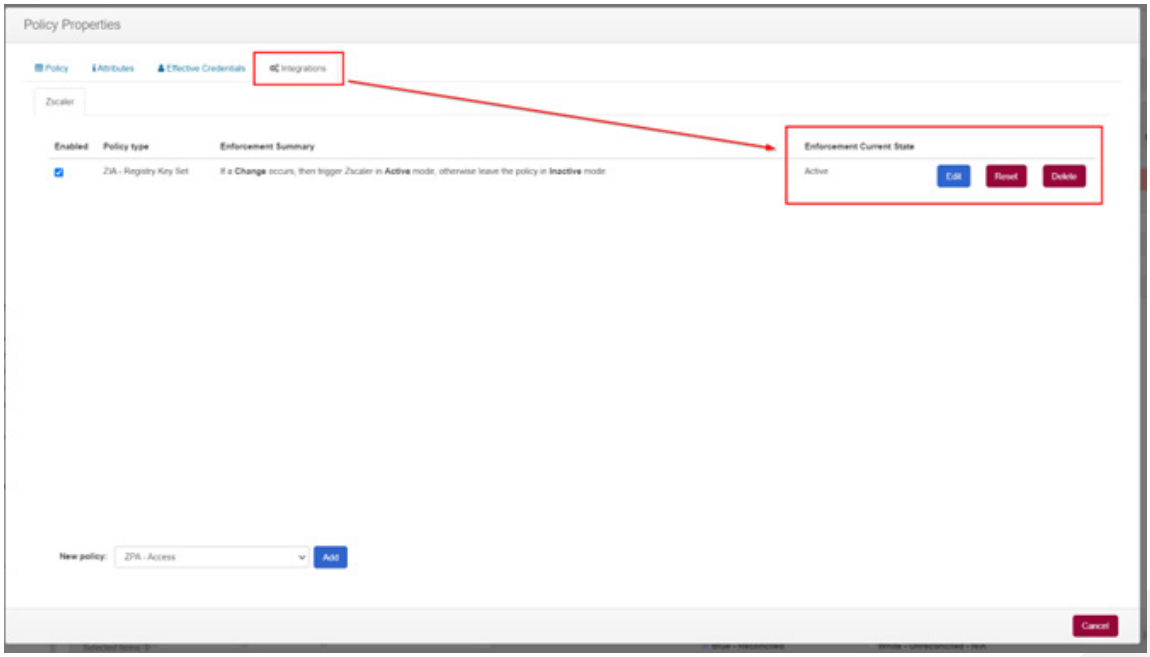

Figure 197. Integrations tab

ZIA Compliance Triggers

The next sections describe ZIA compliance triggers.

Log In to Your CimTrak Console

Go to your CimTrak Web Console in your environment and log in as a CimTrak Administrator. For example:

- `https://CimTrak-Server/cmc`
- `https://192.168.4.15/cmc`

Figure 198. CimTrak Web Console

Creating CimTrak Compliance Policy

In the left-side **Tree View**, find the system in question for which you want to create a policy.

1. Right-click the <agent name> and select **New** > **Policy**.

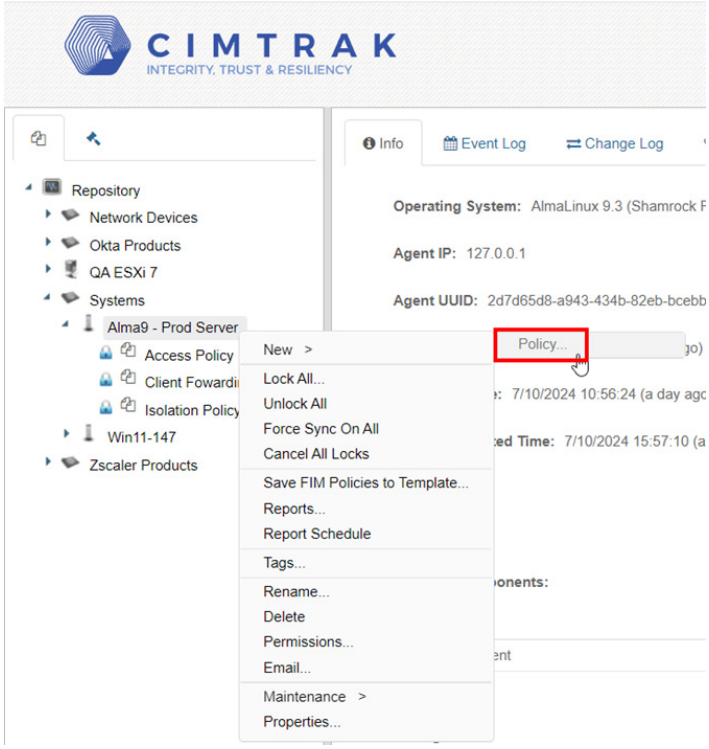

Figure 199. Policy

2. Click **Compliance**.

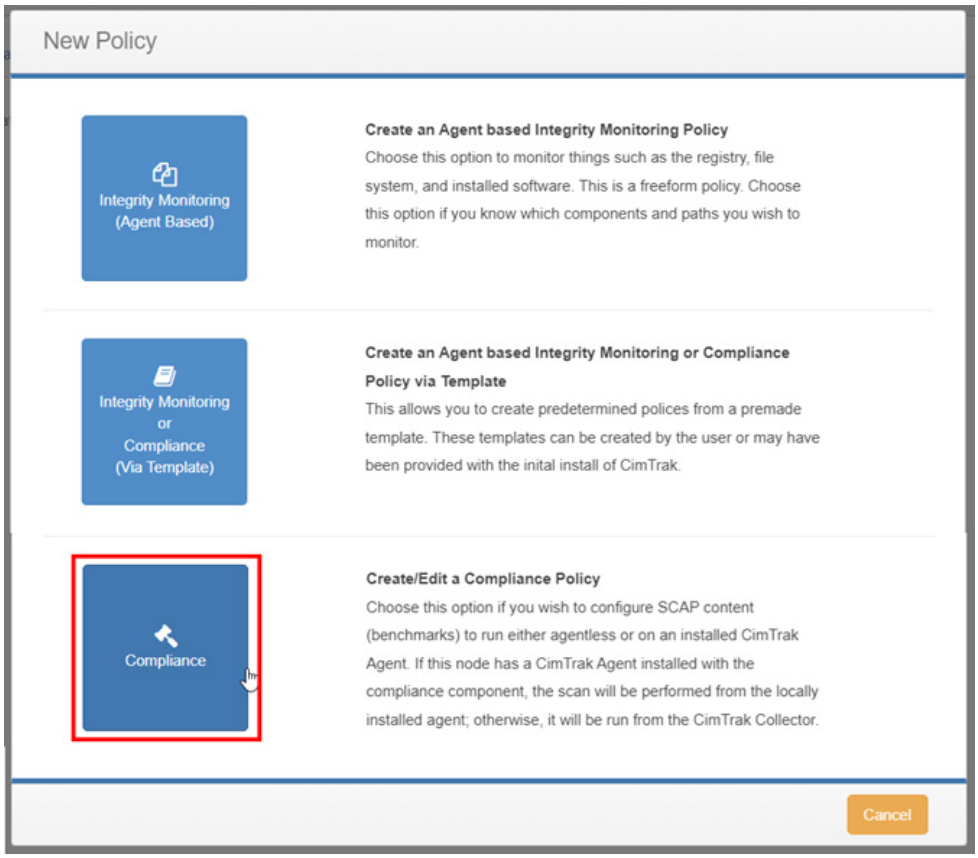

Figure 200. Compliance

3. Expand the **Mappings** node.

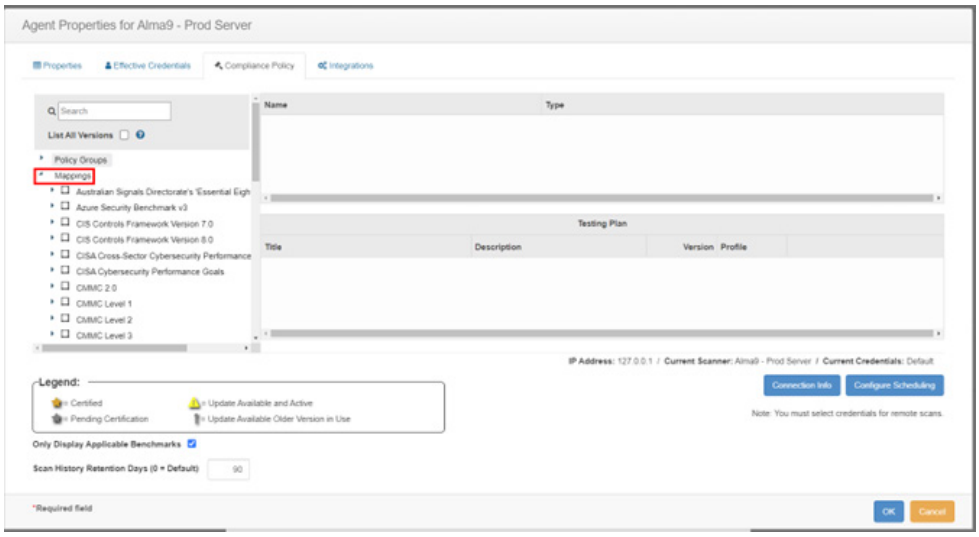

Figure 201. Mappings node

4. Select any **Compliance Frameworks** you are tracking on this system. It automatically chooses the CIS Benchmark you must run to track that Compliance Framework. You can choose multiple if required.
5. Click **Please Select Profile**.

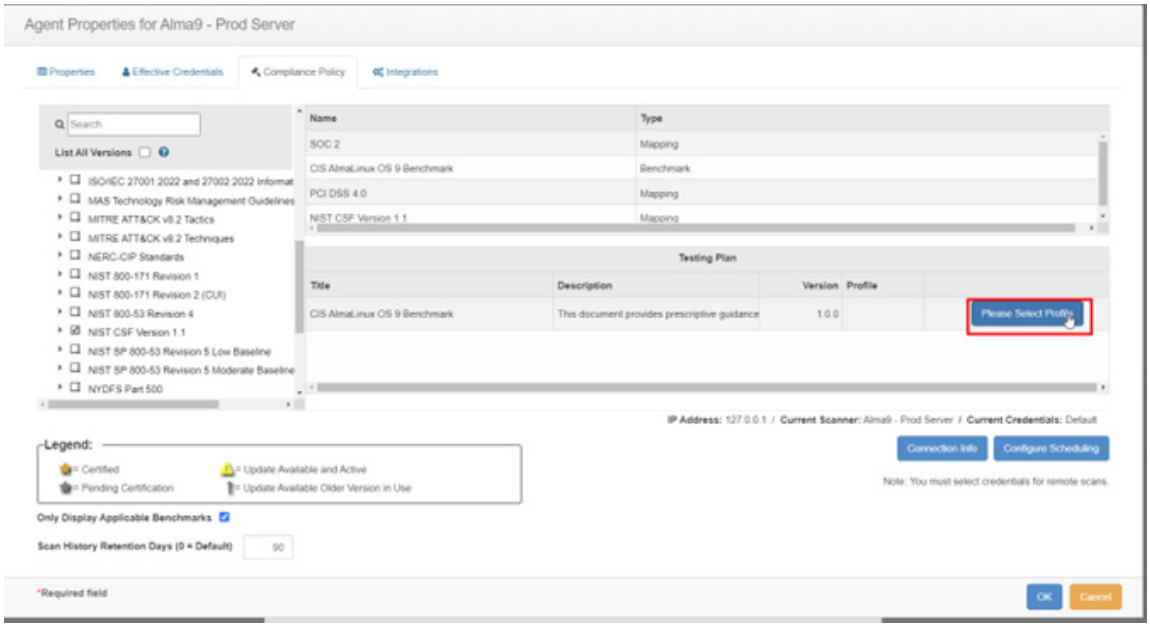

Figure 202. Compliance Framework

6. Select the **Profile** for the benchmark that is applicable for the system (i.e., **Workstation**/**Server**/**Domain Controller**).

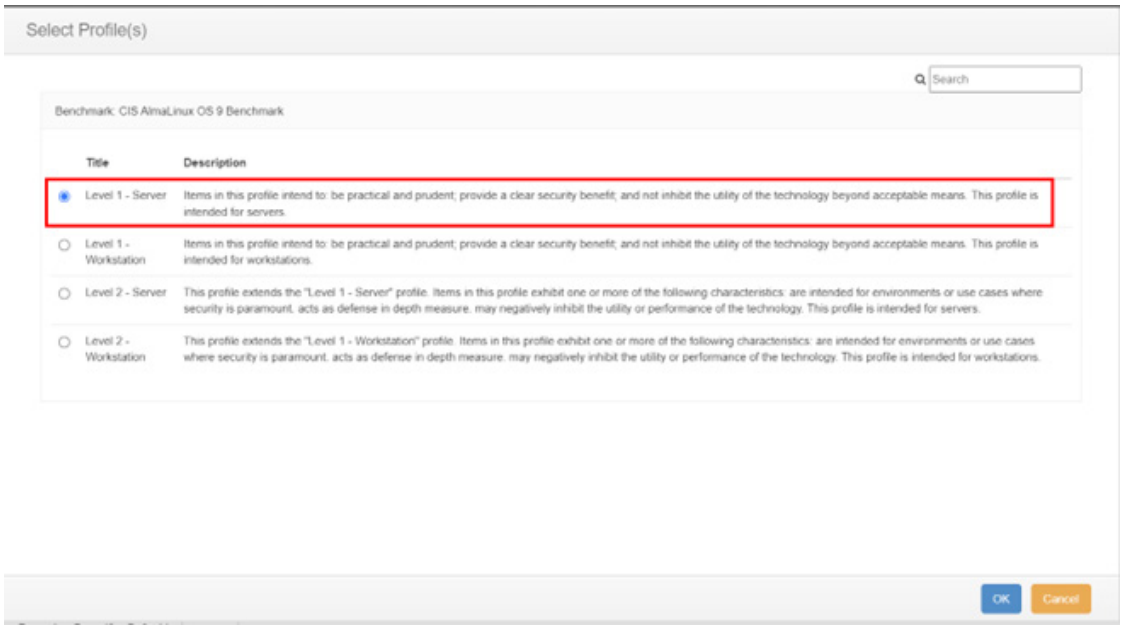

Figure 203. Select profile

7. Configure the schedule by selecting **Configure Scheduling**.

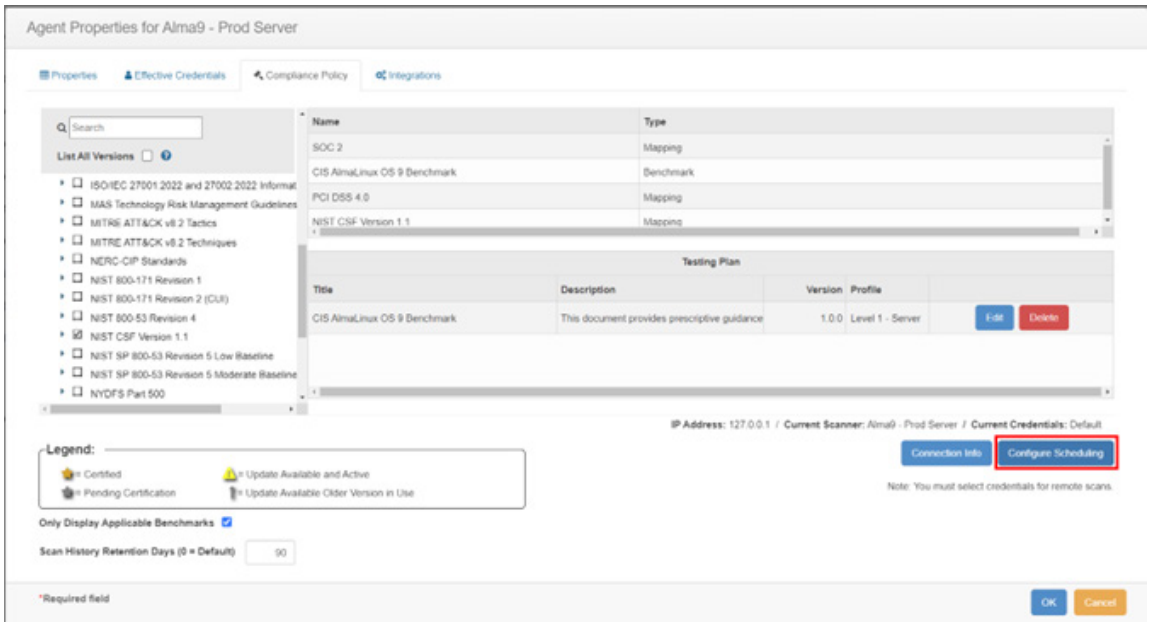

Figure 204. Configure Scheduling

8. Select what you want CimTrak to run the benchmark scans. The default is **Every Day at Midnight Server Time**.

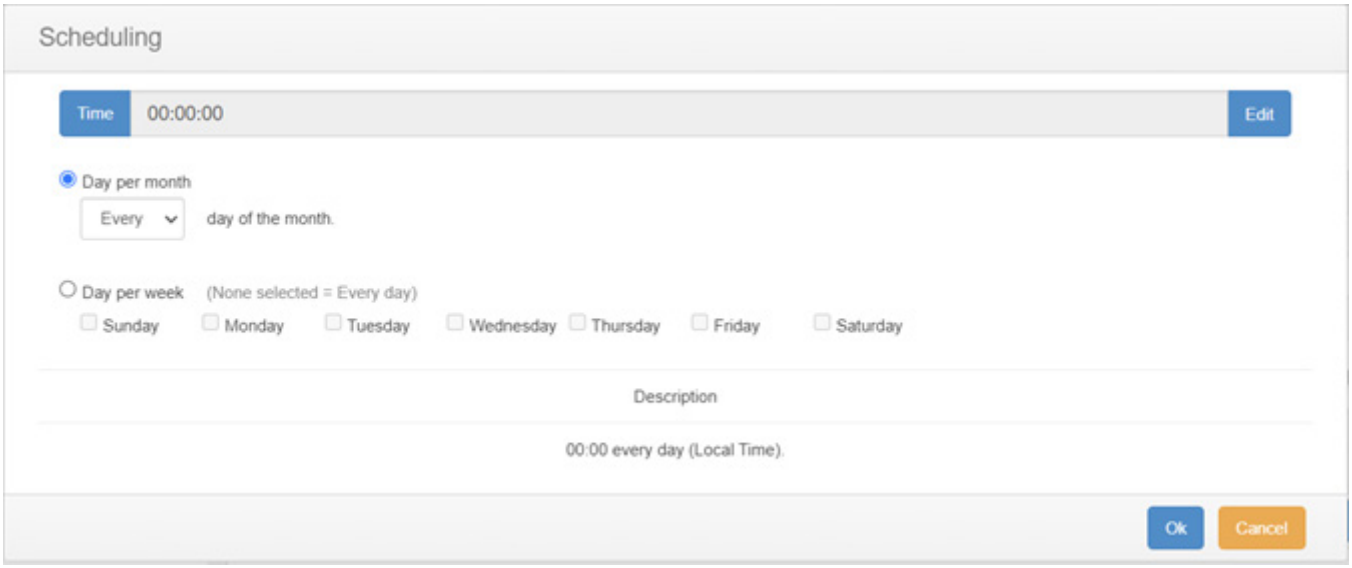

Figure 205. Select time

Configuring Zscaler Integration

To configure the Zscaler integration:

1. Click the **Integration** tab.

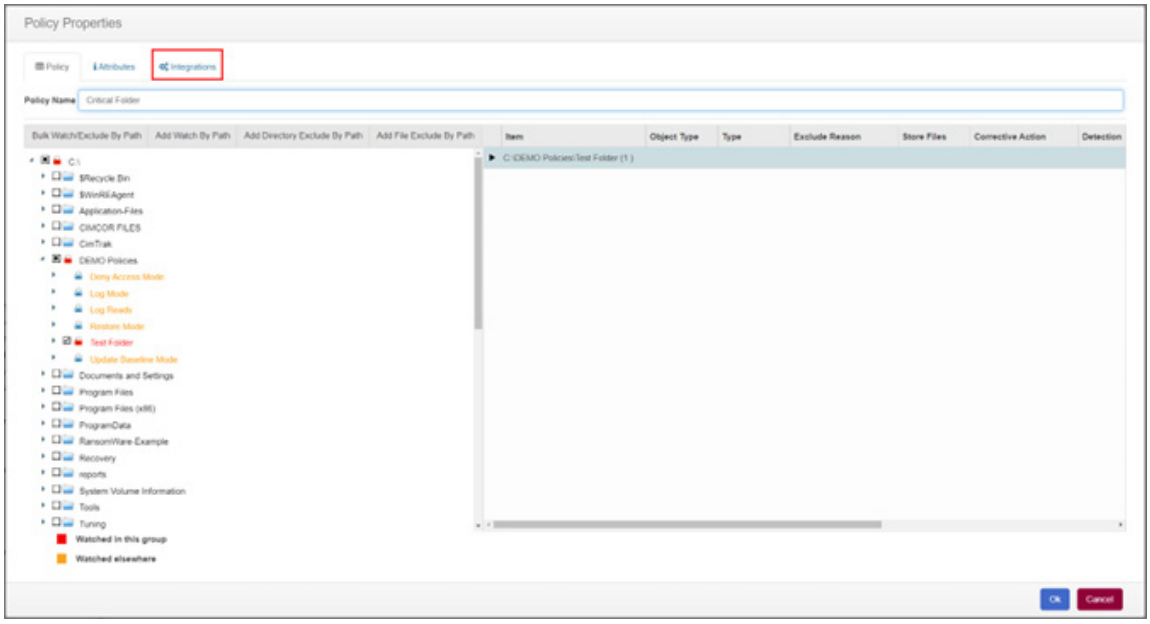

Figure 206. Integration tab

2. Choose **ZIA – Registry Key Set** and click **Add**.

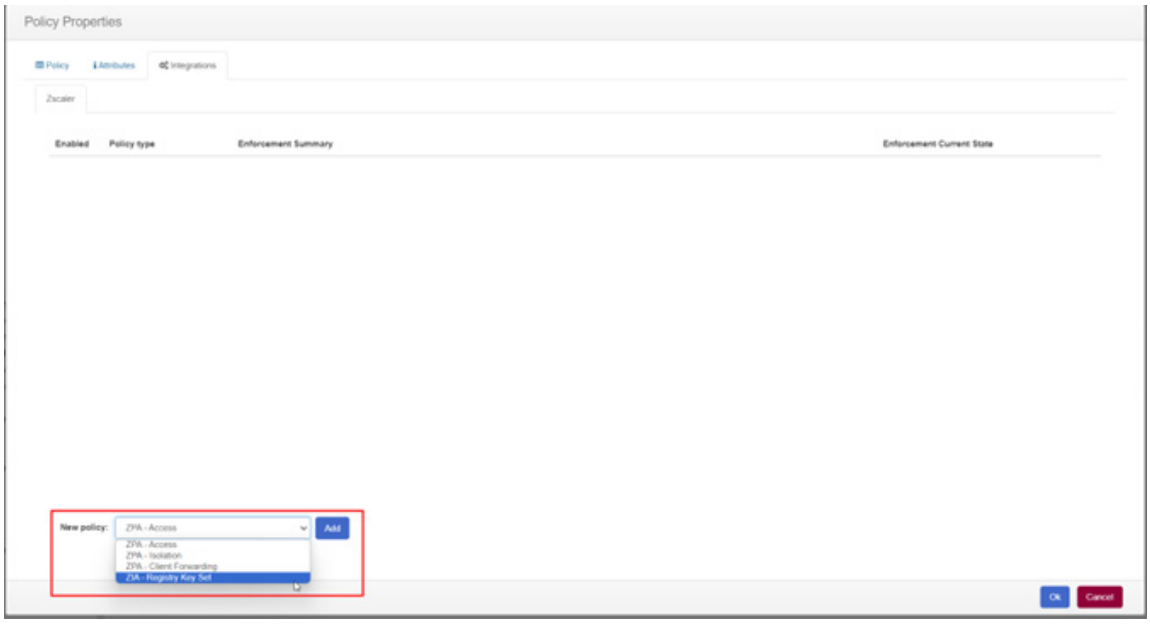

Figure 207. ZIA – Registry Key Set

3. Configure how you want this integration to interact with your policy.

Figure 208. Set Policy

This is a logic statement that you can easily configure and change with a drop-down menu, as follows:

If an <INTEGRITY TRIGGER> occurs, then trigger Zscaler in Active mode, otherwise leave the policy in Inactive mode.

These variables are defined as follows:

- I**NTEGRITY TRIGGERS**: These are the CimTrak Integrity options to trigger the policy you configure.
  - **Change**: If any change that deviates the baseline.
  - **Denied List Item Found**: If any change was a matching hash in the CimTrak Deny List (denylist).
  - **Not in allowed list**: If any change was NOT a matching hash in the CimTrak Allow List (allowlist).

Integrating with ZIA Device Posture

Use the CimTrak Agent to automatically create and manage a Registry Key to represent the Integrity and Compliance states. These values are then tracked via ZIA Device Postures to isolate machines based on the CimTrak states provided. These keys are automatically created and changed based on the state of Integrity and Compliance it detects when the policies are locked.

Registry Key Path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cimcor\CimTrak\CimTrakAgent
```

ZIA DWORD Values:

- **Agent Running**: Either 0 or 1 (0 = shutdown 1 = started)
- **Configuration Assessment Score**: Either 0 or 1 (0 = compliant, 1 = noncompliant)
- **Integrity Score**: Either 0 or 1 (0 = no violations, 1 = integrity violation)

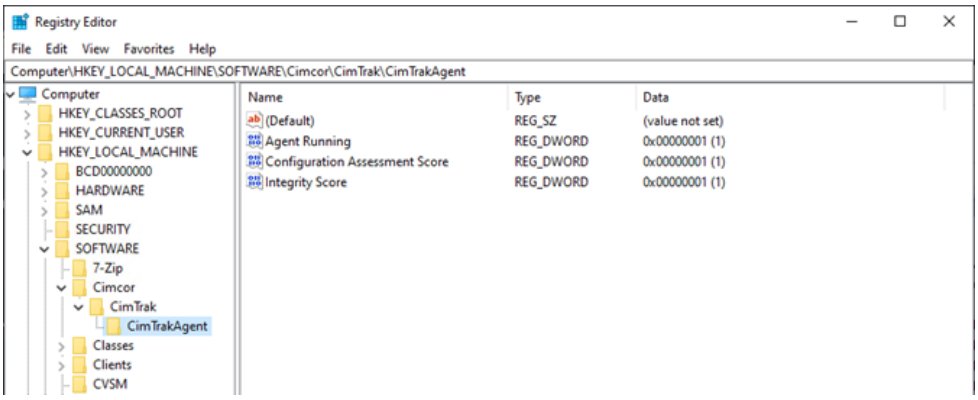

Figure 209. Registry Editor

ZIA Device Postures

To configure ZIA device postures:

1. From the Zscaler Client Connector Portal, go to **Administration** > **Device Posture Dashboard**.
2. Click **Add Device Posture**.

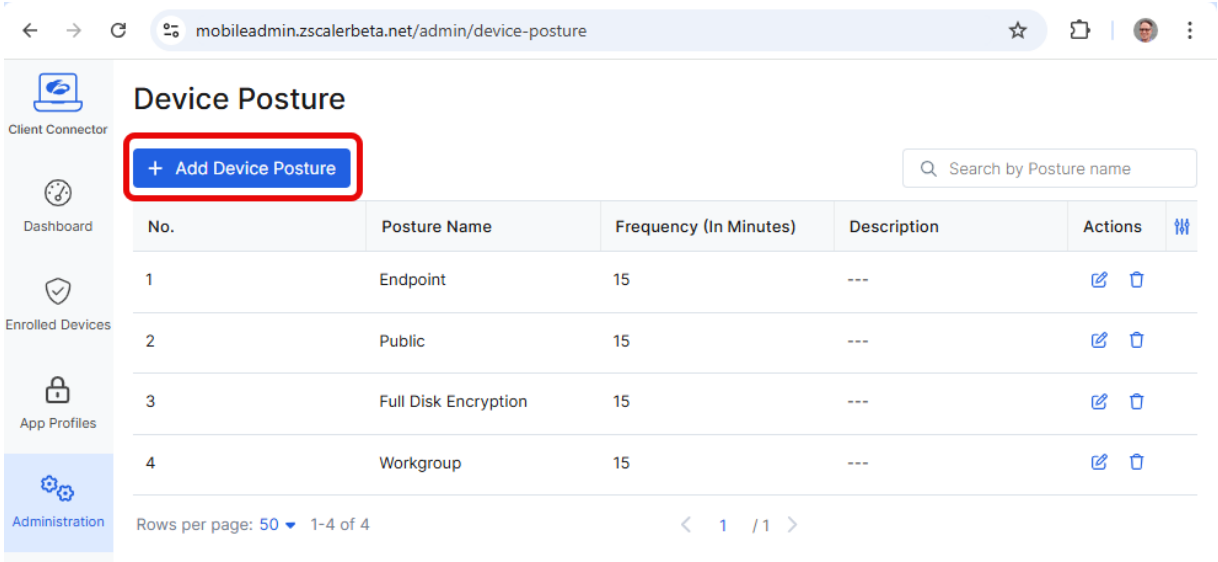

Figure 210. Add Device Posture

3. Create a Posture for the Integrity Registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cimcor\CimTrak\CimTrakAgent\Configuration Assessment Score`

   Create a Device Posture Check for each state (1 and 0). This example uses the following nomenclature, but you can customize to your needs:

   - CimTrak Integrity Verified – GOOD state – Registry key value of 0
   - CimTrak Integrity Violation – BAD state - Registry key value of 1

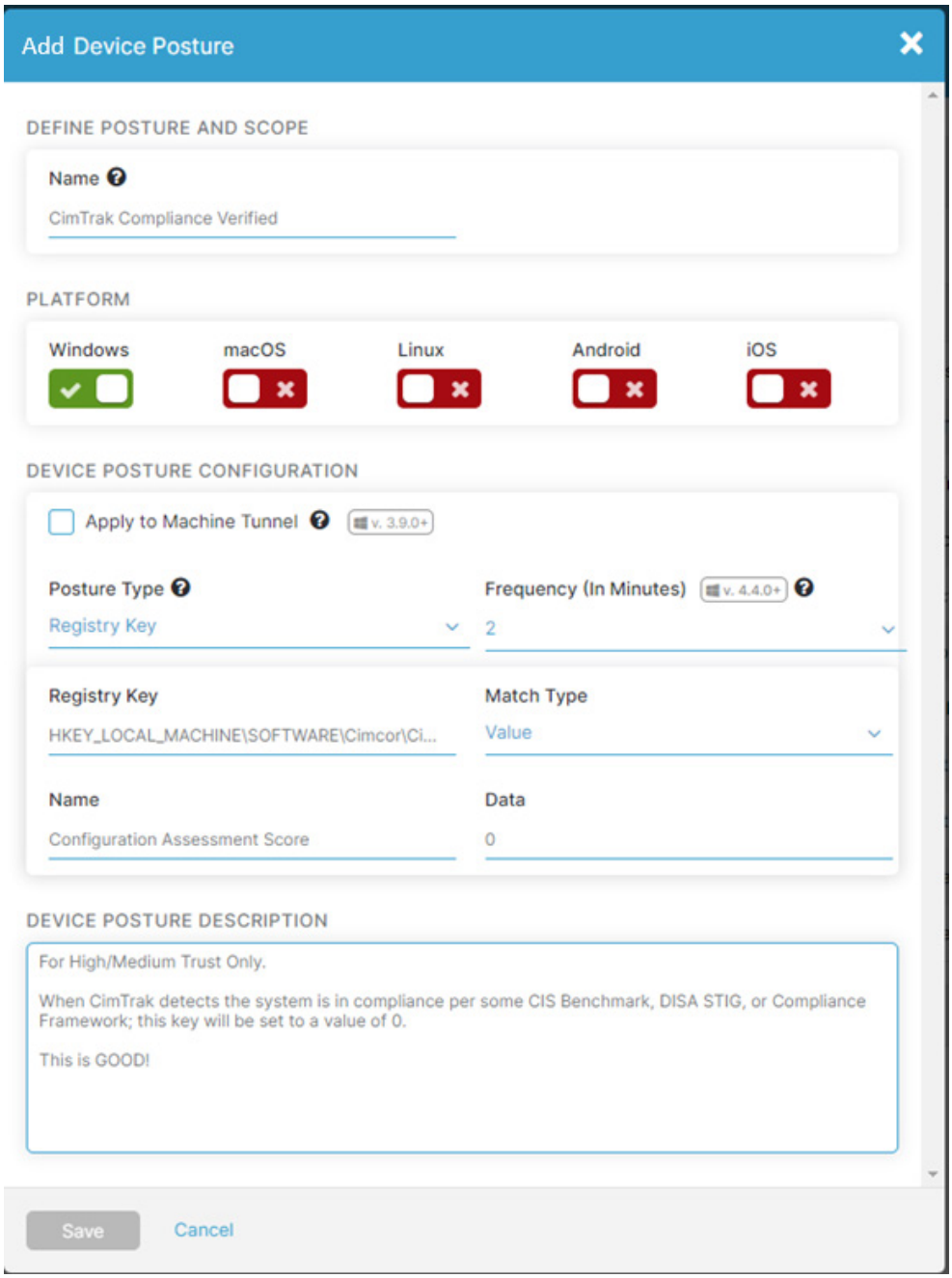

Figure 211. Add Device Posture

You can see the configuration in the following image.

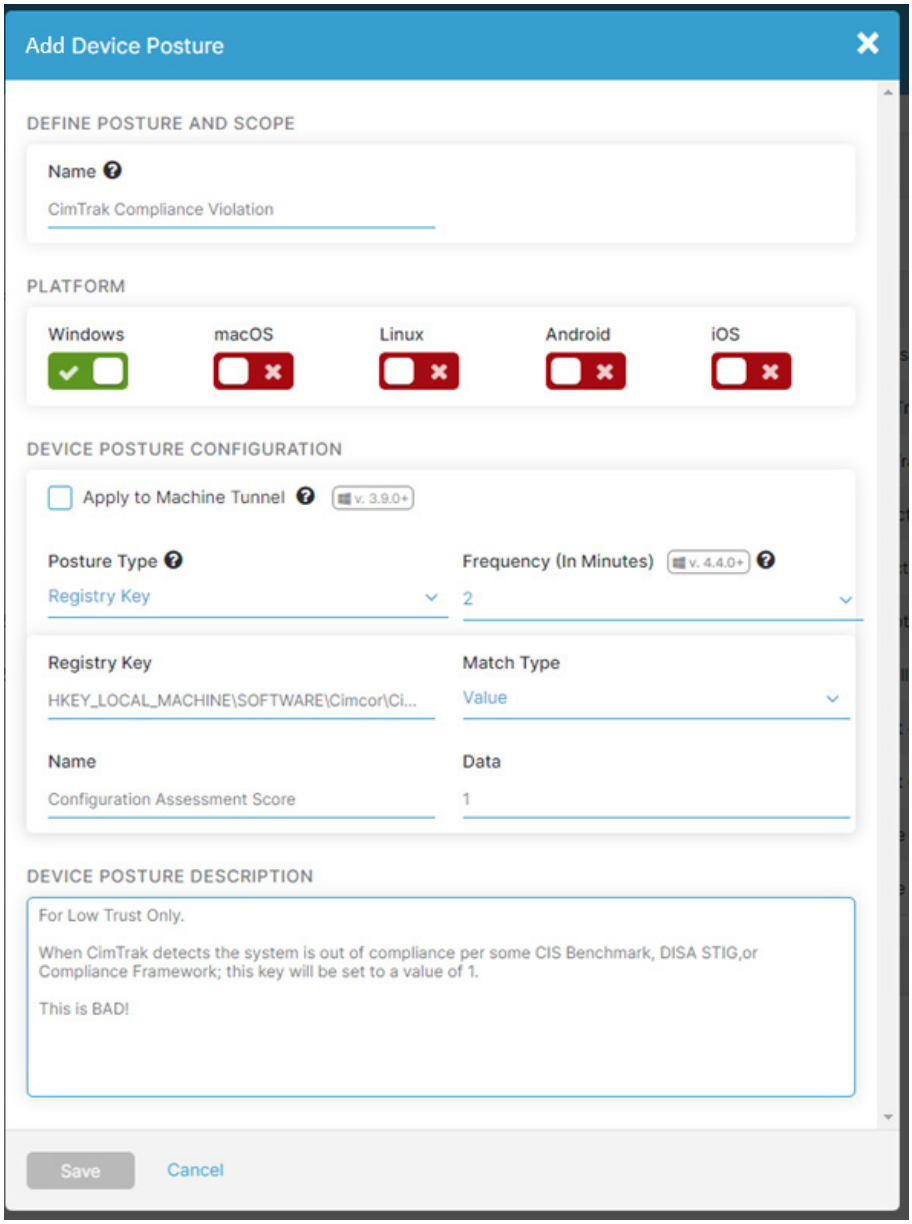

Figure 212. Edit Device Posture

You can take advantage of this Device Posture in ZIA. A common example is if CimTrak detects an Integrity or Compliance violation to cut off access to all cloud apps or all internet or certain networks based on CimTrak's findings.

In this example, CimTrak monitors the user's endpoint (workstations or laptop), and when that endpoint is in a compromised state, to cut off access in any way you specify in ZIA using this Device Posture as the trigger. The possibilities are customizable on the ZIA side to handle what access to give or revoke based on the CimTrak triggers.

While you can use Device Posture in ZPA, that is not needed here, Zscaler recommends you use the other ZPA integrations in this guide.

ZIA Posture Profile

After the Device Postures are set, create a profile to set levels of trust for systems that pass/fail these CimTrak Integrity or Compliance checks.

1. From the Zscaler Client Connector, go to **ZIA Posture Profile** > **Windows** > **Add ZIA Posture**.

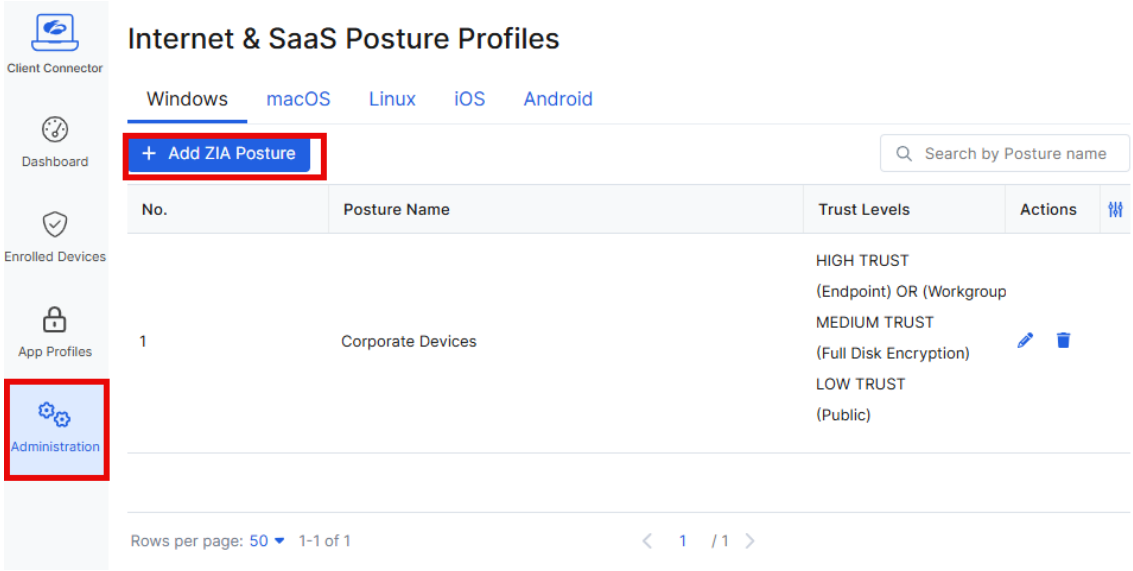

Figure 213. Add ZIA Posture

2. Enter a **Posture Name** (e.g., `CimTrak Posture Profile`).

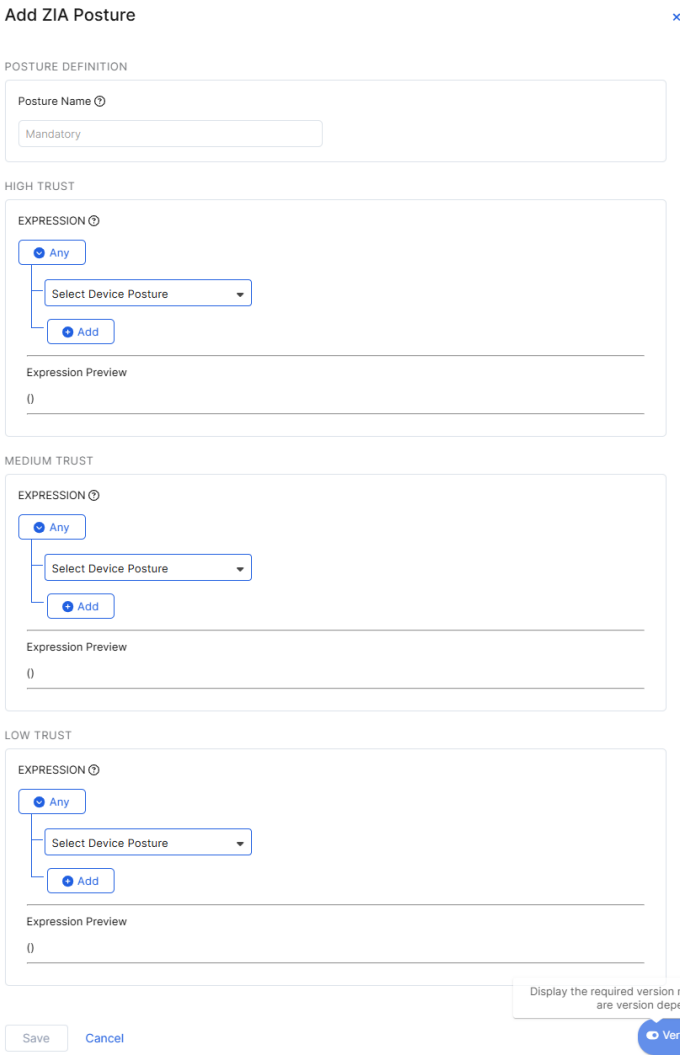

Figure 214. Add ZIA Posture

There are three levels of trust in this profile. The following definitions explain the configuration options:

- **Hight Trust**: Passes both Integrity AND Compliance checks.
- **Medium Trust**: Passes Integrity OR Compliance checks.
- **Low Trust**: Passes NEITHER check.

If you only have CimTrak Integrity features, Zscaler recommends you apply the Integrity Posture check to High trust, and leave blank Medium Trust and Low Trust.

3. For High Trust, click **Add** and select both **CimTrak Compliance Verified** and **CimTrak Integrity Verified.**

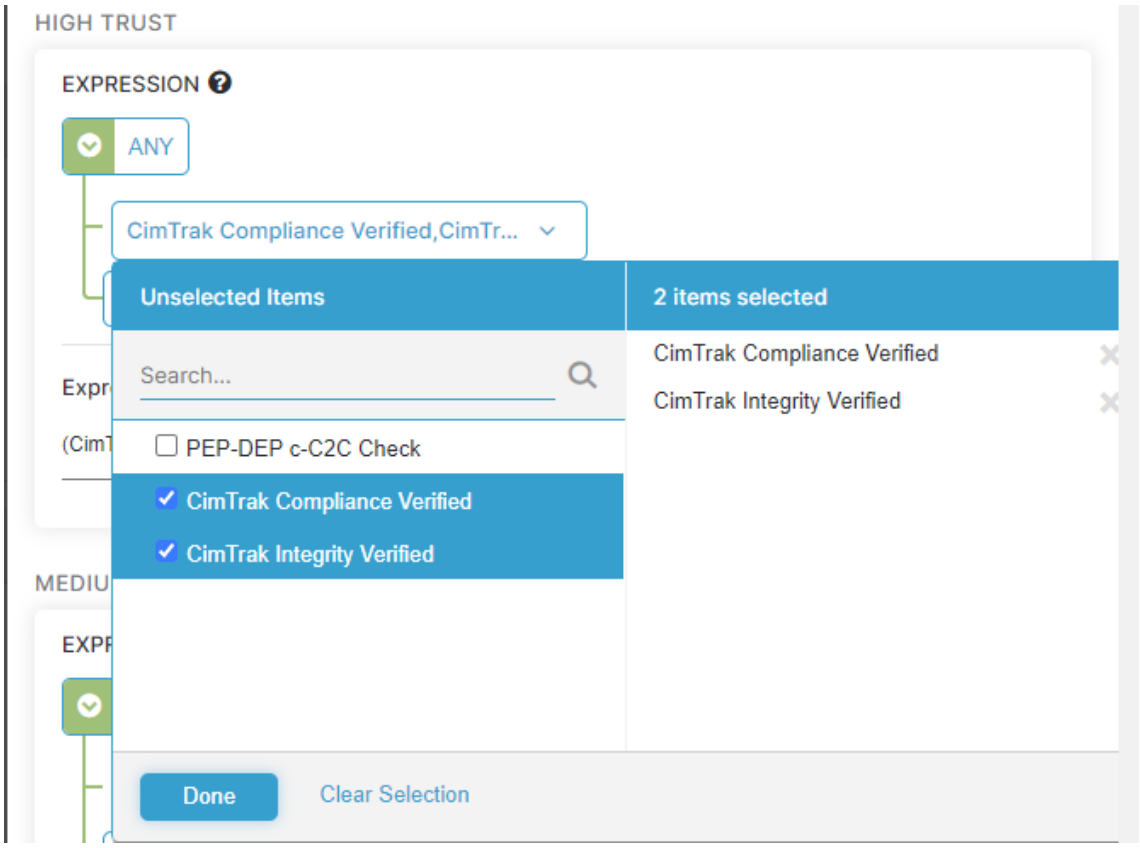

Figure 215. High Trust

4. For Medium Trust, click **Add** twice, one for each posture check to change the logic to OR.

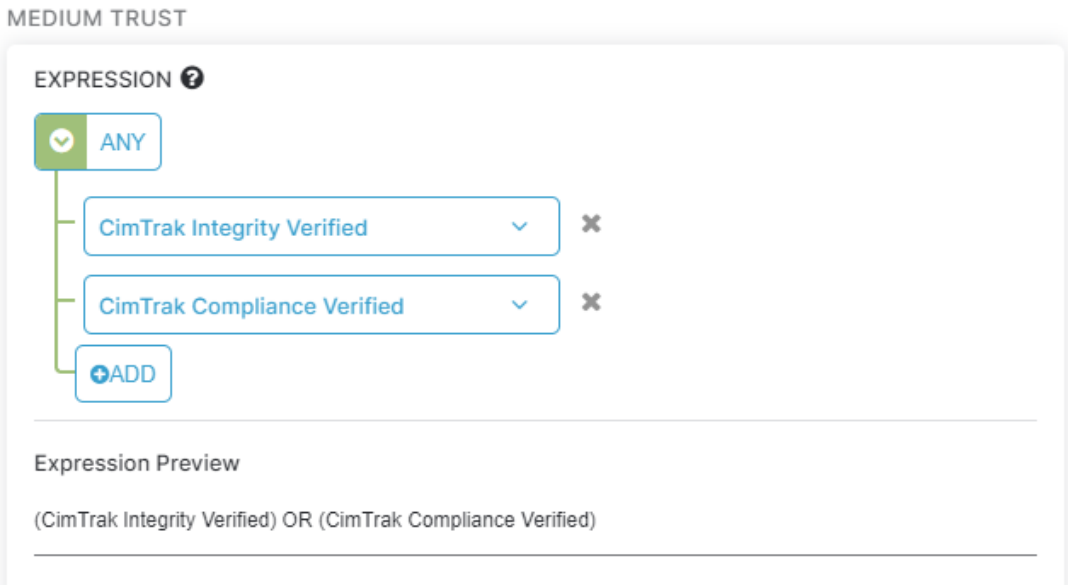

Figure 216. Medium Trust

5. For Low Trust, click **Add** once, and then select both **CimTrak Compliance Violation** and **CimTrak Integrity Violation**.

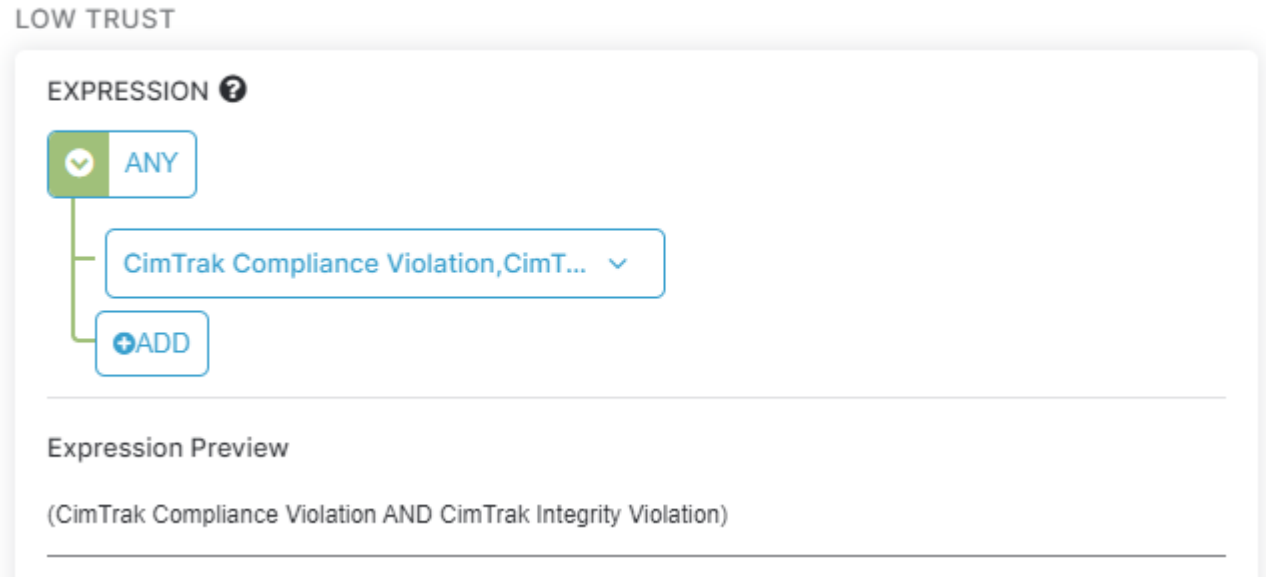

Figure 217. Low Trust

ZIA Isolation Profile

An Isolation profile must be configured to use an option to react to a CimTrak violation.

1. Go to the ZIA Admin Portal.
2. Go to **Secure Browsing** > **Browser Isolation**.

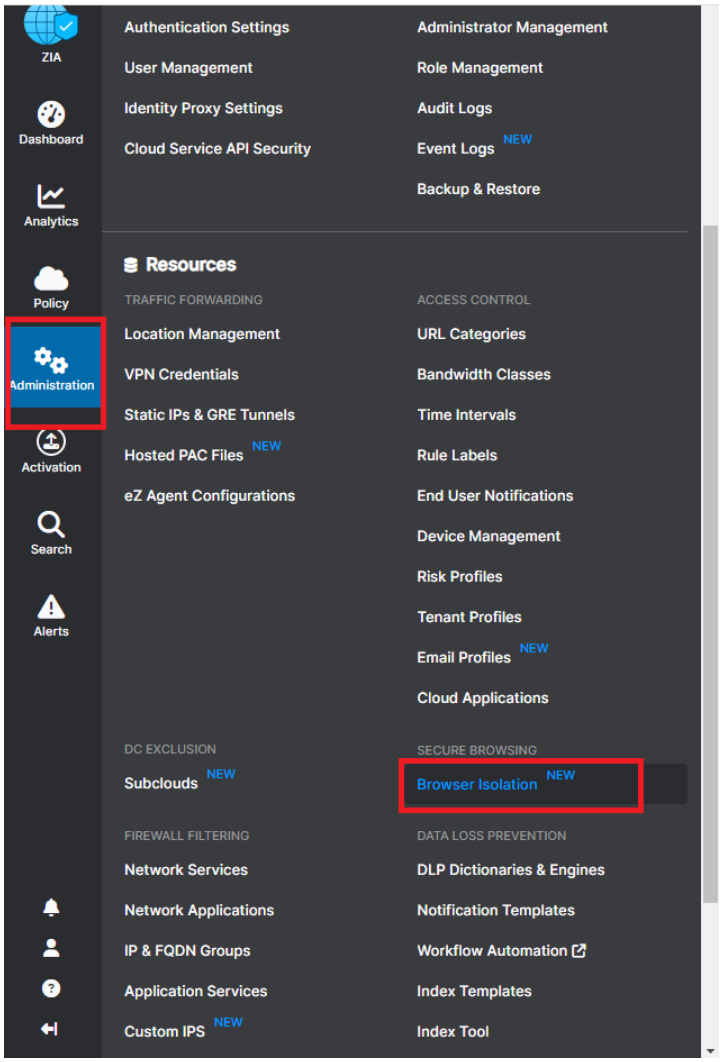

Figure 218. Browser Isolation

3. Click **Add Profile**.

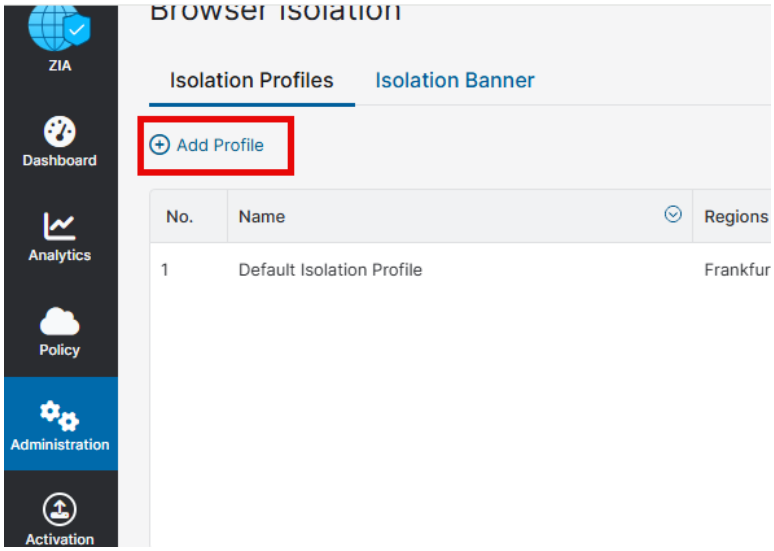

Figure 219. Add Profile

4. Give it a **Name** and **Description**.
5. Click **Next**.

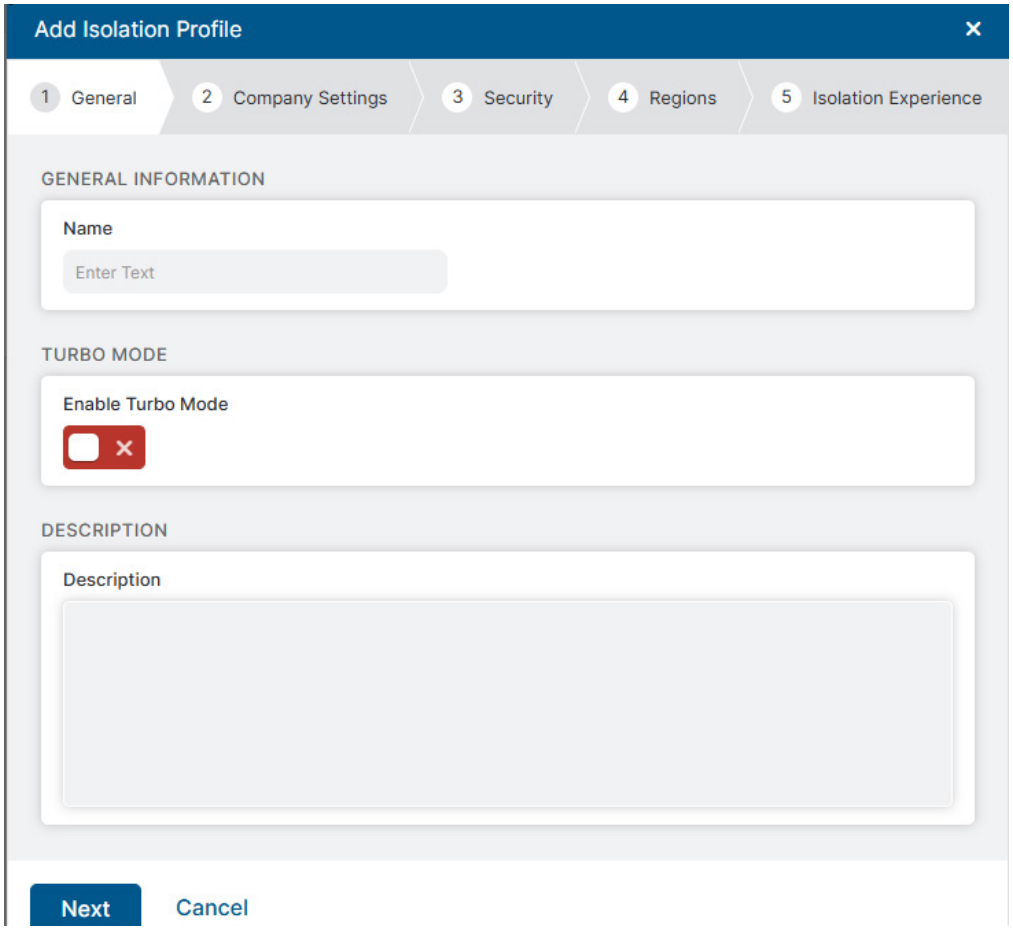

Figure 220. General

6. In the **Company Settings** tab, click **Next**.

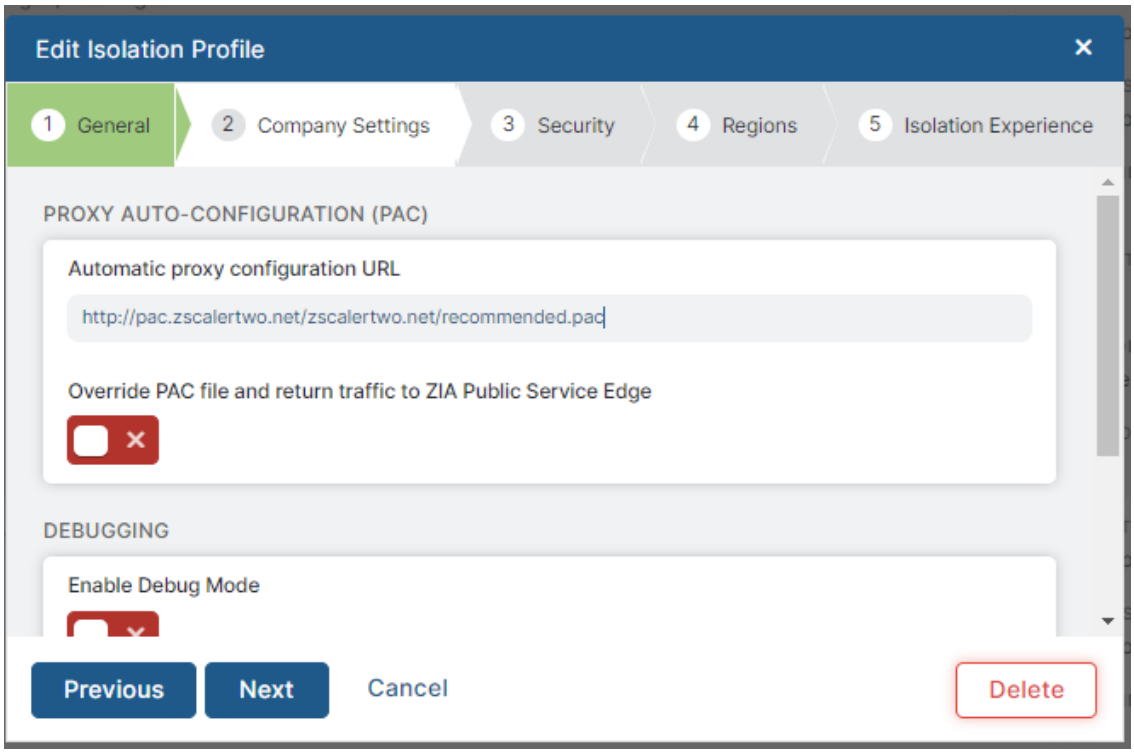

Figure 221. Company Settings

7. Under the **Security** tab, enable **Read-Only Isolation**.
8. Click **Next**.

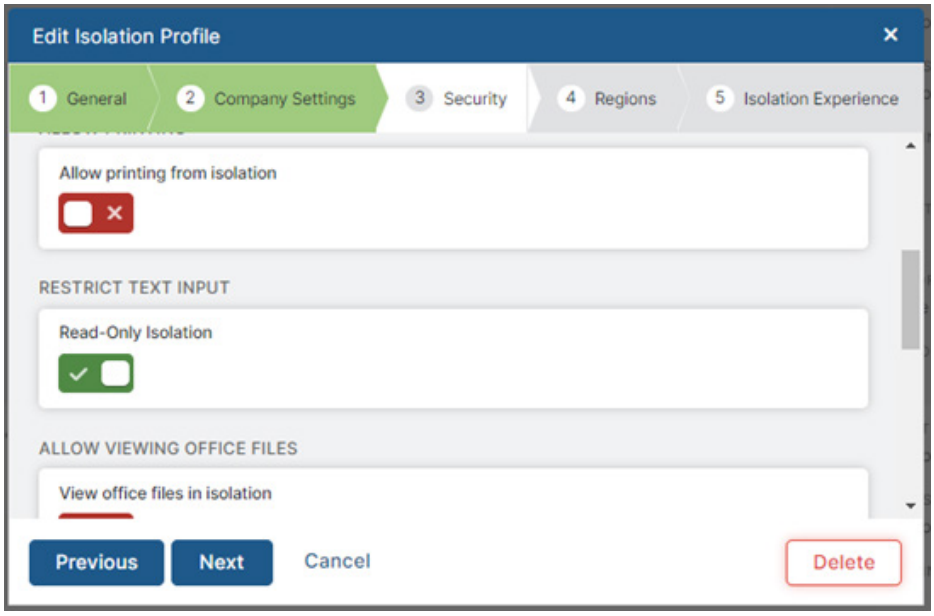

Figure 222. Security

9. In the **Regions** tab, choose what regions to isolate.
10. Click **Next**.

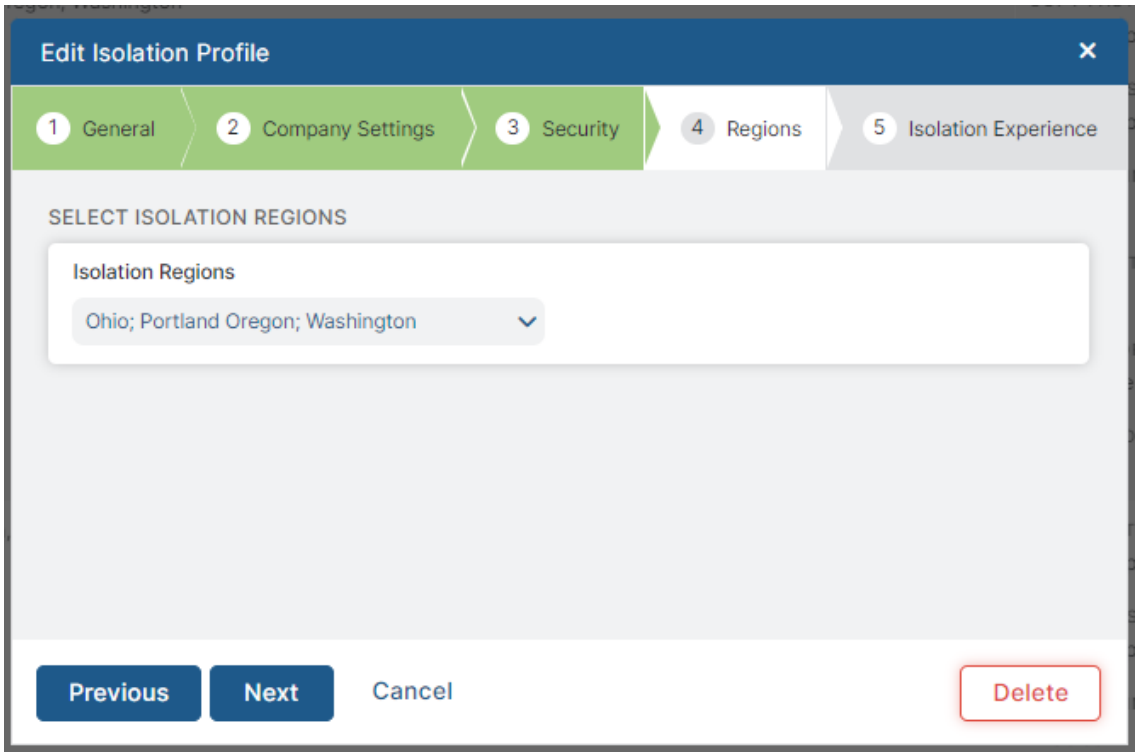

Figure 223. Regions

11. In the **Isolation Experience** tab, click **Save**.

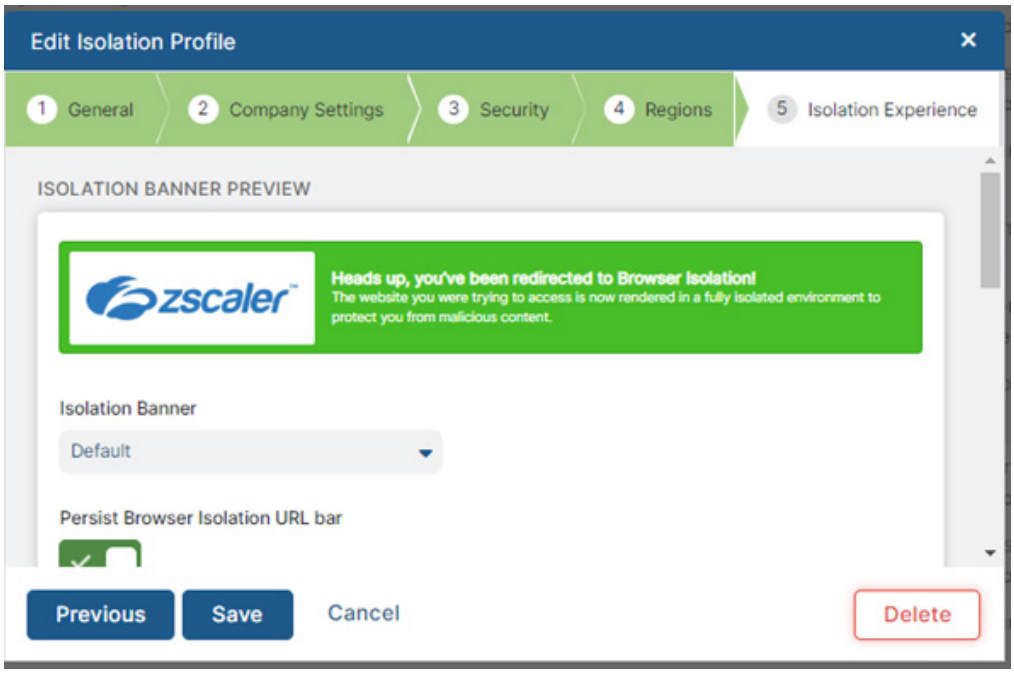

Figure 224. Isolation Experience

ZIA URL and Cloud App Control

To configure ZIA URL and Cloud App Control:

1. Go to the ZIA Admin Portal.
2. Go to **Access Control** > **URL & Cloud App Control**.

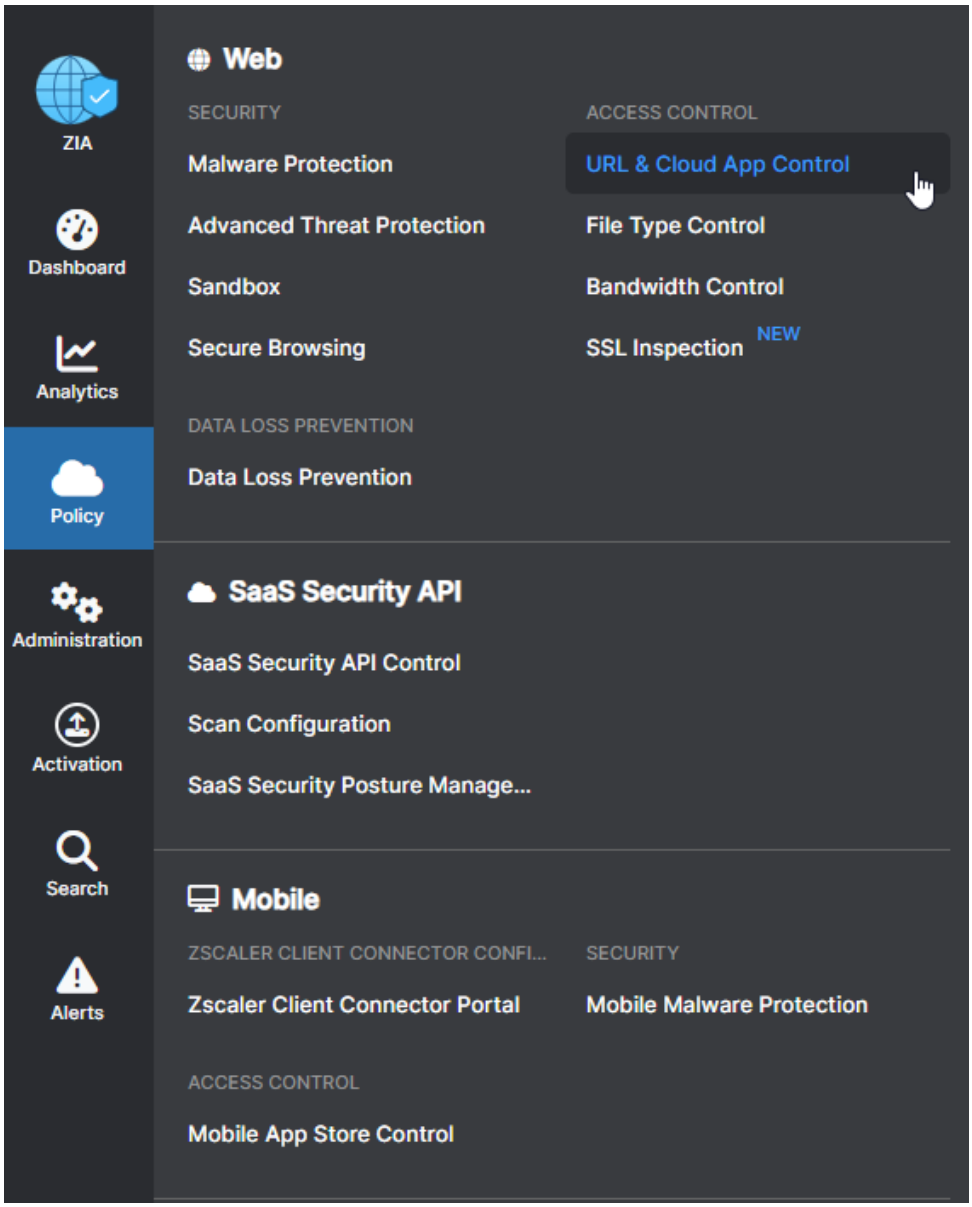

Figure 225. URL & Cloud App Control

3. After configuring the Device Posture Checks and Trust Profiles, create policies to automate security access:
   - If system is LOW Trust (or Unknown): BLOCK all network protocols.
   - If system is MEDIUM Trust: Browser Isolate – Read Only mode – for all HTTP/HTTPS
   - If system is in HIGH Trust: Do nothing. It's in a good state of Integrity and Compliant.

Now that our Posture Profiles are assigned to the appropriate Trust level, we can trigger off those within the Cloud App Control Policies.

Create Cloud App Control Policy for each Category. They should always be Rule Order 1 in most scenarios per Category.

While each category may have different criteria, it doesn't matter. The goal is to select any or all in every option, set Device Trust Level to Low or Medium, and to set the access to Block or Isolate.

For any Category that uses User Agent, select all except Other.

For each category you can do a Low trust and Medium trust rule, as shown in the following:

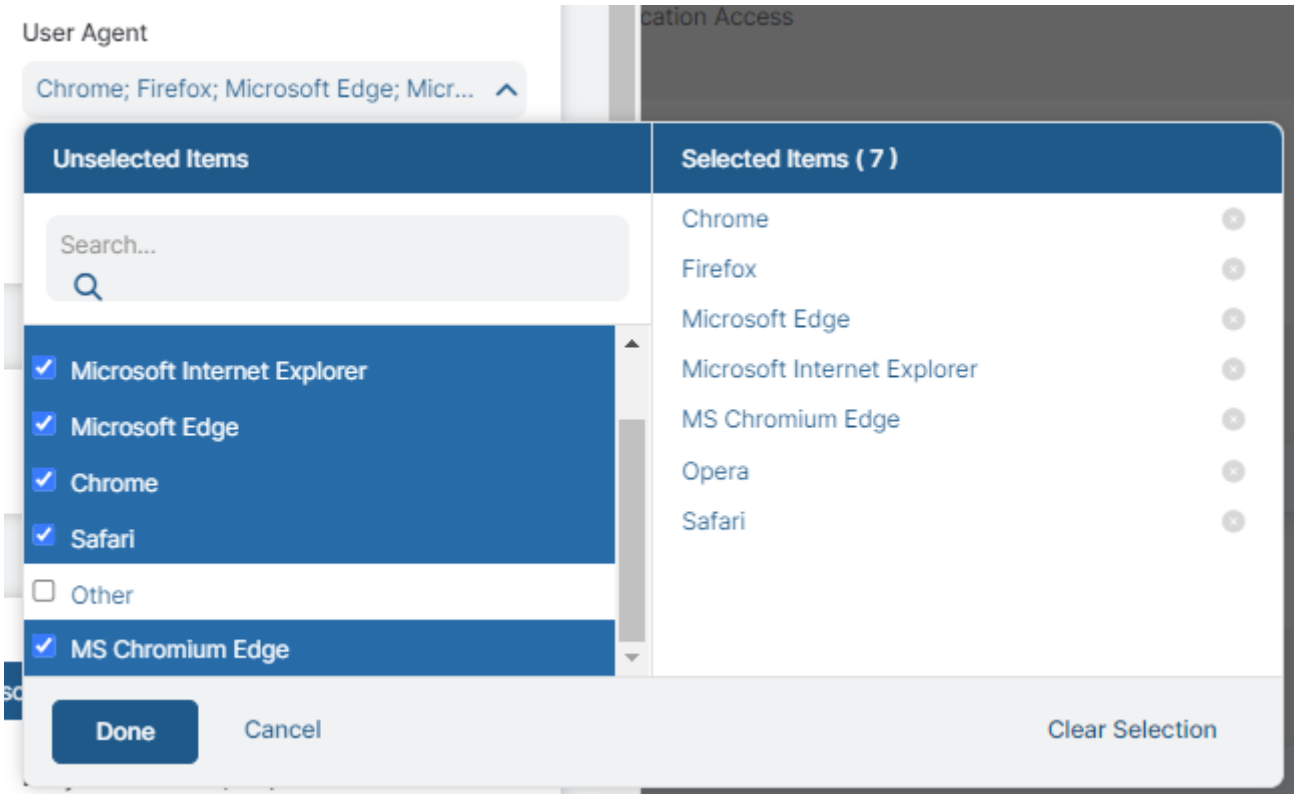

Figure 226. User Agent

You can see the configure in the following image.

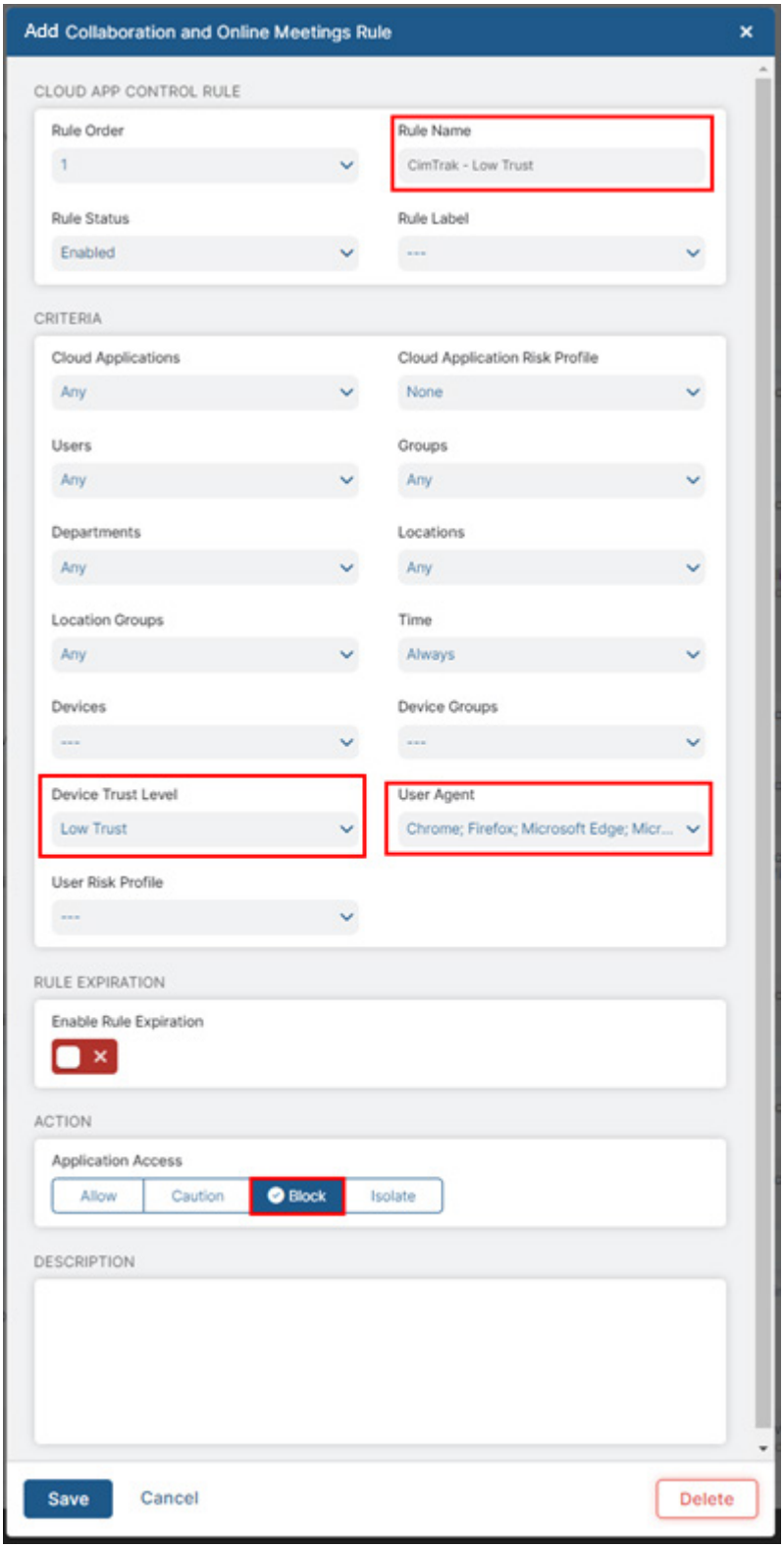

Figure 227. Edit Collaboration and Online Meetings Rule

You can see the configure in the following image.

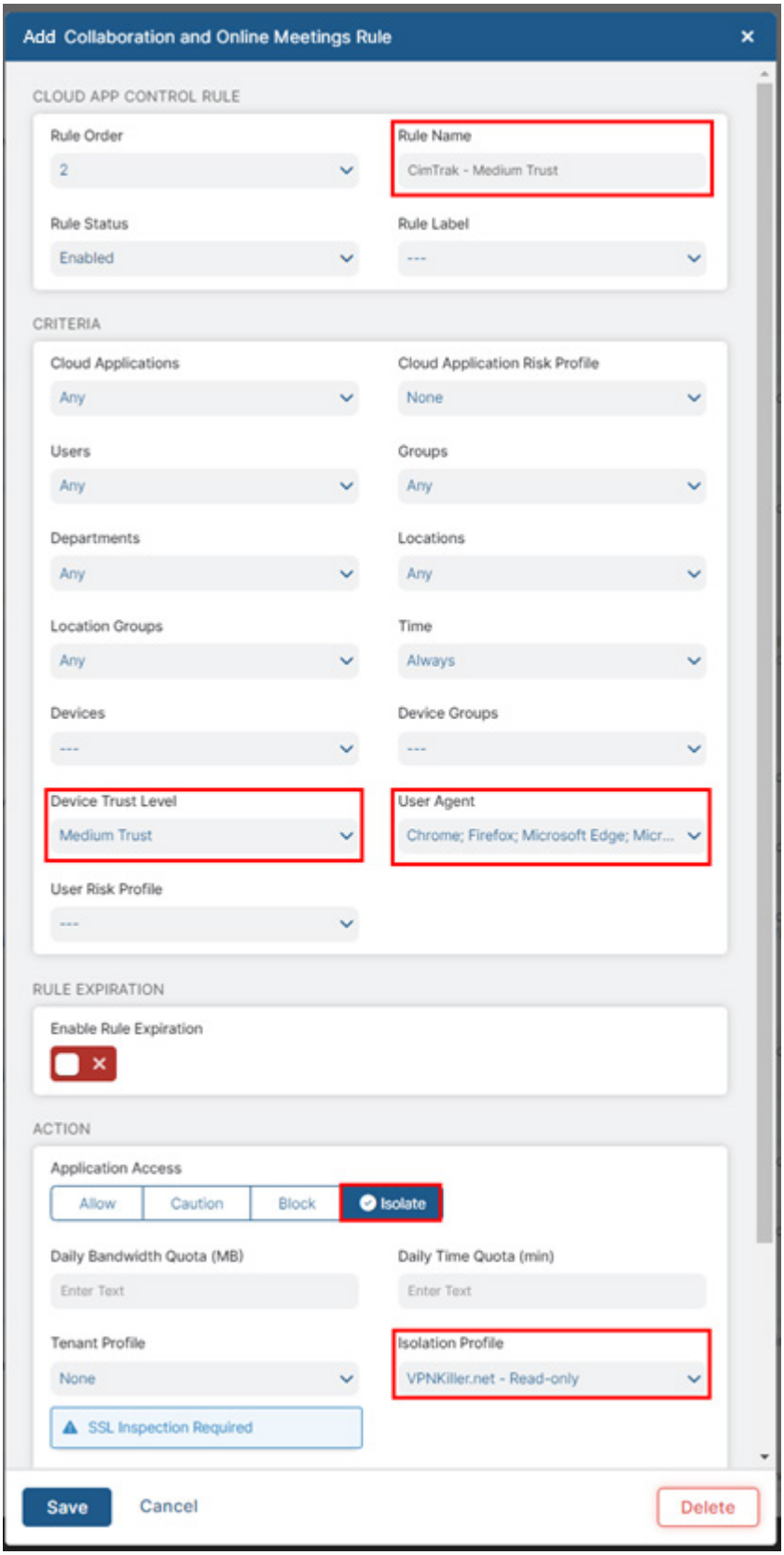

Figure 228. Edit Collaboration and Online Meetings Rule

Log In to Zscaler Client Connector

On any endpoint where you want to enforce these rules:

1. Log in to the Zscaler Client Connector.

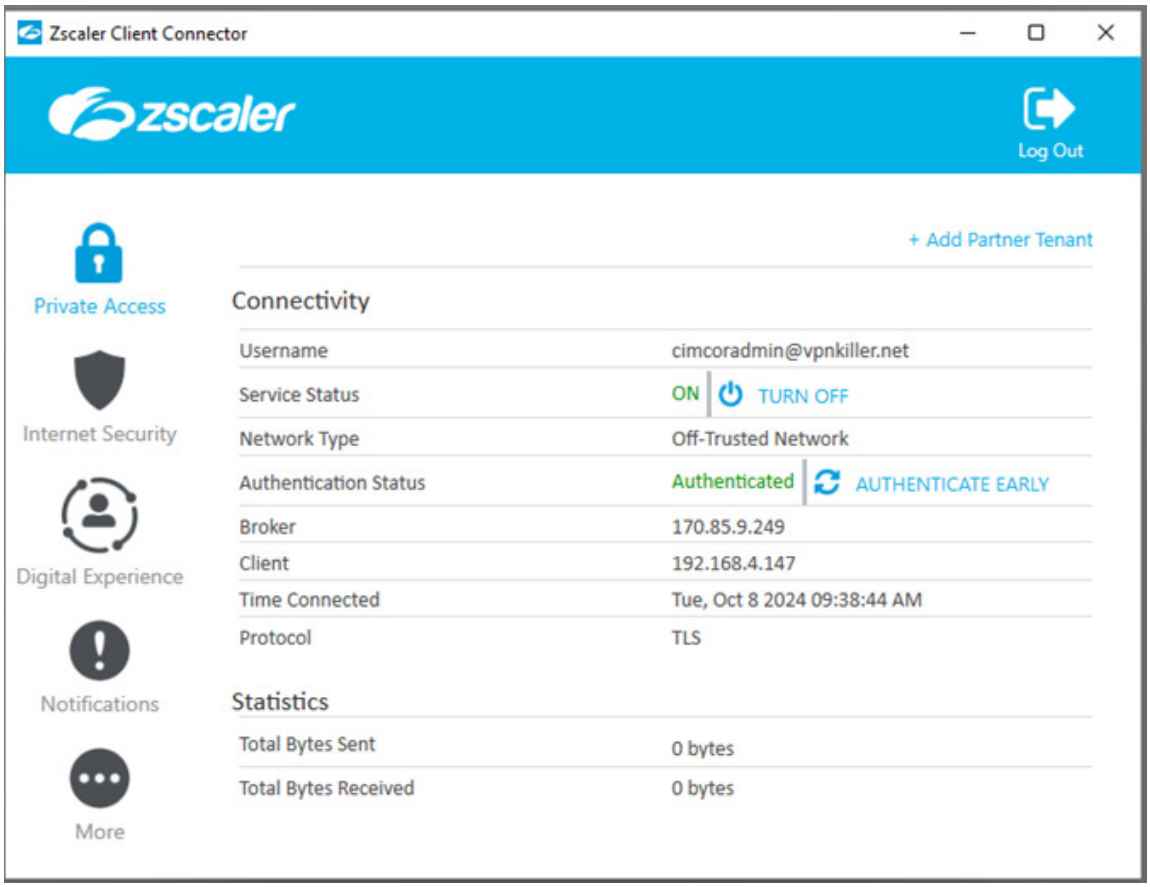

Figure 229. Zscaler Client Connector

2. Click **More**.
3. From the **About** section, select **Update Policy** to have Zscaler Client Connector force pull the latest updates to your policies in ZIA.

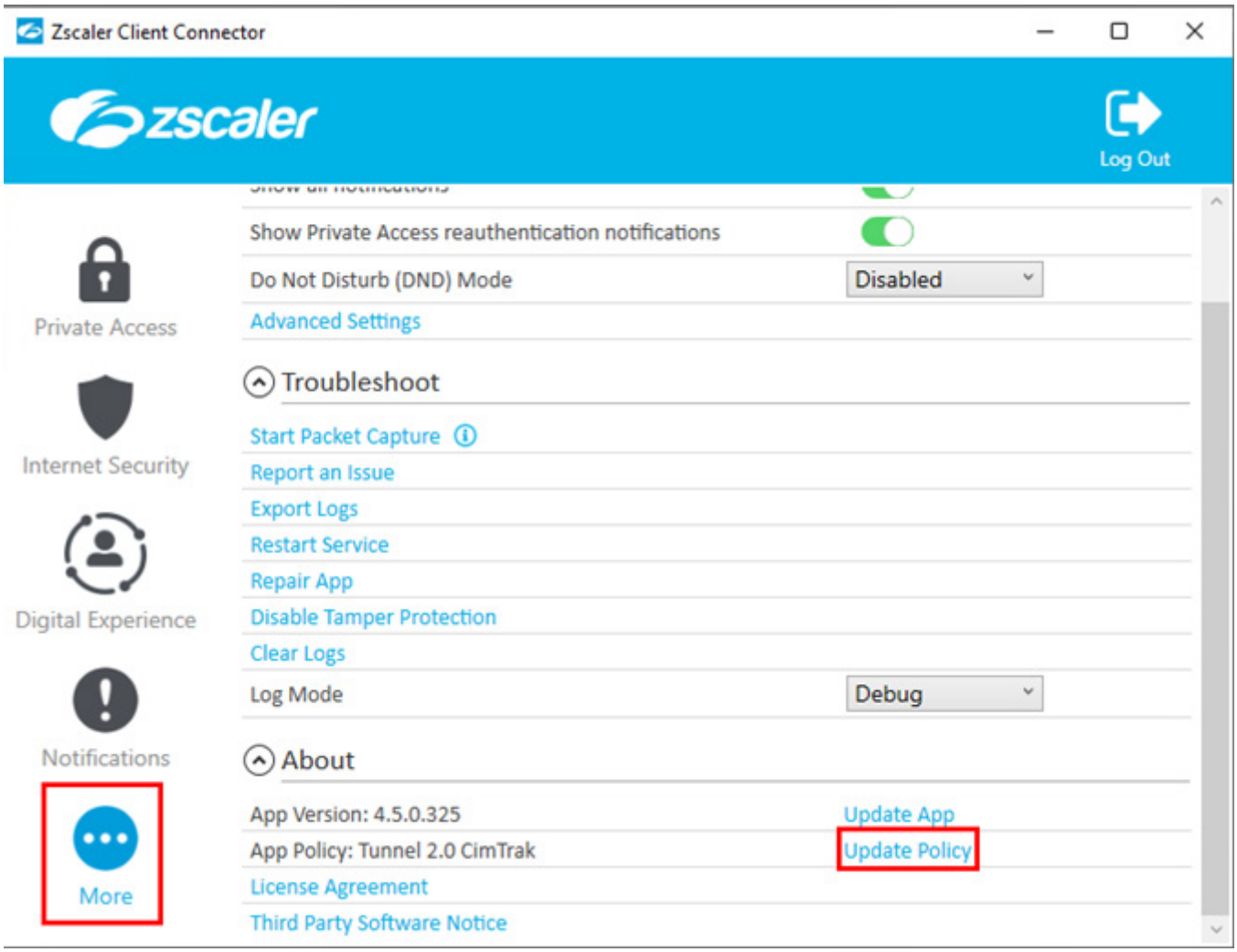

Figure 230. Update Policy

Enable CimTrak Compliance Policy

To enable CimTrak compliance policy:

1. Right-click **Repository**, and then select **Compliance Policy** >**Lock**. CimTrak initiates the scan and completes the Benchmark/Compliance tests. You receive the **Compliance Scan Completed** event in the **Event Log** after it is complete.

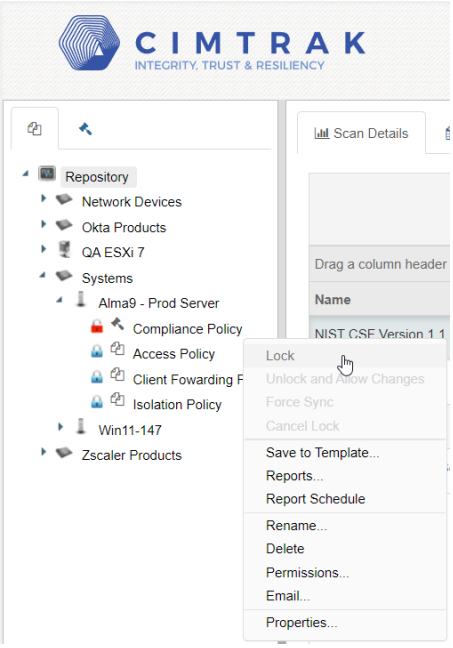

Figure 231. Lock

2. View the score in the **Scan Details** tab.

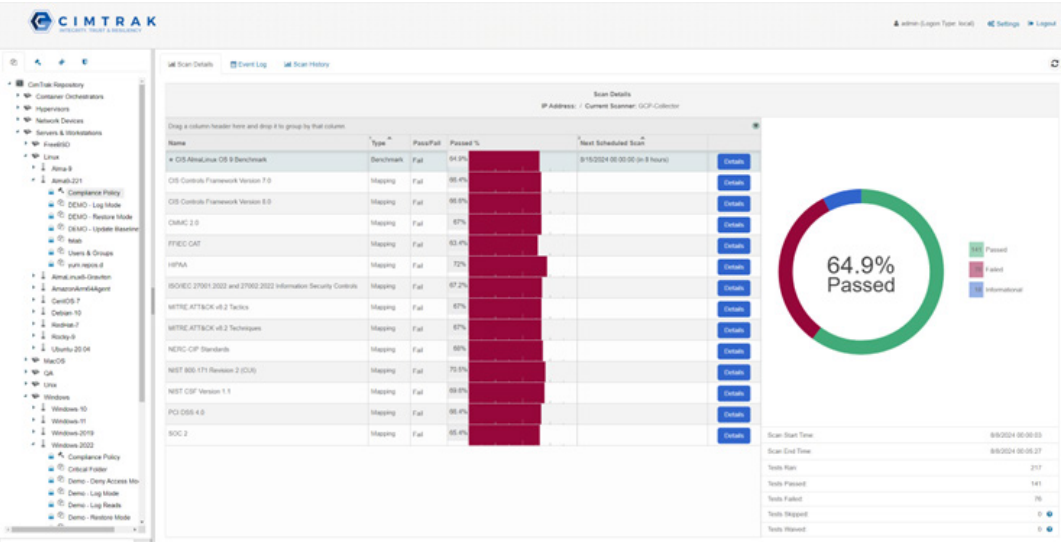

Figure 232. Compliance scan completed

Testing the Integration

After your first scan is completed, you can review your score in the **Scan Details** tab.

If the Benchmark or STIG score was not higher than your configured threshold, CimTrak triggers the state and enables ZIA Device posture.

Click the Event Log to see the full results of the scan and any post-scan actions.

In the following image, the Windows Server scan failed. CimTrak switched the Compliance state and enabled ZIA Device Posture for this system.

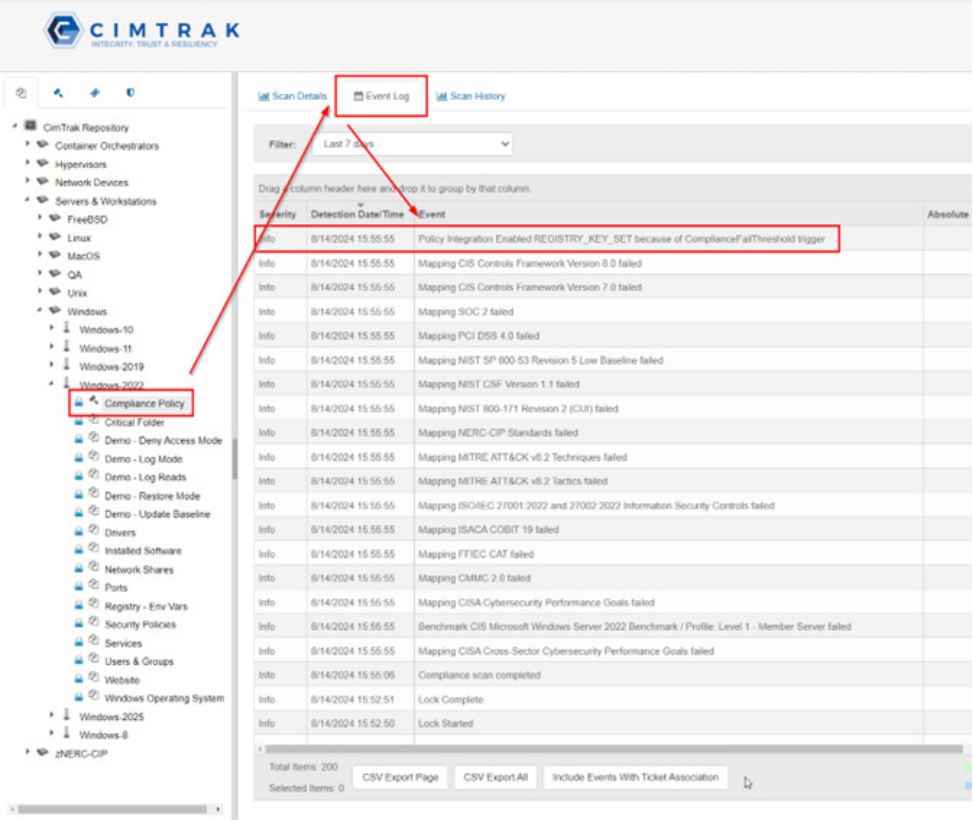

Figure 233. Completed scan

When Set to Block

ZIA blocks all the categories of external sources a user might try to access, based on where these rules are applied.

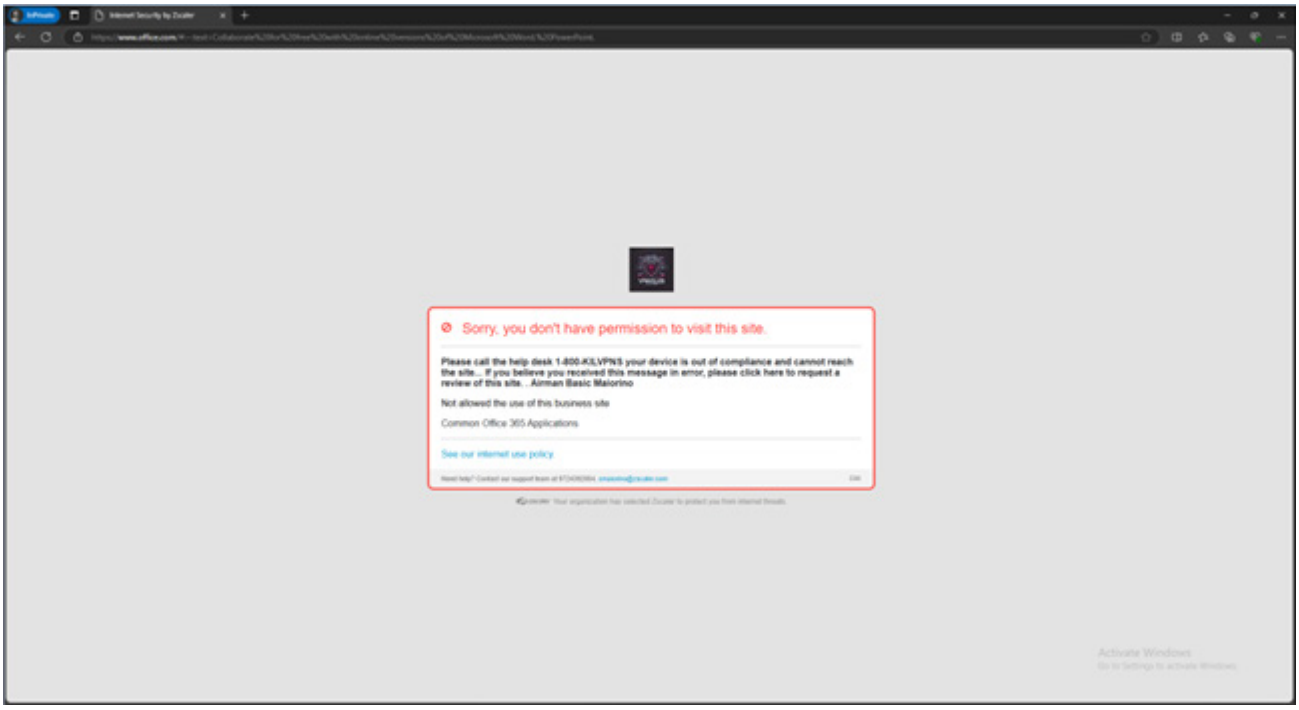

Figure 234. Set to Block

When Set to Isolate

ZIA isolate all the categories of external sources a user might try to access, based on where these rules are applied.

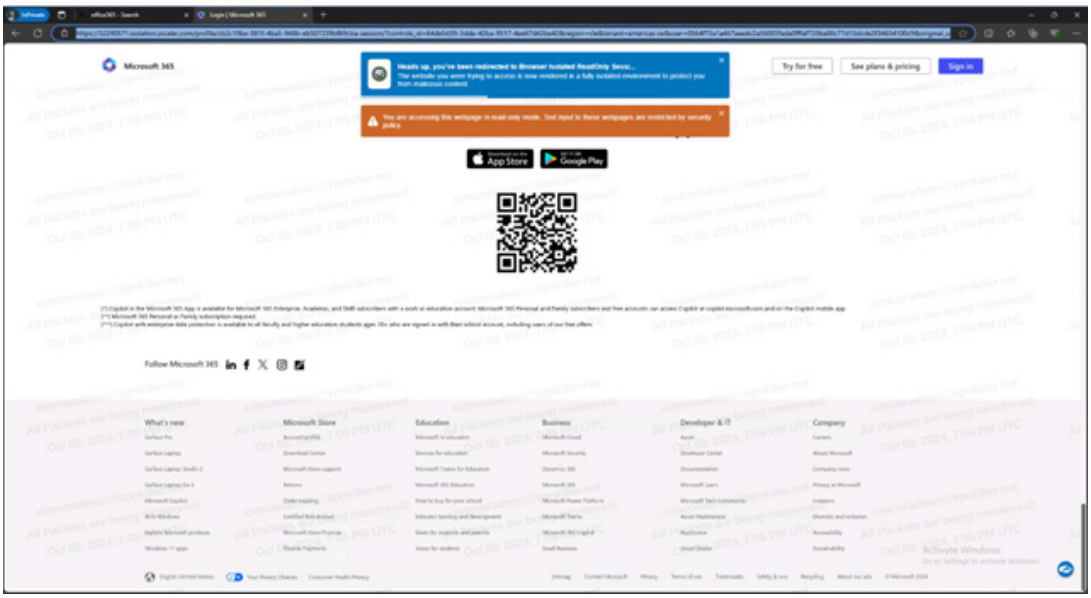

Figure 235. Set to Isolate

Resetting the Integration

When the system is in a good state of integrity, you can reset it in the Policy Properties.

1. Right-click **Compliance Policy** and select **Properties**.

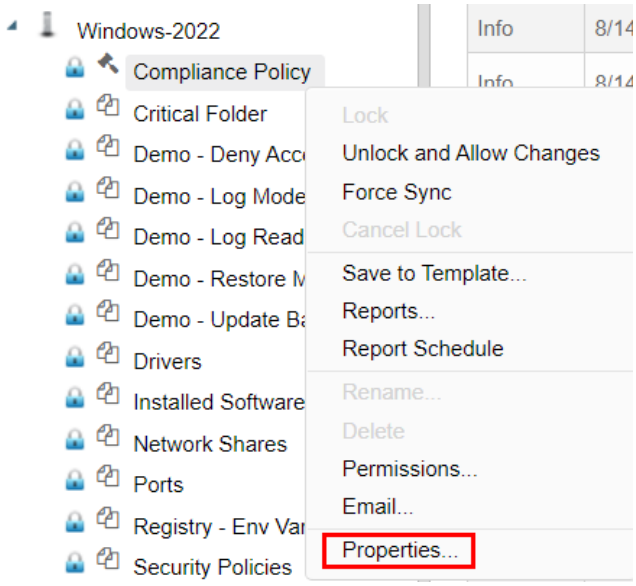

Figure 236. Properties

2. Click the **Integrations** tab and note the **Enforcement Current State**. Click **Reset** to reset the **Integrity State** and disable **ZIA Device Posture** for this system.

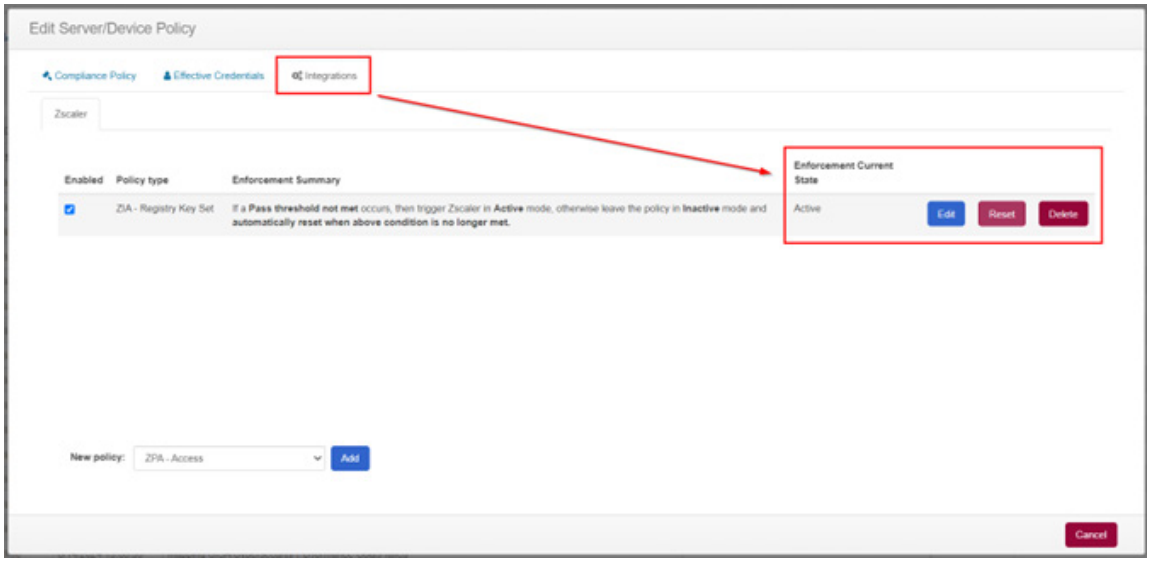

Figure 237. Reset

Appendix A: Requesting CimTrak Support

The following sections details how to contact **CimTrak Support**.

Contacting Support

- Email: support@cimcor.com
- Toll Free: 1-877-424-6267
- Local: 1-219-736-4400 (press 2 for the Support Department)

Managing Support Tickets

You can submit tickets via email or the Cimcor Support Portal. You can manage tickets sent either way in this portal. To learn more about viewing or managing tickets, and accessing the Cimcor Knowledge base, refer to the Support home.

1. Log in to the support portal.

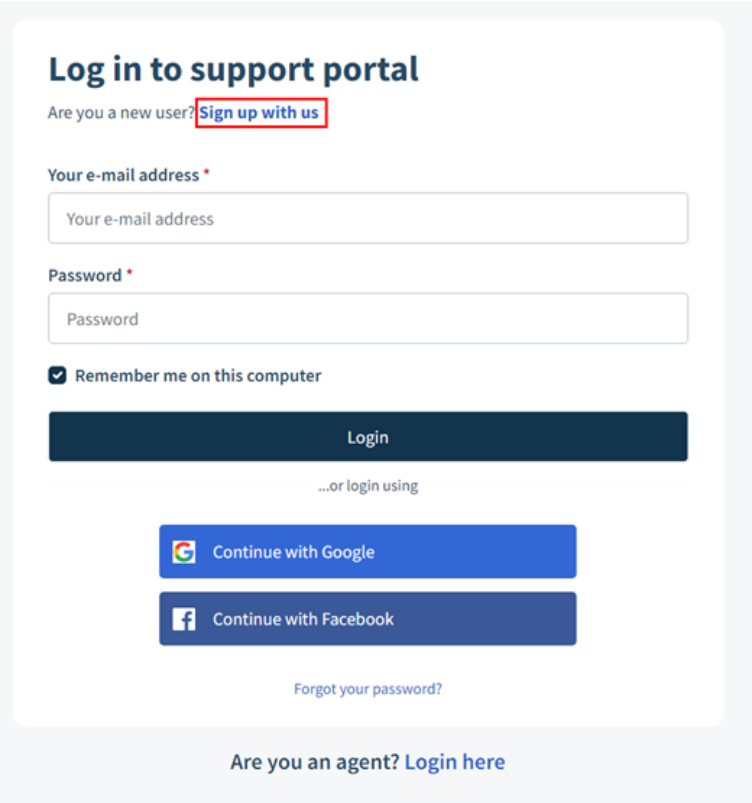

Figure 238. Create account

2. After logging in, you can see the portal homepage and links to your tickets and the Knowledge base articles.

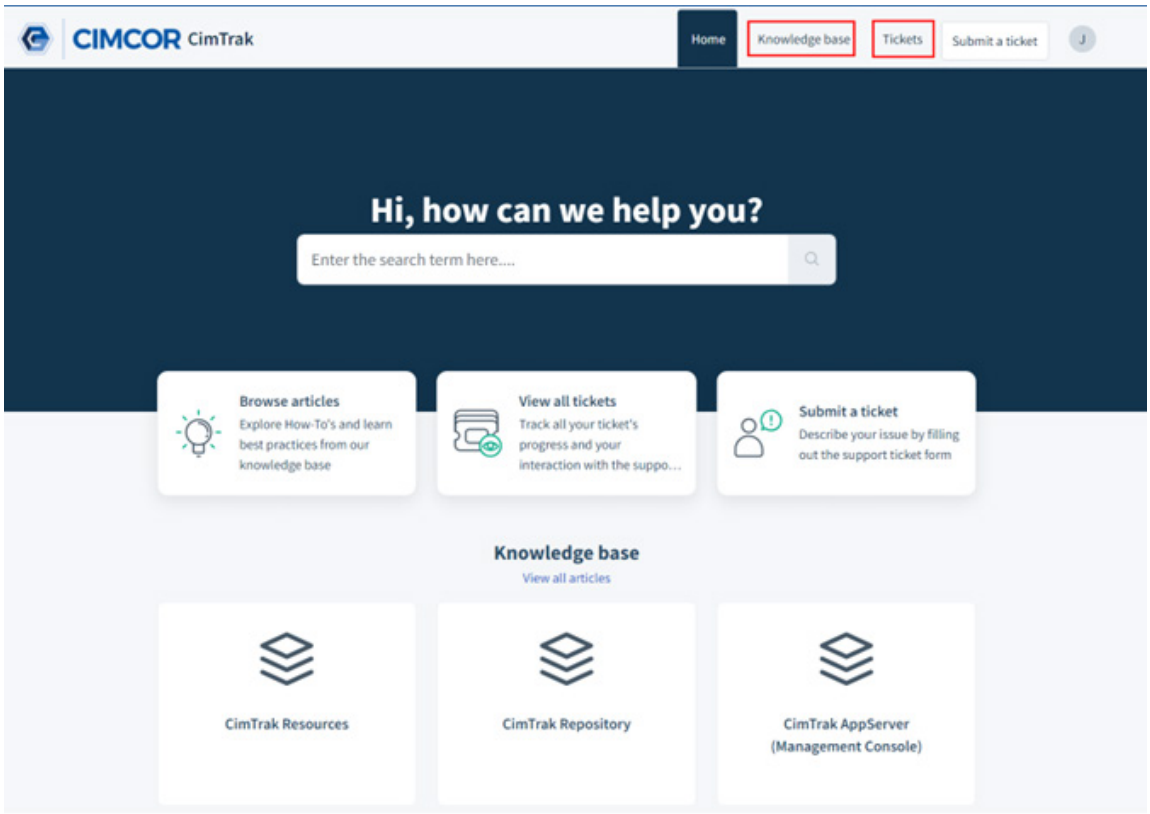

Figure 239. Support tickets and articles

Appendix B: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

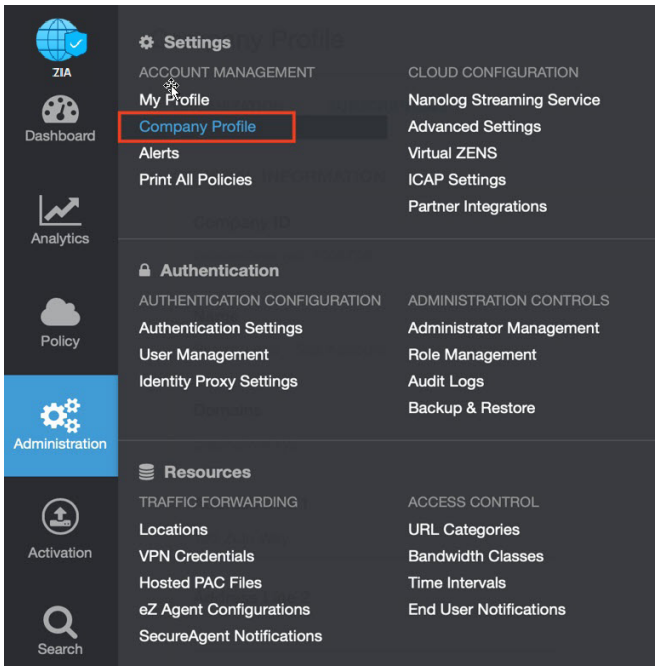

Figure 240. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

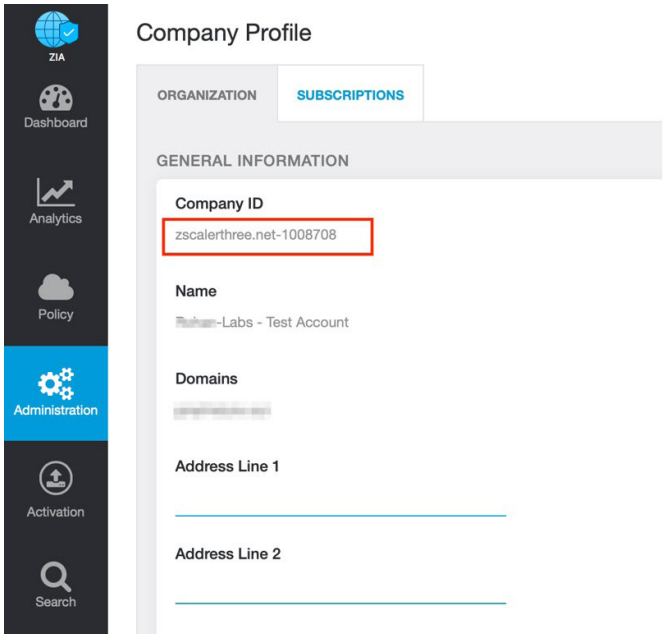

Figure 241. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

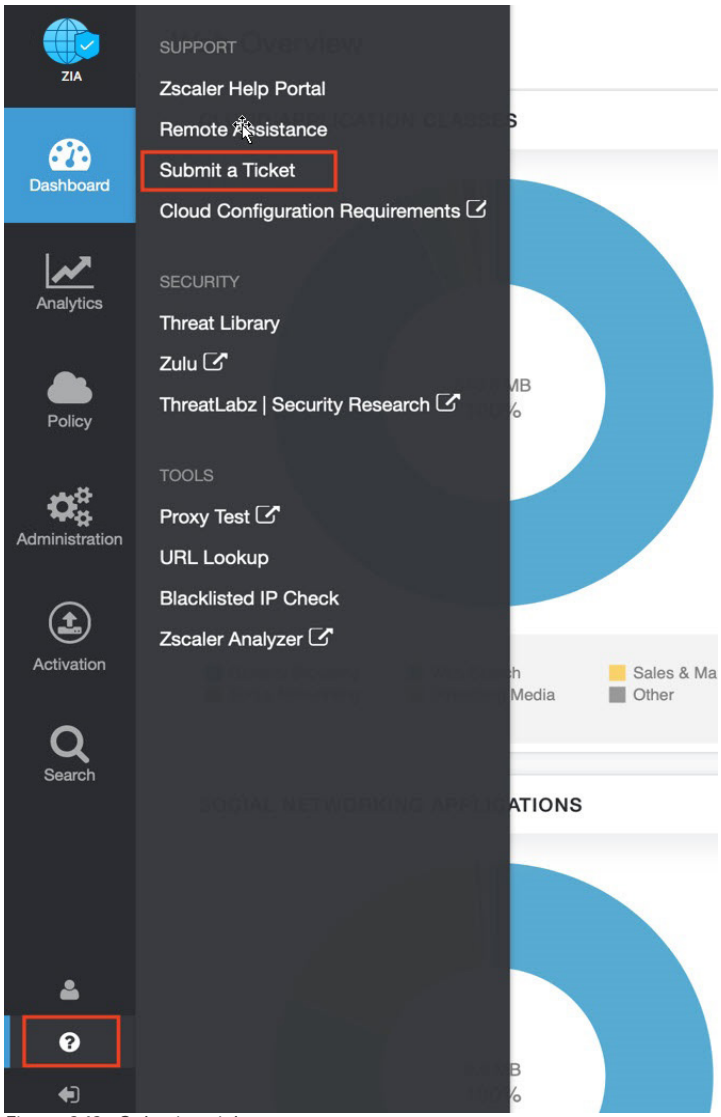

Figure 242. Submit a ticket

