



ZSCALER AND MICROSOFT DEFENDER DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
Trademark Notice	5
About This Document	6
Zscaler Overview	6
Microsoft Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and Microsoft Introduction	7
ZIA Overview	7
ZPA Overview	7
Zscaler Resources	7
Defender Resources	8
ZIA and Microsoft Defender	9
Prerequisites	9
Integrating with Microsoft Defender for Endpoint	10
ZIA Hits Report	13
Viewing the Microsoft Defender Endpoint Hits Report	13
About the Microsoft Defender Endpoint Hits Report	13
Sandbox File Properties (Zscaler)	13
File Detected on Endpoints (Microsoft Defender for Endpoint)	14

ZPA Posture Type	17
Configuring ZPA	18
Log in to ZPA Admin Portal	18
Go to the Zscaler Client Connector	18
Create a New Posture Profile	19
Add New Microsoft Defender Posture Profile	19
Decide Which Applications Need Conditional Access	20
Set Up an Access Policy	21
Tie the Posture Profile to this Access Policy	21
Verify Conditional Access from an Endpoint	22
Contextualizing Risk using Microsoft Defender for Endpoint and Avalor UVM	23
Create an Entra ID App Registration for Programmatic Access to Microsoft Defender for Endpoint	23
Configure the Microsoft Defender for Endpoint UVM Data Connectors	28
Configure the Azure Defender for Endpoints—Assets Data Source	28
Configure the Azure Defender for Endpoints—Vulnerabilities Data Source	32
Configure the Azure Defender for Endpoints—Alerts Data Source	35
Configure the Azure Defender for Endpoints—Software Vulns by Machine Data Source	38
Review and Adjust Data Model Mapping	41
Map Asset Microsoft Defender for Endpoint with the Has EDR Data Model Entity	41
Review and Adjust Risk Scoring	43
Appendix A: Requesting Zscaler Support	45

Terms and Acronyms

This 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
AIR	Automated Investigation and Remediation
APT	Advanced Persistent Threat
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DPD	Dead Peer Detection (RFC 3706)
EDR	Endpoint Detection and Response
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IoA	Indicator of Attack
IoC	Indicator of Compromise
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
MD5	Message Digest Algorithm
P2P	Point to Point
PAC	Proxy Auto-Configuration
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SSL	Secure Socket Layer (RFC6101)
XDR	Extended Detection and Response
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

This section describes the organizations in 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](#).

Microsoft Overview

Microsoft (Nasdaq: [MSFT](#)), Microsoft develops and licenses consumer and enterprise software. It is known for its Windows operating systems and Office productivity suite. The company is organized into three equally sized broad segments: productivity and business processes (legacy Microsoft Office, cloud-based Microsoft 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (infrastructure- and platform-as-a-service offerings Azure, Windows Server OS, SQL Server), and more personal computing (Windows Client, Xbox, Bing search, display advertising, and Surface laptops, tablets, and desktops). To learn more, refer to [Microsoft'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 more information on product and company resources, see:

- [Zscaler Resources](#)
- [Defender Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest version of ZIA and ZPA.

Request for Comments

- **For Prospects and Customers:** We value reader opinions and experiences. Contact us at 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 Microsoft Introduction

This section describes the Zscaler and Microsoft applications in this deployment guide.



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 onramp—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, data loss prevention (DLP), and isolation, allowing you 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.

Defender Overview

Microsoft 365 Defender, part of Microsoft's Extended Detection and Response (XDR) solution, leverages the Microsoft 365 security portfolio to automatically analyze threat data across domains, building a complete picture of each attack in a single dashboard. Microsoft 365 Defender detects and stops attacks anywhere in the cyber kill chain and returns the organization to a secure state.

Microsoft Defender is a next-generation component that brings together machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices (or endpoints) in your organization. Microsoft Defender Antivirus is built into Windows, and it works with Microsoft Defender for Endpoint to provide protection on your device and in the cloud.

Defender Resources

The following table contains links to Microsoft Defender support resources.

Name	Definition
Microsoft Defender documentation	Online help articles for Microsoft Defender.
Microsoft Defender support	Support contact for Microsoft Defender.
Isolate devices from the network	Help article on locking down a device and preventing subsequent attempts of potentially malicious programs from running.
Automated investigation	Help article on starting a new general purpose automated investigation on the device if needed.
Stop and quarantine files	Help article on containing an attack in your organization by stopping the malicious process and quarantining the file.
Block or allow a file	Help article on banning potentially malicious files or suspected malware.

ZIA and Microsoft Defender

Zscaler's integration leverages Microsoft Defender for Endpoint APIs to provide endpoint detection and response (EDR) visibility for Sandbox-detected malware. When configured, the Zscaler service calls the Microsoft Defender for Endpoint API and requests information for endpoints that were exposed to the malicious file. Microsoft Defender for Endpoint uses the new file signature to detect compromised points throughout your organization's network.

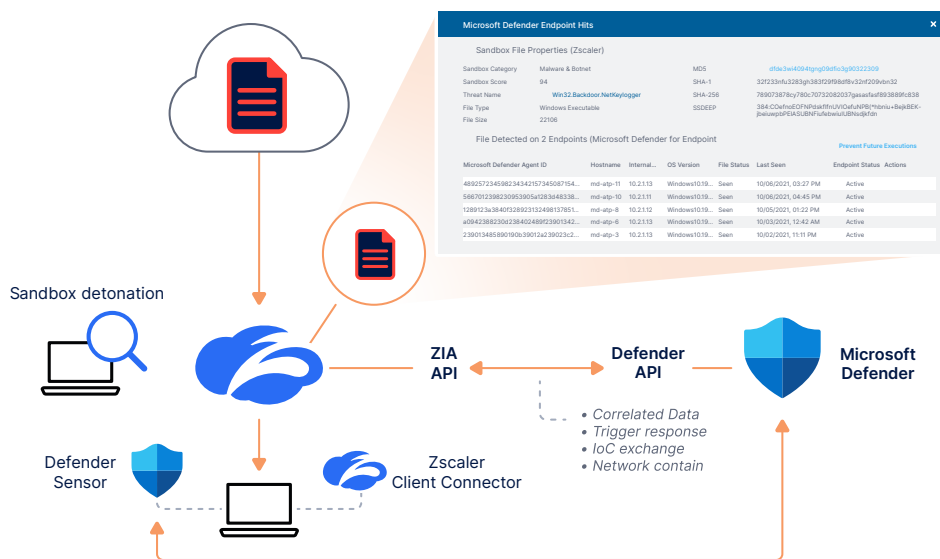


Figure 1. ZIA and Microsoft Defender overview

You can view information about the affected endpoints in the Sandbox logs and reports of the ZIA Admin Portal. You can also isolate endpoints, start automated investigation and remediation (AIR), and stop malicious file executions from the ZIA Admin Portal. For further investigation and remediation, you can go to the Microsoft Defender for Endpoint portal. These automated workflows reduce the threat dwell time and remediation time.

Prerequisites

Before you begin the Microsoft Defender for Endpoint integration, ensure you have:

- A Microsoft Defender for Endpoint admin account
- Advanced Cloud Sandbox

To learn more, see the [Microsoft Defender for Endpoint documentation](#).

Integrating with Microsoft Defender for Endpoint

To integrate the Zscaler service with Microsoft Defender for Endpoint:

1. Go to **Administration > Partner Integrations**.

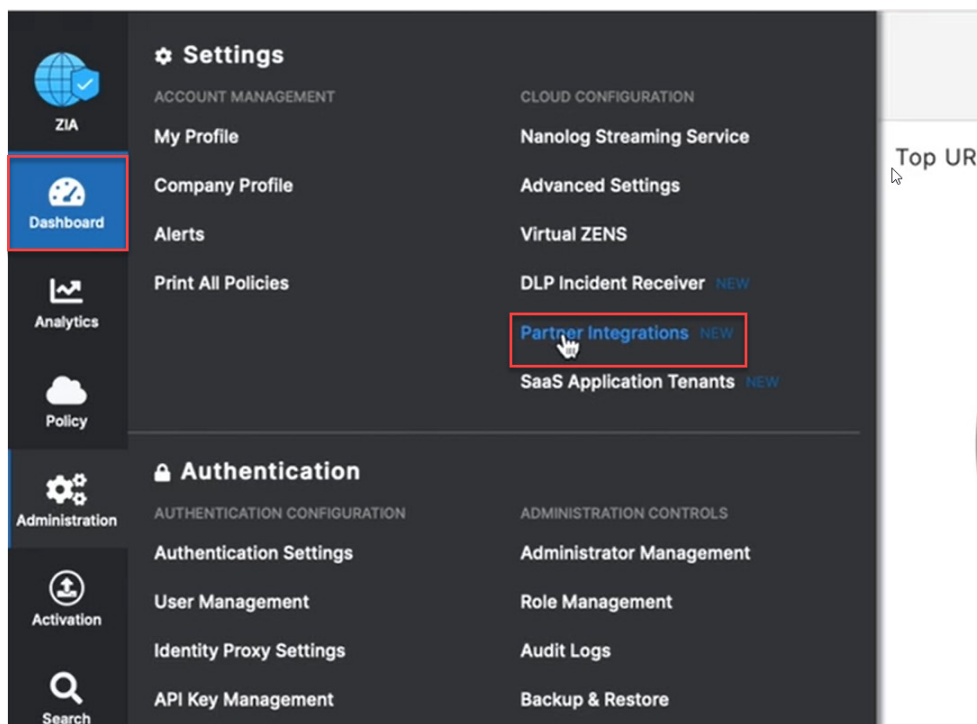


Figure 2. Zscaler Partner Integrations

2. Click the **Microsoft Defender for Endpoint** tab.

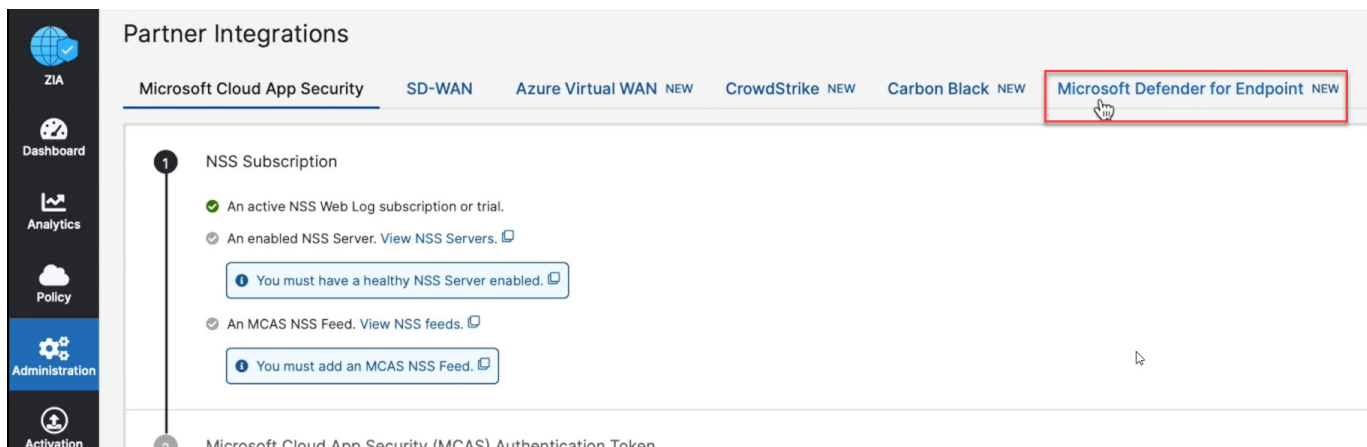


Figure 3. Microsoft Defender for Endpoint

3. Under **Authorize Microsoft Defender for Endpoint**, click **Provide Admin Credentials**. The **Microsoft Defender for Endpoint** portal appears.

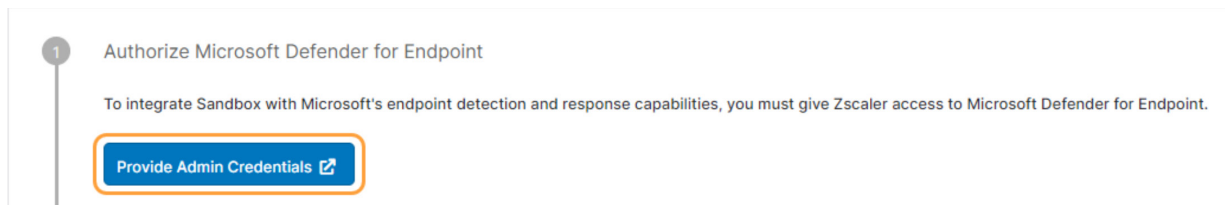


Figure 4. Authorize Microsoft Defender

4. Log in to Microsoft Defender for Endpoint.

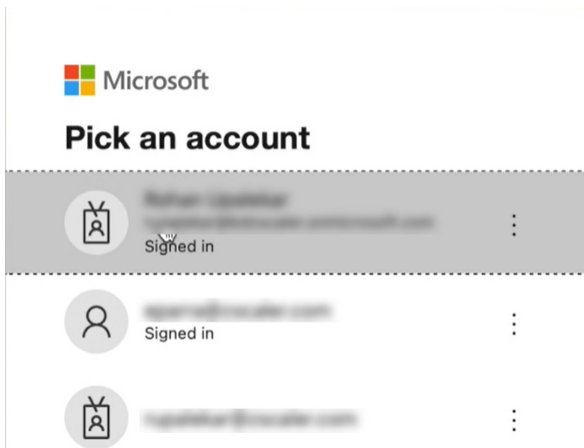


Figure 5. Log in to Microsoft Defender

5. Review the required permissions for the Zscaler service to access Microsoft Defender for Endpoint and click **Accept**.

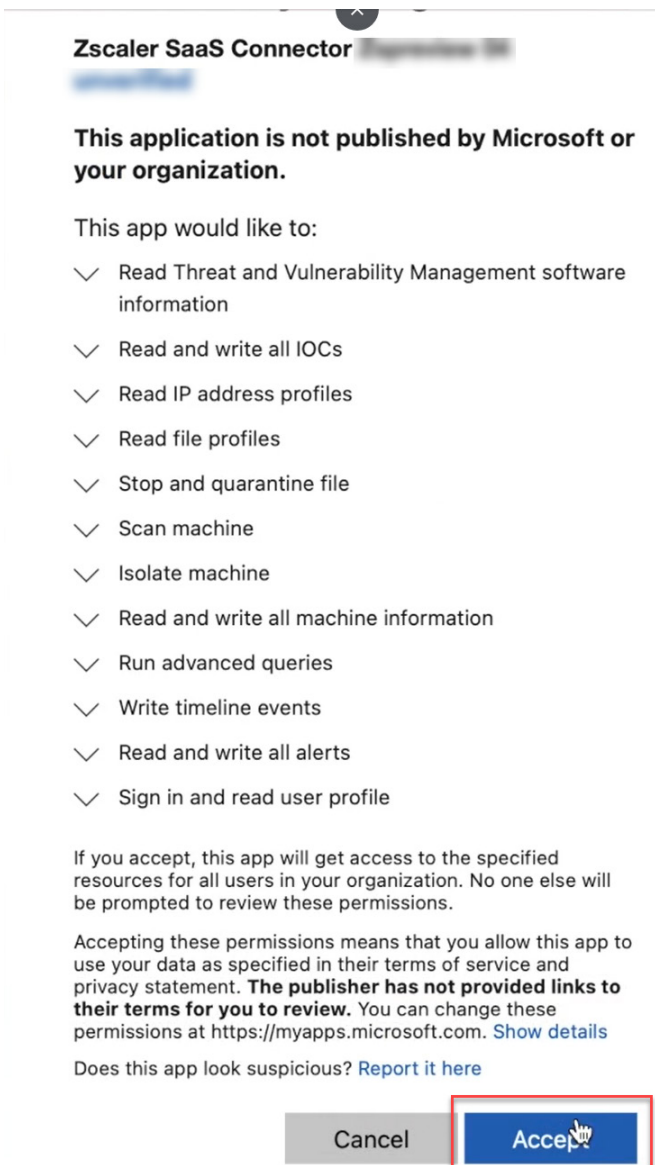


Figure 6. Accept Microsoft Defender permissions

After the authorization is complete, the **Zscaler SaaS Connector** and **Directory (Tenant) ID** appear.

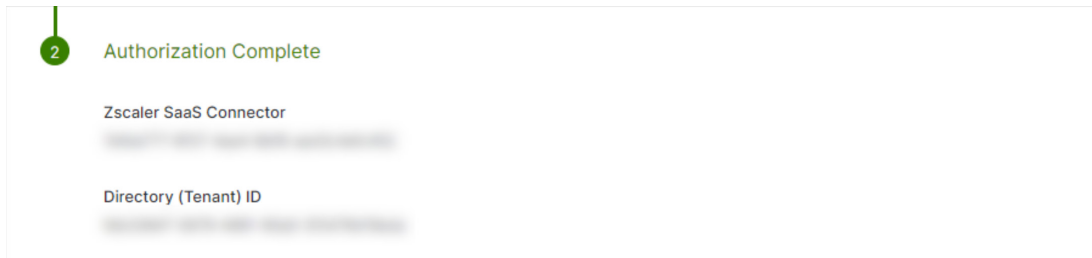


Figure 7. Authorization Complete

6. Click **Save**.

If your Microsoft Defender for Endpoint credentials are valid, the Zscaler service calls the Microsoft Defender for Endpoint APIs and syncs your endpoint hits to the Zscaler service. You then can view file and endpoint information in the Microsoft Defender Endpoint Hits report.

ZIA Hits Report

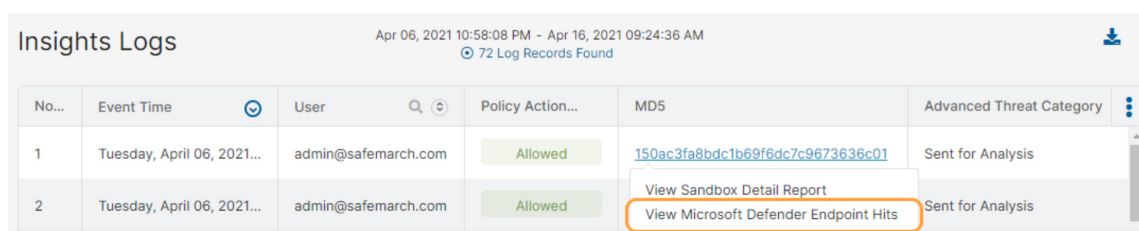
If you integrated with Microsoft Defender for Endpoint, you can view information on endpoints that have been exposed to a potentially malicious file. After the Sandbox analyzes a file, click the MD5 hash and view the Microsoft Defender Endpoint Hits report. The Microsoft Defender Endpoint Hits report provides visibility into all the endpoints installed and detected with Microsoft Defender for Endpoint. The Microsoft Defender for Endpoint integration leverages the Microsoft advanced threat hunting, incident response, and EDR capabilities and allows you to quarantine endpoints detected with the indicator of compromise (IoC). This IoC enrichment is important for:

- Tracing patient 0 events if the Zscaler service is configured to allow unknown files while sandboxing.
- Threat hunting to prevent attackers from spreading malware and moving laterally across your network.
- Incident responses from an infection caused by lateral movement or an out-of-band channel (e.g., USB).

After the integration is configured, admins can go to the Microsoft Defender for Endpoint portal to get more contextual information about the detection of the IoC or indicator of attack (IoA) before deciding to quarantine the endpoint or take remedial action.

Viewing the Microsoft Defender Endpoint Hits Report

To view the Microsoft Defender Endpoint Hits report, click the MD5 hash for any file analyzed by Sandbox and choose **View Microsoft Defender Endpoint Hits**.



No...	Event Time	User	Policy Action...	MD5	Advanced Threat Category
1	Tuesday, April 06, 2021...	admin@safemarch.com	Allowed	150ac3fa8bdc1b69f6dc7c9673636c01	Sent for Analysis
2	Tuesday, April 06, 2021...	admin@safemarch.com	Allowed	150ac3fa8bdc1b69f6dc7c9673636c01	Sent for Analysis

Figure 8. Insights Logs

About the Microsoft Defender Endpoint Hits Report

In the Microsoft Defender Endpoint Hits report, you can view file and endpoint information from the Zscaler service and Microsoft Defender for Endpoint.

Sandbox File Properties (Zscaler)

In this section, you can view general information about the file from the Zscaler Sandbox analysis. The following information appears:

- **Sandbox Category:** The type of file. The following categories appear:
 - **Sandbox Adware:** Files that automatically render advertisements and install adware.
 - **Sandbox Malware/Botnet:** Files that behave like APTs, exploits, botnets, trojans, keyloggers, spyware, and other malware.
 - **Sandbox P2P/Anonymizer:** Files that contain anonymizers and P2P clients.
- **Sandbox Score:** The threat score determined from the Sandbox analysis.
- **Threat Name:** The threat name of the file. Click to go to the Zscaler Threat Library to learn more about the file.
- **File Type:** The type of file (e.g., Windows executable).
- **File Size:** The total bytes of the file.

- **MD5:** The MD5 hash of the file. Click to view the Sandbox Detail Report.
- **SHA-1:** The SHA-1 hash of the file. You can use it to find identical files.
- **SHA-256:** The SHA-256 hash of the file. You can use it to find identical files.
- **SSDEEP:** The ssdeep hash of the file. You can use it to find partial matches with other suspicious files.

Microsoft Defender Endpoint Hits

Sandbox File Properties (Zscaler)

Sandbox Category	Malware & Botnet	MD5	dfd626e933cc64b01074658508bfaa67
Sandbox Score	94	SHA-1	35fc18284b0aaef8bcf1918c9e3183fb4ae6c439
Threat Name	Win32.Backdoor.NetKeylogger	SHA-256	847c030f176e747d392719d11ce823afaa89ea26762b2b109989c04235191ab
File Type	Windows Executable	SSDEEP	384:XTGaRlorFBIFKx5v38y3QLp29Jub/mPkaVikrTMNokpkjUo16+Dy:XSJorvjxZPAgyQRt/7Juo1M
File Size	22016		

File Detected on 2 Endpoints (Microsoft Defender for Endpoint)

Prevent Future Executions

Microsoft Defender Agent ID	Hostname	Internal...	OS Version	File Status	Last Seen		Endpoint Status	Actions
0542835239732ecce2f87f9a726c4bfa4f...	md-atp-11	10.2.1.13	Windows10.19...	Seen	10/06/2021, 03:27 PM		Active	Download, Block, Alert
4973309f7d8835fd764859eb34ff174a03b...	md-atp-9	10.2.1.11	Windows10.19...	Seen	10/04/2021, 04:45 PM		Active	Download, Block, Alert

Figure 9. Microsoft Defender Endpoint Hits—Sandbox File Properties

File Detected on Endpoints (Microsoft Defender for Endpoint)

A list of endpoints on which the file was detected via Microsoft Defender for Endpoint.

Microsoft Defender Endpoint Hits

Sandbox File Properties (Zscaler)

Sandbox Category	Malware & Botnet	MD5	dfd626e933cc64b01074658508bfaa67
Sandbox Score	94	SHA-1	35fc18284b0aaef8bcf1918c9e3183fb4ae6c439
Threat Name	Win32.Backdoor.NetKeylogger	SHA-256	847c030f176e747d392719d11ce823afaa89ea26762b2b109989c04235191ab
File Type	Windows Executable	SSDEEP	384:XTGaRlorFBIFKx5v38y3QLp29Jub/mPkaVikrTMNokpkjUo16+Dy:XSJorvjxZPAgyQRt/7Juo1M
File Size	22016		

File Detected on 2 Endpoints (Microsoft Defender for Endpoint)

Prevent Future Executions







Microsoft Defender Agent ID	Hostname	Internal...	OS Version	File Status	Last Seen		Endpoint Status	Actions
0542835239732ecce2f87f9a726c4bfa4f...	md-atp-11	10.2.1.13	Windows10.19...	Seen	10/06/2021, 03:27 PM		Active	  
4973309f7d8835fd764859eb34ff174a03b...	md-atp-9	10.2.1.11	Windows10.19...	Seen	10/04/2021, 04:45 PM		Active	  

Figure 10. File detected on Microsoft Defender Endpoint

- **Microsoft Defender Agent ID:** The ID of Microsoft Defender agent installed on the host.
- **Hostname:** The name of the host.
- **Internal IP:** The internal IP address of the host.
- **External IP:** The external IP address of the host.
- **OS Version:** The operating system and version of the host.
- **First Seen:** The first time the file was detected on the endpoint.
- **Last Seen:** The last time the file was detected on the endpoint. You can sort this column.
- **File Status:** The status of the file.
 - **Seen:** The Microsoft Defender agent saw the file on the host.
 - **Detected:** The Microsoft Defender agent triggered a detection based on a process or an operation associated with the file.

- **Quarantined:** The Microsoft Defender agent stopped the ongoing processes of the file and removed it from the host.
- **Remediated:** The Microsoft Defender agent used [AIR](#) capabilities to remediate the file.
- **Endpoint Status:** The status of the endpoint. The following states appear:
 - **Active:** The endpoint is not quarantined.
 - **Isolated:** The endpoint is quarantined.
- **Actions:** Call the Microsoft Defender for Endpoint API to perform one of the following actions.
 - **Isolate:** Click to quarantine the endpoint. This option only appears if the endpoint status is Active.

The screenshot displays the 'Microsoft Defender Endpoint Hits' window. It features a 'Sandbox File Properties (Zscaler)' section with details like Malware & Botnet category, a score of 94, and a threat name 'Win32.Backdoor.NetKeylogger'. Below this is a table titled 'File Detected on 2 Endpoints (Microsoft Defender for Endpoint)' with columns for Agent ID, Hostname, Internal IP, OS Version, File Status, Last Seen, Endpoint Status, and Actions. Two endpoints are listed, both with 'Active' status. An arrow points from the 'Isolate Host' button in the Actions column to the 'Isolate Host' text below the table.

Figure 11. Isolate Host

- **Stop Current Executions:** Click to stop any ongoing processes associated with the file on the endpoint.

This screenshot is identical to Figure 11, showing the same file properties and endpoint table. However, the 'Kill ongoing execution & quarantine the file' button in the Actions column is highlighted with a red box, and an arrow points from this button to the text 'Kill ongoing execution & quarantine the file' located below the table.

Figure 12. Stop ongoing execution and quarantine file

- **Trigger Alert & Start AIR:** Click to trigger an alert and start AIR on the endpoint. To learn more about configuring AIR, see the [Microsoft Defender for Endpoint documentation](#).

The screenshot shows the 'Microsoft Defender Endpoint Hits' window. It contains two main sections:

Sandbox File Properties (Zscaler)

Sandbox Category	Malware & Botnet	MD5	dfd626e933cc64b01074658508bfaa67
Sandbox Score	94	SHA-1	35fc18284b0aeaf8bcf1918c9e3183fb4ae6c439
Threat Name	Win32.Backdoor.NetKeylogger	SHA-256	847c030f176e747d392719d11ce823fafa89ea26762b2b109989c04235191ab
File Type	Windows Executable	SSDEEP	384:XTGaRlorFBIFKx5v38y3QLp29Jub/mPkaVikvtMNokpkjUo16+Dy:XSJorvjxZPAgyQRU7jUo1M
File Size	22016		

File Detected on 2 Endpoints (Microsoft Defender for Endpoint)

Microsoft Defender Agent ID	Hostname	Internal...	OS Version	File Status	Last Seen	Endpoint Status	Actions
0542835239732ecce2f87f9a726c4bfa4f...	md-atp-11	10.2.1.13	Windows 10.19...	Seen	10/06/2021, 03:27 PM	Active	
4973309f7d8835fd64859eb34ff174a03b...	md-atp-9	10.2.1.11	Windows 10.19...	Seen	10/04/2021, 04:45 PM	Active	

Below the table, there is a button labeled 'Prevent Future Executions' and a link 'Generate alert and trigger AutoIR'.

Figure 13. Generate alert and trigger

- **Prevent Future Executions:** Click to stop any future processes of the file on all endpoints.

The screenshot shows the 'Microsoft Defender Endpoint Hits' window, similar to Figure 13, but with an additional button 'Prevent Future Executions' highlighted in the top right corner of the table section. The table data is the same as in Figure 13.

Figure 14. Prevent future executions

ZPA Posture Type

In this use case:

- ZPA verifies the presence of a running Microsoft Defender process on the endpoint as an assessment of end device posture. You can configure ZPA to allow only compliant endpoints (ones that pass the posture check) to access selected applications.
- ZPA evaluates ZPA access policies for conditional access. The policies, in turn, reference device-level posture check profiles. The ZPA administrator can specify (for Windows and macOS workstations) that a Microsoft Defender agent must be installed and running on the endpoint so that the endpoint can grant access to internal applications referenced via ZPA access policy.

See the following conceptual diagram for an overview of the integration.

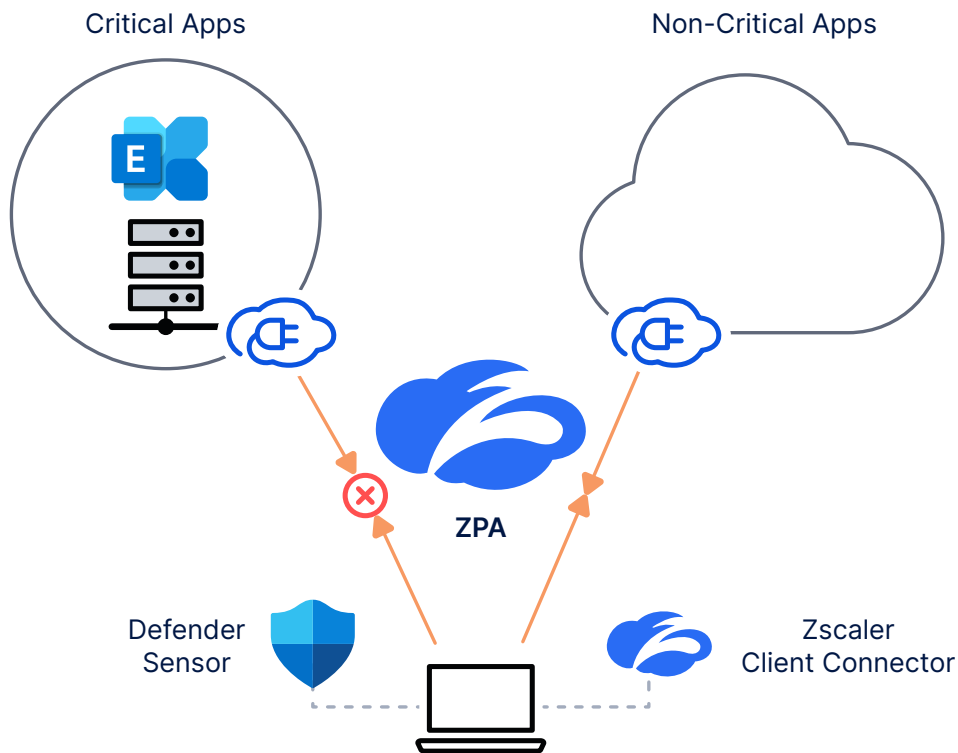
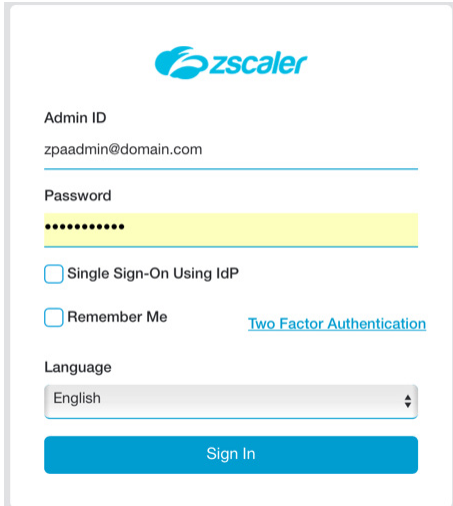


Figure 15. ZPA and Microsoft Defender overview

Configuring ZPA

This guide assumes that you have a working ZPA setup and provides instructions to integrate posture-based conditional access as part of your existing ZPA deployment.

Log in to ZPA Admin Portal



The login form for the Zscaler ZPA Admin Portal. It features the Zscaler logo at the top. Below the logo, there are fields for 'Admin ID' (containing 'zpaadmin@domain.com') and 'Password' (masked with dots). There are two checkboxes: 'Single Sign-On Using IdP' and 'Remember Me'. A link for 'Two Factor Authentication' is next to the 'Remember Me' checkbox. A 'Language' dropdown menu is set to 'English'. A blue 'Sign In' button is at the bottom.

Figure 16. Log into ZPA Admin Portal

Go to the Zscaler Client Connector

Click the Client Connector icon to open the Zscaler Client Connector.

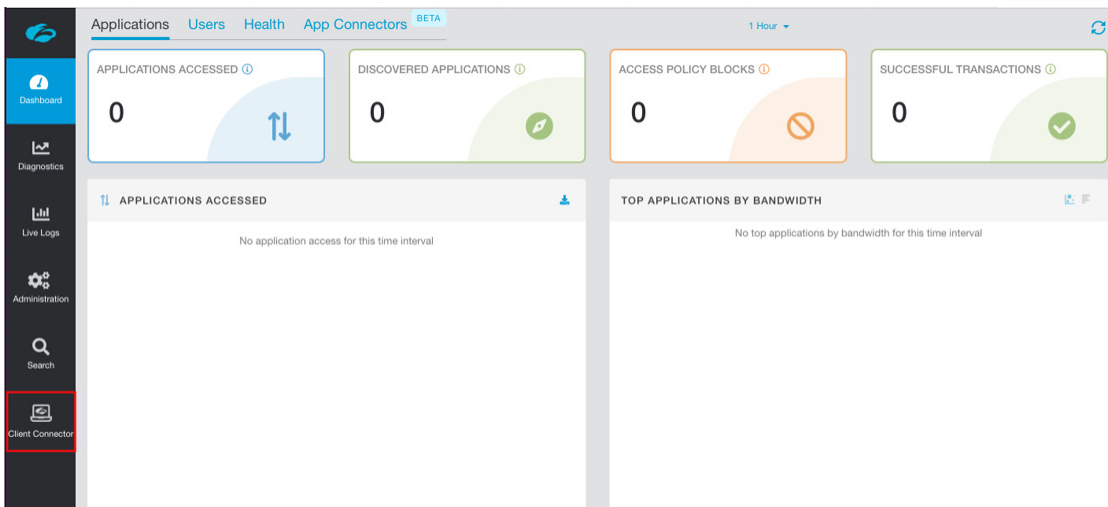


Figure 17. Click the Client Connector icon

Create a New Posture Profile

Log in to the Zscaler Client Connector and go to **Administration > Device Posture**. Then click **Add Device Posture Profile**.

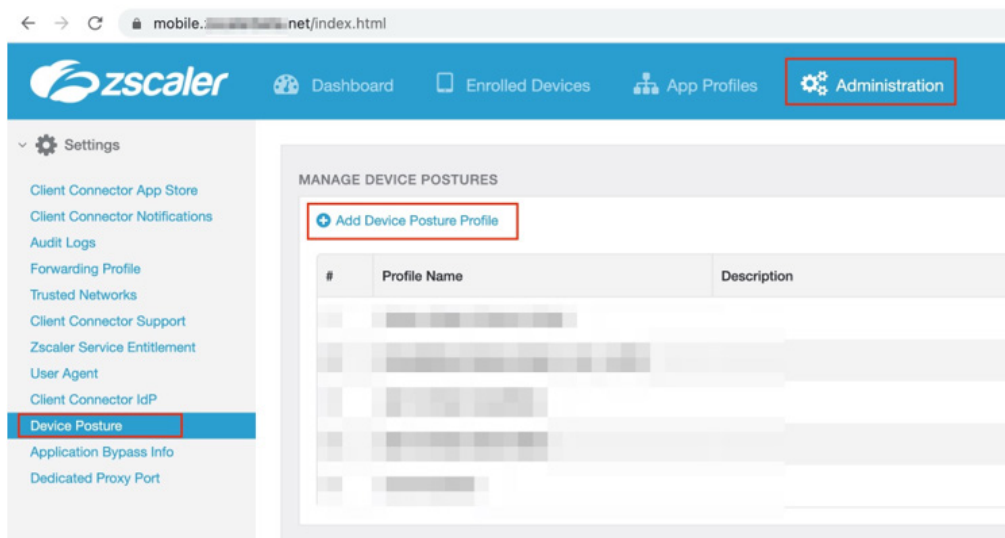


Figure 18. Add a device posture profile

Add New Microsoft Defender Posture Profile

Complete the following steps:

1. Enter a **Name** for this policy.
2. Select only **Windows**, **macOS**, or both.
3. Click the **Posture Type** drop-down menu.
4. Select **Detect Microsoft Defender**.
5. Click **Save**.

This posture profile is referenced in a ZPA access policy. You can set up access policies to allow or deny application access based on whether the posture check passes or fails.

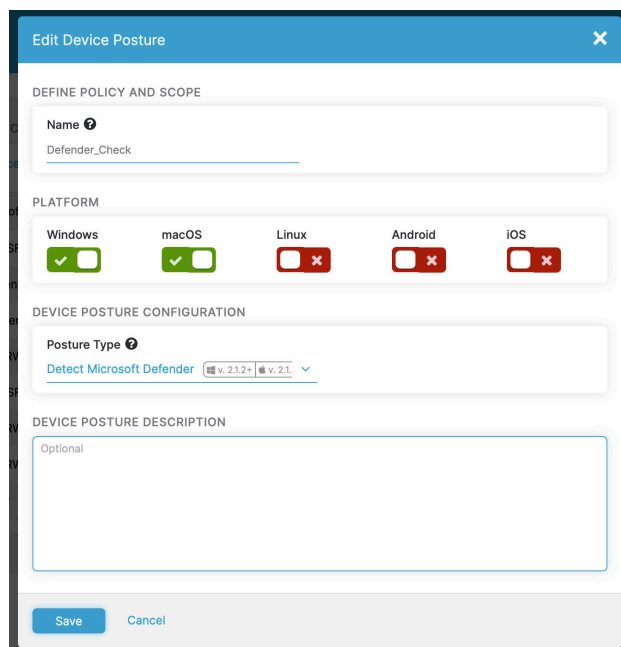


Figure 19. Add a detect Microsoft Defender posture profile

Decide Which Applications Need Conditional Access

Within the ZPA Admin Portal, go to **Administration > Application Segment**.

This page lists which applications are accessed by ZPA. Select one of these applications and reference it in an access policy so that access to it is granted based on the end device's posture.

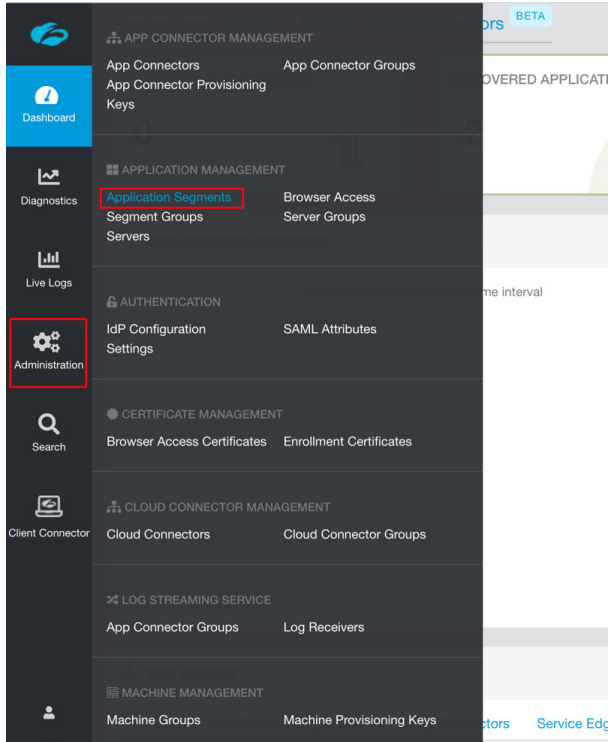


Figure 20. Go to application segments

In this example, ZPA can access applications hosted under the domain `*.bd-dev.com`, based on the posture of the end device.

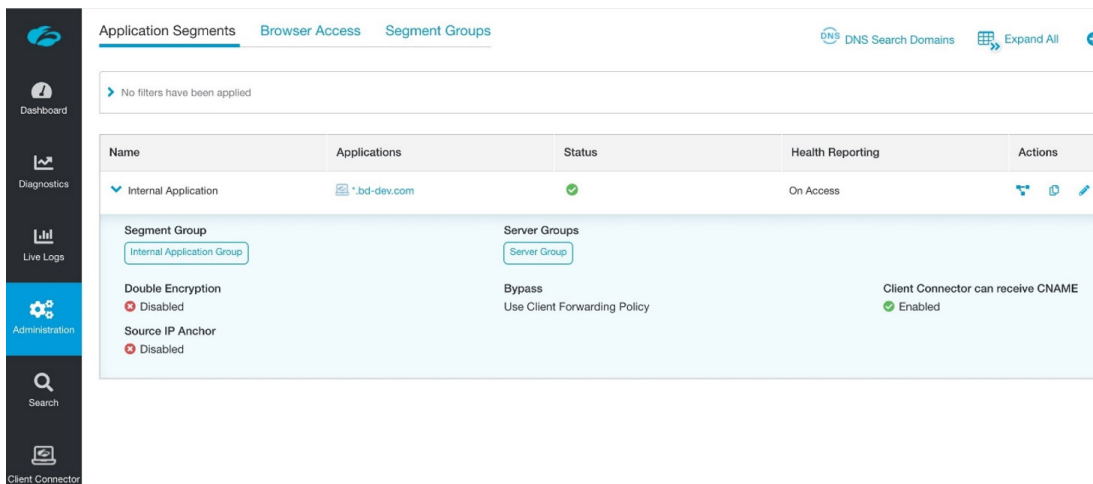


Figure 21. Decide which application needs conditional access

Set Up an Access Policy

Within the ZPA Admin Portal, go to **Administration > Access Policy**.

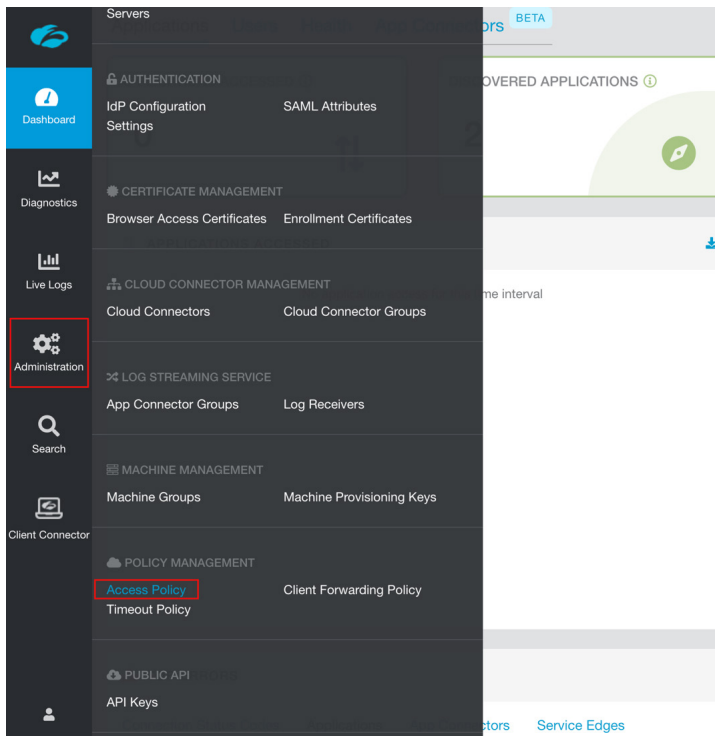


Figure 22. Open access policy configuration dialog

Tie the Posture Profile to this Access Policy

Create a new access policy by clicking **Add Rule** and reference the previously created posture profile. Customers can set up different access policies to protect different internal applications. You can set up a customizable (and optional) message to the end users when application access is allowed or denied, informing them about the policy evaluation.

In this example, an access policy has been added to block user access to the application if the Microsoft Defender posture check fails (Rule#1). If Microsoft Defender is not running on the endpoint, Rule#1 is marked true and access is blocked. Otherwise, the policy evaluation proceeds to Rule#2 (which grants application access).

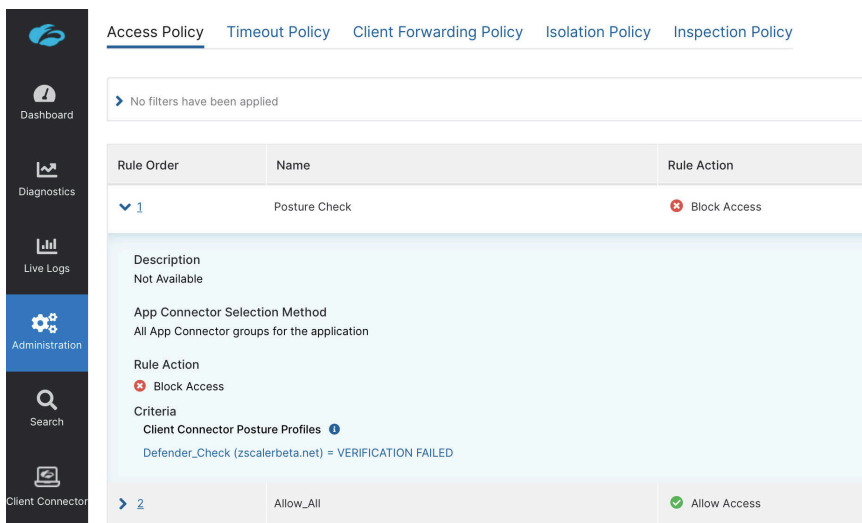


Figure 23. Set up an access policy

Verify Conditional Access from an Endpoint

The endpoint accesses the application if the endpoint device has a Microsoft Defender agent installed and running. Otherwise, the access is blocked by ZPA.

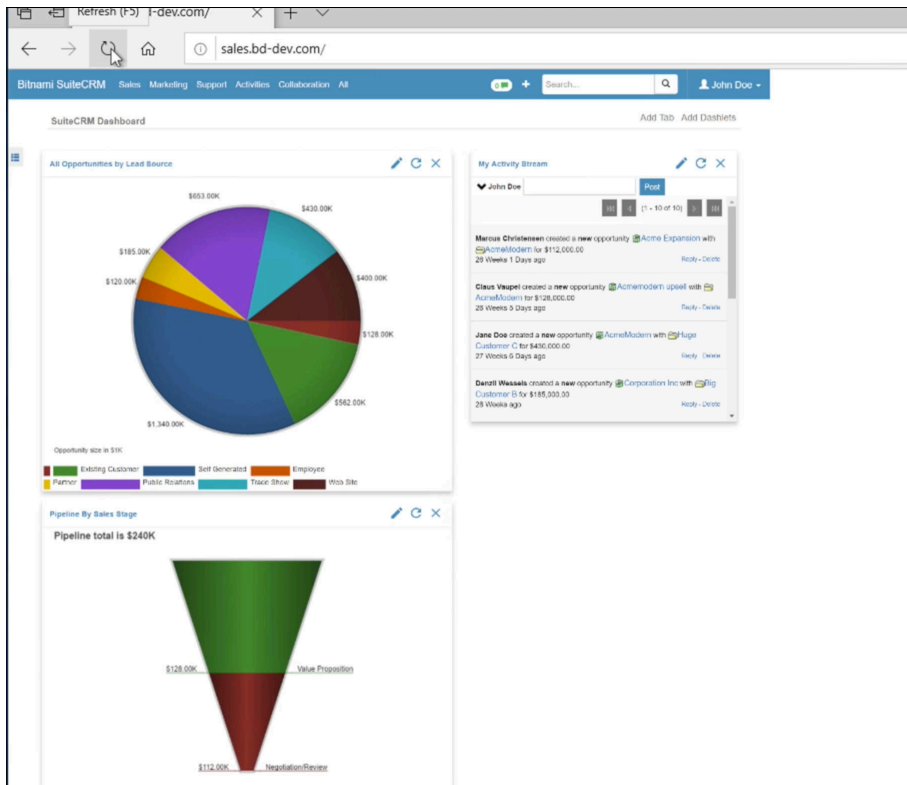


Figure 24. Access granted from an endpoint with the Microsoft Defender agent installed and running

The following image shows access blocked from an endpoint without Microsoft Defender.

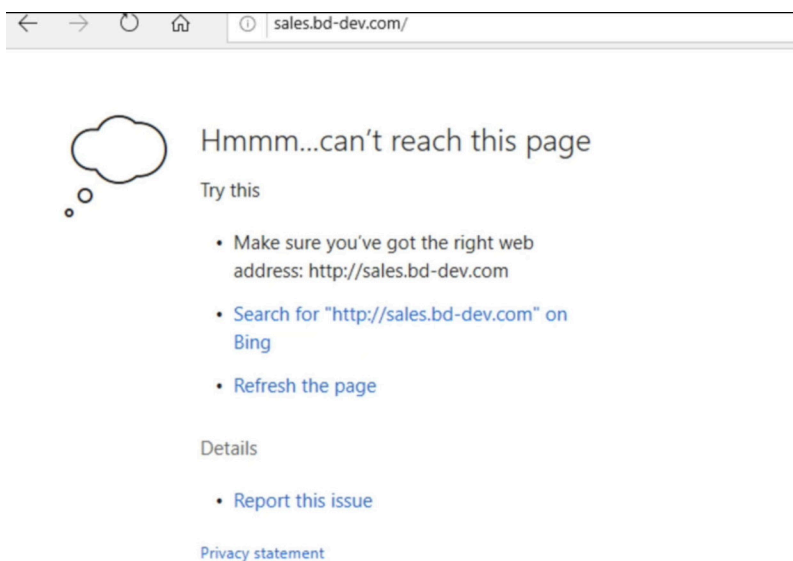


Figure 25. Access blocked from an endpoint if the Microsoft Defender agent is not running

Contextualizing Risk using Microsoft Defender for Endpoint and Avalor UVM

Avalor's Data Fabric and Unified Vulnerability Management (UVM) solution integrates, normalizes, and unifies data from various enterprise security and business systems to provide actionable insights, analytics, and operational efficiencies.

Avalor offers a preconfigured connectors for a variety of Microsoft services including Microsoft Defender for Endpoint, Microsoft Intune, Microsoft Defender for Cloud and Microsoft Azure (Assets and Blobs).

This guide specifically covers the following Microsoft Defender for Endpoint sources:

- Microsoft Defender for Endpoint – Vulnerabilities
- Microsoft Defender for Endpoint – Alerts
- Microsoft Defender for Endpoint – Assets
- Microsoft Defender for Endpoint – Software vulnerabilities by machine

The following steps outline how to start ingesting data from these sources, while also (optionally) combining Microsoft Defender for Endpoint Asset data with Microsoft Defender for Endpoint Vulnerability information to provide a more contextualized and personalized risk assessment for your organization.

Create an Entra ID App Registration for Programmatic Access to Microsoft Defender for Endpoint

To create an Entra ID:

1. Sign in to the Azure portal.
2. Go to **Microsoft Entra ID > App registrations > New registration**.

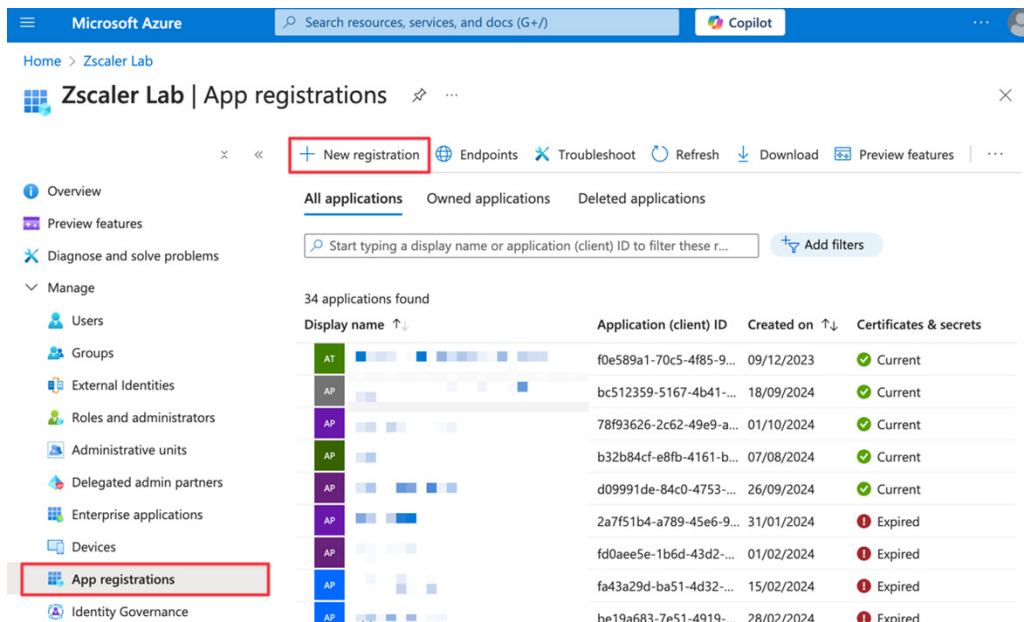


Figure 26. New registration

3. In the **Register an application** window, enter a **Name** for your application, click **Accounts in this organizational directory only**, and then select **Register**.

Microsoft Azure Search resources, services, and docs (G+/I) Copilot

Home > Zscaler Lab | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

app-avalor-demo

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Zscaler Lab only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Figure 27. Register an application

4. Enable programmatic access to Defender for Endpoint by selecting **API permissions** > **Add a permission**.

Microsoft Azure Search resources, services, and docs (G+/I) Copilot

Home > Zscaler Lab | App registrations > app-avalor-demo

app-avalor-demo | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems Favorites

API permissions

Manage Support + Troubleshooting

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) Grant admin consent for Zscaler Lab

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user ...	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Figure 28. Add a permission

5. Click **APIs my organization uses**, then search for `WindowsDefenderATP`, and click **WindowsDefenderATP**.

Request API permissions



Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

WindowsDefenderATP	
Name	Application (client) ID
WindowsDefenderATP	fc780465-2017-40d4-a0c5-307022471b92

Figure 29. APIs my organization uses

6. On the **Request API permissions** modal, click **Application permissions** and select the appropriate permissions for the Defender for Endpoint connector you want to set up from the following list. For example, for **Read all machine profiles**, search for `Machine.Read.All`.

For Assets connector:

Permission Type	Permission	Permission Display Name
Application	Machine.Read.All	Read all machine profiles

For Vulnerabilities / Vulns by Machine connector:

Permission Type	Permission	Permission Display Name
Application	Machine.Read.All	Read all machine profiles
Application	Vulnerability.Read.All	Read Threat and Vulnerability Management vulnerability information
Delegated (work or school account)	Vulnerability.Read	Read Threat and Vulnerability Management vulnerability information
Application	SecurityRecommendation.Read.All	Read Threat and Vulnerability Management security recommendation information
Delegated (work or school account)	SecurityRecommendation.Read	Read Threat and Vulnerability Management security recommendation information

For Alerts connector:

Permission Type	Permission	Permission Display Name
Application	Alert.Read.All	Read all alerts
Application	Alert.ReadWrite.All	Read and write all alerts
Delegated (work or school account)	Alert.Read	Read alerts'
Delegated (work or school account)	Alert.ReadWrite	Read and write alerts

7. Click the permission required, and then click **Add permissions**.

Request API permissions

[← All APIs](#)

WindowsDefenderATP

https://userrequestsgraphapi-prd.trafficmanager.net/

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Machine.Read.All

Permission	Admin consent required
Machine (1)	
<input checked="" type="checkbox"/> Machine.Read.All ⓘ Read all machine profiles	Yes

Add permissions

Discard

Add permissions

Figure 30. Add permissions

8. Click **Grant admin consent for <org name>**, then **Yes**. Ensure you have granted admin consent for each permission selected.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

☒ Grant admin consent for Zscaler Lab

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
WindowsDefenderATP (1)				...
Machine.Read.All	Application	Read all machine profiles	Yes	⚠ Not granted for Zscaler ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Figure 31. Grant admin consent

9. To add a secret to the application, select **Certificates & secrets**, then **+ New client secret**.

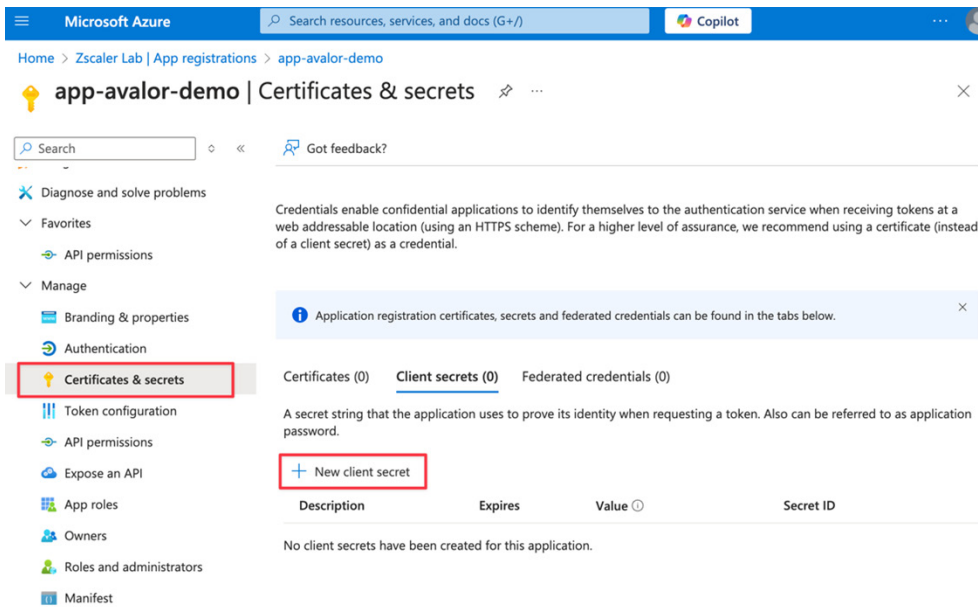


Figure 32. New client secret

10. Enter a **Description**, and then click **Add**.

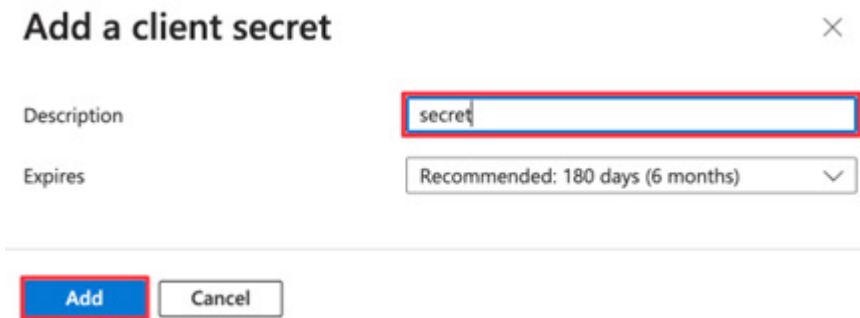


Figure 33. Add a client secret

11. Copy the **Secret Value**.

Configure the Microsoft Defender for Endpoint UVM Data Connectors

The following sections describe how to configure Microsoft Defender UVM data connectors.

Configure the Azure Defender for Endpoints—Assets Data Source

To configure the asset data source:

1. Log in to the Avalor UVM Platform
2. Click **Configure**.

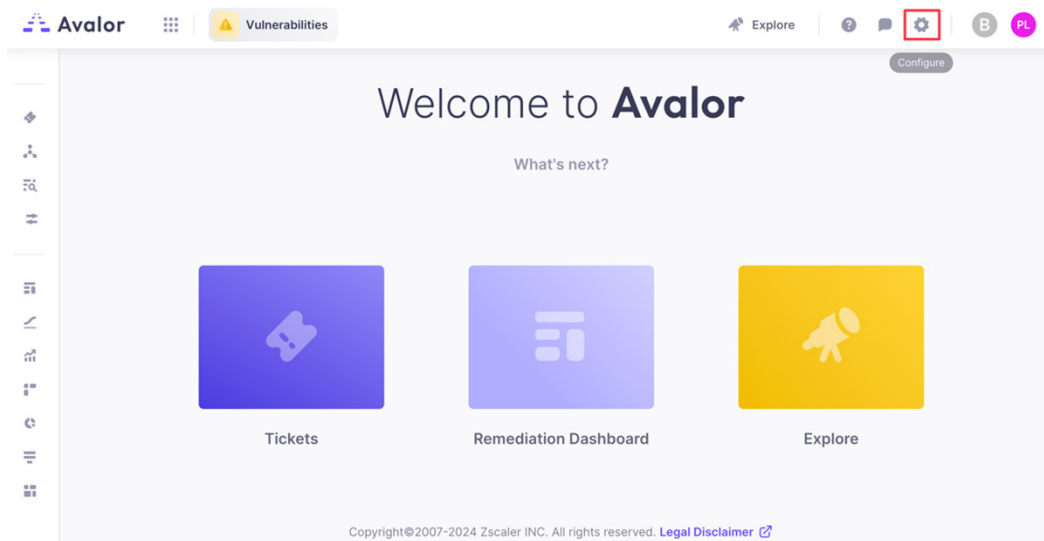


Figure 34. Configure

3. Click **Create**, then search for Azure Defender for Endpoints—Assets.

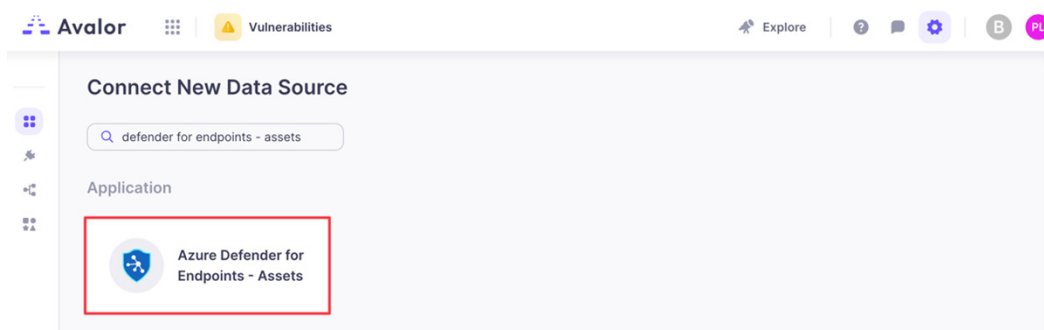


Figure 35. Azure Defender for Endpoints

4. Click the **Azure Defender for Endpoints—Assets** application.
5. On the **Create Azure Defender for Endpoints—Assets Source** page, complete the following:
 - a. **Name:** Enter a **Name** for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.

- c. **Resource URI:** Enter `https://api.securitycenter.microsoft.com/` or for better performance, you can select a server closer to your geolocation:
 - `https://api-us.securitycenter.microsoft.com/`
 - `https://api-eu.securitycenter.microsoft.com/`
 - `https://api-uk.securitycenter.microsoft.com/`
 - `https://api-au.securitycenter.microsoft.com/`
- d. **Directory (tenant) ID:** Enter the **Directory ID** from the Overview section of the App registration you created earlier.

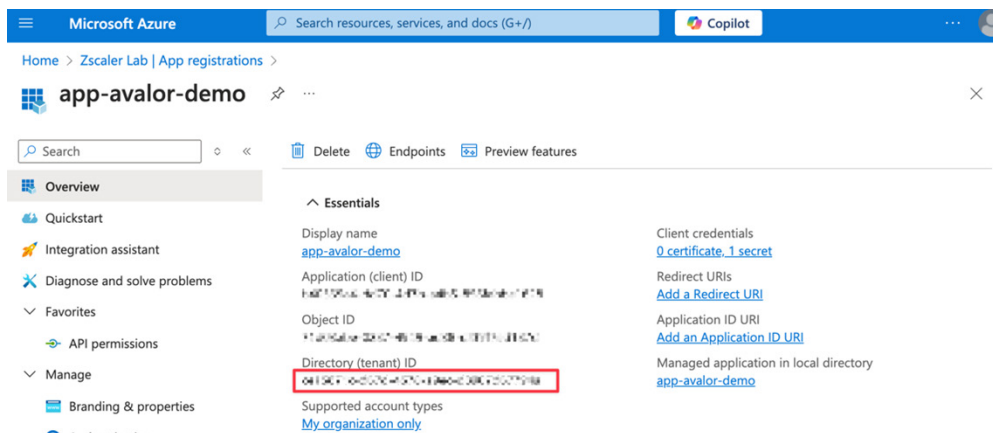


Figure 36. Directory ID

- e. **Application (client) ID:** Enter the **Application (client) ID** from the Overview section of the App registration you created earlier.

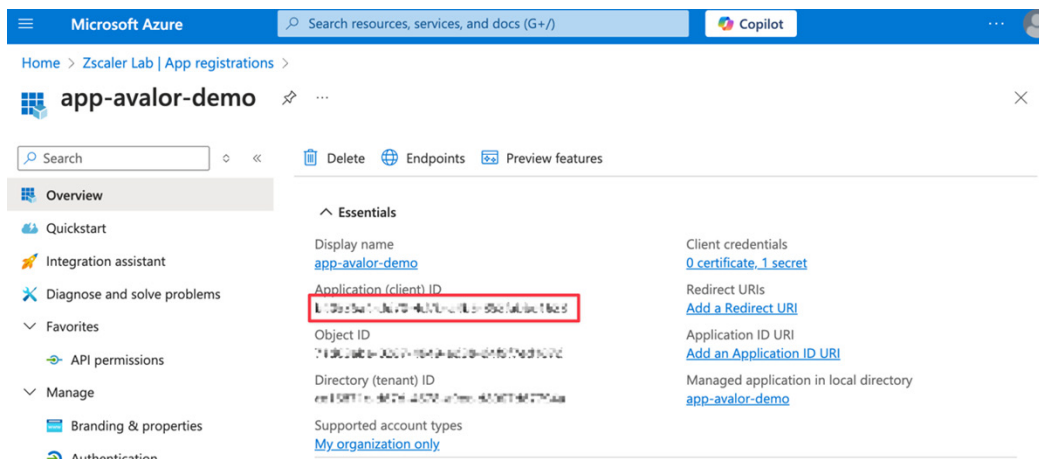


Figure 37. Application ID

- f. **Client Secret:** Enter the **Secret Value** from the App registration.
- g. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
- h. **Remediation Detection Settings:** Select your desired option to determine when findings automatically become undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
- i. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials have been entered in correctly, the system responds with Test Passed.

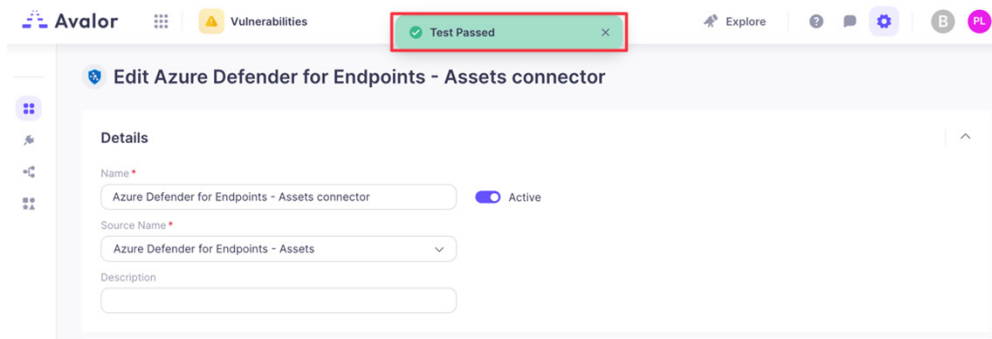


Figure 38. Test Passed

7. Click **Save**.

Avalor Vulnerabilities Explore

Edit Azure Defender for Endpoints - Assets connector

Details

Name: Azure Defender for Endpoints - Assets connector ☒ Active

Source Name: Azure Defender for Endpoints - Assets

Description:

Retrieval

Resource URI: https://api.securitycenter.microsoft.com/

Directory (Tenant) ID: [redacted]

Application (Client) ID: [redacted]

Client Secret: [redacted]

Scheduling

Full Refresh Frequency: Daily

Time (UTC): 12:00 AM

Remediation Detection Settings

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting.

Aging criteria [+ Add Rule](#)

☐ Age immediately if Finding was not seen, while Asset was seen in the latest data refresh

Fallback

☐ Age immediately if Finding was not seen for day(s)

Advanced Settings

Suppression Rules

Select Field Contains Type Value

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 39. Advanced Settings

Configure the Azure Defender for Endpoints—Vulnerabilities Data Source

To configure vulnerabilities data sources in the Azure Defender for endpoints:

1. Log in to the Avalor UVM Platform
2. Click **Configure**.

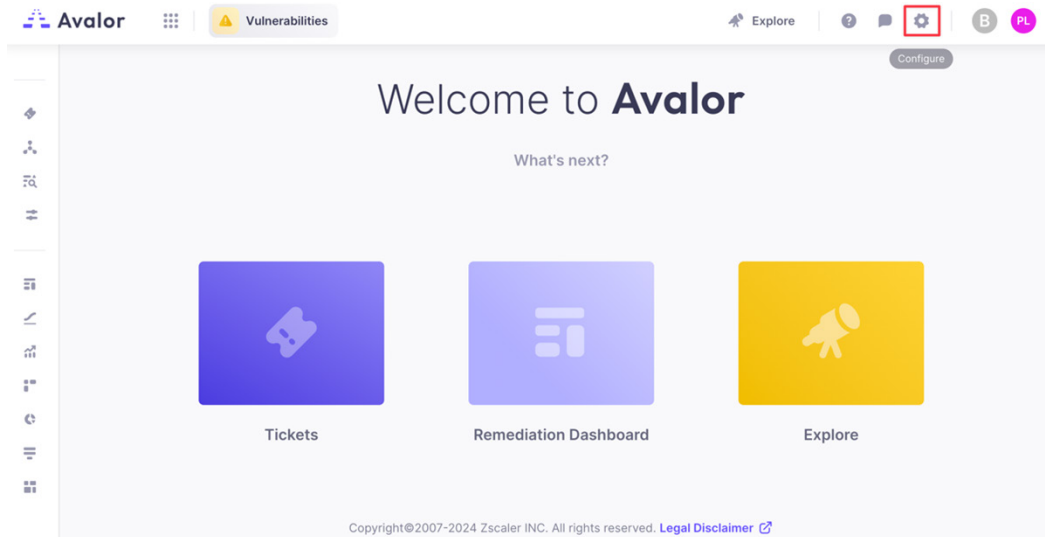


Figure 40. Configure

3. Click **Create**, then search for Azure Defender for Endpoints—Vulnerabilities.

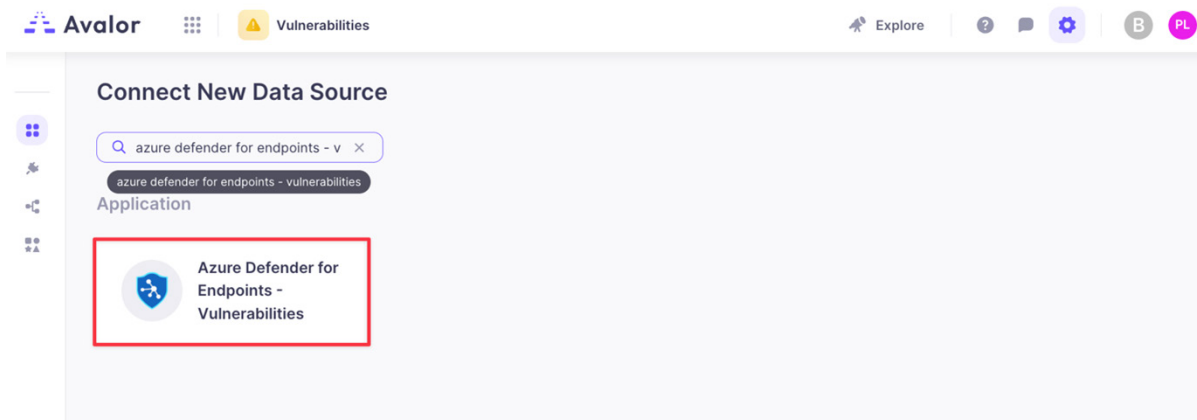


Figure 41. Azure Defender for Endpoints—Vulnerabilities

4. Click the **Azure Defender for Endpoints—Vulnerabilities** application.
5. On the **Create Azure Defender for Endpoints—Vulnerabilities Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Resource URI:** Enter `https://api.securitycenter.microsoft.com/` or for better performance, you can select a server closer to your geolocation:
 - `https://api-us.securitycenter.microsoft.com/`
 - `https://api-eu.securitycenter.microsoft.com/`
 - `https://api-uk.securitycenter.microsoft.com/`
 - `https://api-au.securitycenter.microsoft.com/`

- d. **Directory (tenant) ID:** Enter the Directory ID from the Overview section of the App registration you created earlier.

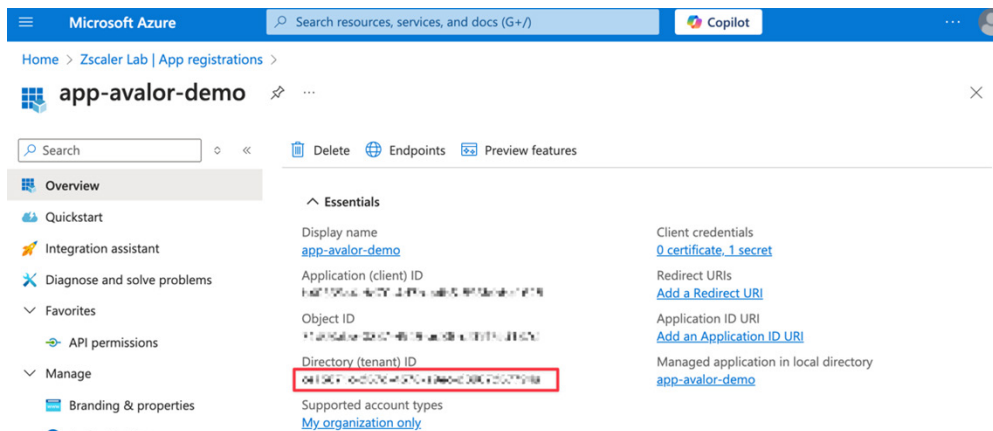


Figure 42. Directory ID

- e. **Application (client) ID:** Enter the Application (client) ID from the Overview section of the App registration you created earlier.

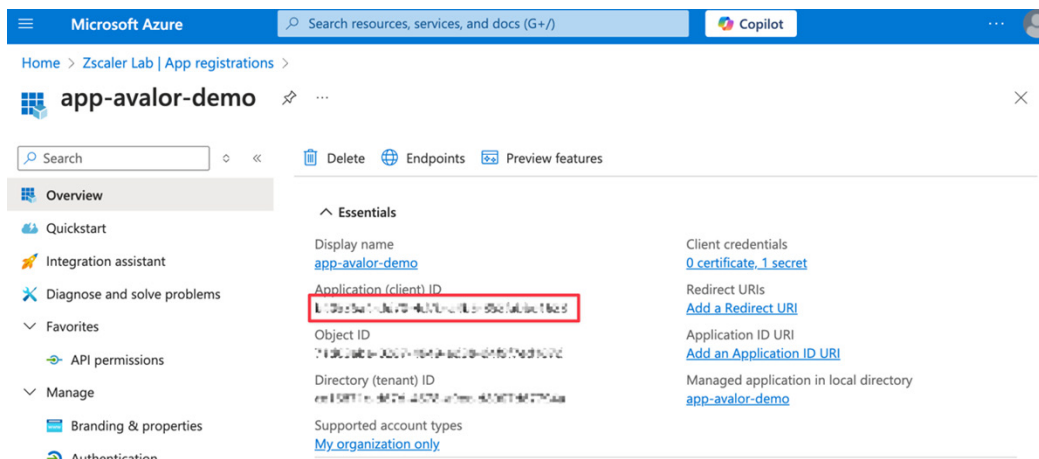


Figure 43. Application ID

- f. **Client Secret:** Enter the **Secret Value** from the App registration.
- g. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
- h. **Remediation Detection Settings:** Select your desired option to determine when findings automatically become undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
- i. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials have been entered correctly, the system responds with **Test Passed**.

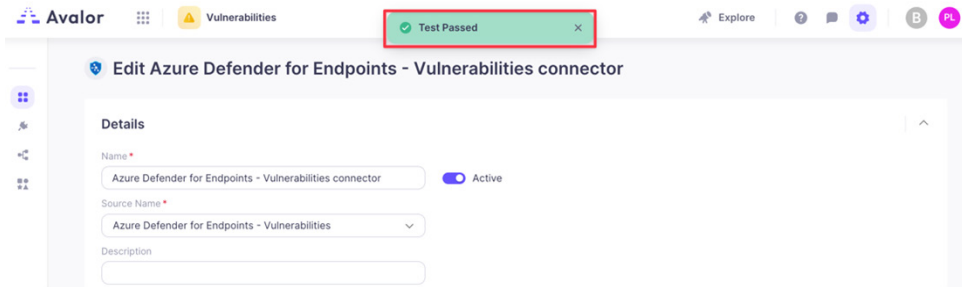


Figure 44. Test Passed

- Click **Save**.

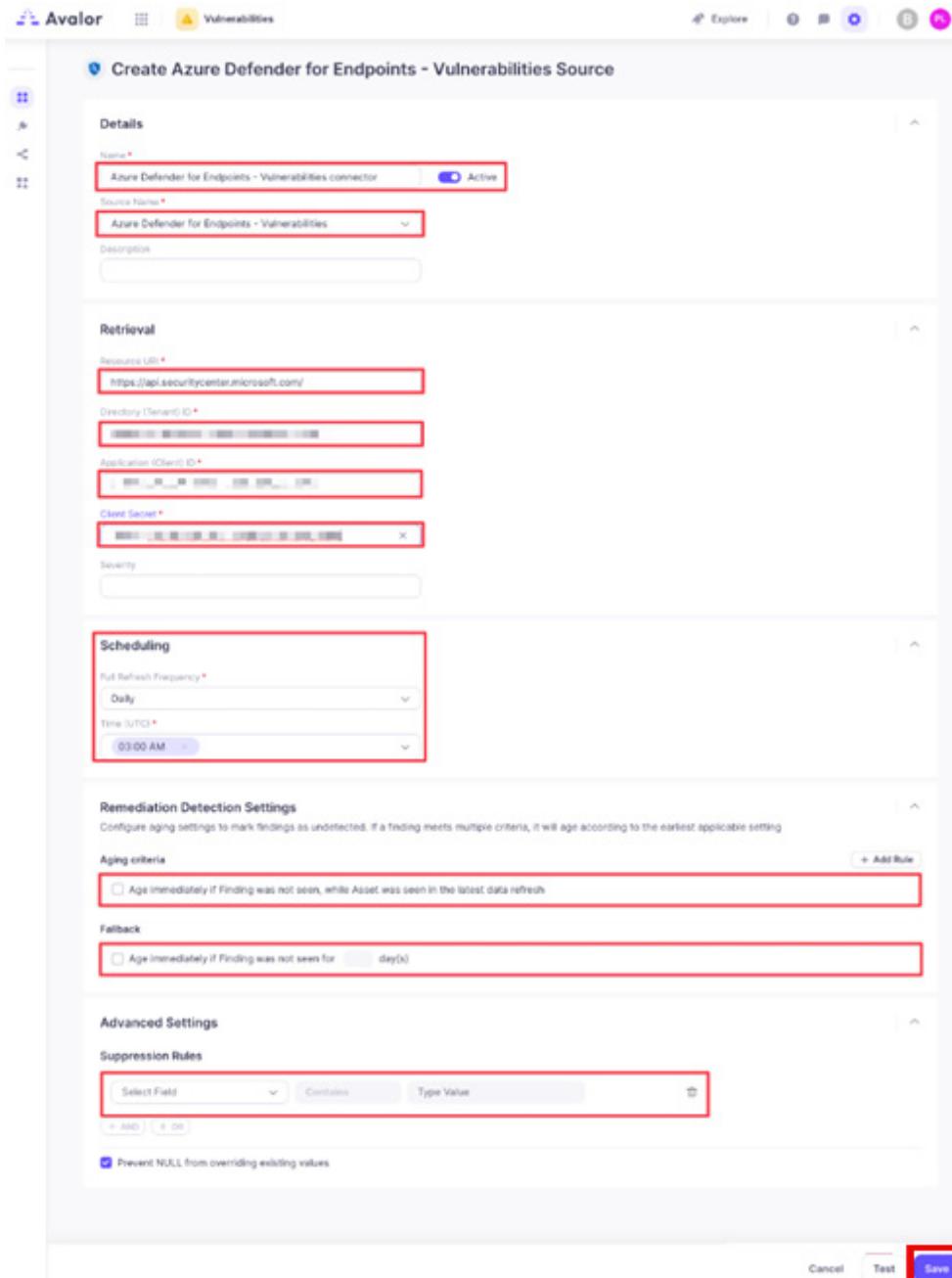


Figure 45. Advanced Settings

Configure the Azure Defender for Endpoints—Alerts Data Source

To configure Alerts data source for Azure Defender for endpoints:

1. Log in to the Avalor UVM Platform
2. Click **Configure**.

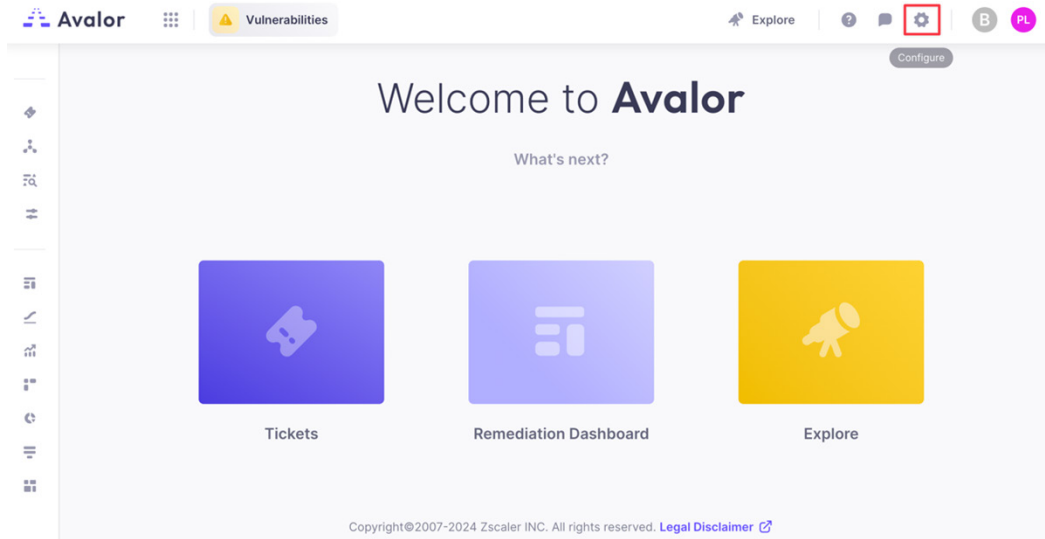


Figure 46. Configure

3. Click **Create**, then search for Azure Defender for Endpoints—Alerts.

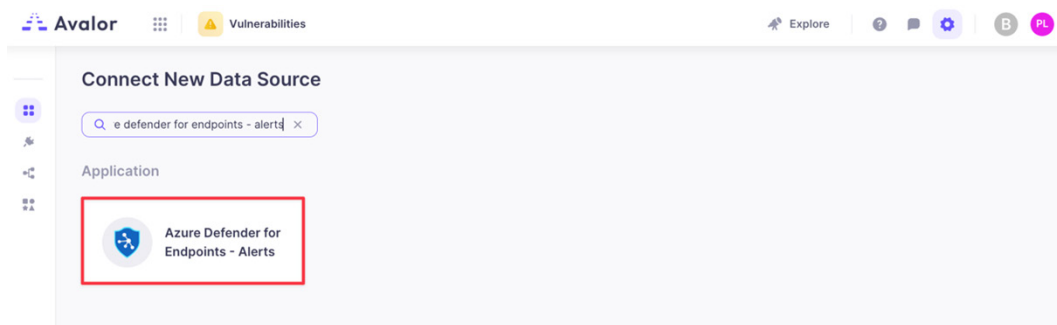


Figure 47. Azure Defender for Endpoints

4. Click the **Azure Defender for Endpoints—Alerts** application.
5. On the **Create Azure Defender for Endpoints—Alerts Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Resource URI:** Enter `https://api.securitycenter.microsoft.com/` or for better performance, you can select a server closer to your geolocation:
 - `https://api-us.securitycenter.microsoft.com/`
 - `https://api-eu.securitycenter.microsoft.com/`
 - `https://api-uk.securitycenter.microsoft.com/`
 - `https://api-au.securitycenter.microsoft.com/`

- d. **Directory (tenant) ID:** Enter the Directory ID from the Overview section of the App registration you created earlier.

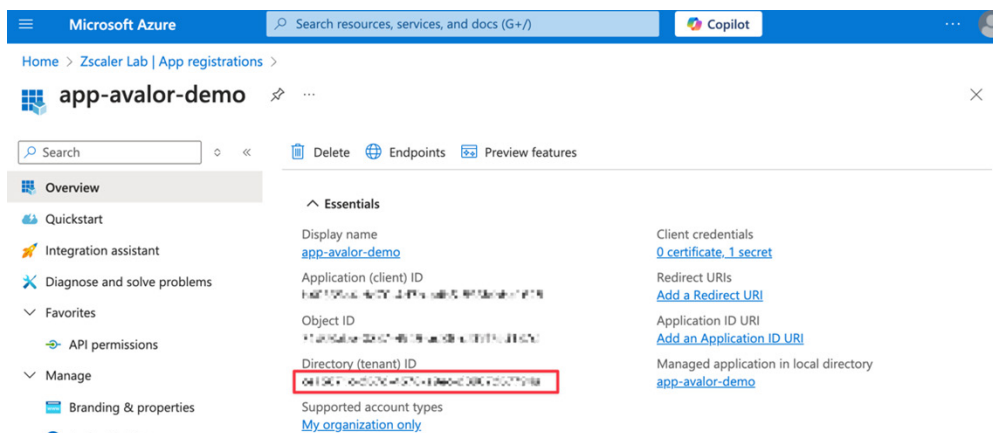


Figure 48. Directory ID

- e. **Application (client) ID:** Enter the Application (client) ID from the Overview section of the App registration you created earlier.

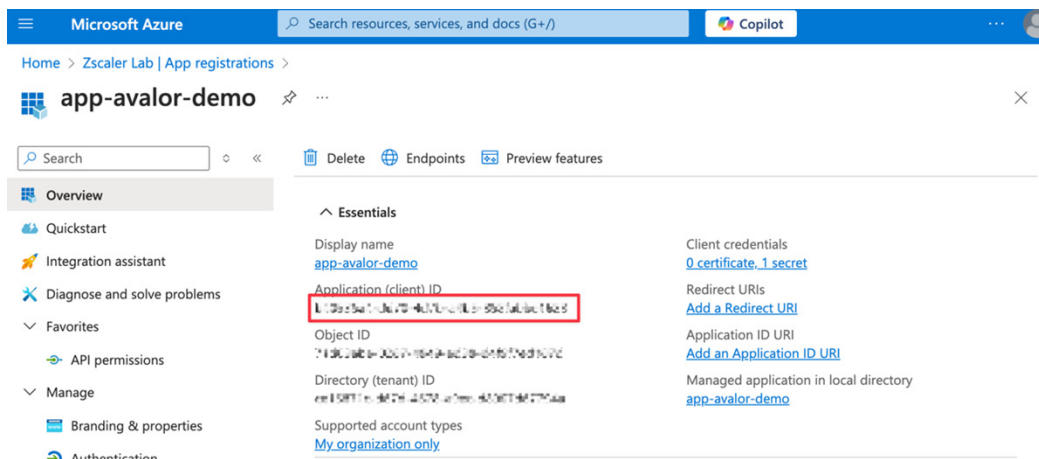


Figure 49. Application ID

- f. **Client Secret:** Enter the **Secret Value** from the App registration.
- g. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
- h. **Remediation Detection Settings:** Select your desired option to determine when findings automatically become undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
- i. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials have been entered correctly, the system responds with Test Passed.

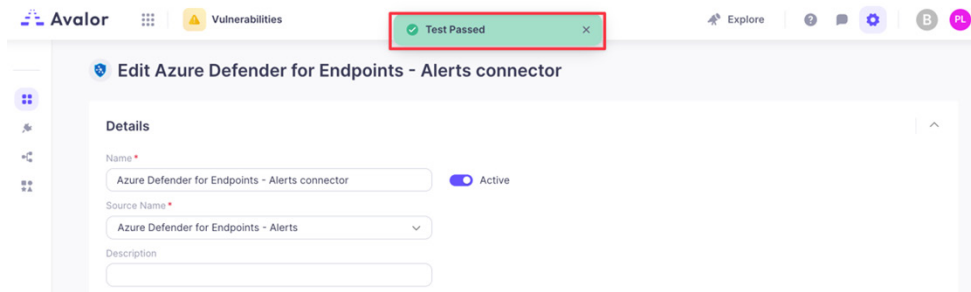


Figure 50. Test Passed

7. Click **Save**.

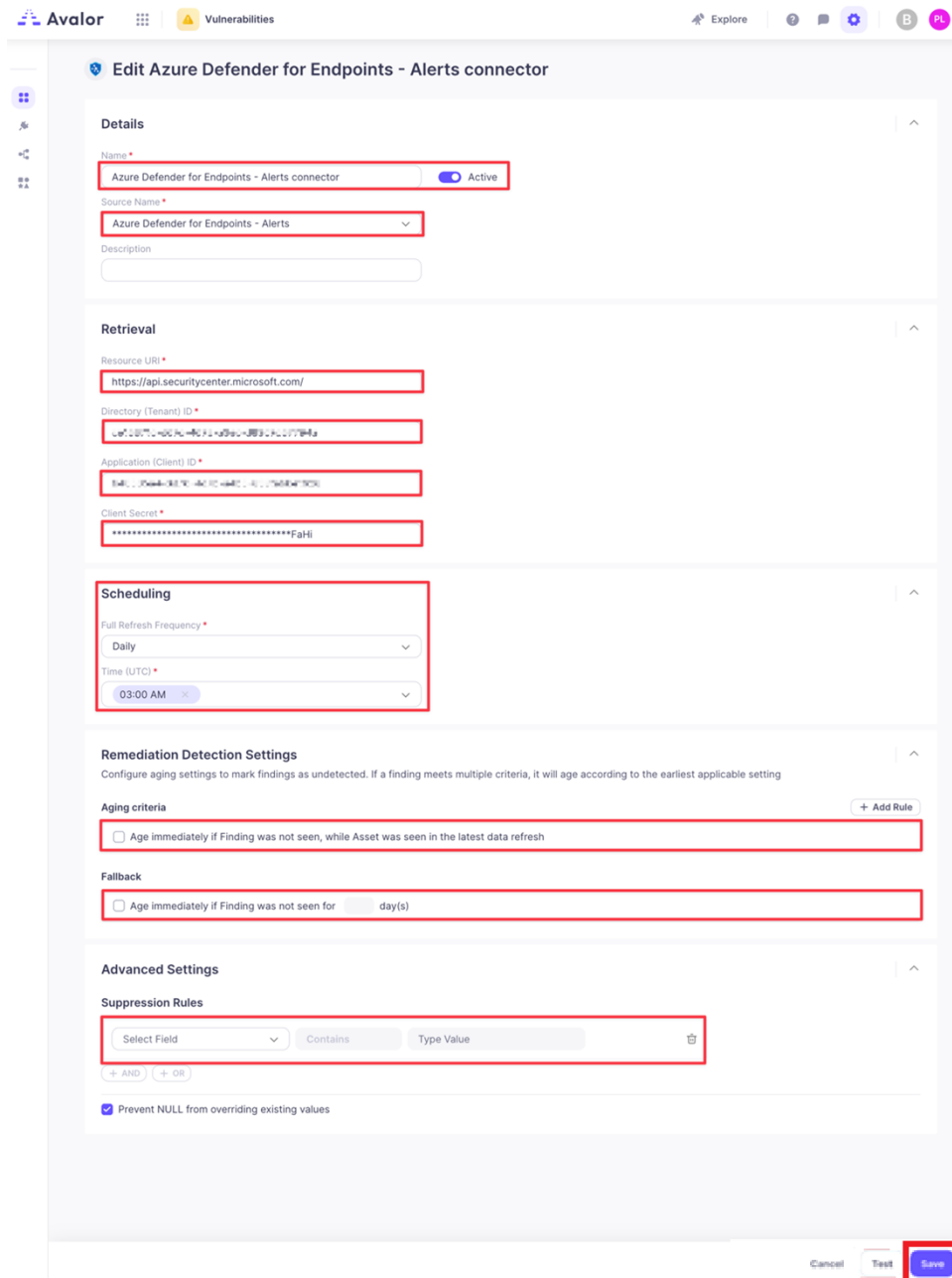


Figure 51. Advanced Settings

Configure the Azure Defender for Endpoints—Software Vulns by Machine Data Source

To configure the software vulns for Azure Defender for endpoints:

1. Log in to the Avalor UVM Platform
2. Click **Configure**.

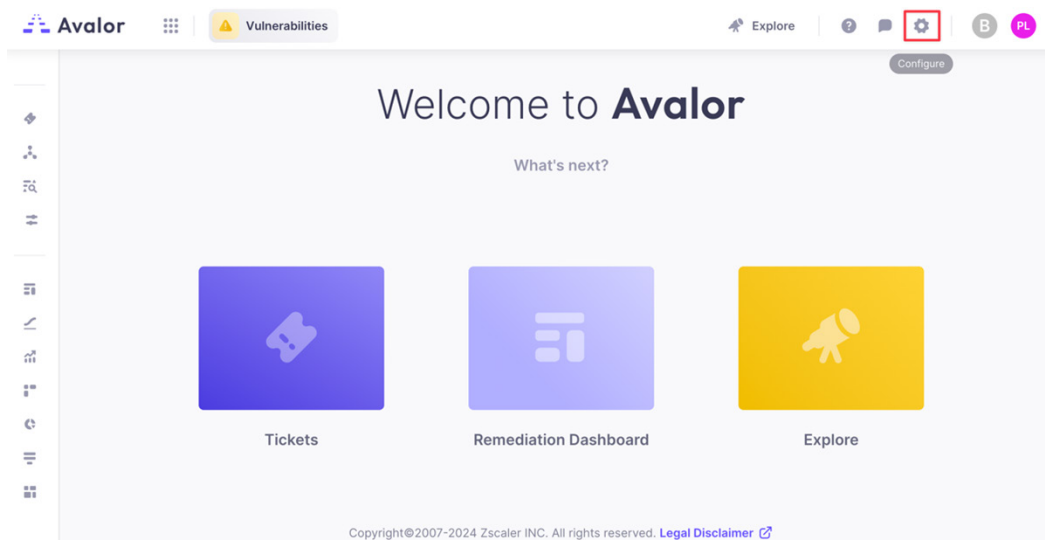


Figure 52. Configure

3. Click **Create**, then search for Azure Defender for Endpoints—Software Vulns by Machine.

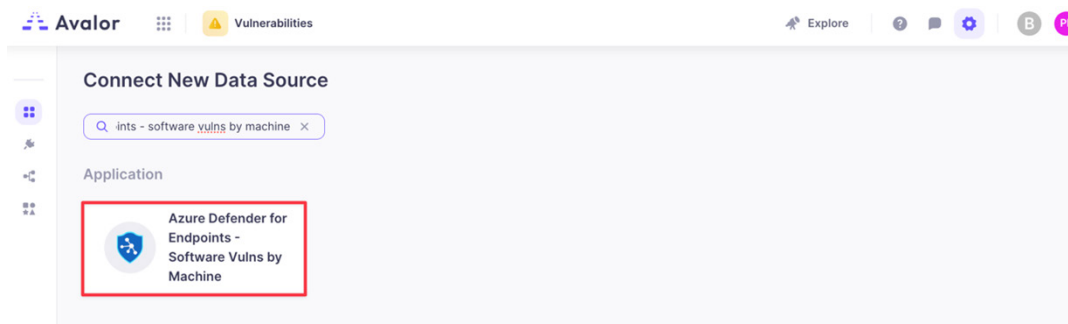


Figure 53. Azure Defender for Endpoints—Software Vulns by Machine

4. Click the **Azure Defender for Endpoints—Vulnerabilities** application.
5. On the **Create Azure Defender for Endpoints—Vulnerabilities Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Resource URI:** Enter `https://api.securitycenter.microsoft.com/` or for better performance, you can select a server closer to your geolocation:
 - `https://api-us.securitycenter.microsoft.com/`
 - `https://api-eu.securitycenter.microsoft.com/`
 - `https://api-uk.securitycenter.microsoft.com/`
 - `https://api-au.securitycenter.microsoft.com/`

- d. **Directory (tenant) ID:** Enter the Directory ID from the Overview section of the App registration you created earlier.

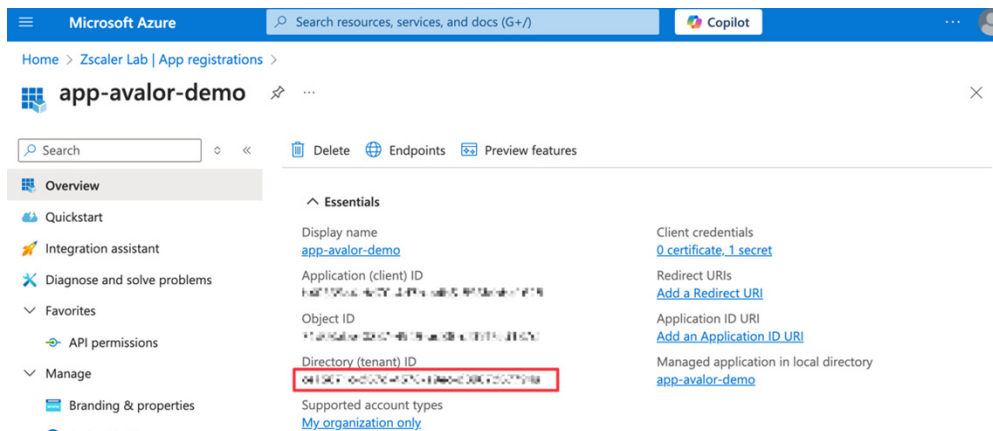


Figure 54. Directory ID

- e. **Application (client) ID:** Enter the Application (client) ID from the Overview section of the App registration you created earlier.

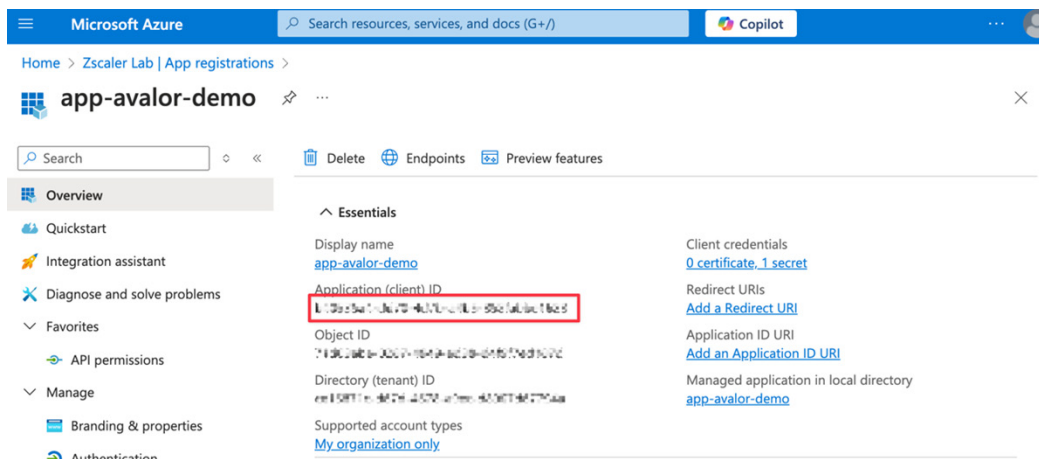


Figure 55. Application ID

- f. **Client Secret:** Enter the **Secret Value** from the App registration.
- g. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
- h. **Remediation Detection Settings:** Select your desired option to determine when findings automatically become undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
- i. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials have been entered correctly, the system responds with Test Passed.

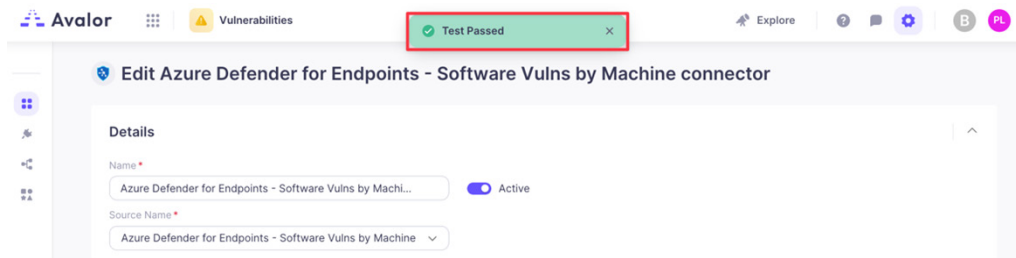


Figure 56. Test Passed

7. Click **Save**.

Review and Adjust Data Model Mapping

(Optional) Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin immediately. However, many data sources also provide additional data points that may provide additional context to risk prioritization.

The following example shows how to leverage the Has EDR Data Model Entity to the ingested Microsoft Defender for Endpoint Asset data so that this field can be used as a mitigating score factor when calculating risk.

Map Asset Microsoft Defender for Endpoint with the Has EDR Data Model Entity

To map asset Microsoft Defender for Endpoint with the Has EDR data model entity:

1. Go to **Configure > Azure Defender for Endpoints—Assets Connector > Map Data**.

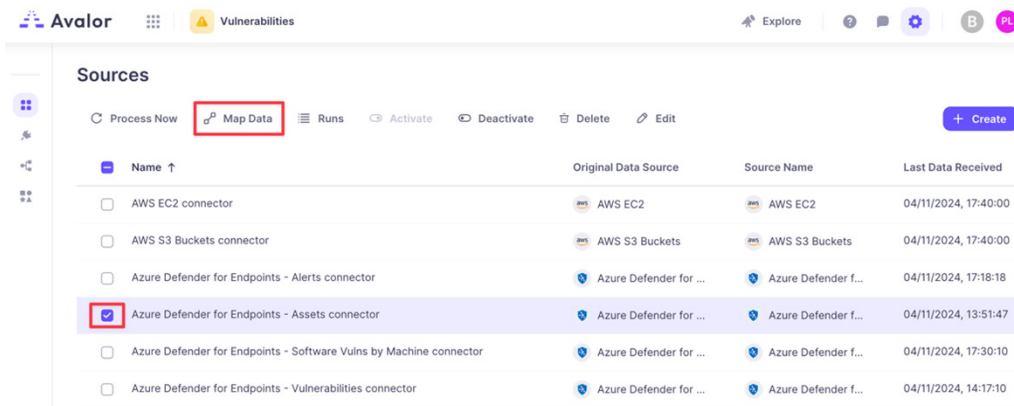


Figure 57. Map Data

2. (Optional) Click **+** under **Asset**, then:
 - a. **Field Name:** Enter **Has EDR**.
 - b. **Field Type:** Select **Boolean**.
 - c. Click **Add**.

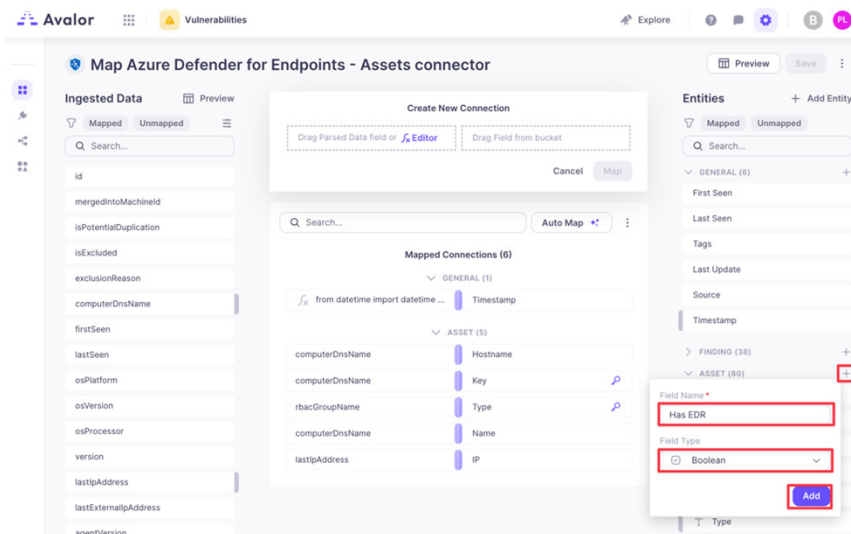


Figure 58. Add Asset

3. Double-click **Has EDR** under **Asset**, and then click the **Editor** hyperlink.

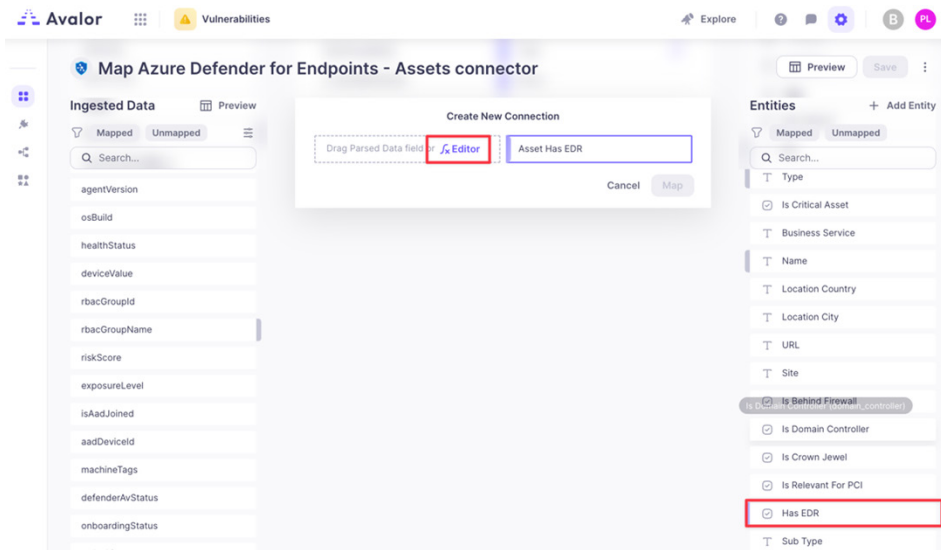


Figure 59. Editor

4. Enter **True**, then click **Map**.

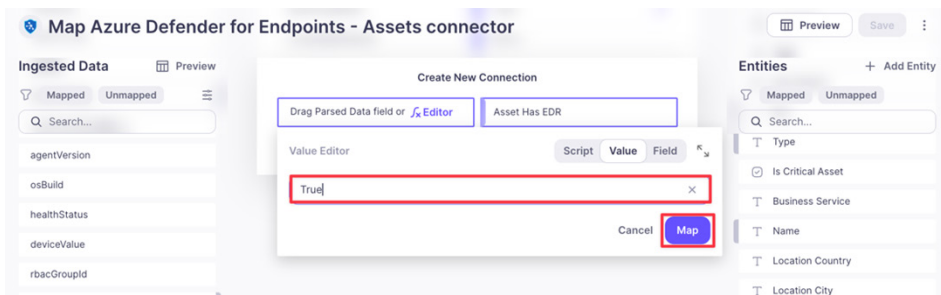


Figure 60. Map

5. Click **Save**.
6. Select the **Azure Defender for Endpoints—Assets** connector, then click **Process Now**.

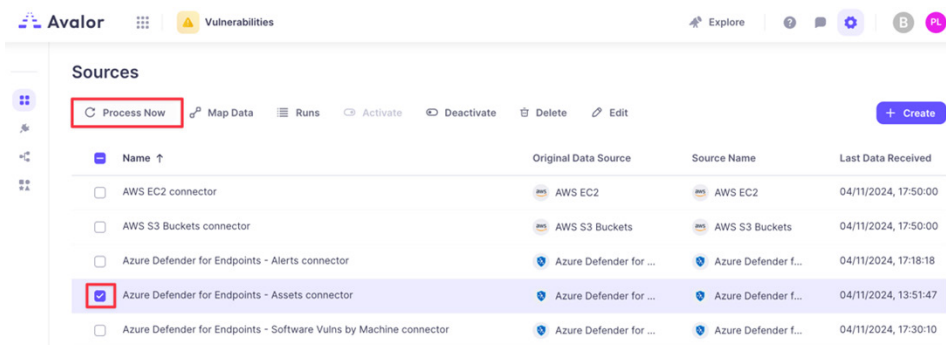


Figure 61. Process Now

Review and Adjust Risk Scoring

After ingested data has been normalized and mapped to the Data Model, Avalor UVM can evaluate risk.

The following example shows how the Mitigating Factors was selected in the Factor Type field for risk scoring. A value of True reduces the risk calculation (since the asset mitigating software was installed).

1. From the **Vulnerabilities** tab in the Avalor dashboard (**Remediation Hub**):
 - a. In the left-side navigation, select **Settings > Score**.
 - b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
2. In the **Add new factor** modal:
 - a. Choose **Mitigating Factors** for **Factor Type** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
 - b. Enter a **Factor Name**.
 - c. Choose **Asset has EDR** for **Field**.
 - d. In the **When Has EDR Equals** section, under **True**, enter a percentage by which the risk is reduced.

The screenshot shows the 'Add new factor' modal in the Avalor dashboard. The modal is divided into two main sections: 'Score Settings' on the left and 'Has EDR' on the right. In the 'Score Settings' section, the 'Base Score' is set to 55%, and the 'Risk & Mitigating Factors' section shows a total of 80% with a list of factors including 'CVSS', 'EPSS', and 'Original Severity Score'. The 'Has EDR' section contains the following fields: 'FACTOR TYPE' set to 'Mitigating Factors', 'FACTOR NAME' set to 'Has EDR', and 'FIELD' set to 'Asset Has EDR'. Below these fields is the 'When Has EDR Equals' section, which has three rows: 'True' (reduce score by 5%), 'False' (raise score by 5%), and 'Else' (raise score by 0%). The '5%' value in the 'True' row is highlighted with a red box. At the bottom right of the modal, there are 'Cancel' and 'Apply' buttons, with the 'Apply' button also highlighted with a red box.

Figure 62. Enter percentage

- e. Click **Apply**, then **Save & Run**.

3. In the left-side navigation, select the **Assets** dashboard. From the **Assets** dashboard:
 - a. Set a filter by clicking **More** and adding the **Has EDR = True Entity**.

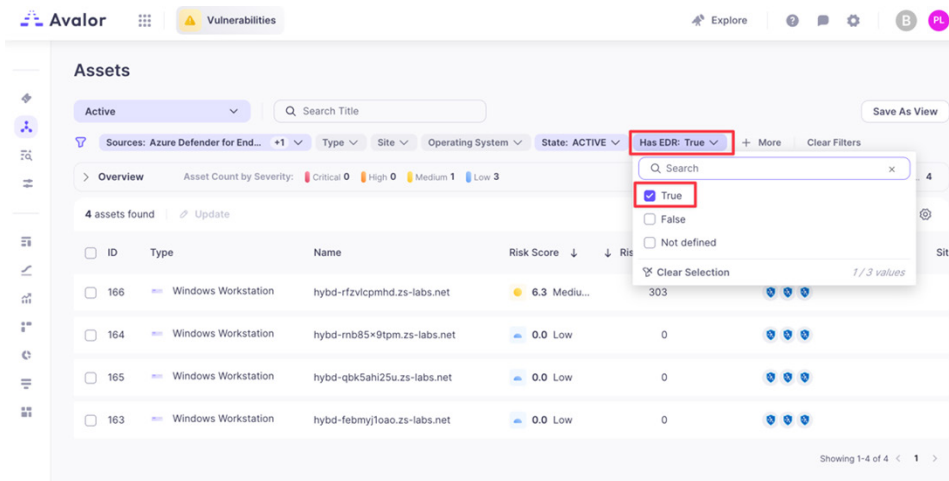


Figure 63. Has EDR = True Entity

- b. Select one of your **Assets** in the filtered list.
- c. In the **Asset** modal that appears, click the **Findings** tab.
- d. Select one of the **Findings**.
- e. Review the output (notice the **Score Adjustment** section and whether **Has EDR** has modified the risk scoring).

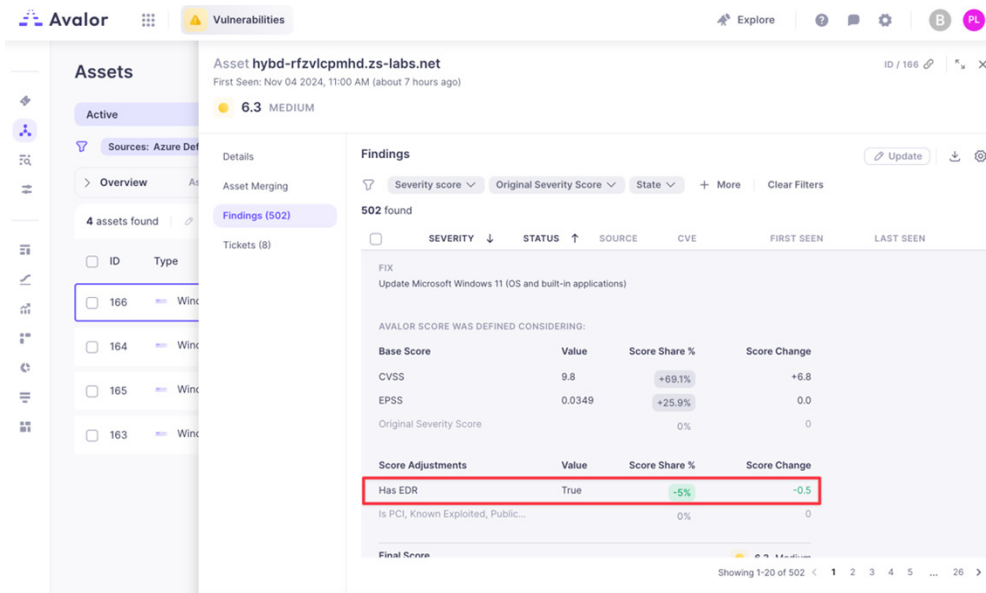


Figure 64. Score Adjustment

Appendix A: Requesting Zscaler Support

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7/365.

To contact Zscaler support:

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

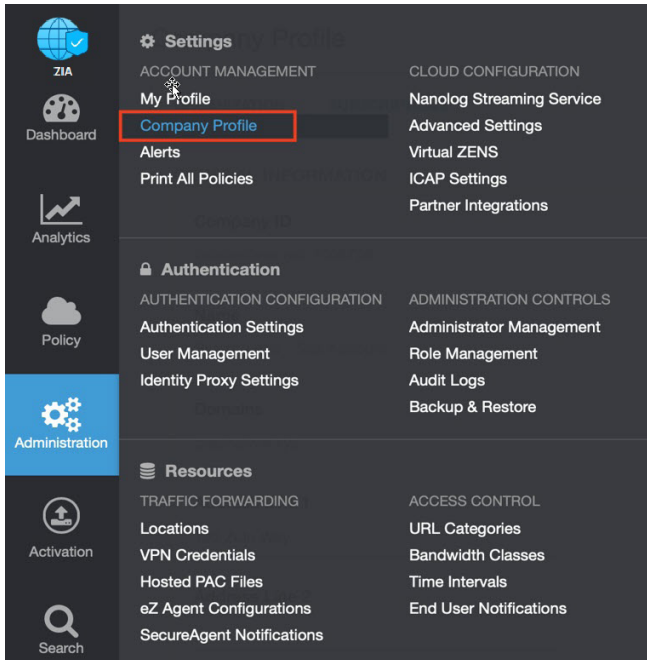


Figure 65. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

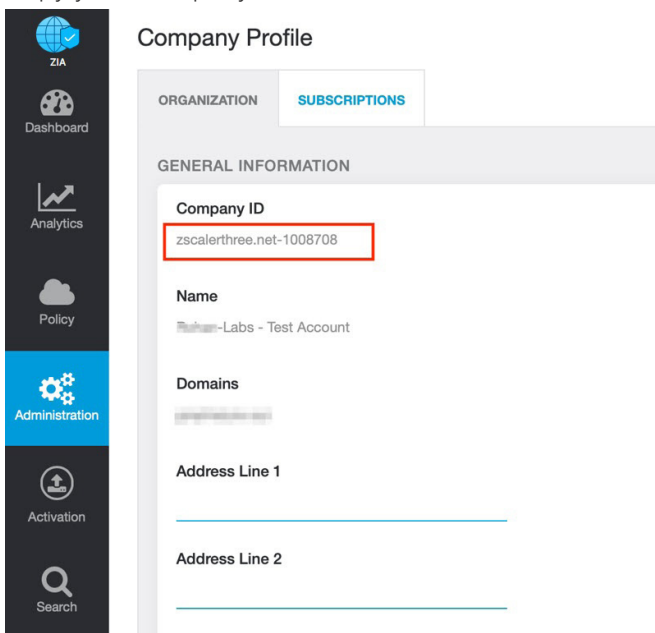


Figure 66. Company ID

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

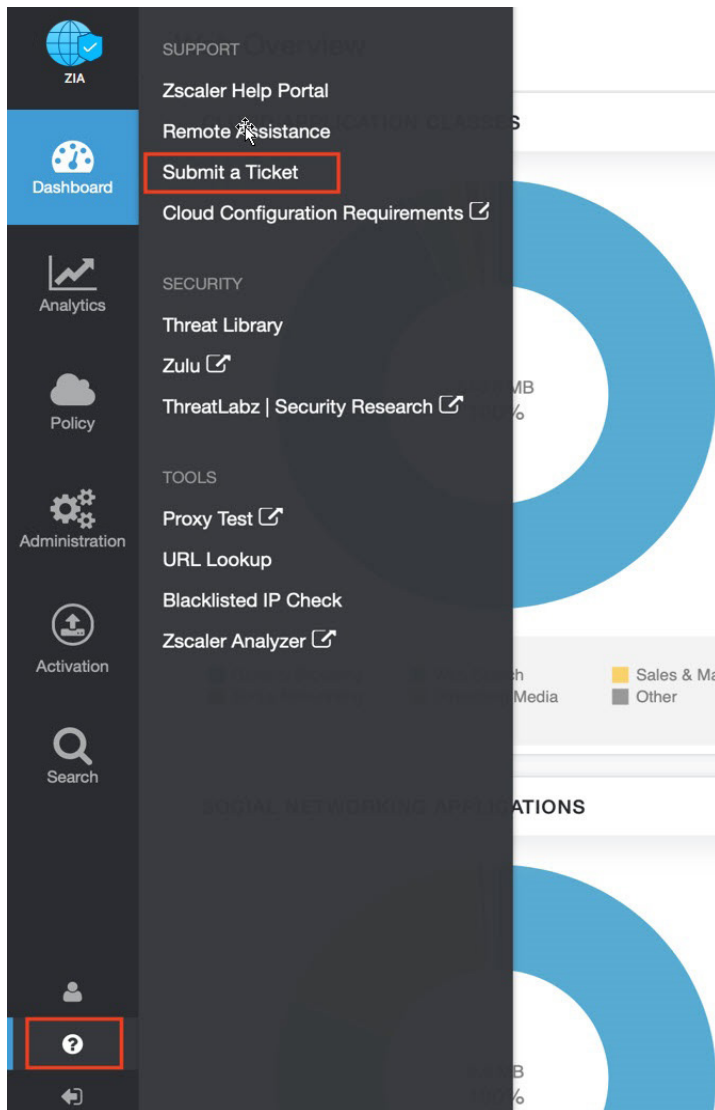


Figure 67. Submit a ticket