Zscaler and Microsoft Defender Deployment Guide

February 2022
Version 1.0
Table of Contents

Terms and Acronyms.................................................................................................................. 3
About This Document .................................................................................................................. 4
  Zscaler Overview...................................................................................................................... 4
  Microsoft Overview ................................................................................................................ 4
  Audience ................................................................................................................................. 4
  Software Versions ................................................................................................................... 4
  Request for Comments .......................................................................................................... 4

Zscaler and Microsoft Introduction ............................................................................................. 5
  Zscaler Overview .................................................................................................................... 5
    Zscaler Internet Access (ZIA) Overview ............................................................................. 5
    Zscaler Private Access (ZPA) Overview ........................................................................... 5
    Zscaler Resources ............................................................................................................. 5
  Defender Overview ................................................................................................................ 6
    Defender Resources .......................................................................................................... 6

ZIA and Microsoft Defender ........................................................................................................ 7
  Prerequisites .......................................................................................................................... 7
  Integrating with Microsoft Defender for Endpoint .............................................................. 8

ZIA Hits Report .......................................................................................................................... 11
  Viewing the Microsoft Defender Endpoint Hits Report ......................................................... 11
  About the Microsoft Defender Endpoint Hits Report ........................................................... 12
    Sandbox File Properties (Zcaler) ..................................................................................... 12
    File Detected on Endpoints (Microsoft Defender for Endpoint) ....................................... 13

ZPA Posture Type ........................................................................................................................ 16
  Configuring Zscaler Private Access (ZPA) .......................................................................... 17
    Log into ZPA Admin Portal ................................................................................................. 17
    Navigate to the Zcaler Client Connector .......................................................................... 17
    Create a New Posture Profile ............................................................................................. 18
  Add New Microsoft Defender Posture Profile .................................................................... 18
  Decide Which Applications Need Conditional Access ........................................................ 19
  Set Up an Access Policy ....................................................................................................... 20
  Tie the Posture Profile to this Access Policy ...................................................................... 20
Verify Conditional Access from an Endpoint

Appendix A: Requesting Zscaler Support

Gather Support Information
Save Company ID
Enter Support Section
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC2411)</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Share Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
About This Document

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. For more information on Zscaler, visit www.zscaler.com or follow Zscaler on Twitter @zscaler.

Microsoft Overview

Microsoft (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 Office 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).

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, refer to:

- Zscaler Resources
- Defender Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using Zscaler Internet Access and Zscaler Private Access (with Zscaler Client Connector) along with Microsoft Defender on Windows 10.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please 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

Zscaler Overview

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

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (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), cloud access security broker (CASB), and browser isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on 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, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
**Defender Overview**

Microsoft 365 Defender, part of Microsoft’s 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 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Defender documentation</td>
<td>Online help articles for Microsoft Defender</td>
</tr>
<tr>
<td>Microsoft Defender support</td>
<td>Support contact for Microsoft Defender</td>
</tr>
<tr>
<td>Restrict app execution</td>
<td>Help article on locking down a device and preventing subsequent attempts of potentially malicious programs from running.</td>
</tr>
<tr>
<td>Automated investigation</td>
<td>Help article on starting a new general purpose automated investigation on the device if needed.</td>
</tr>
<tr>
<td>Stop and quarantine files</td>
<td>Help article on containing an attack in your organization by stopping the malicious process and quarantining the file.</td>
</tr>
<tr>
<td>Block or allow a file</td>
<td>Help article on banning potentially malicious files or suspected malware.</td>
</tr>
</tbody>
</table>
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. Once 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.

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](image)

2. Click the Microsoft Defender for Endpoint tab.

![Figure 3. Microsoft Defender for Endpoints](image)
3. Under **Authorize Microsoft Defender for Endpoint**, click **Provide Admin Credentials**.

![Authorize Microsoft Defender for Endpoint](image)

*Figure 4. Authorize Microsoft Defender*

4. The **Microsoft Defender for Endpoint** portal appears. Log in to **Microsoft Defender for Endpoint**.

![Pick an account](image)

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

![Zscaler SaaS Connector](image1)

*Figure 6. Accept Microsoft Defender permissions*

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

![Authorization Complete](image2)

*Figure 7. Authorization Complete*

7. 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, you can click the MD5 hash and choose **View Microsoft Defender Endpoint Hits**. 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 Zcaler 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**.

*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:

<table>
<thead>
<tr>
<th>Sandbox File Properties (Zscaler)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sandbox Category</strong></td>
</tr>
<tr>
<td><strong>Sandbox Score</strong></td>
</tr>
<tr>
<td><strong>Threat Name</strong></td>
</tr>
<tr>
<td><strong>File Type</strong></td>
</tr>
<tr>
<td><strong>File Size</strong></td>
</tr>
<tr>
<td><strong>MD5</strong></td>
</tr>
<tr>
<td><strong>SHA-1</strong></td>
</tr>
<tr>
<td><strong>SHA-256</strong></td>
</tr>
<tr>
<td><strong>SSDEEP</strong></td>
</tr>
</tbody>
</table>

Figure 9. Microsoft Defender endpoint hits Sandbox File Properties

- **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.
- **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.
**File Detected on Endpoints (Microsoft Defender for Endpoint)**

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

<table>
<thead>
<tr>
<th>File Detected on 2 Endpoints (Microsoft Defender for Endpoint)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Defender Endpoint ID</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>06428352307323e02f9f39c72b48da55e...</td>
</tr>
<tr>
<td>497333039708s35f79660b7e51d6103a03b...</td>
</tr>
</tbody>
</table>

**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 automated investigation and remediation (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**.
**Figure 11. Isolate Host**

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

**Figure 12. Kill 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](#).
Figure 13. Generate alert and trigger

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

Figure 14. Prevent future executions
ZPA Posture Type

In this use case:

- Zscaler Private Access (ZPA) verifies the presence of a running Microsoft Defender process on the endpoint as an assessment of end device posture. ZPA can be configured 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 Mac workstations) that a Microsoft Defender agent must be installed and running on the endpoint so that the endpoint can be granted access to internal applications referenced via ZPA Access policy.

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

![Conceptual Diagram](image-url)

*Figure 15. ZPA and Microsoft Defender overview*
Configuring Zscaler Private Access (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 into ZPA Admin Portal

![Log into ZPA Admin Portal](image)

**Figure 16. Log into ZPA Admin Portal**

Navigate to the Zscaler Client Connector

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

![Click the Zscaler Client Connector icon](image)

**Figure 17. Click the Zscaler Client Connector icon**
Create a New Posture Profile

Log into the Zscaler Client Connector and navigate 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. Select only Windows, macOS, or both.
2. Click the Posture Type dropdown menu.
3. Select Detect Microsoft Defender.
4. Name this policy and click Save.

This posture profile is referenced in a ZPA Access Policy. Access policies can be setup 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, navigate to Administration > Application Segment

This page lists which applications can be 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. Navigate to application segments

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

Figure 21. Decide which application needs conditional access
Set Up an Access Policy

Within the ZPA Admin Portal, navigate 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 on Add Rule and reference the previously created posture profile. Customers can setup different access policies to protect different internal applications.

A customizable (and optional) popup message can be shown to the end users when application access is allowed or denied, informing them about the policy evaluation.

In this example, we added an access policy 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 will grant application access).
**Figure 23. Setup an access policy**

<table>
<thead>
<tr>
<th>Rule Order</th>
<th>Name</th>
<th>Rule Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Posture Check</td>
<td>Block Access</td>
</tr>
</tbody>
</table>

- **Description**: Not Available
- **App Connector Selection Method**: All App Connector groups for the application
- **Rule Action**: Block Access
- **Criteria**: Client Connector Posture Profiles
  - Defender_Check (zscalaerbeta.net) = VERIFICATION FAILED

| 2          | Allow_All        | Allow Access     |
Verify Conditional Access from an Endpoint

The endpoint should be able to access 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*
Figure 25. Access blocked from an endpoint if the Microsoft Defender agent is not running
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 hours a day, year-round.

Gather Support Information

To contact Zscaler support, select Administration > Settings > and then click Company profile.

![Figure 26. Collecting details to open support case with Zscaler TAC](image)

**Save Company ID**

Copy your Company ID.

![Figure 27. Company ID](image)
Enter Support Section

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

Figure 28. Submit a ticket