zscaler™ | Windows Autopilot

ZSCALER AND MICROSOFT WINDOWS AUTOPILOT DEPLOYMENT GUIDE

NOVEMBER 2022, VERSION 1.0

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
AD	Active Directory
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)
PAC	Programmable Automation Controller
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)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

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. For more information, see Zscaler's website or follow Zscaler on Twitter @zscaler.

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 Office 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (Infrastructure as a Service 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, see:

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

Software Versions

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

Prerequisites

Before you begin the Microsoft Windows Autopilot integration, ensure you have configured and tested Windows Autopilot to function under the Hybrid Microsoft Entra ID Join approach, with a device successfully enrolled that has line-of-sight to Active Directory (AD).

To learn more, see the Microsoft Windows Autopilot Hybrid documentation.

Request for Comments

- **For prospects and customers**: Zscaler values 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

Overviews of the Zscaler and Microsoft 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, please contact your Zscaler Account team.

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, 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
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
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.

Windows Autopilot Overview

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices to get them ready for productive use. Windows Autopilot can reset, repurpose, and recover devices.

Windows Autopilot simplifies the Windows device life cycle, for both IT and end users, from initial deployment to End-of-Life. Using cloud-based services, Windows Autopilot:

- Reduces the time IT spends on deploying, managing, and retiring devices.
- Reduces the infrastructure required to maintain the devices.
- Maximizes ease of use for all types of end users.

When initially deploying new Windows devices, Windows Autopilot uses the OEM-optimized version of Windows client. This version is preinstalled on the device, so you don't have to maintain custom images and drivers for every device model. Instead of re-imaging the device, transform your existing Windows installation into a "business-ready" state that can:

- Apply settings and policies
- Install apps
- Change the edition of Windows being used to support advanced features (for example, from Windows Pro to Windows Enterprise).

Hybrid Microsoft Entra ID Join vs. Microsoft Entra ID Join

Windows Autopilot offers two approaches for onboarding devices (dependent on whether an existing on-premises Active Directory (AD) deployment exists). The two approaches are:

- Windows Autopilot with Microsoft Entra ID Join. This is the cloud native approach to onboarding devices, where devices are "cloud-domain" joined to Microsoft Entra ID as part of the Autopilot provisioning process. The device is auto-enrolled to Intune thereby receiving any applicable configuration policies and applications. Under this scenario, there is no dependency for any on-premises connectivity as the solution is cloud native, and does not interact with AD.
- Windows Autopilot with Hybrid Microsoft Entra ID Join. This is the hybrid approach to onboarding devices, where devices first get enrolled to Intune during the autopilot process and receive a ODJ blob to complete the "domain join" process. Note that this process requires line-of-sight to an AD Controller, and as such, devices must be either connected to the corporate network for provisioning or connected via a VPN like service if provisioning is to occur off site.

This guide covers the second approach, using Windows Autopilot with Hybrid Microsoft Entra ID Join. It leverages ZPA for connectivity to on-premises AD during the enrollment process.

Microsoft Resources

The following table contains links to Microsoft support resources.

Name	Definition
Windows Autopilot Documentation	Online help for Windows Autopilot.
Windows Autopilot Support	Online tech support for Windows Autopilot.
Microsoft Community	Online community support for Microsoft products.

Create a Machine Tunnel for Pre-Logon Connectivity to Active Directory Resources

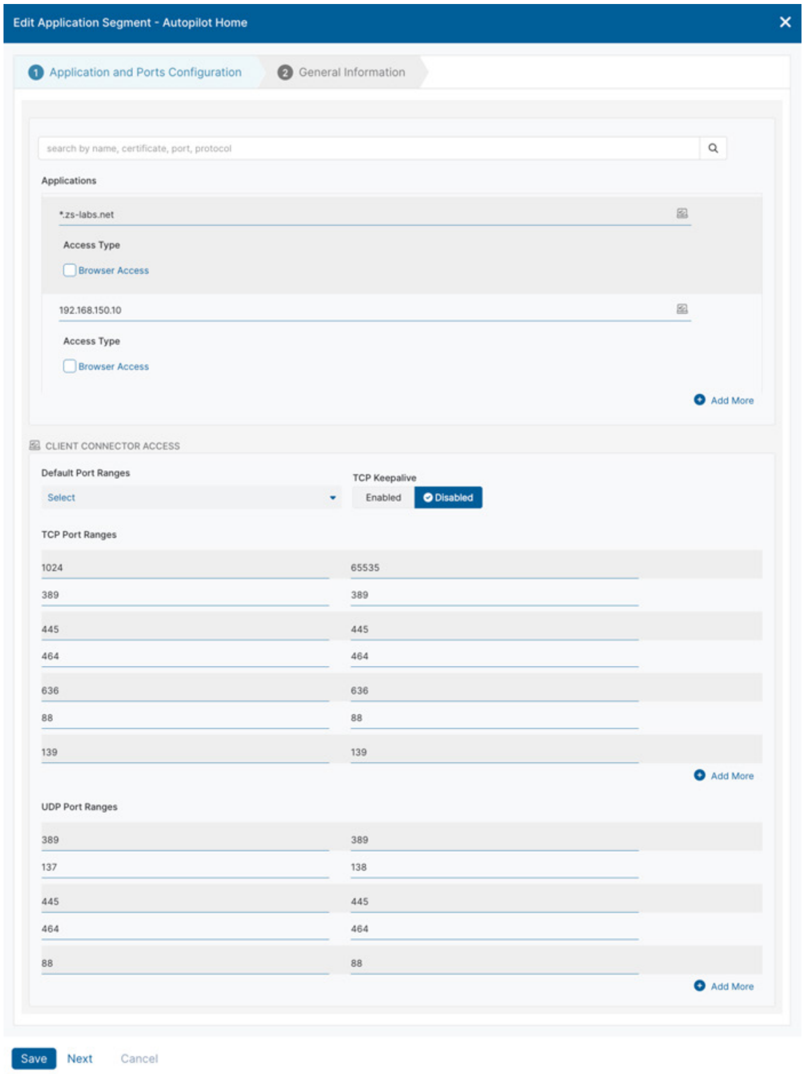
Within the ZPA Admin Portal, you can create App Connectors, App Connector groups, and provisioning keys. Follow these instructions to create a new App Connector if required.

You can also optionally create a new App Connector which has line-of-sight to your AD Domain Controller.

Configure an Application Segment for AD Traffic

To add an application segment for AD traffic:

1. Log in to the ZPA Admin Portal with admin credentials.
2. Go to **Administrator** > **Application Segments** > **Defined Application Segments,** and click **Add Application Segment**.
3. In the **Edit Application Segment** window, replace the domain `*.zs-labs.net` with your domain, and the IP address `192.168.150.10` with the IP address of your domain controller and enter in the following TCP Port Ranges and UDP Port Ranges as shown in Figure 1.


Edit Application Segment - Autopilot Home
① Application and Ports Configuration
② General Information
search by name, certificate, port, protocol
Add More
Save
Next
Cancel

Applications

*.zs-labs.net

Access Type

□ Browser Access

192.168.150.10

Access Type

□ Browser Access

CLIENT CONNECTOR ACCESS

Default Port Ranges: Select

TCP Keepalive: Enabled [✓ Disabled]

TCP Port Ranges

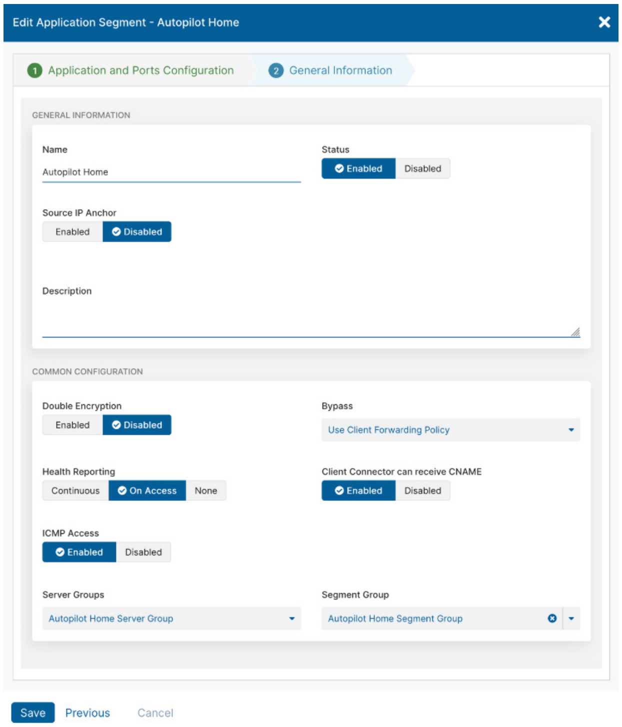
1024	65535
389	389
445	445
464	464
636	636
88	88
139	139

UDP Port Ranges

389	389
137	138
445	445
464	464
88	88

Figure 1. Edit Application Segment

4. Click the General Information tab to configure the **Application Segment** to define the server groups in your data center that host the AD traffic you've defined.
5. Click **Save**.



Edit Application Segment - Autopilot Home

1 Application and Ports Configuration · 2 General Information

GENERAL INFORMATION

Name: Autopilot Home

Status: [✓ Enabled] Disabled

Source IP Anchor: Enabled [✓ Disabled]

Description:

COMMON CONFIGURATION

Double Encryption: Enabled [✓ Disabled]

Bypass: Use Client Forwarding Policy

Health Reporting: Continuous [✓ On Access] None

Client Connector can receive CNAME: [✓ Enabled] Disabled

ICMP Access: [✓ Enabled] Disabled

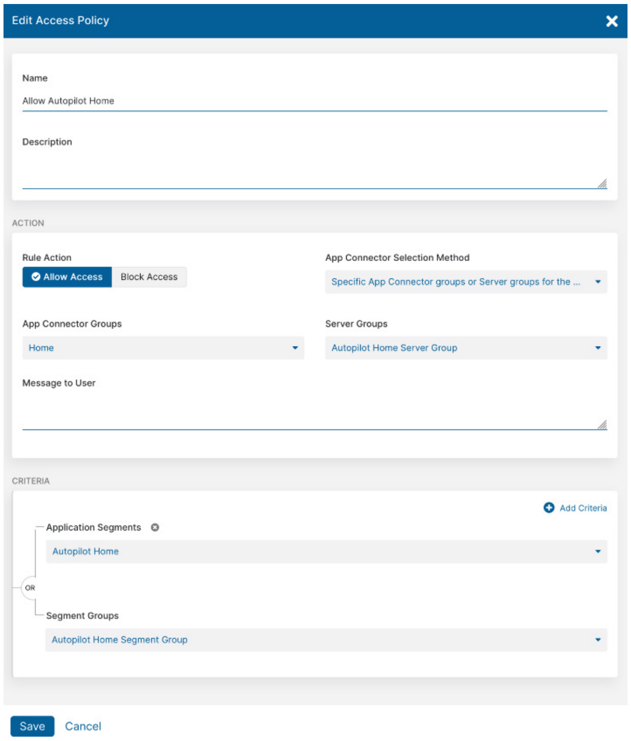
Server Groups: Autopilot Home Server Group

Segment Group: Autopilot Home Segment Group

Save · Previous · Cancel

Figure 2. Autopilot Home

6. Open the **Edit Access Policy** dialog by navigating to **Administration** > **Access Policy**.
7. Create an access policy that allows access to AD traffic.



Edit Access Policy

Name: Allow Autopilot Home

Description:

ACTION

Rule Action: [✓ Allow Access] Block Access

App Connector Selection Method: Specific App Connector groups or Server groups for the ...

App Connector Groups: Home

Server Groups: Autopilot Home Server Group

Message to User:

CRITERIA

Add Criteria

Application Segments: Autopilot Home

OR

Segment Groups: Autopilot Home Segment Group

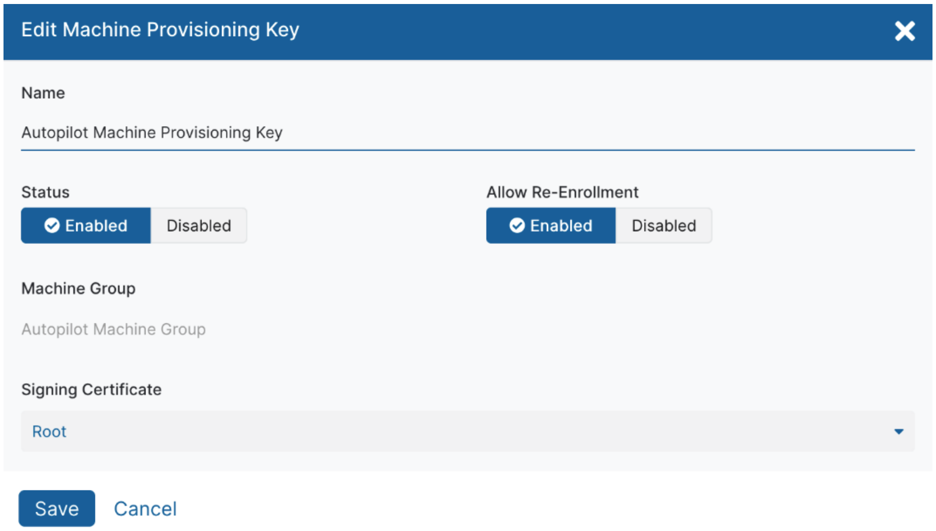
Save · Cancel

Figure 3. Access Policy Criteria

Configure a Machine Tunnel for Pre-Logon Connectivity to On-Premises AD

A machine tunnel allows a Windows device to establish a connection to a private service before the user is logged in to the Zscaler Client Connector.

To use a machine tunnel, configure a Machine Group and Machine Provisioning Key as shown in [Deploying Machine Tunnels for Pre-Windows Login]() (government agencies, see [Deploying Machine Tunnels for Pre-Windows Login]()). See the example Machine Provisioning Key example:



Edit Machine Provisioning Key

Name: Autopilot Machine Provisioning Key

Status: Enabled

Allow Re-Enrollment: Enabled

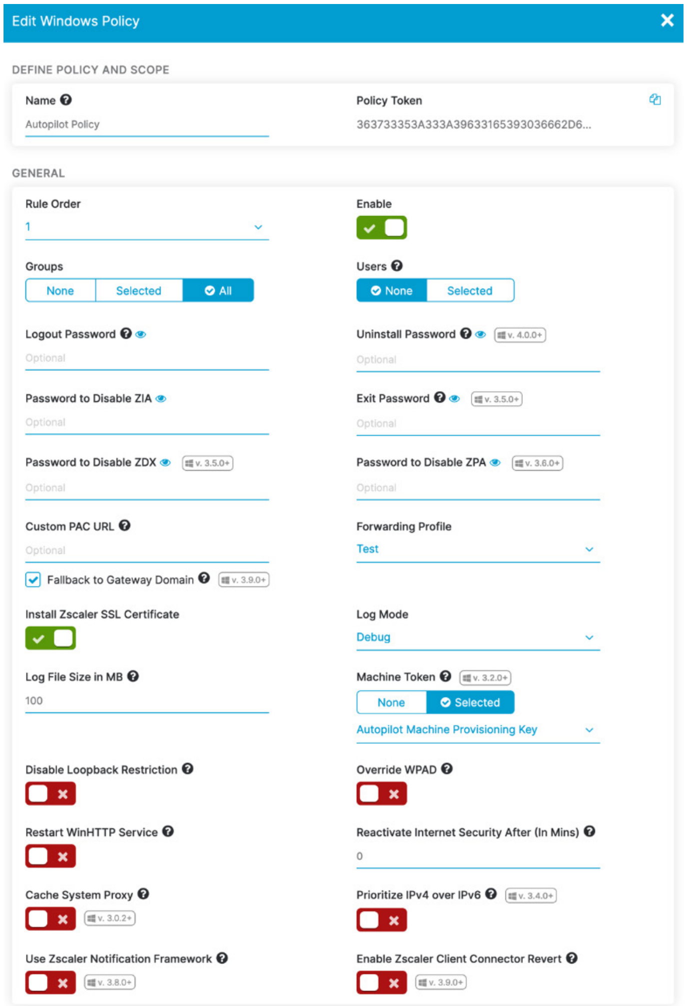
Machine Group: Autopilot Machine Group

Signing Certificate: Root

Figure 4. Machine Provisioning Key example

Create a Windows Policy

Create a new Windows Policy as shown in Configuring Zscaler Client Connector Profiles (government agencies, see Configuring Zscaler Client Connector Profiles). Ensure that you select the Machine Token you created when you configured the Machine Tunnel.



Edit Windows Policy

DEFINE POLICY AND SCOPE

Name: Autopilot Policy

Policy Token: 363733353A333A3963316539303666 2D6...

GENERAL

Rule Order: 1

Enable: ✓

Groups: None | Selected | ● All

Users: ● None | Selected

Logout Password: Optional

Uninstall Password (v. 4.0.0+): Optional

Password to Disable ZIA: Optional

Exit Password (v. 3.5.0+): Optional

Password to Disable ZDX (v. 3.5.0+): Optional

Password to Disable ZPA (v. 3.6.0+): Optional

Custom PAC URL: Optional

Forwarding Profile: Test

☑ Fallback to Gateway Domain (v. 3.9.0+)

Install Zscaler SSL Certificate: ✓

Log Mode: Debug

Log File Size in MB: 100

Machine Token (v. 3.2.0+): None | ● Selected

Autopilot Machine Provisioning Key

Disable Loopback Restriction: ✗

Override WPAD: ✗

Restart WinHTTP Service: ✗

Reactivate Internet Security After (In Mins): 0

Cache System Proxy: ✗ (v. 3.0.2+)

Prioritize IPv4 over IPv6 (v. 3.4.0+): ✗

Use Zscaler Notification Framework: ✗ (v. 3.8.0+)

Enable Zscaler Client Connector Revert: ✗ (v. 3.9.0+)

Figure 5. Edit Windows Policy

Deploy the Zscaler Client Connector Using Intune

After you have set up the Machine Tunnel options, you need to deploy the Zscaler Client Connector using Intune with custom options. Without any options, Zscaler Client Connector installation requires a guided GUI.

Installing with options also allows for connectivity to AD before a user logs in, via the Machine Tunnel.

When installing manually, these options can be used as part of the command line statement used to run the MSI installer (e.g., `–userDomain`). When distributing through Intune, these command line options are configured with the MSI file and a MST transform file. Finally, for Intune, these are both packaged into an .intunewin file.

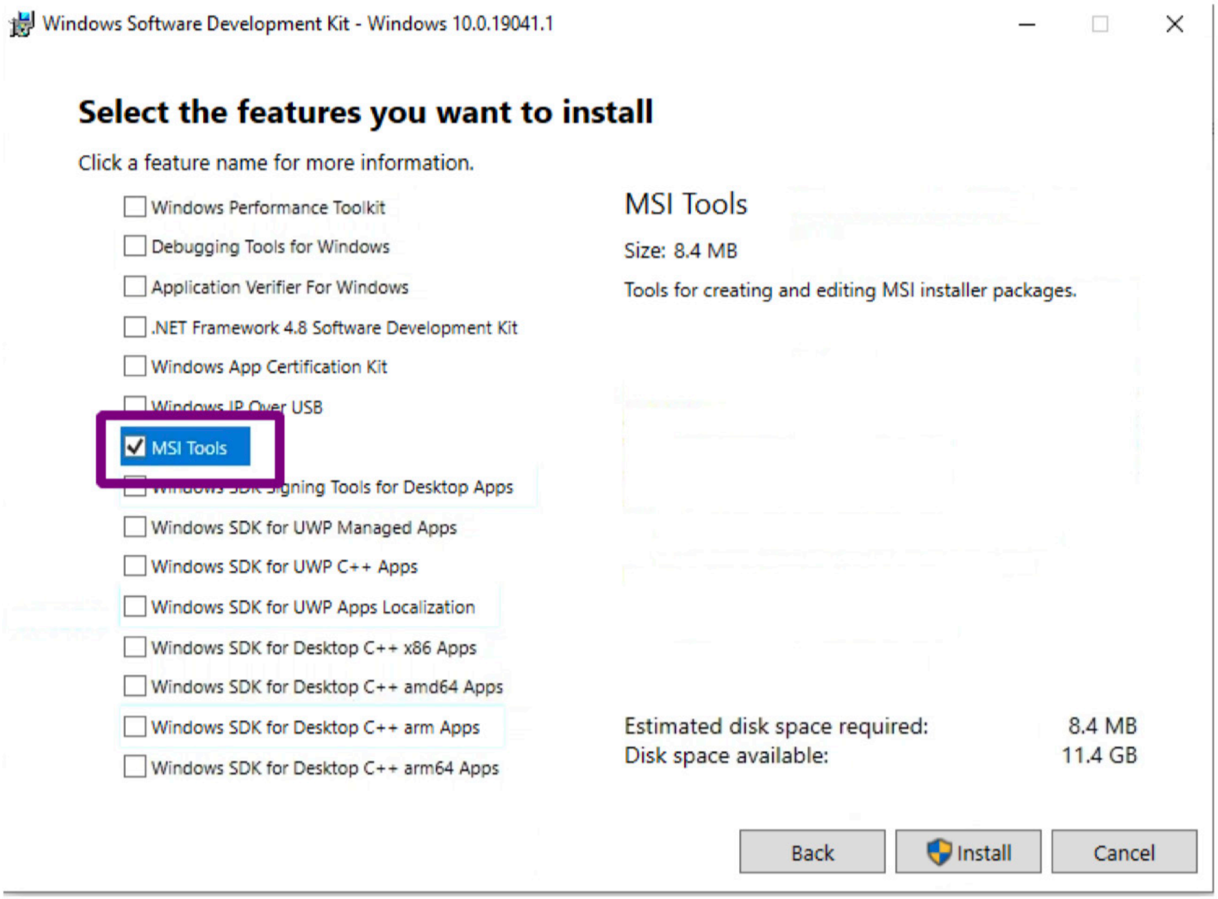
You need two utilities to create the package needed for Intune:

- Microsoft Orca to create the .MST transform file.
- Microsoft Win32 Content Prep Tool to create the .intunewin file.

Creating the MST File

To create the .MST file, you need Orca. Orca is part of the Windows 10 SDK download, which can be downloaded from the Microsoft developer site.

1. Run the downloaded installer and during the feature selection, deselect everything except **MSI Tools**.



Windows Software Development Kit - Windows 10.0.19041.1

Select the features you want to install

Click a feature name for more information.

- □ Windows Performance Toolkit
- □ Debugging Tools for Windows
- □ Application Verifier For Windows
- □ .NET Framework 4.8 Software Development Kit
- □ Windows App Certification Kit
- □ Windows IP Over USB
- ☑ MSI Tools
- □ Windows SDK Signing Tools for Desktop Apps
- □ Windows SDK for UWP Managed Apps
- □ Windows SDK for UWP C++ Apps
- □ Windows SDK for UWP Apps Localization
- □ Windows SDK for Desktop C++ x86 Apps
- □ Windows SDK for Desktop C++ amd64 Apps
- □ Windows SDK for Desktop C++ arm Apps
- □ Windows SDK for Desktop C++ arm64 Apps

MSI Tools

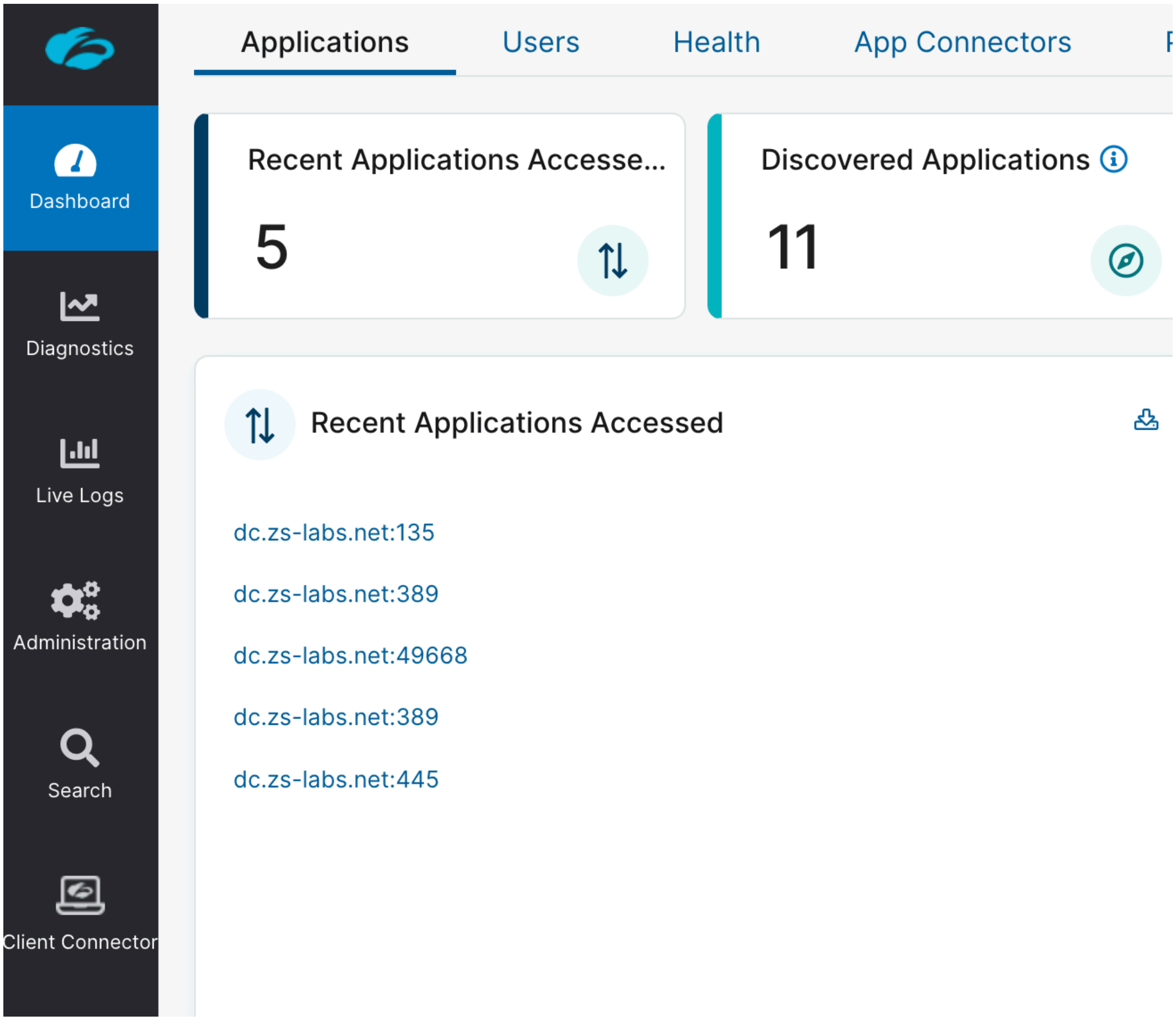
Size: 8.4 MB

Tools for creating and editing MSI installer packages.

Estimated disk space required: 8.4 MB
Disk space available: 11.4 GB

Figure 6. Windows Software Development Kit

2. Run the **Orca-x86_en-us.msi** file which is in the installer directory c:\Program Files(x86)\Windows Kits\10\bin\10.0.19041.0\x86\.
3. Download a copy of the **Zscaler Client Connector Installer**.
4. In the ZPA Admin Portal, click **Client Connector**.



Recent Applications Accesse...
5

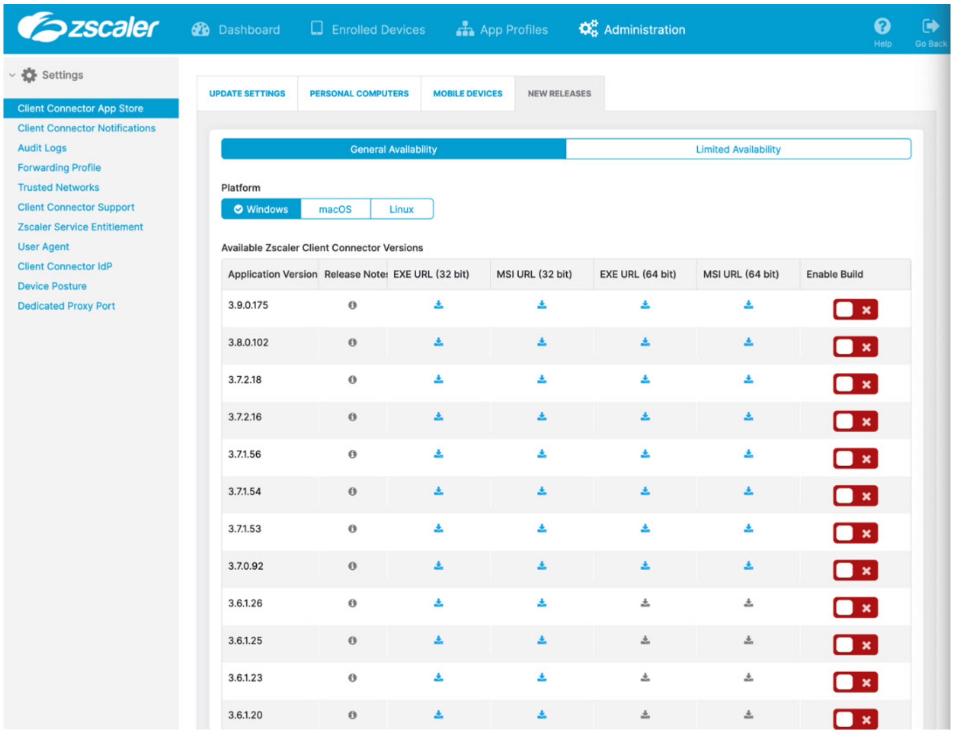
Discovered Applications
11

Recent Applications Accessed

dc.zs-labs.net:135
dc.zs-labs.net:389
dc.zs-labs.net:49668
dc.zs-labs.net:389
dc.zs-labs.net:445

Figure 7. Client Connector

5. In Client Connector, go to **Administration** > **Client Connector App Store** > **New Releases** and download the version of Zscaler Client Connector you want (this guide was tested with 3.6.1.26 – 32 bit).



Available Zscaler Client Connector Versions

Application Version	Release Notes	EXE URL (32 bit)	MSI URL (32 bit)	EXE URL (64 bit)	MSI URL (64 bit)	Enable Build
3.9.0.175	ⓘ	⭳	⭳	⭳	⭳	☒
3.8.0.102	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.2.18	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.2.16	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.1.56	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.1.54	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.1.53	ⓘ	⭳	⭳	⭳	⭳	☒
3.7.0.92	ⓘ	⭳	⭳	⭳	⭳	☒
3.6.1.26	ⓘ	⭳	⭳	⭳	⭳	☒
3.6.1.25	ⓘ	⭳	⭳	⭳	⭳	☒
3.6.1.23	ⓘ	⭳	⭳	⭳	⭳	☒
3.6.1.20	ⓘ	⭳	⭳	⭳	⭳	☒

Figure 8. Client Connector New Releases

6. To create the MST file, see [Customizing Zscaler Client Connector with Install Options for MSI]() (government agencies, see [Customizing Zscaler Client Connector with Install Options for MSI]()) and ensure that when creating the MST, you set the following options:
   a. Set **USERDOMAIN** to your domain.
   b. Set **CLOUDNAME** to the Zscaler cloud you are being hosted on.
   c. Set **POLICYTOKEN** to the policy token taken from the Windows policy you created.
   d. Set **REINSTALLDRIVER** to **1**.

Creating the .intunewin File

To create the .intunewin file:

1. Download the Win32 Content Prep Tool from [GitHub]().
2. Put only the MSI and MST files together in the same directory, with nothing else, and run the tool:

```
Intunewinapputil.exe -c <dir containing MSI and MST> -s Zscaler-windows-x.x.x.xx-
installer.msi -o <directory to put the .intunewin file>
```

Configuring Intune

To configure Intune:

1. Go to the Microsoft endpoint site and go to **Apps**.

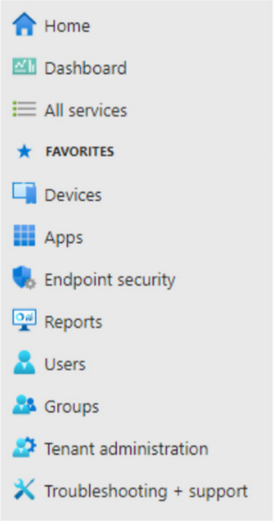
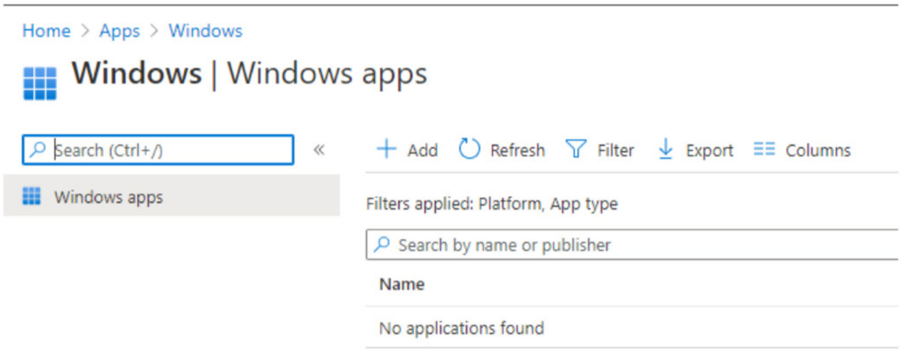


Figure 9. Microsoft Endpoint Apps

2. Click **Windows** > **+ Add** to add an application.

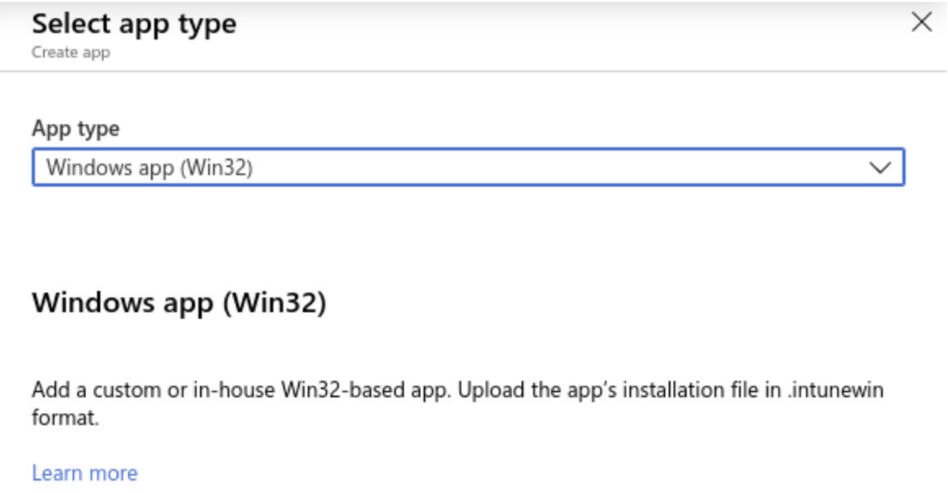


Filters applied: Platform, App type

No applications found

Figure 10. Add application

3. For the **App type**, select **Windows App (Win32)**.



App type: Windows app (Win32)

Windows app (Win32)

Add a custom or in-house Win32-based app. Upload the app's installation file in .intunewin format.

Figure 11. Select Windows app (Win32)

4. Click **Select app package file**.

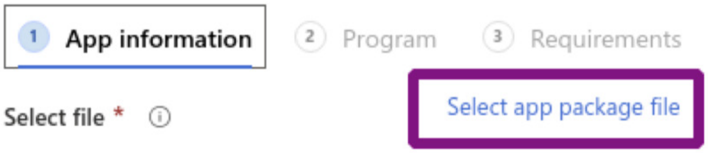
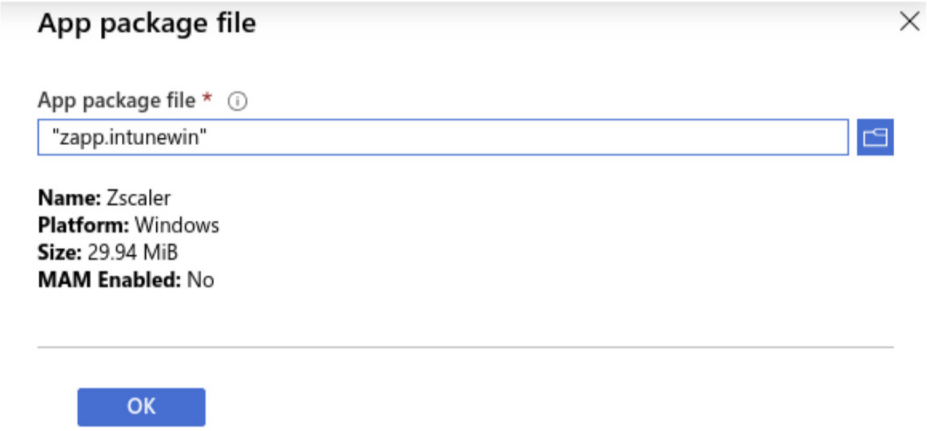


Figure 12. Select app package file

5. Browse and select your intunewin file.

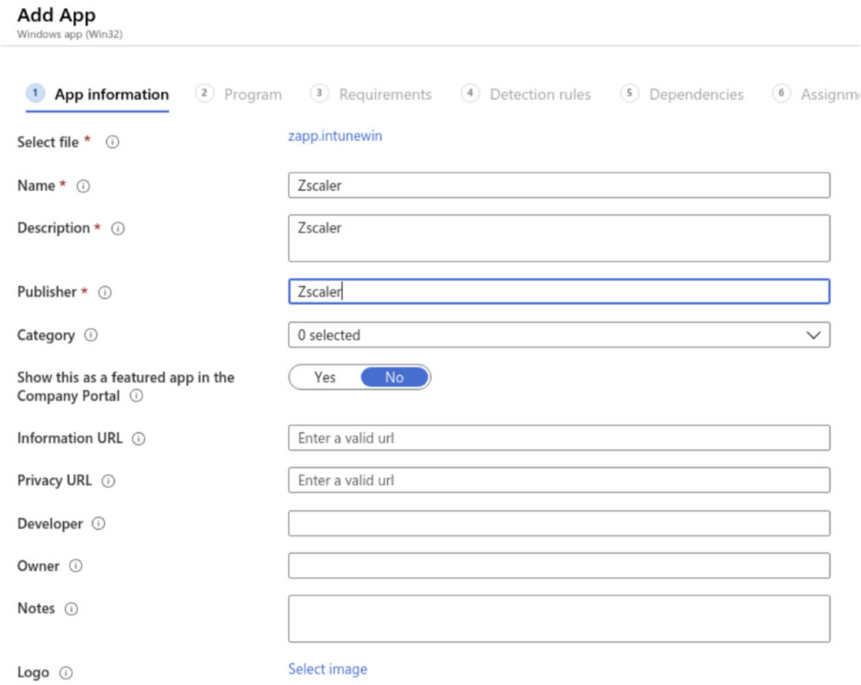


App package file *: "zapp.intunewin"

Name: Zscaler
Platform: Windows
Size: 29.94 MiB
MAM Enabled: No

Figure 13. App package file

6. Complete the required fields. Other fields can be left empty.



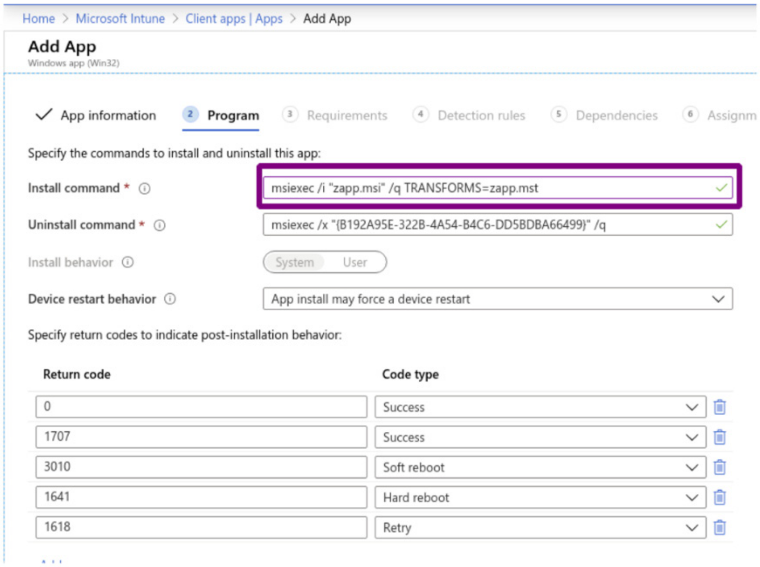
Select file *	zapp.intunewin
Name *	Zscaler
Description *	Zscaler
Publisher *	Zscaler
Category	0 selected
Show this as a featured app in the Company Portal	Yes [✓ No]
Information URL	Enter a valid url
Privacy URL	Enter a valid url
Developer	
Owner	
Notes	
Logo	Select image

Figure 14. App information

7. Click **Next**.
8. Enter the following for the install command:

```
Msiexec /I "<zscalerapp_installer_file>.msi" /qn TRANSFORMS=<transformFile>.mst
```

9. In example, the MSI file is called zapp.msi and the MST `zapp.mst`. The other fields are okay as they are, including the uninstall command.
10. Click **Next**.



Specify the commands to install and uninstall this app:

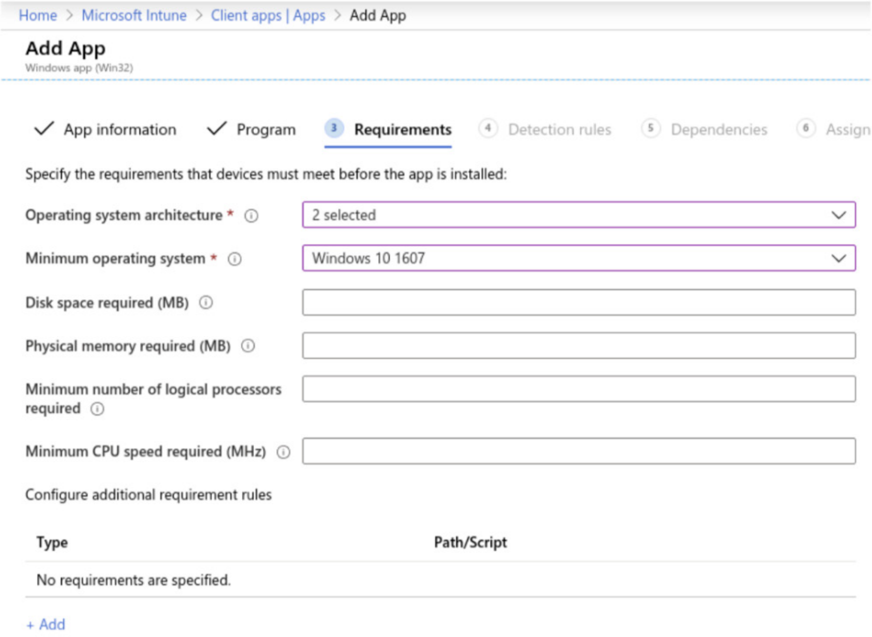
Install command *	msiexec /i "zapp.msi" /q TRANSFORMS=zapp.mst
Uninstall command *	msiexec /x "{B192A95E-322B-4A54-B4C6-DD5BDBA66499}" /q
Install behavior	System User
Device restart behavior	App install may force a device restart

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

Figure 15. Add App Program

11. For the Requirements screen, select both **32** and **64** bit for the **Operating system architecture** and **Windows 10 1607** as the **Minimum operating system**. (The other fields are not required and can be left empty.)
12. Click **Next**.



Home > Microsoft Intune > Client apps | Apps > Add App

Add App

Windows app (Win32)

✓ App information ✓ Program 3 Requirements 4 Detection rules 5 Dependencies 6 Assign

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * : 2 selected

Minimum operating system * : Windows 10 1607

Disk space required (MB):

Physical memory required (MB):

Minimum number of logical processors required:

Minimum CPU speed required (MHz):

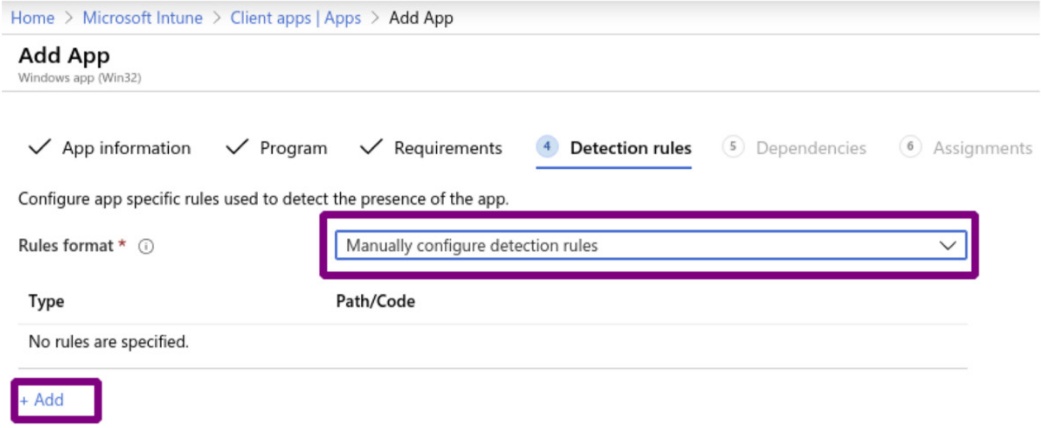
Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Figure 16. Requirements

13. For the **Detection rules**, select **Manually configure detection rules** as the **Rules format**.
14. Click **Add**.



Home > Microsoft Intune > Client apps | Apps > Add App

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements 4 Detection rules 5 Dependencies 6 Assignments

Configure app specific rules used to detect the presence of the app.

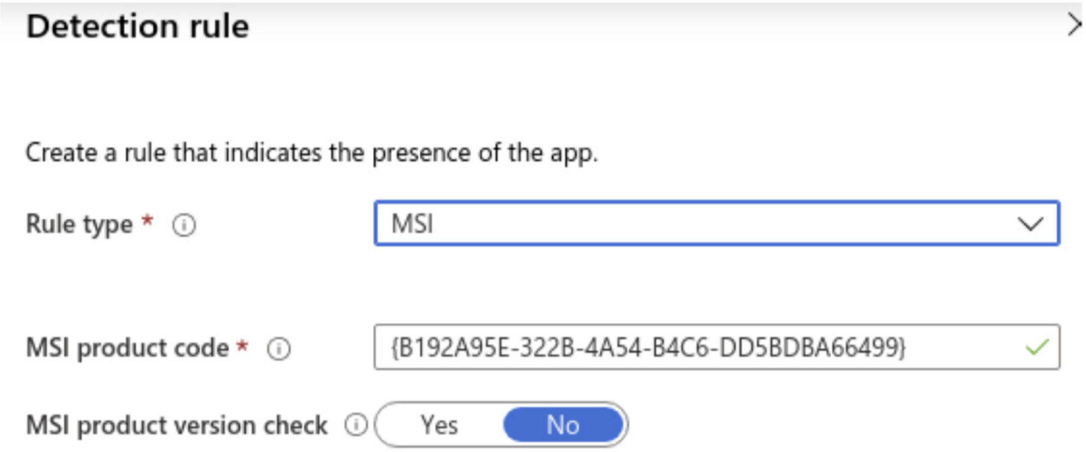
Rules format * : Manually configure detection rules

Type	Path/Code
No rules are specified.	

+ Add

Figure 17. Detection Rules

15. Select **MSI**. The MSI product code is pre-filled.
16. Click **OK**, then **Next**.



Detection rule

Create a rule that indicates the presence of the app.

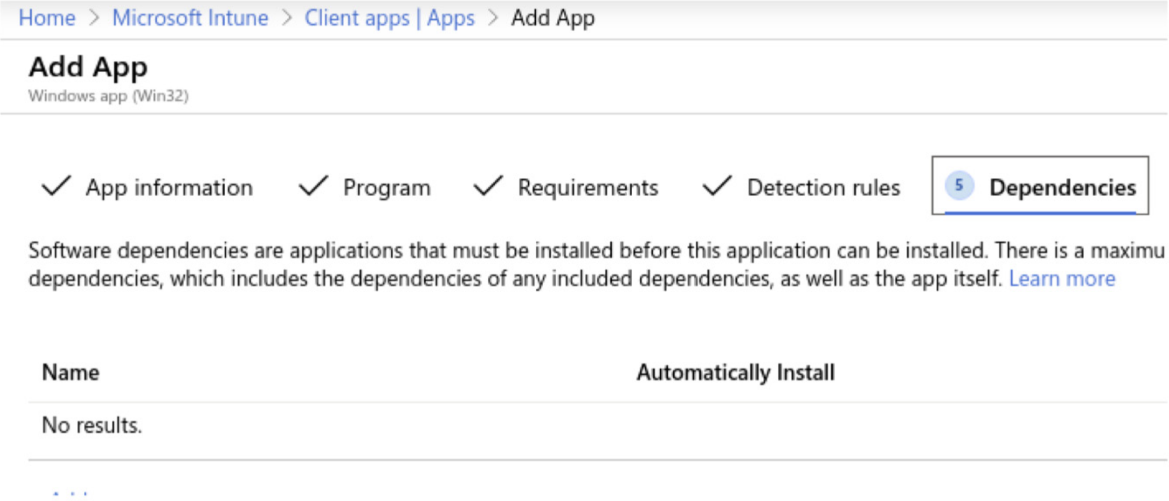
Rule type * : MSI

MSI product code * : {B192A95E-322B-4A54-B4C6-DD5BDBA66499}

MSI product version check: Yes [✓ No]

Figure 18. Detection rule

17. There are no dependencies. Click **Next**.



Home > Microsoft Intune > Client apps | Apps > Add App

Add App

Windows app (Win32)

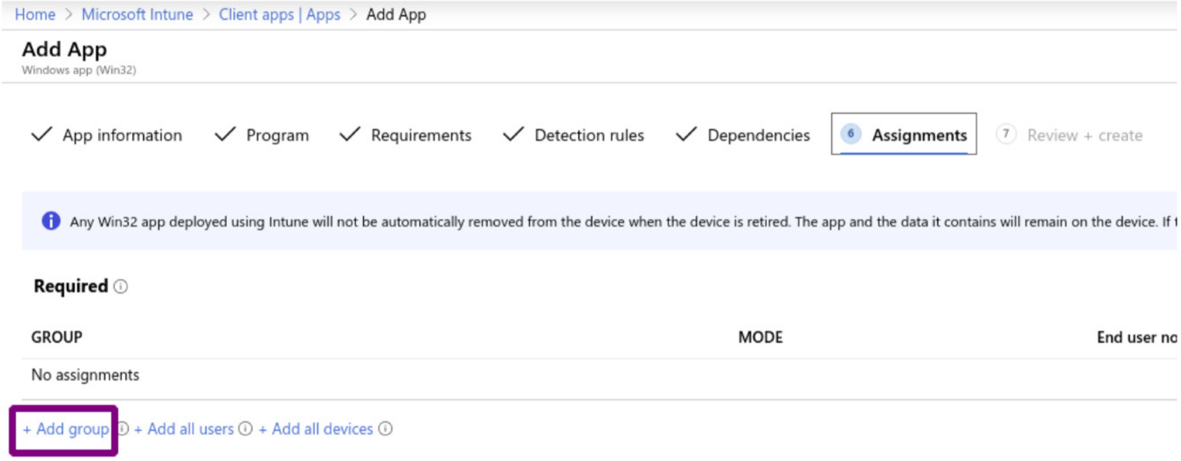
✓ App information ✓ Program ✓ Requirements ✓ Detection rules 5 Dependencies

Software dependencies are applications that must be installed before this application can be installed. There is a maximu dependencies, which includes the dependencies of any included dependencies, as well as the app itself. Learn more

Name	Automatically Install
No results.	

Figure 19. Dependencies

18. Assign this app to the Autopilot group you created as part of the prerequisites. Click **Add Group**.



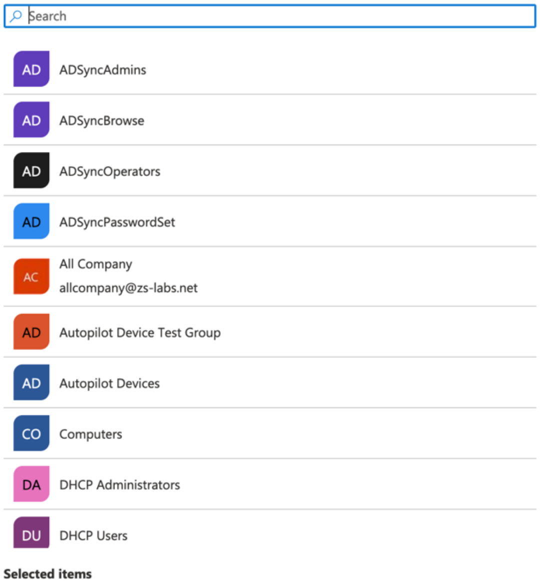
Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device. If t

Required

GROUP	MODE	End user no
No assignments		

Figure 20. Assignments

19. Select **Autopilot Devices** from the list.

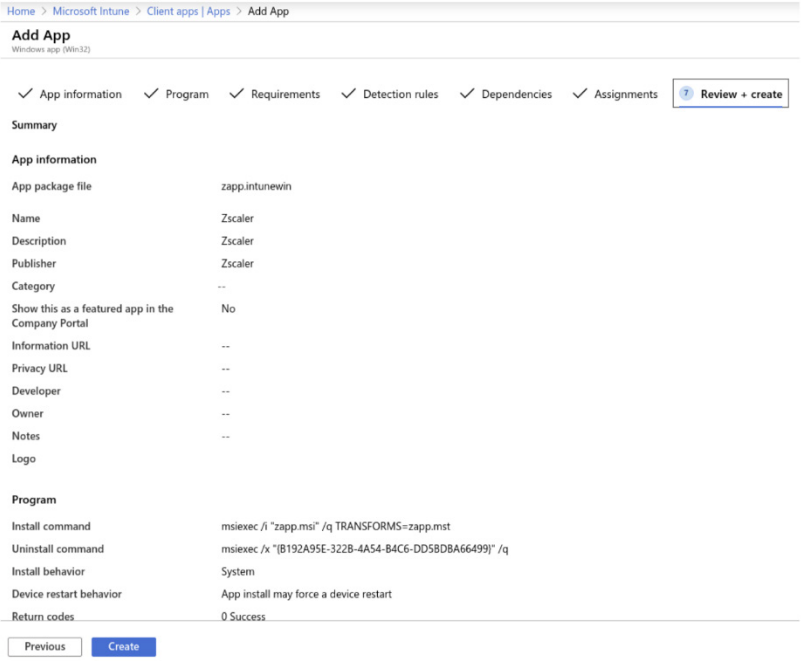


AD ADSyncAdmins
AD ADSyncBrowse
AD ADSyncOperators
AD ADSyncPasswordSet
AC All Company allcompany@zs-labs.net
AD Autopilot Device Test Group
AD Autopilot Devices
CO Computers
DA DHCP Administrators
DU DHCP Users

Selected items

Figure 21. Search

20. Review and click **Create**.



Add App

Windows app (Win32)

Summary

App information

App package file	zapp.intunewin
Name	Zscaler
Description	Zscaler
Publisher	Zscaler
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	

Program

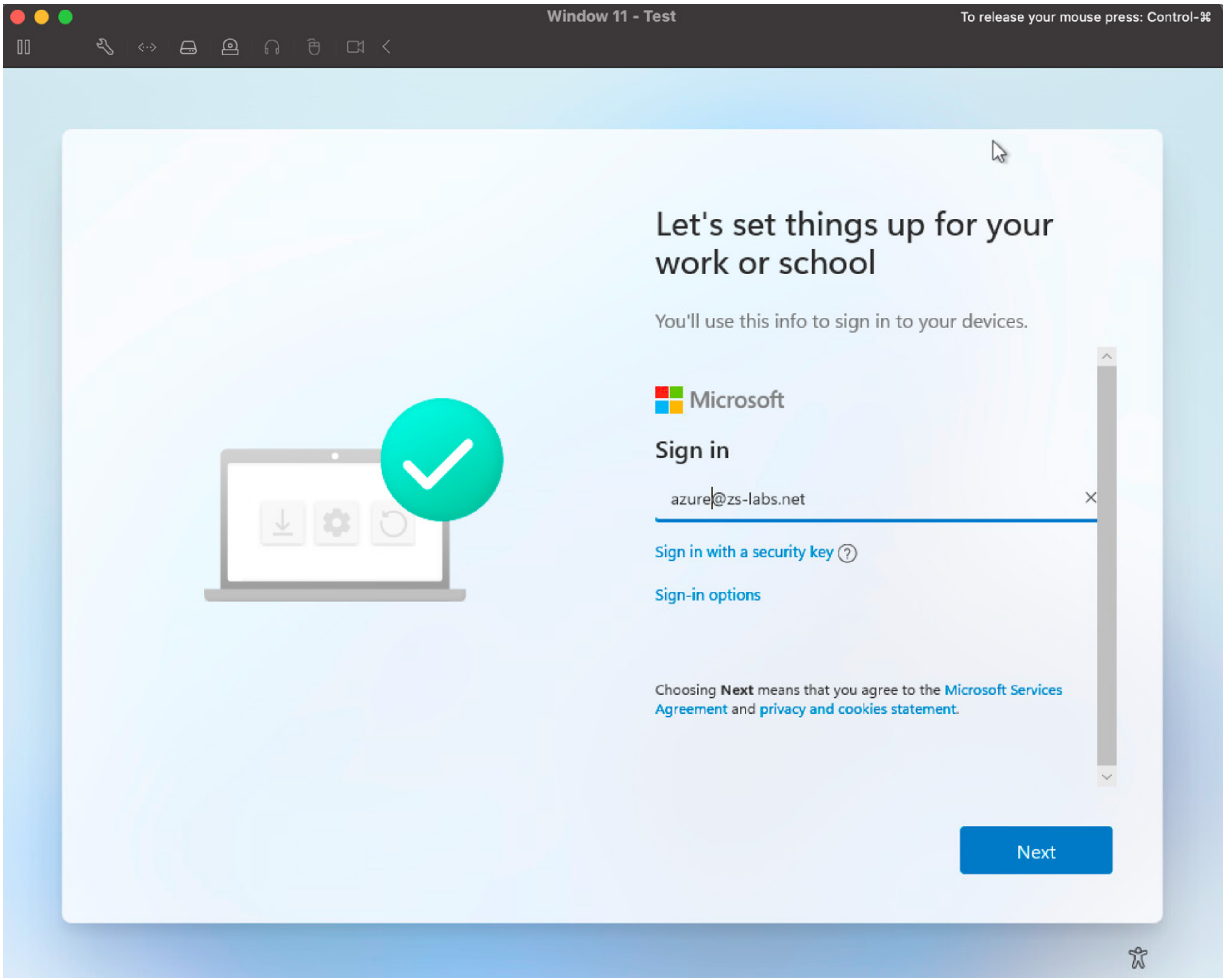
Install command	msiexec /i "zapp.msi" /q TRANSFORMS=zapp.mst
Uninstall command	msiexec /x "{B192A95E-322B-4A54-B4C6-DD5BDBA66499}" /q
Install behavior	System
Device restart behavior	App install may force a device restart
Return codes	0 Success

Figure 22. Review + create

Zscaler Client Connector now installs automatically as part of the Autopilot provisioning process and provides a device access to on premises AD resources before a user logs in for the first time.

Verify Zscaler Client Connector is Deployed as Part of the Enrollment Process

The following screenshots show a successful enrollment of a Windows 11 device using Hybrid Microsoft Entra ID Join with ZPA for connectivity to on-premises AD.



Window 11 - Test
To release your mouse press: Control-⌘

Let's set things up for your work or school

You'll use this info to sign in to your devices.

Microsoft

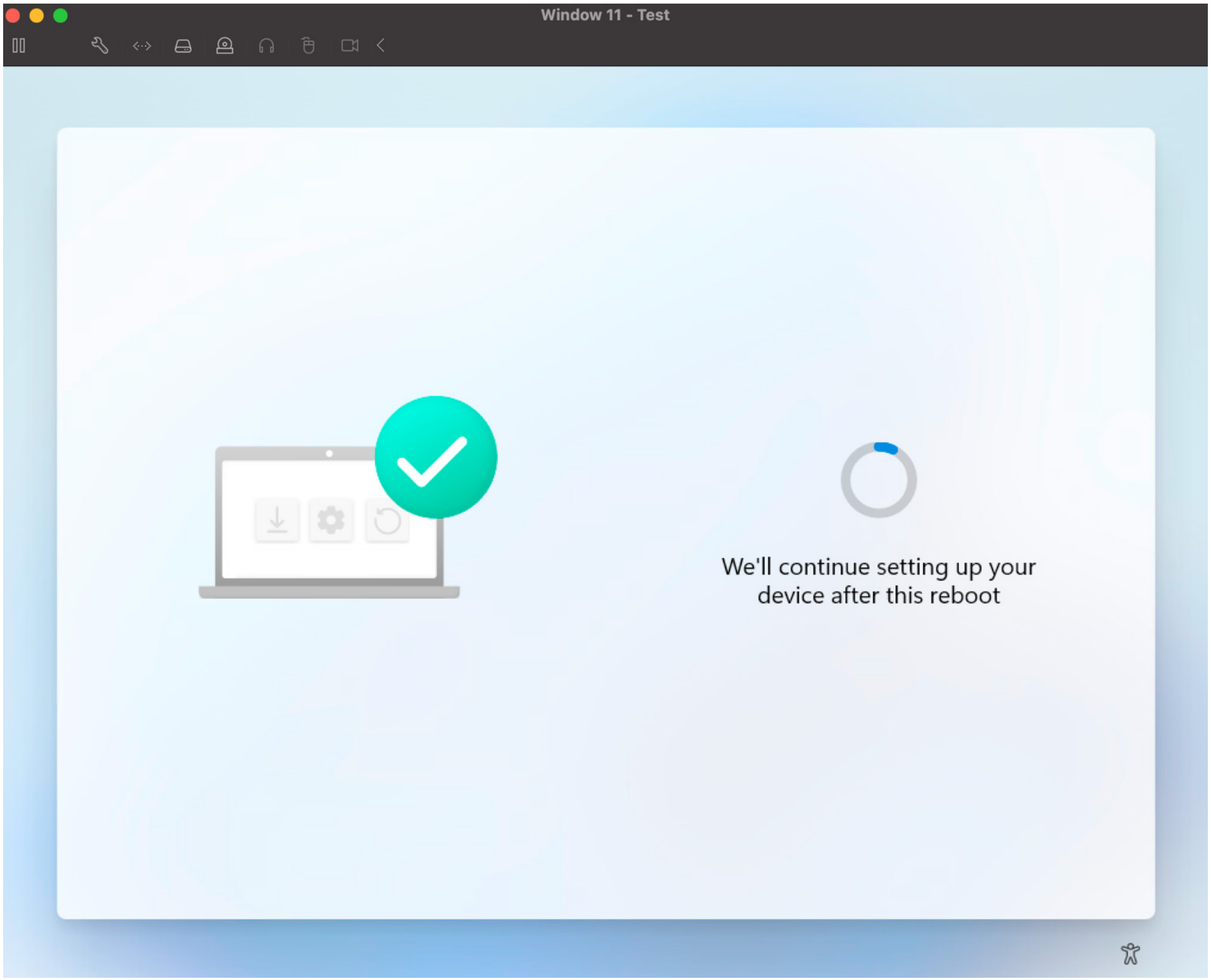
Sign in

azure@zs-labs.net

Sign in with a security key
Sign-in options

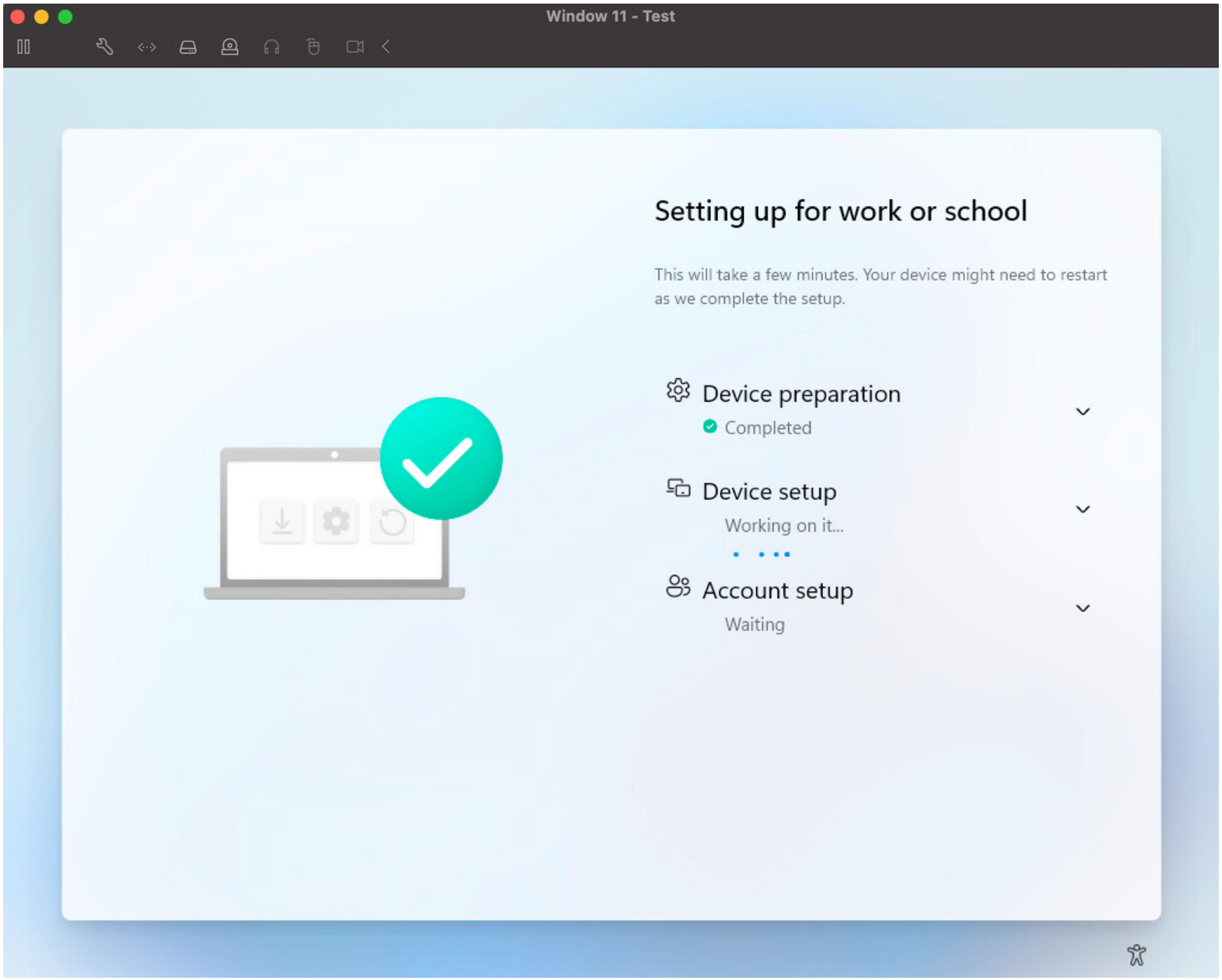
Choosing **Next** means that you agree to the Microsoft Services Agreement and privacy and cookies statement.

Figure 23. Enter in login credentials (Ensure account has assigned Intune License)



We'll continue setting up your device after this reboot

Figure 24. Device reboots once initial settings have been applied



Setting up for work or school

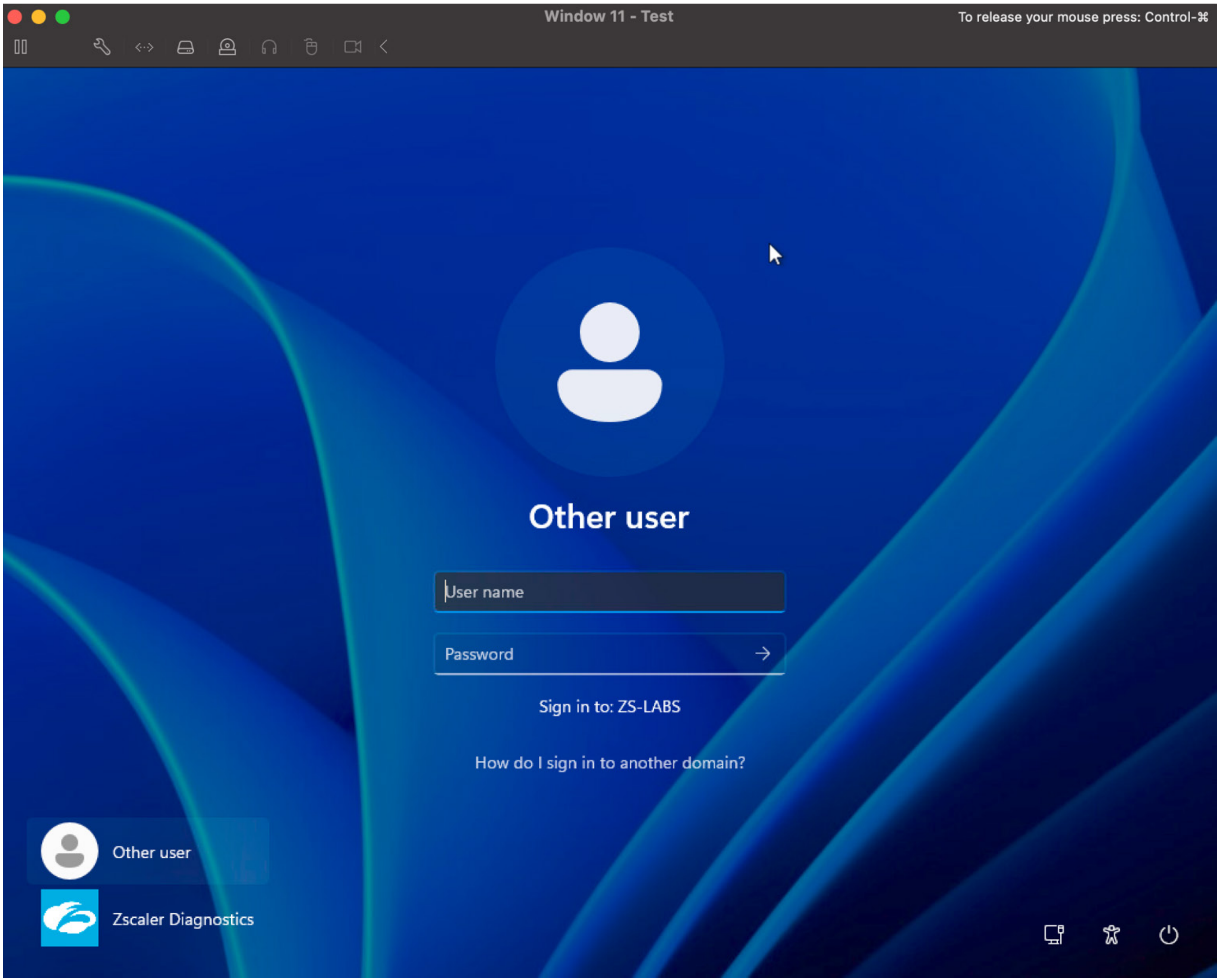
This will take a few minutes. Your device might need to restart as we complete the setup.

Device preparation
Completed

Device setup
Working on it...

Account setup
Waiting

Figure 25. Device profile settings is applied after reboot



Window 11 - Test

To release your mouse press: Control-⌘

Other user

User name

Password

Sign in to: ZS-LABS

How do I sign in to another domain?

Figure 26. Login screen with Zscaler Diagnostics icon confirming ZCC is installed with pre-login connectivity to AD

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//365. To contact Zscaler Support:

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

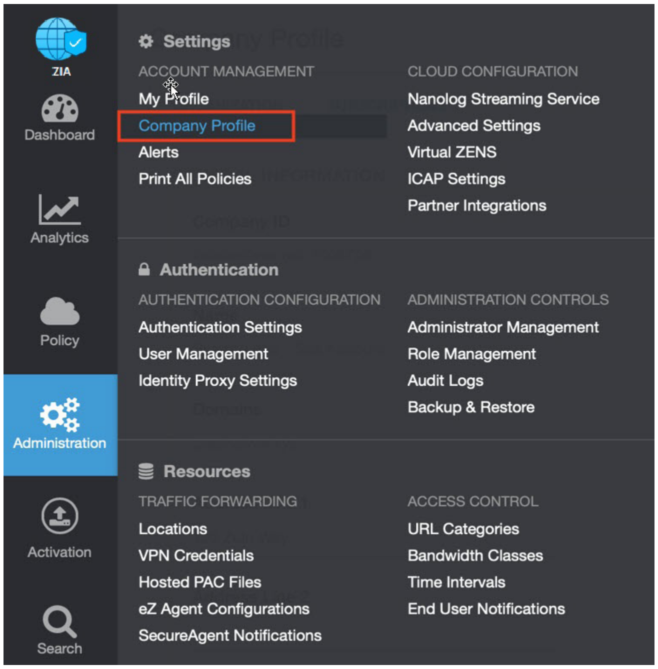
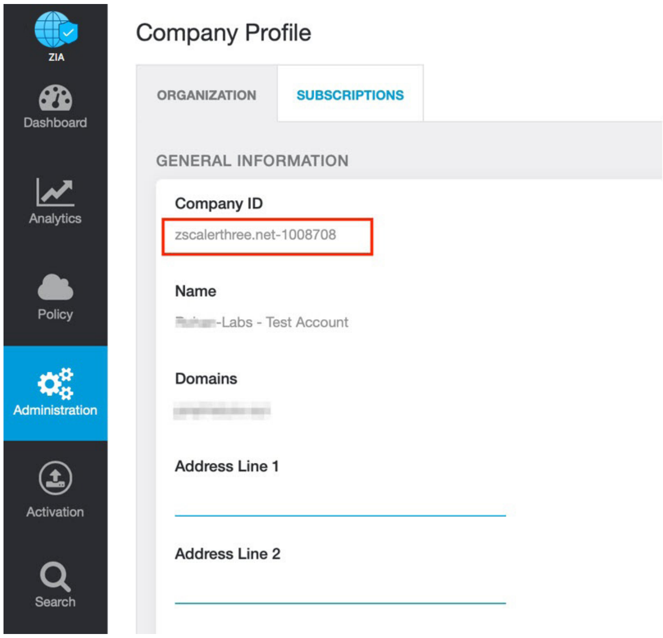


Figure 27. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 28. Company ID

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

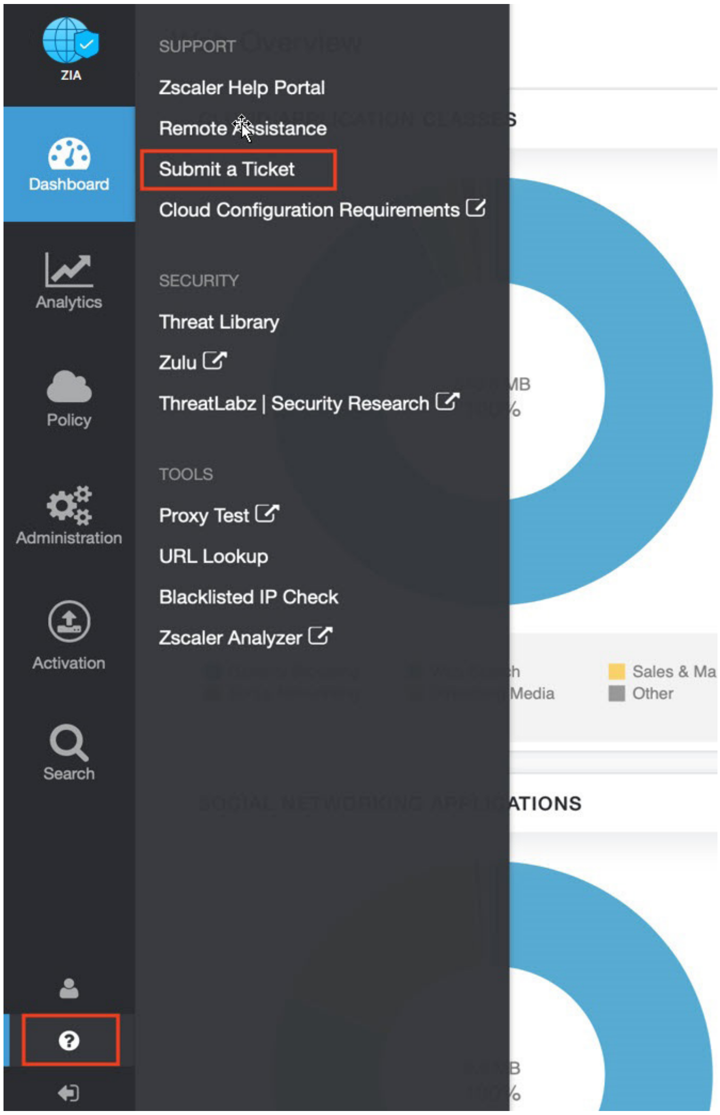


Figure 29. Submit a Ticket