

# **Unveiling the Power of Defender for Endpoint for macOS New Features and Public Preview**

# About me



Security Architect



Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



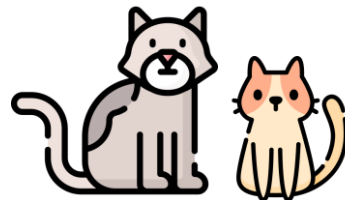
Google Cloud



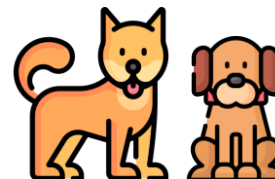
1 Husband



1 Daughter



2 cats



2 dogs



Detective stories



Photography

# Agenda

Microsoft Defender for Endpoint – a short introduction

Enrollment process

What's new in Microsoft Defender for Endpoint on Mac

Microsoft Copilot for Security

# Microsoft Defender for Endpoint

- Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Example endpoints may include laptops, phones, tablets, PCs, access points, routers, and firewalls.



Core Defender  
Vulnerability  
Management



Attack surface  
reduction



Next-generation  
protection



Endpoint detection  
and response



Automated investigation  
and remediation



Microsoft  
Threat Experts

---

Centralized configuration and administration, APIs

---

Microsoft Defender XDR

# Microsoft Defender for Endpoint

## Microsoft Defender for Endpoint Plans

- Microsoft Defender for Endpoint is available in two plans, Defender for Endpoint Plan 1 and Plan 2.
- A new Microsoft Defender Vulnerability Management add-on is now available for Plan 2.

## macOS devices

Before starting the onboarding, see the main Microsoft Defender for Endpoint on macOS page for a description of prerequisites and system requirements for the current software version.

<https://learn.microsoft.com/en-us/defender-endpoint/mac-install-with-intune#prerequisites-and-system-requirements>

## Onboarding Defender for Endpoint to macOS

The macOS devices can be added to the ABM portal via Apple Reseller or via Apple Configurator tool). For more information, you can reach to Apple's documentation Device eligibility for Apple Business Manager (ABM).



## Onboarding Defender for Endpoint to macOS

It is possible to add the following to Apple School Manager, Apple Business Manager, or Apple Business Essentials using Apple Configurator on your iPhone, even if the devices weren't purchased directly from Apple or an Apple Authorized Reseller or cellular carrier:

- iPhone
- iPad
- Mac computers with Apple silicon or with an Apple T2 Security Chip

## Onboarding Defender for Endpoint to macOS

- Anyway, for Mac's it doesn't matter how they are Enrolled to MDM because will be always Supervised therefore single MDE Onboarding process for all of them.
- It is possible to Set a default MDM server for all device types like Mac, meaning that any added devices to the ABM portal will be automatically assigned to favorite MDM platform.

Microsoft Intune admin center

Home > Devices

## Devices | Configuration

Search

Overview  
All devices  
Monitor

By platform

- Windows
- iOS/iPadOS
- macOS
- Android
- Linux

Device onboarding

- Windows 365
- Enrollment

Manage devices

- Configuration
- Compliance

Policies Import ADMX Monitor

August 30th, 2024 marks the end of Microsoft Intune support for Android device administrator management on devices with access to Google Mobile Services (GMS). Use alternate Intune Android management options instead. [Learn more about ending support for Android device administrator.](#)

+ Create Refresh Export Columns 7 policies

MDE Add filters

Policy name	Platform	Policy type	Last modified
<a href="#">MDE Background Services profile on macOS</a>	macOS	Custom	3/20/2023, 11:12:35 PM
<a href="#">MDE Full Disk Access profile on macOS</a>	macOS	Custom	3/20/2023, 4:11:19 PM
<a href="#">MDE Network Filter profile on macOS</a>	macOS	Custom	3/20/2023, 4:23:32 PM
<a href="#">MDE Notifications profile on macOS</a>	macOS	Custom	3/20/2023, 4:31:34 PM
<a href="#">MDE Offboarding profile on macOS</a>	macOS	Custom	5/17/2023, 12:21:54 PM
<a href="#">MDE Onboarding profile on macOS</a>	macOS	Custom	3/19/2023, 8:17:42 PM
<a href="#">MDE System Extensions profile on macOS</a>	macOS	Extensions	3/20/2023, 3:45:51 PM

# Intune Configuration Policies

## Enroll My Mac

Go to [Enroll My Mac](#).

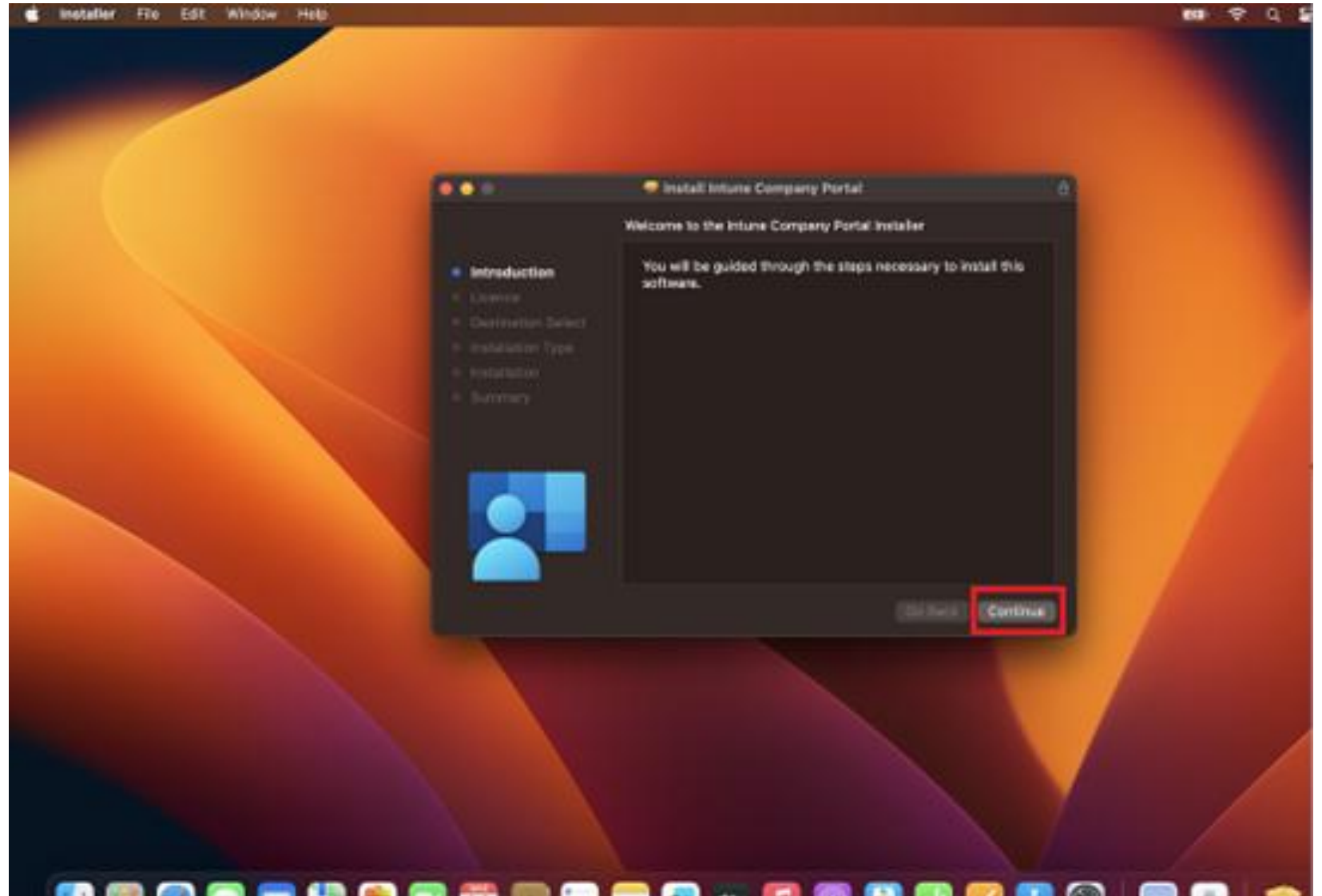
The **Company Portal** installer .pkg file will be downloaded. Open the installer and **follow the on-screen instructions**.

**Note:** These steps may vary slightly depending on the brand of the macOS device.

# Enroll My Mac



# Enroll My Mac

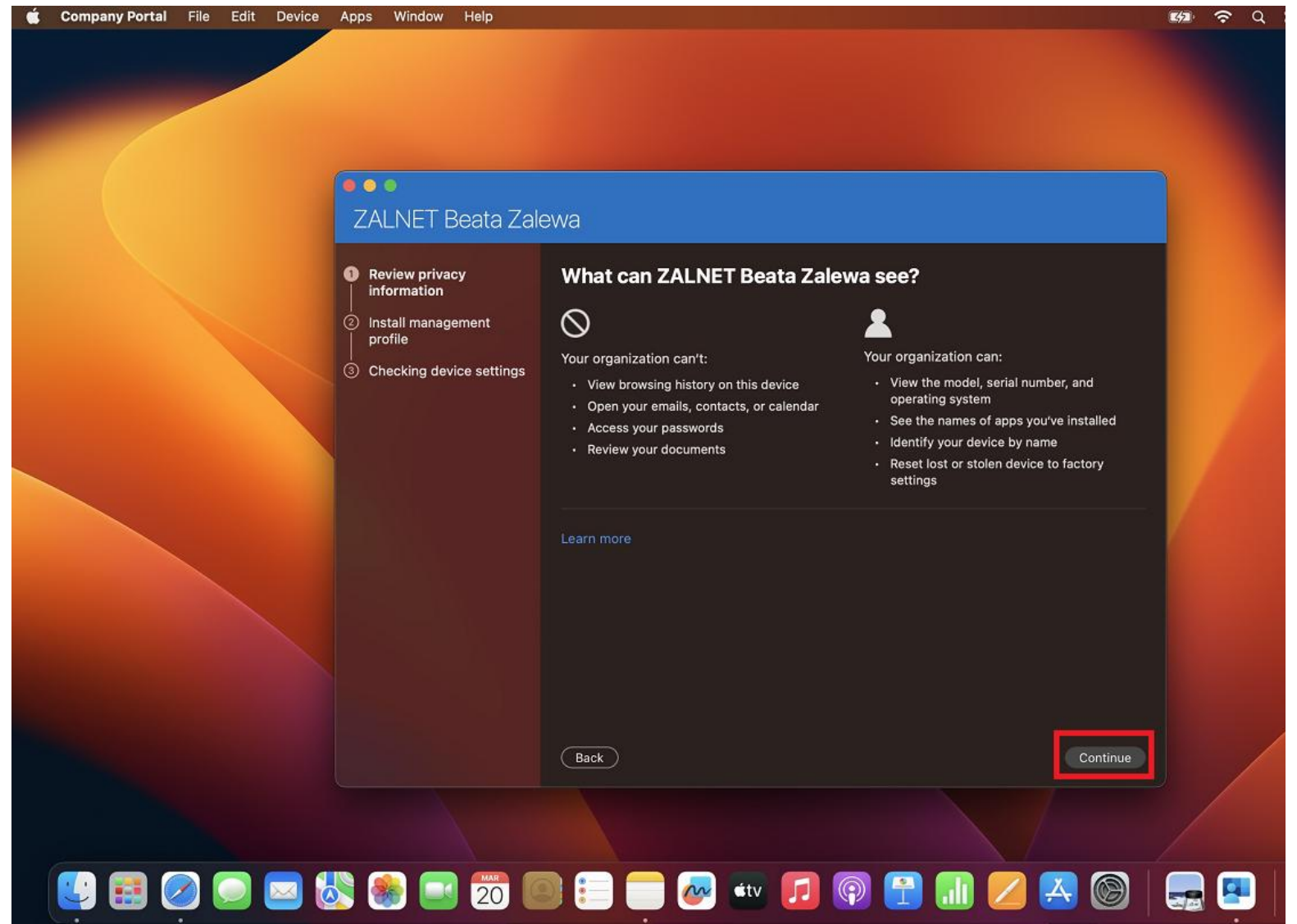


# Company Portal



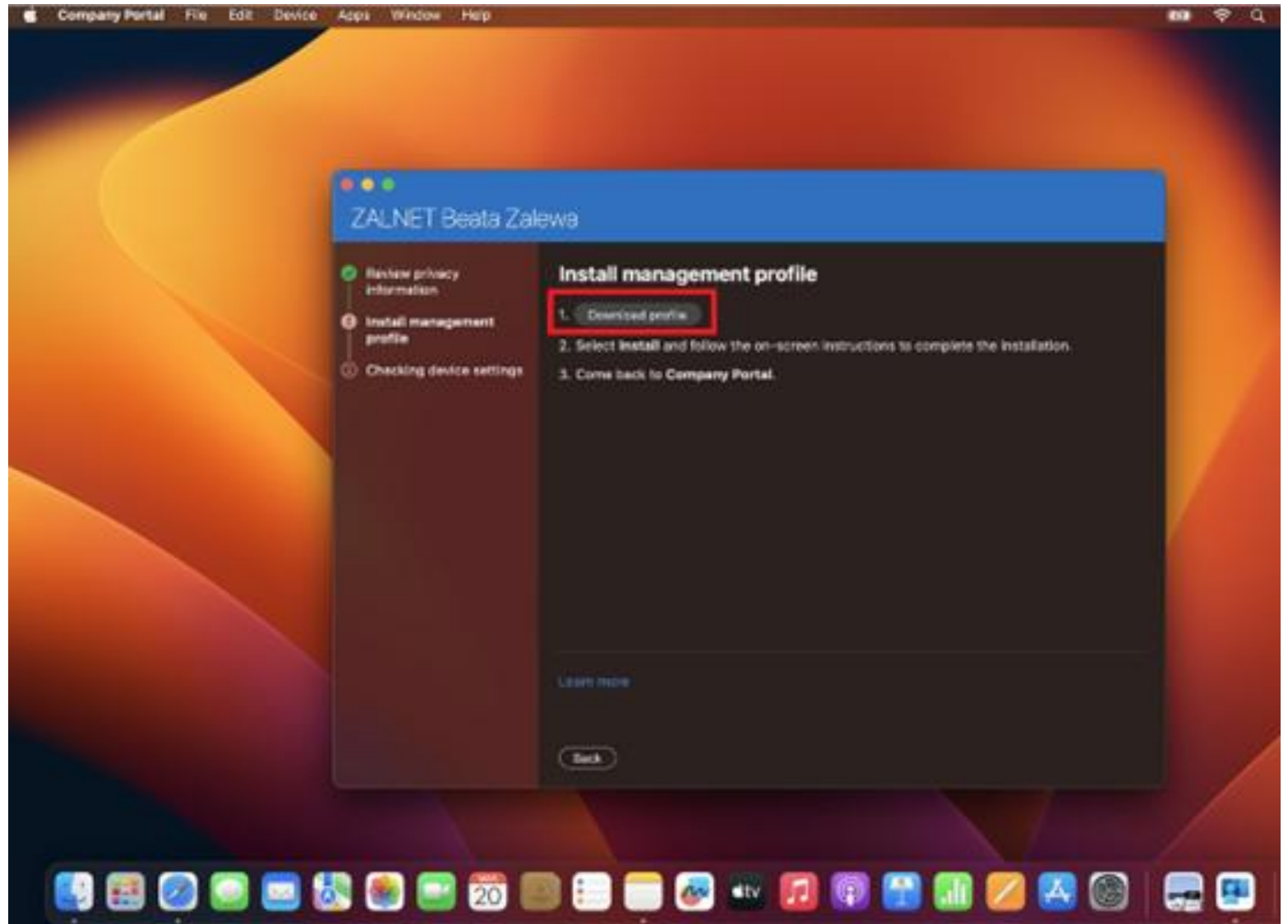


# Company Portal

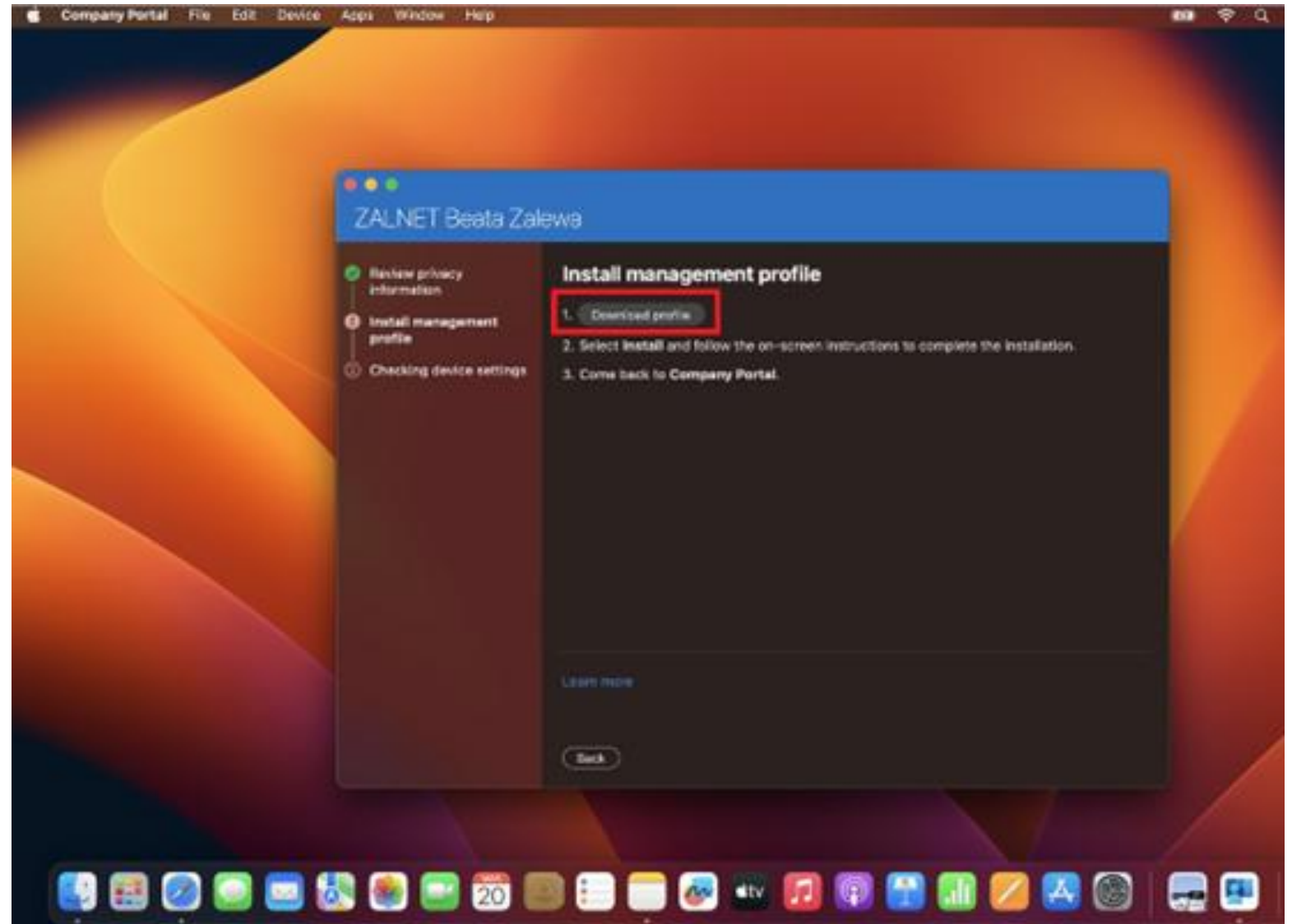




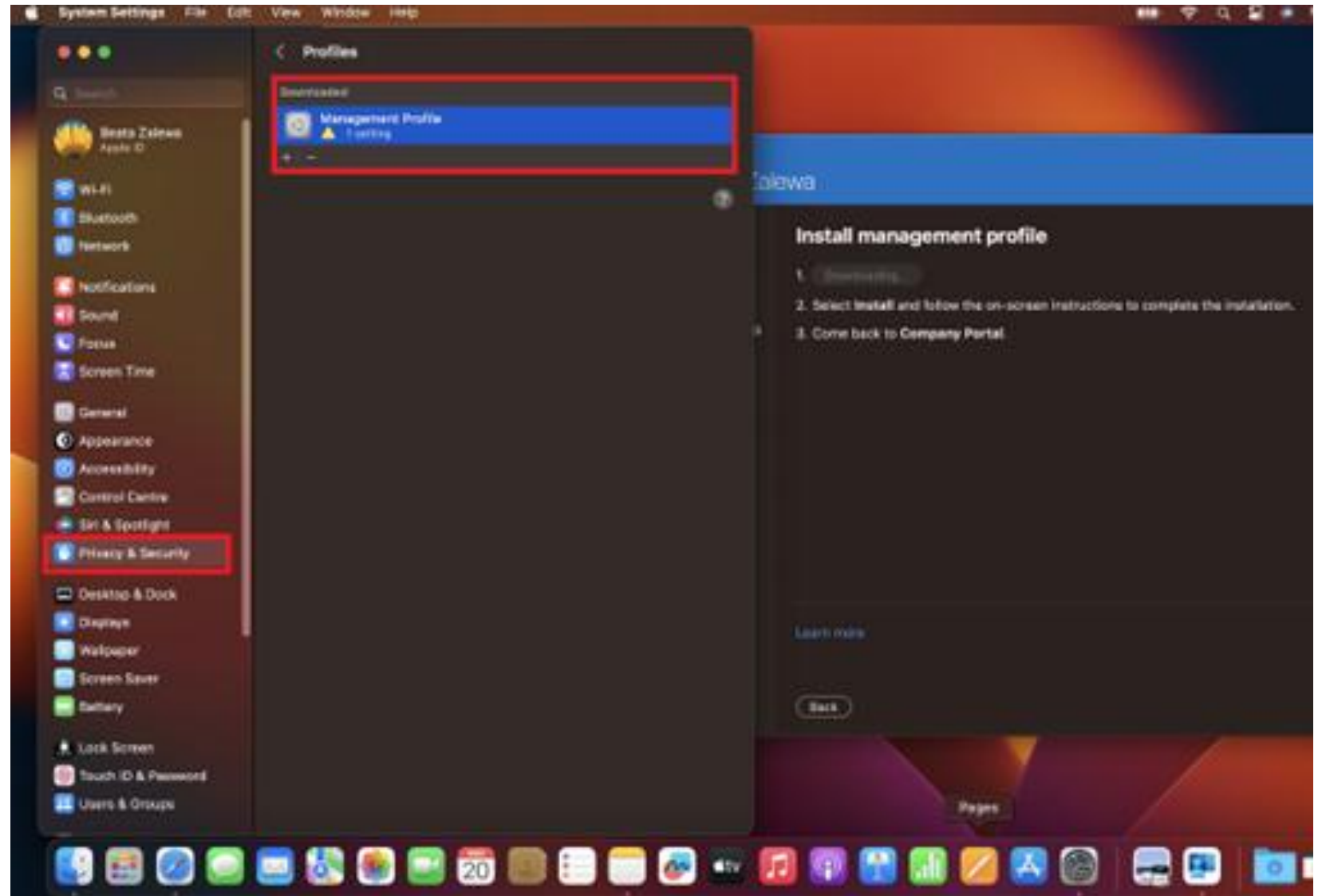
# Company Portal



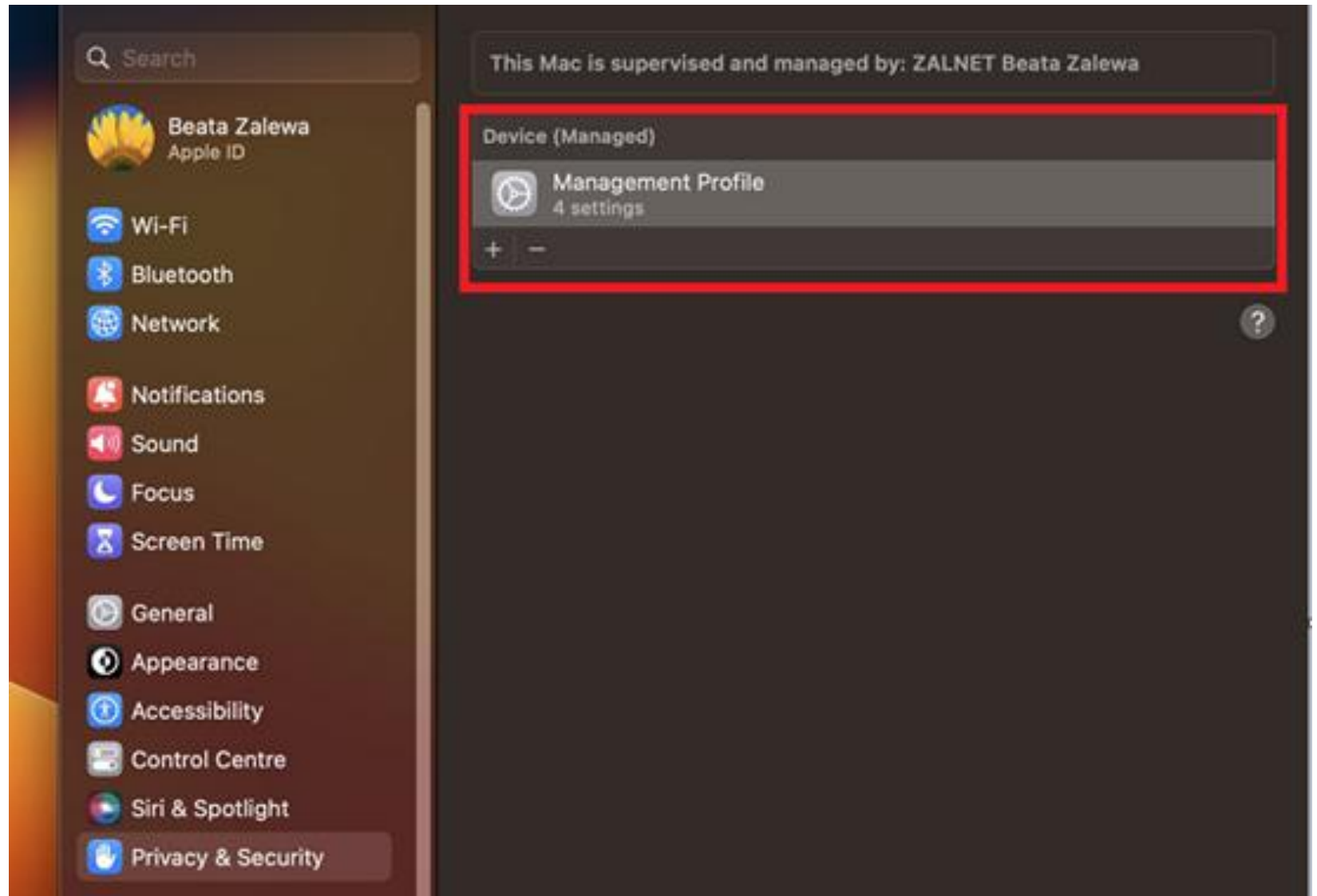
# Company Portal



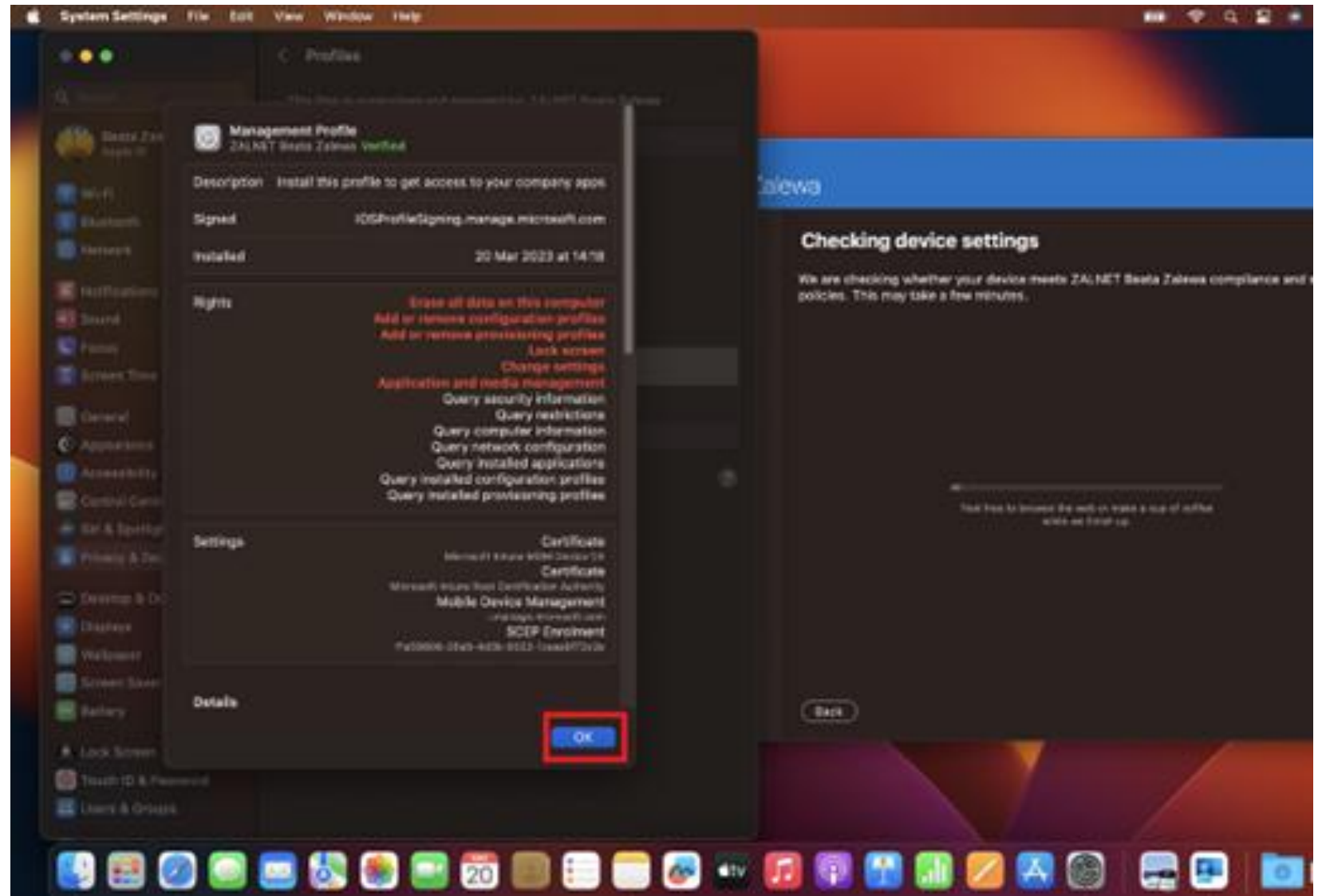
# Company Portal



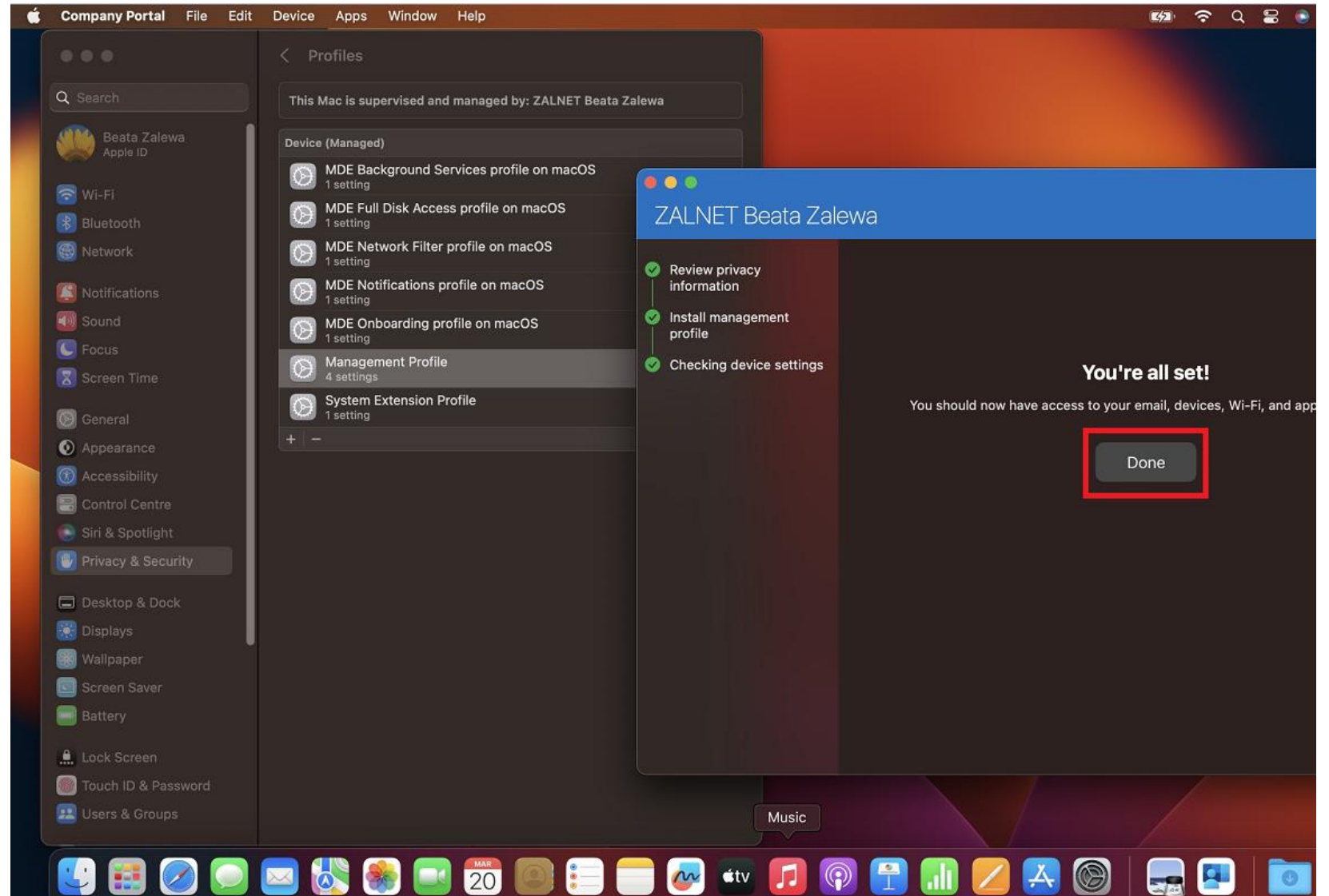
# Company Portal



# Company Portal

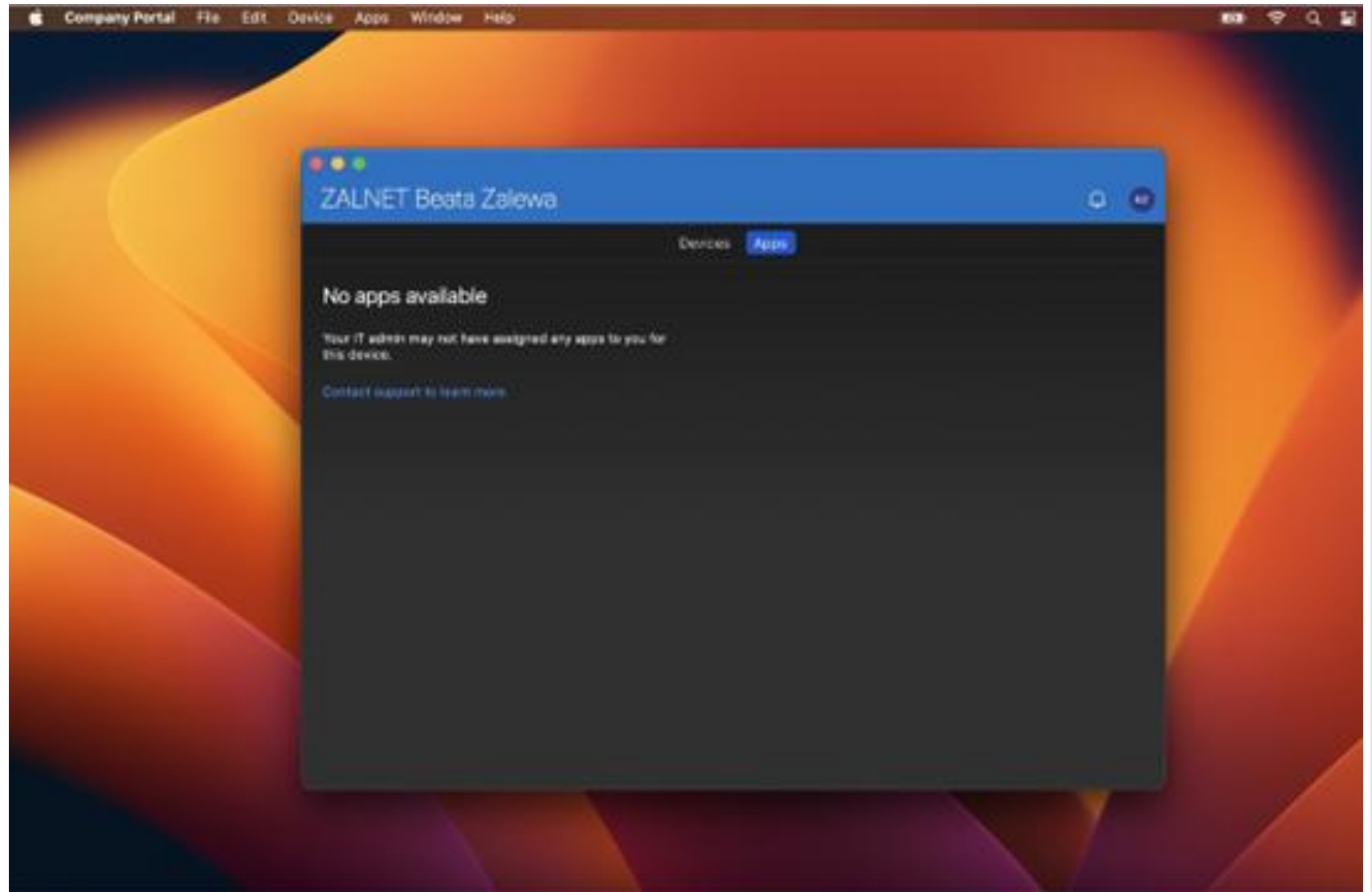


# Company Portal





# Company Portal



## Microsoft Defender XDR portal

Upon successful onboarding, the device will start showing up on the Devices list in the Microsoft Defender XDR portal  
<https://security.microsoft.com/>





# Microsoft Defender XDR portal

Defender

Search


## Device Inventory



 **Upgrade your vulnerability management capabilities** ...  
Try app control, baseline assessments, and more.


 Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.

Computers & Mobile   Network devices   IoT devices   Uncategorized devices

Total **3**   Critical assets **0**   High risk **0**   High exposure **0**   Not onboarded **0**

 Export   Search   30 Days   Current

Filters: Transient device: No    Exclusion state: Not Excluded 

<input type="checkbox"/>	Name	Domain	Device AAD id	Risk level  ↓	Exposure level
<input type="checkbox"/>	zalnet-dell5300	AAD joined	17fd599b-61f9-4b43-a727-6e65be8b6a28	■■■ No known risks ▲ Low	
<input type="checkbox"/>	Beatas-MacBook-Air	Workgroup		■■■ No known risks No data available	
<input type="checkbox"/>	Macbook-MDE-034525	Workgroup		■■■ No known risks ▲ Low	

# Microsoft Defender XDR portal

The screenshot displays the Microsoft Defender XDR portal interface. On the left is a navigation sidebar with categories like Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Configuration management, Identities, Dashboard, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, and Exchange message trace. The main content area is titled 'Device Inventory > Beatas-MacBook-Air'. It features a header with a search bar and user profile. Below the header, the device name 'Beatas-MacBook-Air' is prominently displayed with a status bar indicating 'No known risks' and 'Criticality: None'. A tabbed interface shows 'Overview' as the active tab, with other tabs including 'Incidents and alerts', 'Timeline', 'Security recommendations', 'Inventories', 'Discovered vulnerabilities', and 'Security policies'. The 'Overview' section is divided into three panels: 'Device details' on the left, 'Active alerts (Last 180 days)' in the center, and 'Security assessments' on the right. The 'Device details' panel lists attributes such as Domain (Workgroup), OS (macOS 64-bit), SAM name (Asset group), Health state (Active), and IP addresses (192.168.1.01.37). The 'Active alerts' panel shows 'No active alerts or incidents' with a graphic of three floating cards. The 'Security assessments' panel displays 'Exposure level: Info' and '0 active security recommendations'. At the bottom, the 'Logged on users (Last 30 days)' section shows '0 logged on users'.

Microsoft Defender

Search

Device Inventory > Beatas-MacBook-Air

Beatas-MacBook-Air

No known risks Criticality: None MacOS devices group

Copilot View in map

Overview Incidents and alerts Timeline Security recommendations Inventories Discovered vulnerabilities Security policies

Device details

Domain	OS
Workgroup	macOS 64-bit (Release Sonoma 14.5)
SAM name	Asset group MacOS devices group
Health state	Data sensitivity
Active	None
IP addresses	First seen
192.168.1.01.37	May 21, 2024 3:25:22 PM
<a href="#">See IP addresses info</a>	

Active alerts (Last 180 days)

No active alerts or incidents

Security assessments

Exposure level: Info

0 active security recommendations

Logged on users (Last 30 days)

0 logged on users

There were no logged on users during the given time range

## Unsupported macOS versions

Microsoft Defender for Endpoint no longer supports macOS Catalina (10.15) as Apple ended support for Catalina (10.15) in December 2022.

Microsoft Defender for Endpoint no longer supports Big Sur (11).

## What's new

- Improvements to **mdatp threat** command
- Fix Bluetooth support on Sonoma (You need to deploy a new MDM configuration profile for Defender to access Bluetooth)
- Endpoint Attack Notifications

# What's new

Search

Settings > Endpoints

## Endpoints

**General**

**Advanced features**

Licenses

Email notifications

Auto remediation

**Permissions**

Roles

Device groups

**APIs**

SIEM

☒ On

**Preview features**

Allow access to preview features. Turn on to be among the first to try upcoming features.

See the [Microsoft Defender for Endpoint preview features](#) section in the [Microsoft Defender for Endpoint guide](#).

**Endpoint Attack Notifications**

Enables Microsoft to actively hunt for critical threats to be prioritized based on urgency and impact over your endpoint data. For proactive hunting across the full scope of Microsoft Defender XDR including threats that span email, collaboration, identity, cloud applications, as well as endpoints, [learn more](#) about Microsoft Defender Experts.

Apply

Save preferences

## Behaviour monitoring in Microsoft Defender Antivirus on macOS

Behaviour monitoring monitors process behaviour to detect and analyze potential threats based on the behaviour of the applications, daemons, and files within the system.

As behavior monitoring observes how the software behaves in real-time, it can adapt quickly to new and evolving threats and block them.

<https://learn.microsoft.com/en-us/defender-endpoint/behavior-monitor-macos>

# Behaviour monitoring in Microsoft Defender Antivirus on macOS

## Prerequisites:

- Device is onboarded to Microsoft Defender for Endpoint.
- [Preview features](https://security.microsoft.com) is enabled in the Microsoft XDR portal (<https://security.microsoft.com>).
- Device must be in the [Beta channel](#) (formerly InsiderFast).
- Minimal Microsoft Defender for Endpoint version number must be Beta (Insiders-Fast): 101.24042.0002 or newer. Version number refers to the **app\_version** (also known as **Platform update**).
- Ensure that Real-Time Protection (RTP) is enabled.
- Ensure [cloud-delivered protection](#) is enabled.
- Device must be explicitly enrolled into the preview.

# Behaviour monitoring in Microsoft Defender Antivirus on macOS

Microsoft Intune admin center

Home >

## MDE Behavior monitoring on macOS

Device Configuration Profiles

Summarize with Copilot Delete

### Properties

#### Basics Edit

Name	MDE Behavior monitoring on macOS
Description	Behavior monitoring in Microsoft Defender Antivirus on macOS
Platform	macOS
Profile type	Custom

#### Assignments Edit

Included groups	All Users All Devices
Excluded groups	No Excluded groups

#### Scope tags Edit

Default

#### Configuration settings Edit

Custom Configuration Profile

Custom configuration profile name com.microsoft.wdav

Configuration profile file

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
```



# Behaviour monitoring in Microsoft Defender Antivirus on macOS

## Manual deployment

You can enable Behavior Monitoring on Microsoft Defender for Endpoint on macOS by running the following command from the Terminal:

```
sudo mdatp config behavior-monitoring --value enabled
```

## Verifying Behavior Monitoring detection

The existing Microsoft Defender for Endpoint on macOS command line interface can be used to review behavior monitoring details and artifacts.

```
sudo mdatp threat list
```

# Enable troubleshooting mode on macOS

The screenshot shows the Microsoft Defender Security Center interface for a device named "Beatas-MacBook-Air". The interface is in the "Device Inventory" section, showing the device's status as "No known risks" with a "Criticality: None" and it belongs to the "MacOS devices group". The "Overview" tab is selected, displaying "Device details" on the left and "Active alerts (Last 180 days)" on the right. The "Device details" section shows the following information:

Device details	
Domain	OS
Workgroup	macOS (Release Sonoma 14.5)
SAM name	Asset group
-	MacOS devices group
Health state	Data sensitivity
Active	None

The "Active alerts (Last 180 days)" section shows "No active alerts or incidents". The "Security assessments" section shows "Exposure level: Info" and "0 active security recommendations". On the right side, a "Copilot" button is visible, and a list of actions is displayed, including "View in map", "Device value", "Set criticality", "Manage tags", "Report device inaccuracy", "Run Antivirus Scan", "Collect Investigation", "Initiate Live Response", "Isolate Device", "Ask Defender Expert", "Action center", "Exclude", "Go hunt", and "Turn on troubleshooting" (highlighted in yellow).


# Advanced hunting query for detection

<https://learn.microsoft.com/en-us/defender-endpoint/mac-troubleshoot-mode#advanced-hunting-queries-for-detection>

## Get troubleshooting events for a particular device

You can use the following query to search by `deviceId` or `deviceName` by commenting out the respective lines.

Kusto

 Copy

```
//let deviceName = "<deviceName>"; // update with device name
let deviceId = "<deviceId>"; // update with device id
DeviceEvents
| where DeviceId == deviceId
//| where DeviceName == deviceName
| where ActionType == "AntivirusTroubleshootModeEvent"
| extend _tsmodeproperties = parse_json(AdditionalFields)
| project Timestamp, DeviceId, DeviceName, _tsmodeproperties,
_tsmodeproperties.TroubleshootingState, _tsmodeproperties.TroubleshootingPreviousState, _tsmodeproperties.1
_tsmodeproperties.TroubleshootingStateExpiry, _tsmodeproperties.TroubleshootingStateRemainingMinutes,
_tsmodeproperties.TroubleshootingStateChangeReason, _tsmodeproperties.TroubleshootingStateChangeSource
```

# Microsoft Copilot for Security

securitycopilot.microsoft.com/tour/admin

Copilot for Security

Copilot for Security is a generative AI-first platform with asset mapping, tiered storage, policy services, integration services, and more. It powers all workloads of the security platform.

Azure Subscription ⓘ

ZALNET-PAYG

Resource group ⓘ

CopilotForSecurityRG

[Create a new one](#)

Capacity name ⓘ

copilotforsecuritydemo11042024

Prompt evaluation location ⓘ

Europe

☒ If this location has too much traffic, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region ⓘ

Europe West

# Microsoft Copilot for Security

Microsoft Copilot for Security

## Learn how Copilot for Security works

Explore essentials like prompting, pinning, and providing feedback—to get the most from your AI-powered partner.

[Training](#) [Documentation](#)

❖ Get started using these promptbooks

Promptbooks contain one or more prompts that run in sequence automatically. [Learn more](#)

### Microsoft Sentinel incident invest...

Get a report about a specific incident, along with related alerts, reputation scores, users, and...

Microsoft Security · 7 prompts

### Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 4 prompts

### Suspicious script analysis

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

Microsoft Security · 6 prompts

[View promptbook library](#)

?

I am actively seeking new opportunities and exciting challenges.

If you would like to get in touch, please feel free to reach out through the following channels:

Email: [beata@zalnet.pl](mailto:beata@zalnet.pl)

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa/>

GitHub: <https://github.com/beatazalewa/Conferences/>

