

M365

Defender

iOS

Intune

Defender for Endpoint on iOS

Prerequisites

- Intune and Defender correctly set up. See [Fresh Tenant Setup](#) for how to prepare a test tenant.
- Test devices. You'll want at least 2 iOS devices to compare unsupervised vs supervised on iOS.

The deployment and configuration varies based on if the iOS devices are supervised or unsupervised.

Deploy Defender Endpoint App to iOS devices

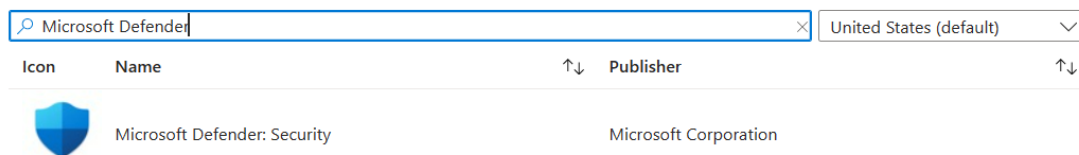
 [Portal](#)

 [Docs](#)

Applies to: Supervised and unsupervised devices

1. Add the iOS store app for Microsoft Defender, target all users you want to have Defender for Endpoint. As of writing, the name in the App Store is Microsoft Defender: Security.

Search the App Store



Configure Defender for Endpoint

App Supervision Policy

 [Portal](#)

 [Docs](#)

Applies to: Supervised and unsupervised devices

This is confusing in the docs, but because it uses a token that will be resolved on the device, you can safely deploy this policy to both supervised and unsupervised devices.

1. Create an app configuration policy for Managed Devices for platform iOS and targeted app Microsoft Defender: Security

[Home](#) > [Apps | App configuration policies](#) >

Create app configuration policy ...

1 Basics 2 Settings 3 Assignments 4 Review + create

Name * ✓

Description

Device enrollment type ▾

Platform * ⓘ ▾

Targeted app * ⓘ [Microsoft Defender: Security](#)

2. Use the configuration designer to set a string key/value pair Key: `issupervised`

Type: `string`

Value: `{{issupervised}}`

[Home](#) > [Apps | App configuration policies](#) >

Create app configuration policy ...

✓ Basics 2 Settings 3 Assignments 4 Review + create

Configuration settings format * ⓘ ▾

ⓘ Once the policy is created, the format cannot be changed

Enter values for the XML property list. The values in the list will vary depending on the app you are configuring. Contact the supplier of the app to learn the values you can use.

[Learn more about XML property lists](#)

Configuration key	Value type	Configuration value
<input type="text" value="issupervised"/> ✓	<input type="text" value="String"/> ▾	<input type="text" value="{{issupervised}}"/> ✓ ...
<input type="text"/>	<input type="text" value="Select one"/> ▾	<input type="text"/>

3. Target both supervised and unsupervised devices.

Onboarding Profiles

 Portal

 Docs

*Applies to: Unsupervised devices

For unsupervised devices, there are two ways to finalize the configuration of Defender for Endpoint after its been deployed.

Zero-Touch onboarding: This automatically configures Defender for Endpoint without any user interaction. Recommended.

Simplified onboarding: This requires users to [open Defender to finalize onboarding](#) before the VPN functions.

1. Create an device configuration policy for iOS/iPadOS devices with the template type VPN with the following settings
Connection Name = `Microsoft Defender for Endpoint`
VPN server address = `127.0.0.1`
Auth method = `Username and password`
Split Tunneling = `Disable`
VPN identifier = `com.microsoft.scmx`
For Zero-Touch onboarding:
Key/Value Pairs:
Key: `SilentOnboard`
Value: `True`
For Simplified onboarding:
Key/Value Pairs:
Key: `AutoOnboard`
Value: `True`
Type of Automatic VPN = `On-demand VPN`
Add a on-demand rule:
I want to do the following: `Connect VPN`
I want to restrict to: `All domains`
2. To prevent users from disabling the VPN in iOS Settings, set
Block users from disabling automatic VPN: `Yes`
3. To disable the On/Off Toggle for the VPN in the Defender app itself, add the following key/value pair:
Key: `EnableVPNToggleInApp`
Value: `TRUE`
4. Target unsupervised devices

Control Filter

 Portal

 Docs

Applies to: Supervised devices

The Control Filter allows Defender for Endpoint's Web Protection **without** the loopback VPN whatsoever. This does not work with other always-on VPNs.

1. Create a Device Config profile with the following settings:

Platform: iOS/iPadOS

Profile Type: Templates





Template Name: Custom


2. Download the **ControlFilterZeroTouch .mobileconfig** profile and upload it.

[Home](#) > [Devices | Configuration](#) >


Custom

iOS/iPadOS

 Basics  **Configuration settings**  Assignments  Review + create

Custom configuration profile name *  

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/Property
3 <plist version="1.0">
4 <dict>
5   <key>ConsentText</key>
6   <dict>
7     <key>default</key>
8     <string>This profile will be used to analyze network traffic to ensure a safe br
9   </dict>
10  <key>PayloadContent</key>
11  <array>
12    <dict>
13      <key>FilterBrowsers</key>
14      <true/>
15      <key>FilterSockets</key>
16      <false/>
17      <key>FilterType</key>
18      <string>Plugin</string>
19      <key>PayloadDescription</key>
20      <string>Configures content filtering settings</string>
```

3. Target supervised devices. If you accidentally target unsupervised it won't apply on those.