

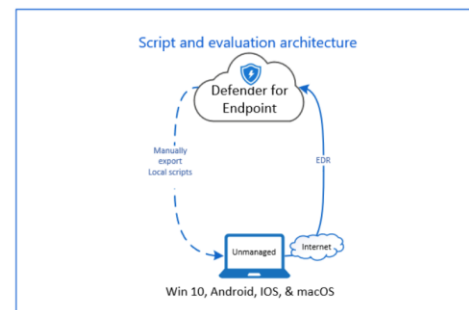
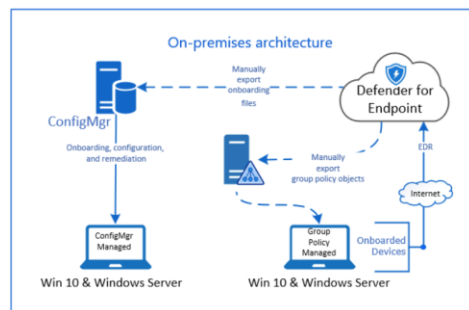
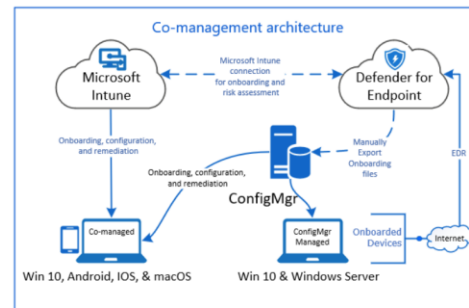
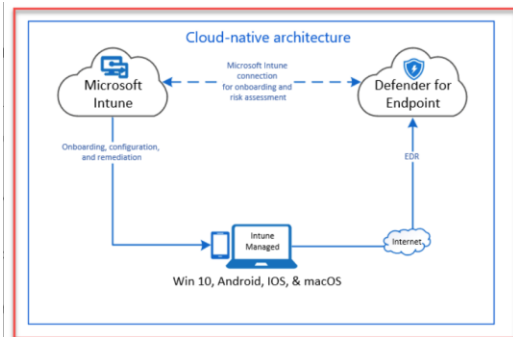
# Defender for Endpoint Intune을 이용한 Onboarding

Microsoft Korea

# I. Introduction

Defender for Endpoint를 사용하는 경우 Microsoft Intune에서 EDR Profile을 배포하여 MDE Onboarding 과정을 수행할 수 있습니다. (Entra ID Join , Intune 등록된 Device 환경 권고)

[Onboarding using Microsoft Intune - Microsoft Defender for Endpoint | Microsoft Learn](#)



## 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 discovered devices. To disable this automatic filtering, navigate to the filter menu.

**All devices** Computers & Mobile Network devices IoT/OT devices Uncategorized

Total **1** Critical assets **0** High risk **0** High exposure **0** Not onboarded **0**

Filters: Transient device: No Exclusion state: Not Excluded

Name	IP	Criticality level	Device category	Device type
win11-m365x0413	10.0.0.7		Computers and Mo...	Worksta...

**win11-m365x0413**  
No known risks Medium

Open device page View in map Device value

Logged on users (last 30 days)

VM details

DLP policy sync details

Configuration status

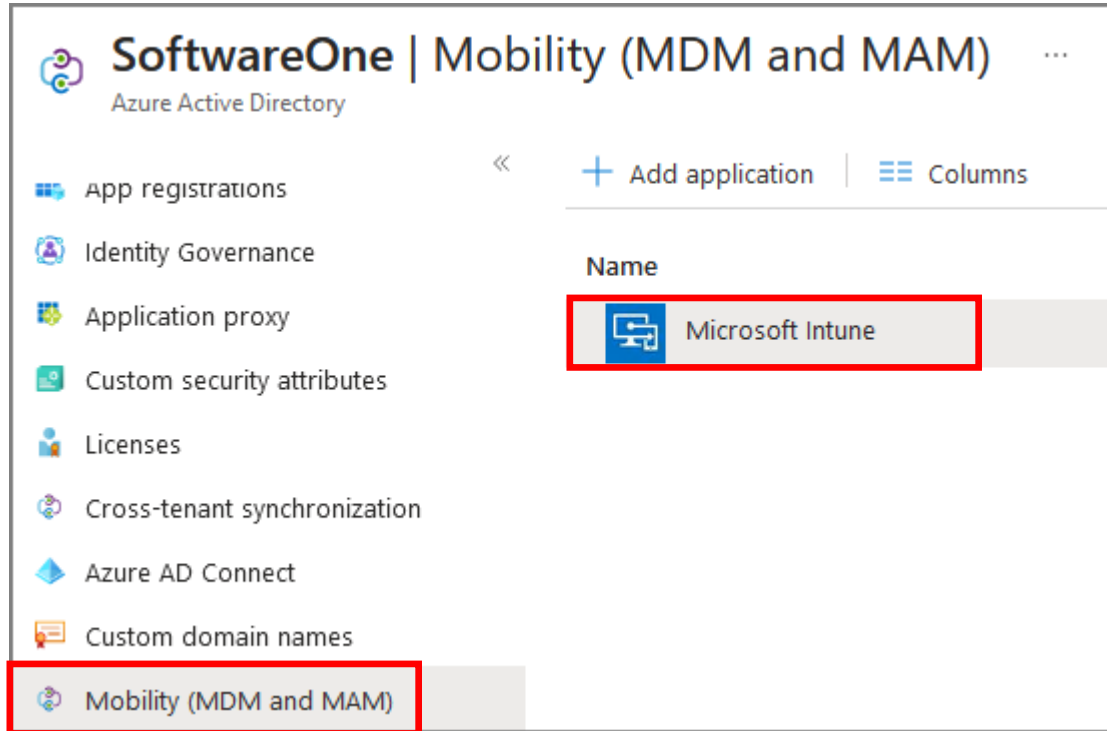
Cloud resource details

Device management

Managed by Intune MDE Enrollment status N/A [Learn more about MDE enrollment](#)

## II. Enrollment MDM




Azure Portal → Azure Active Directory → Mobility (MDM 및 MAM) → Microsoft Intune



## II. Enrollment MDM

MDM User scope → All or Some → Save

**Configure** ...  
Microsoft Intune

 Save  Discard  Delete

MDM user scope ⓘ

None

Some

All

MDM terms of use URL ⓘ

✓

MDM discovery URL ⓘ

✓

MDM compliance URL ⓘ

✓

[Restore default MDM URLs](#)

MAM user scope ⓘ

None

Some

All

MAM terms of use URL ⓘ

✓

MAM discovery URL ⓘ

✓






MAM compliance URL ⓘ

✓

[Restore default MAM URLs](#)

### III. Onboarding (for Windows Client OS)

Security Admin Center → 설정 → Microsoft 365 Defender

설정		
이름	설명	
 보안 센터	Microsoft 365 보안 센터에 대한 일반 설정	
 Microsoft 365 Defender	Microsoft 365 Defender에 대한 일반 설정	
 전자 메일 및 공동 작업	전자 메일 및 공동 작업에 대한 일반 설정	
 ID	ID에 대한 일반 설정	
 클라우드 앱	클라우드 앱에 대한 일반 설정	

# III. Onboarding

온보딩 진행 중



**잠시만 기다려 주세요! 데이터용 새 공간을 준비하고 연결하고 있습니다.**










로드 중...

이 작업은 몇 분 정도 걸립니다. 작업이 완료되면 데이터가 점진적으로 통합되고 다음 몇 시간 후 콘솔에 표시됩니다. [Microsoft 365 보안에 대한 자세한 정보](#)

# III. Onboarding (for Windows Client OS)

## Endpoints

Settings		
	Name	Description
	Security center	General settings for the Microsoft 365 security center
	Microsoft 365 Defender	General settings for Microsoft 365 Defender
	Endpoints	General settings for endpoints
	Email & collaboration	General settings for email & collaboration
	Identities	General settings for identities
	Device discovery	Select your device discovery mode and customize standard discovery settings
	Cloud Apps	General settings for cloud apps

### III. Onboarding (for Windows Client OS)

Microsoft Intune connection → On. 이 설정으로 Intune → Defender 방향으로 동기화 할 수 있습니다.

Settings > Endpoints > Advanced features

## Endpoints

**General**

- Advanced features**
- Licenses
- Email notifications
- Auto remediation

**Permissions**

- Roles

**Microsoft Intune connection** (On)

Connects to [Microsoft Intune](#) to enable sharing of device information. Intune provides additional information about managed devices for...



# III. Onboarding (for Windows Client OS)

## Intune 연결 전

홈 > 엔드포인트 보안

엔드포인트 보안 | 엔드포인트용 Microsoft Defender

검색

새로 고침 저장 취소 삭제

개요

개요  
모든 디바이스  
보안 기준  
보안 작업

관리

바이러스 백신  
디스크 암호화  
방화벽  
엔드포인트 권한 관리  
엔드포인트 검색 및 응답  
공격 표면 감소  
계정 보호  
디바이스 준수  
조건부 액세스

모니터

할당 실패

설치

엔드포인트용 Microsoft Defender

연결 상태  
마지막 동기화

사용할 수 없음 --

Microsoft Defender for Endpoint를 사용하여 조직의 보안 상태를 파악하고 개선하기 위한 권장 사항을 확인합니다.

Microsoft Intune 및 Microsoft Defender for Endpoint를 연결하여 Intune 준수 평가 및 Azure Active Directory 조건부 액세스 정책을 Microsoft Defender에서 보안 설정 관리를 적용하도록 설정할 수 있습니다. 이 설정은 Microsoft Intune에 연결된 디바이스에 적용됩니다.

[Microsoft Defender for Endpoint에 대한 자세한 정보](#)  
[Intune에 Microsoft Defender for Endpoint\(를\) 연결하는 방법에 대한 자세한 정보](#)  
[Intune 엔드포인트 보안 프로파일 사용하여 Microsoft Defender for Endpoint 에이전트 구성에 대해 자세히 알아보십시오.](#)

Microsoft Defender for Endpoint 구성 중

1. Microsoft Defender 보안 센터를 통해 Intune에 대한 연결을 설정합니다. [Microsoft Defender 보안 센터에서 Microsoft Defender for Endpoint 에이전트 구성](#)

2. 연결이 설정된 후 이 섹션의 맨 위에 있는 "새로 고침"을 클릭하여 이 가이드를 숨기고 아래 설정을 사용하도록 설정합니다.

3. 아래 설정을 구성합니다.

커넥터 설정

Microsoft Defender for Endpoint(가) 이 계정의 Intune과 적극적으로 통신하고 있지 않으므로 일부 토글을 사용할 수 없습니다. 연결이 정상 상태(활성 또는 프로비전됨)로 돌아가면 토글을 다시 사용할 수 있고 기존 설정 상태가 복원됩니다.

# III. Onboarding (for Windows Client OS)

## Intune 연결 후

홈 > 엔드포인트 보안

엔드포인트 보안 | 엔드포인트용 Microsoft Defender

검색

새로 고침 저장 취소 삭제

개요

개요

모든 디바이스

보안 기준

보안 작업

관리

바이러스 백신

디스크 암호화

방화벽

엔드포인트 권한 관리

엔드포인트 검색 및 응답

공격 표면 감소

계정 보호

디바이스 준수

조건부 액세스

모니터

할당 실패

연결 상태

마지막 동기화

사용 가능한 공간

2023. 3. 24. 오후 4:58:55

엔드포인트 보안 프로필 설정

엔드포인트 보안 구성을 적용하려면 Microsoft Defender for Endpoint를(를) 허용합니다.

고기

켜기

준수 정책 평가

Android 장치 버전 6.0.0 이상을 Microsoft Defender for Endpoint에 연결

고기

켜기

iOS/iPadOS 장치 버전 13.0 이상을 Microsoft Defender for Endpoint에 연결

고기

켜기

버전 10.0.15063 이상인 Windows 디바이스를 Microsoft Defender for Endpoint에 연결

고기

켜기

iOS/iPadOS 디바이스에 대해 앱 동기화(애플리케이션 인벤토리 보내기) 사용

고기

켜기

개인 소유 iOS/iPadOS 장치에서 전체 애플리케이션 인벤토리 데이터 보내기

고기

켜기

지원되지 않는 OS 버전 차단

고기

켜기

정책 평가 앱 보호

# III. Onboarding (for Windows Client OS)

## Endpoint 보안 프로필 설정

엔드포인트 보안 | 엔드포인트용 Microsoft Defender

검색

새로 고침 저장 취소 삭제

개요

개요

모든 디바이스

보안 기준

보안 작업

관리

바이러스 백신

디스크 암호화

방화벽

엔드포인트 권한 관리

엔드포인트 검색 및 응답

공격 표면 감소

계정 보호

디바이스 준수

조건부 액세스

모니터

연결 상태

마지막 동기화

사용 가능한 공간

2023. 3. 24. 오후 4:58:55

엔드포인트 보안 프로필 설정

엔드포인트 보안 구성을 적용하려면 Microsoft Defender for Endpoint(를) 허용합니다.

준수 정책 평가

Android 장치 버전 6.0.0 이상을 Microsoft Defender for Endpoint에 연결

iOS/iPadOS 장치 버전 13.0 이상을 Microsoft Defender for Endpoint에 연결

버전 10.0.15063 이상인 Windows 디바이스를 Microsoft Defender for Endpoint에 연결

iOS/iPadOS 디바이스에 대해 앱 동기화(애플리케이션 인벤토리 보내기) 사용

개인 소유 iOS/iPadOS 장치에서 전체 애플리케이션 인벤토리 데이터 보내기

지원되지 않는 OS 버전 차단

끄기 켜기

끄기 켜기

끄기 켜기

끄기 켜기

끄기 켜기

끄기 켜기

끄기 켜기

끄기 켜기

# Create EDR Profile

- MDE에서 실시간으로 Endpoint 장치를 검사 및 보호 조치를 취하려면 센서를 설치 해야 합니다.
- Intune → MDE 동기화 및 Sample 수집이 목적

# Create EDR Profile

Endpoint security → Endpoint detection and response → Create Policy → Windows 10, Windows 11, and Windows Server → Create

The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane is open, with the 'Endpoint security' option highlighted by a red rectangle. Within this pane, the 'Endpoint detection and response' sub-option is also highlighted with a red rectangle. The main content area shows the 'Endpoint security | Endpoint detection and response' page. A red rectangle highlights the '+ Create Policy' button. Below this, a search bar and a list of policies are visible, with 'No results' displayed. On the right side, a 'Create a profile' modal window is open. In this modal, the 'Platform' dropdown menu is set to 'Windows 10, Windows 11, and Windows Server' (highlighted with a red rectangle), and the 'Profile' dropdown menu is set to 'Endpoint detection and response' (highlighted with a blue rectangle). At the bottom of the modal, a 'Create' button is highlighted with a red rectangle. The top of the interface shows the user's name 'lim@contoso.kr' and the organization 'CONTOSO'.

# Create EDR Profile

Profile Name 입력 → Next

[Home](#) > [Endpoint security](#) | [Endpoint detection and response](#) >

## Create profile ...

Endpoint detection and response

✓ Basics

② Configuration settings

③ Scope tags

④ Assignments

⑤ Review + create

Name \*

Windows\_Client\_Server\_Profile ✓

Description

Platform

Windows 10 and later ▼

Previous

Next

# Create EDR Profile

Auto from connector → All → Next

## Create profile

Endpoint detection and response

✓ Basics

**2 Configuration settings**

3 Scope tags

4 Assignments

5 Review + create

^ Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type ⓘ

Auto from connector

Sample Sharing ⓘ

All

[Deprecated] Telemetry Reporting Frequency ⓘ

Normal

Previous

Next

Intune은 Defender for Endpoint 배포에서 온보딩 패키지를 자동으로 가져옵니다.

클라우드 계층을 최대한 활용하려면 항상 샘플 공유를 사용하는 것이 좋습니다.

# Create EDR Profile

Next

## Create profile

Endpoint detection and response

✓ Basics

✓ Configuration settings

**3 Scope tags**

4 Assignments

5 Review + create

Scope tags

Scope tags

Default

[+ Select scope tags](#)

Previous

Next



# Create EDR Profile

Add groups → 대상 그룹 추가 → Next

## Create profile

Endpoint detection and response

✓ Basics

✓ Configuration settings

✓ Scope tags

**4 Assignments**

5 Review + create

Included groups

Add groups

Add all users

Add all devices

Groups	Group Members ⓘ	Filter	Filter mode
Dynamic_WindowsClientOS	4 devices, 0 users	None	None
Dynamic_WinServerOS	14 devices, 0 users	None	None

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

Add groups

Groups	Group Members ⓘ	Remove
No groups selected		

Previous

**Next**

EDR 프로필에 추가할 디바이스를 지정합니다.

# Create EDR Profile

Create

**Create profile** ...  
Endpoint detection and response

✓ Basics

✓ Configuration settings

✓ Scope tags

✓ Assignments

5 Review + create

Summary

Basics

Name

Windows\_Client\_Server\_Profile

Description

--

Platform

Windows 10 and later

Configuration settings

▼ Microsoft Defender for Endpoint

Scope tags

Default

Assignments




Previous


Create

# Create EDR Profile

아래와 같이 적용됨 확인 → Device assignment status

[Home](#) > [Endpoint security](#) | [Endpoint detection and response](#) >

 **Windows Client\_OS**    
Endpoint detection and response

 Delete

**Device and user check-in status**

Succeeded

1

Error

0

Conflict

0

Not applicable

0

In Progress

0

[View report](#)

[Device assignment status](#)  
This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

[Per setting status](#)  
View the configuration status of each setting for this policy across all devices and users.

# Create EDR Profile

자동으로 집계되지 않는 것으로 확인됩니다. → Generate again

[Home](#) > [Endpoint security | Endpoint detection and response](#) > [Windows Client\\_OS](#) >

## Windows Client\_OS ...

Columns

Export

All Assignment status

Generate again

Cancel

Report generated on:

Success	Conflict	Error	Pending	Not applicable	Total
---	---	---	---	---	---

Search by device name, last active user, Intune device ID, Azure AD user ID

Showing 0 to 0 of 0 records

Device name ↑↓Last active user ↑↓

No data to display

# Create EDR Profile

아래와 같이 업데이트됨 확인

[Home](#) > [Endpoint security | Endpoint detection and response](#) > [Windows Client\\_OS](#) >

## Windows Client\_OS ...

[Columns](#) [Export](#)

All Assignment status ▾

[Generate again](#) [Cancel](#) Report generated on: 7/12/2023, 9:46:19 AM

Success	Conflict	Error	Pending	Not applicable	Total
1	0	0	0	0	1




[Search by device name, last active user, Intune device ID, Azure AD user ID](#)

Showing 1 to 1 of 1 records


Device name ↑↓	Last active user ↑↓	Assignment status ↑↓
DESKTOP-RMC3MT0	cloud-user1@contoso.kr	Success

# Create EDR Profile


Per setting status

 **Windows Client\_OS**  

Endpoint detection and response

 Delete

**Device and user check-in status**



Succeeded	Error	Conflict	Not applicable	In Progress
1	0	0	0	0

[View report](#)

**Device assignment status**

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

**Per setting status**

View the configuration status of each setting for this policy across all devices and users.




# Create EDR Profile


Client OS Profile에서는 Connector / Sample Sharing 정책이 적용된 것을 알 수 있습니다.

Home > Endpoint security | Endpoint detection and response > Windows Client\_OS >

**Windows Client\_OS** ...

Device configuration profile

 Refresh  Columns  Export

 Search by setting name

Showing 1 to 2 of 2 records

Setting Name ↑↓	Success ↑↓
Onboarding blob from Connector	1
Sample Sharing	1

# Create EDR Profile

반면에 Server OS Profile에서는 Connector 연결에 대한 정책은 적용되지 않았습니다.

Home > Endpoint security | Endpoint detection and response > Windows\_Server\_Profile >

## Windows\_Server\_Profile ...

Device configuration profile

Refresh Columns Export

Search by setting name

Showing 1 to 3 of 3 records

Setting Name ↑↓	Success ↑↓
Onboarding blob from Connector	0
Sample Sharing	14

해당 설정은 Intune → Defender로 연결해주는 설정이기 때문에, 이미 MDE 온보딩되어 있는 Server OS는 적용할 필요가 없기 때문인 것으로 보여집니다.



# Create EDR Profile

Intune Onboarding의 경우 EDR Profile 동작이 완료되어야 장치 페이지에 표시됩니다.

**장치 인벤토리**

합계 | 높은 위험 수준 | 높은 노출  
6 | 0 | 0


내보내기 | 검색 | 30일 | 열 사용자 지정

필터: 제외 상태: 아니요 | 관리자: Intune

<input type="checkbox"/>	이름	도메인	OS 플랫폼	Windows 버전	센서 상태	관리자 ①
<input type="checkbox"/>	desktop-rmc3mt0	AAD joined	Windows 11	22H2	● 활성	Intune
<input type="checkbox"/>	onboarding4	AAD joined	Windows 10	22H2	● 활성	Intune
<input type="checkbox"/>	onboarding3	AAD joined	Windows 11	22H2	● 활성	Intune
<input type="checkbox"/>	onboarding5	AAD joined	Windows 11	22H2	● 활성	Intune
<input type="checkbox"/>	onboarding23	AAD joined	Windows 11	22H2	● 활성	Intune
<input type="checkbox"/>	on-win11-test1.corp.contoso.kr	corp.contoso.kr	Windows 11	22H2	● 활성	Intune

# Create EDR Profile

Sample 수집이 이루어 지면 아래와 같이 Endpoint의 활동내역이 수집됩니다.

**onboarding4**  
알려진 위험 없음

개요

인시던트 및 경고

시간 표시줄

보안 권장 사항

보안 정책

소프트웨어 인벤토리

브라우저 확장

발견된 취약점

누락된 KB

보안 기준

인증서 인벤토리

Feb 2023Mar 2023Apr 2023May 2023Jun 2023

내보내기

검색

1주

<input type="checkbox"/> 이벤트 시간 ↓	이벤트	추가 정보	사용자
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:30....	WmiPrvSE.exe enumerated the Local Group membership of ONBOAR...	T1069.001: Local Groups T1087.001: Local Account	network service
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:30....	WmiPrvSE.exe enumerated the Local Group membership of ONBOAR...	T1069.001: Local Groups T1087.001: Local Account	network service
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:30....	WmiPrvSE.exe enumerated the Local Group membership of ONBOAR...	T1069.001: Local Groups T1087.001: Local Account	network service
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:30....	svchost.exe이(가) 프로세스 DeviceCensus.exe을(를) 만들었습니다.		system
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:26....	MsSense.exe established connection to 52.168.112.66:443 over an asymm...	T1573: Encrypted Channel +1	system
<input type="checkbox"/> 2023년 7월 14일 오전 5:16:26....	MsSense.exe established a connection to 52.168.112.66 over TLS protocol...	T1071: Application Layer Protocol +1	system