Microsoft Intune compliance requirements for Linux (preview) | Microsoft Docs

Microsoft Intune compliance requirements for Linux (preview)

> [!Note]
> This information relates to a private preview feature which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

Microsoft Intune sends a notification to your device when your device settings do not meet your organization's compliance requirements. To ensure access to work or school resources such as Wi-Fi, email, and apps, update your settings to meet the requirements. Microsoft Intune checks your device settings every time your device syncs with Microsoft Intune, starting at time of enrollment.

This article describes the requirements that Microsoft Intune can enforce on behalf of your organization. For information about how to change settings on a supported Linux device, see the Ubuntu help documentation.

OS requirements

Microsoft Intune supports devices running these Linux distributions:

- Ubuntu LTS 18.04
- Ubuntu LTS 20.04

If your device isn't running one of the supported distributions, update the OS or contact your support person to find out if there are other ways to enroll your device.

Password requirements

Microsoft Intune enforces the following password requirements.

- Minimum password length
- Password quality
  - Minimum number of digits
  - Minimum length
  - Minimum number of lowercase letters
  - Minimum number of uppercase letters

- Minimum number of symbols

Check the notifications you receive for exact minimum/maximum values. Microsoft Intune only enforces password requirements if your organization requires you to have a device password.

Remediating password requirement compliance

Per policy password are required to be compliant to a minimum length of 2 characters, and have at least one Uppercase, Lowercase, Number, and Symbol. Intune checks the `pam.pwquality` configuration for enforcement.

```
sudo apt install libpam-pwquality
```

```
# check that the pam_pwquality line in /etc/pam.d/common-password
contains at least the required settings:
password    requisite          pam_pwquality.so retry=3 dcredit=-1
ocredit=-1 ucredit=-1 lcredit=-1 minlen=12
```

If you need to alter the policy to be compliant, follow these steps

```
sudo nano /etc/pam.d/common-password
```

Scroll down to locate the entry and update it match

```
password requisite pam_pwquality.so retry=3 minlen=12 ucredit=-1
lcredit=-1 dcredit=-1 ocredit=-1
```

After editing use ctrl-o, hit enter to save the file, and then ctrl-x to close the file.

Encryption requirements

Your organization can require you to encrypt your device.

Drive encryption compliance policy

The Intune Linux agent only recognizes the dm-crypt encryption. The dm-crypt encryption is built into the Linux kernel. In order for your device to be compliant with device encryption requirements, all local filesystems with the below criteria must be encrypted with dm-crypt:

- Writable (not mounted read-only)
- Not a pseudo filesystem (like /proc or /sys)
- Not the EFI boot partition (/boot/efi)

There is no need to encryption the below

- Not mounted read-only drives
- Not pseudo filesystem (like /proc or /sys)
- Not the EFI boot partition (/boot/efi)

How to encrypt drives

- Any frontend that works with dm-crypt should give the tools to encrypt a drive in a way that LinuxAgent will recognize.
  - cryptsetup is a command-line tool that will help with encryption.
  - The Ubuntu "Disks" utility will also do encryption.
- Encrypting an existing system partition in place after it has already been created is possible. See for example here.

How to encrypt drives

- Any frontend that works with dm-crypt should give the tools to encrypt a drive in a way that LinuxAgent will recognize.
  - cryptsetup is a command-line tool that will help with encryption.
  - The Ubuntu "Disks" utility will also do encryption.
- Encrypting an existing system partition in place after it has already been created is possible. See for example here.
- Linux team recommendation is to enable encryption during machine provisioning when setting the machine for testing.