

Configure Umbrella Certificate Provisioning with MS Intune

Contents

[Introduction](#)

[Overview](#)

[Prerequisites](#)

[Umbrella Dashboard](#)

[MS Intune Console](#)

Introduction

This document describes the configuration of Umbrella certificate provisioning with MS Intune.

Overview

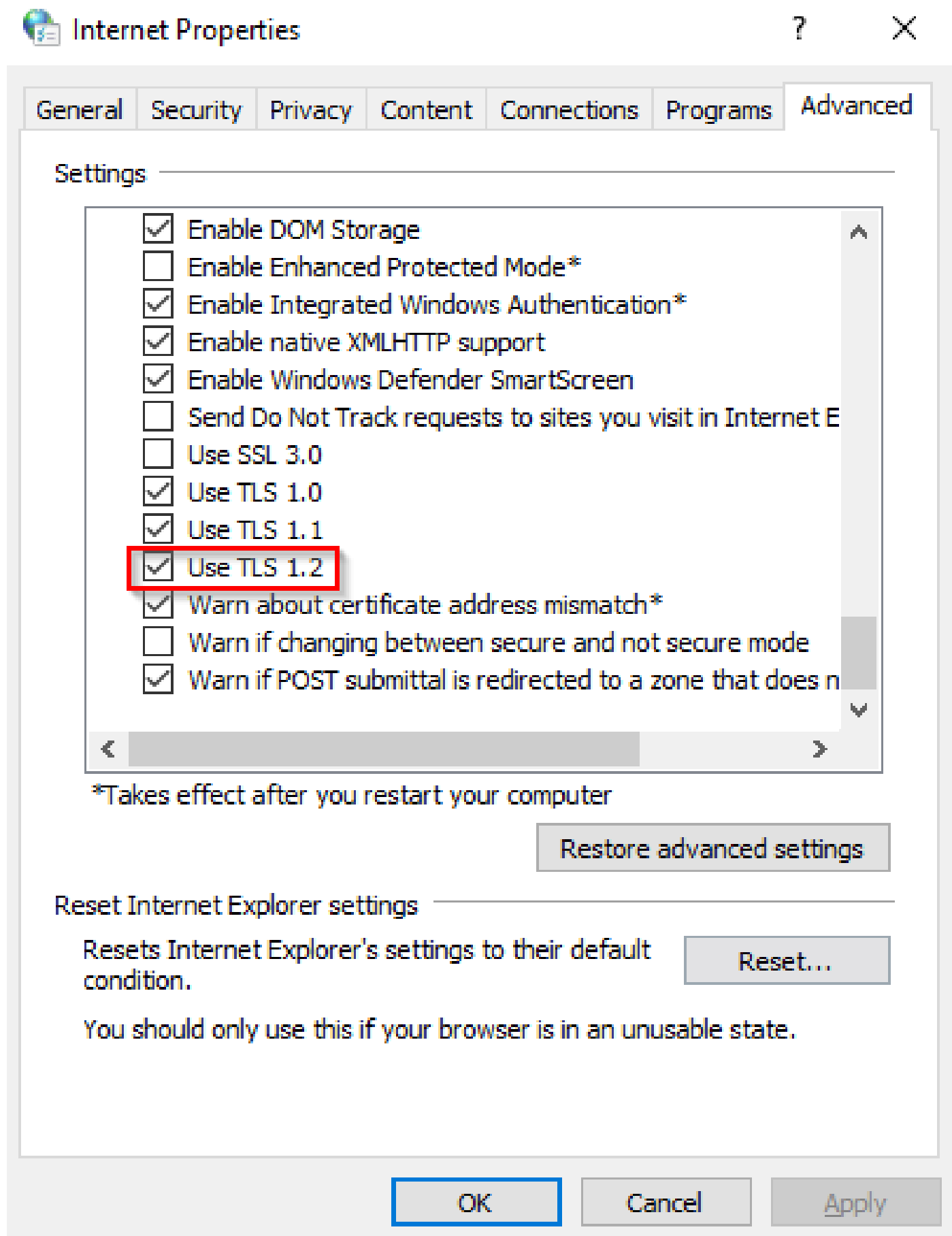
This configuration guide covers the elements required to provision the Umbrella Root CA via MS Intune.

Prerequisites

- Umbrella Dashboard Access
- Umbrella Root CA
- MS Intune Console access

Umbrella Dashboard

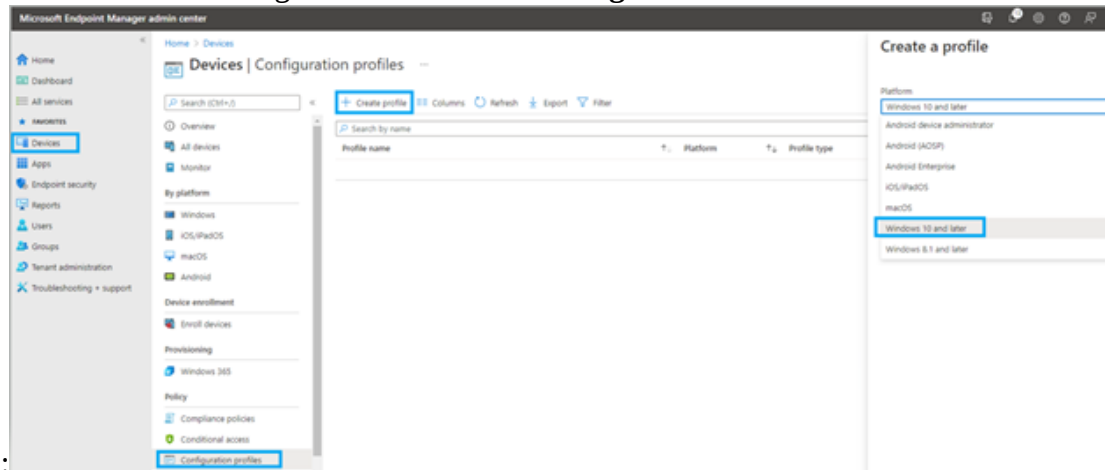
1. Access to your Umbrella Dashboard under **Deployments > Configuration > Root Certificate** and download the Umbrella Root CA:



blobid0.png

MS Intune Console

1. Access to your MS Intune MDM and go under **Devices > Configuration Profiles > Create Profile >**

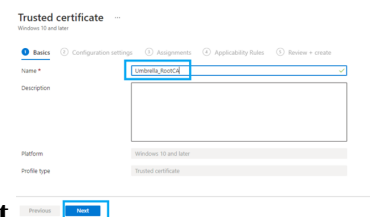


Select Platform:

86b492a7fb03fb72fa2c255ed5f34309fc7427aee918937b6990a66f956dc9ac.png

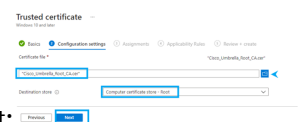
2. Specify the “Profile Type” and use “Templates” and look for “Trusted Certificate” and click **Create:**

ca00d2c34ecac4f6fe2584d61b9c8a9832c458d7c083e0aabb532b8c8ebcd7aa.png



3. Enter a meaningful name for the Trusted Certificate profile and click **Next.**

dfd78f03070787c9ffc4c6c968929d7a12be36429590740ed27641144cf143cf.png



4. Upload the Umbrella Root CA and specify the Destination Store and click **Next:**

a318563a22a600910b206f01cdfcb483ccc04cb0e15a1757c48e663cfe234ec0.png

Trusted certificate ...

Windows 10 and later

- ✓ Basics
- ✓ Configuration settings
- 1 Assignments**
- 4 Applicability Rules
- 5 Review + create

Included groups

Add groups Add all users Add all devices

Groups

All devices

Remove

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

No groups selected

Previous

Next

93effe94c92c3b063c406e89c4b6d0f759cb8c5d606302e3701b702b1a8cb213.png

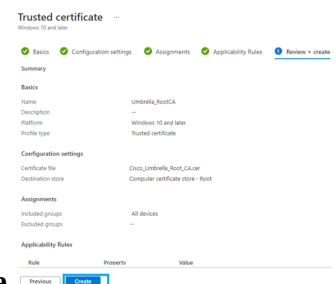
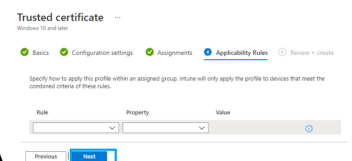
5. Specify the group of user/devices you want to assign the Umbrella Root CA.

c436635d3e0dce29ec76802ffb26e604964abe08862c00ec25866dbf4a9d5b95.png

6. Optionally, specify “Applicability Rules” and click **Next**.

7. Review the configuration has been properly performed and then click **Create**.

6329621f732c63ec97b6ef656b78dc1c392fe976105a0c3dbb7a779b945ba7e8.png



The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane shows the 'Devices' section selected, with 'Configuration profiles' further highlighted. The main content area is titled 'Devices | Configuration profiles'. It includes a search bar and a table of configuration profiles. The table has columns for 'Profile name', 'Platform', 'Profile type', and 'Assigned'. A single profile, 'Umbrella_RootCA', is listed with a platform of 'Windows 8.1 and later', a profile type of 'Trusted certificate', and an assigned status of 'Yes'.

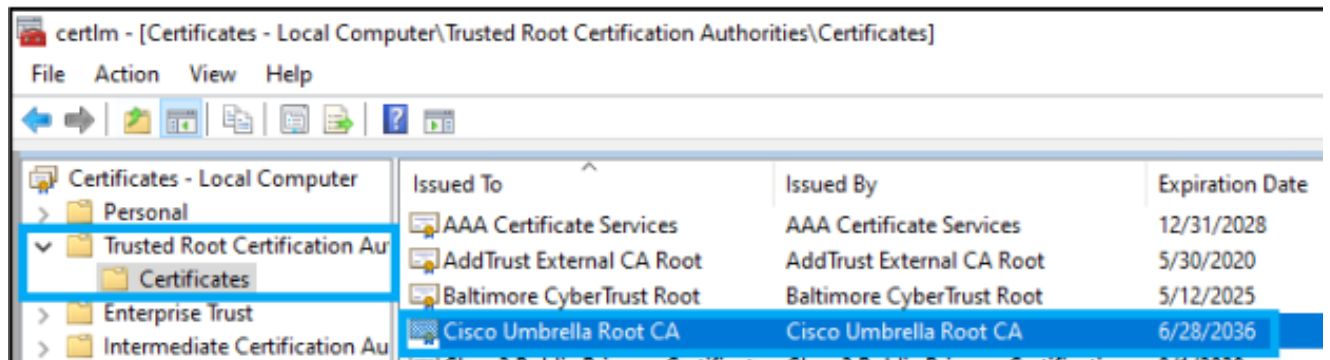
Profile name	Platform	Profile type	Assigned
Umbrella_RootCA	Windows 8.1 and later	Trusted certificate	Yes

Umbrella_RootCA
 Overview
 Search CAID(s)
 Details
 Overview
 Manage
 Properties
 Monitor
 Device status
 User status
 Pending status
 Profile assignment status — Windows 8.1 and later devices
 Profile type: Trusted certificate
 Platform supported: Windows 8.1 and later
 Groups enrolled: 0
 Assigned to non-Windows 8.1 and later devices: 0
 Profile assignment status — Windows 8.1 and later devices
 1 enrolled
 0 trusted
 0 untrusted
 0 unassigned
 10 unrevoked

The screenshot displays the 'Device status' section of the Windows Defender Security Center. The left-hand navigation pane includes 'Overview', 'Manage', 'Monitor', and 'Device status' (which is highlighted). Under 'Monitor', there are sub-options for 'Device status', 'User status', and 'Per-setting status'. The main content area shows a message 'Data in this view is live.' and a search bar. Below this is a table with the following data:

Device	User Principal Name	Deployment Status
DESKTOP-0PLUFO3	m...@microsoft.com	Succeeded

11. You can also confirm the installation on the end device Root CA store:



a9e8eabad6df501ad7627dbc87f5ea6cf9488b273925c5277fbf8a396ae1a49.png