MICROSOFT INTUNE INTEGRATION

Delivering seamless authentication to corporate IT resources

Overview

DigiCert® Trust Lifecycle Manager integrates digital certificates with Microsoft Intune, a cloud-based mobile device management (MDM) and mobile application management (MAM) service used by organizations to control how their devices and data are used.

This integration enables mobile devices, workstations, and desktops enrolled or managed in Intune to authenticate to corporate applications and resources without the need for usernames, passwords, or tokens for access.

Trust Lifecycle Manager further streamlines certificate lifecycle management with preconfigured certificate templates and automation of certificate enrollment, renewal, and revocation.

Preconfigured Templates

Device Authentication for Microsoft Intune
for authentication of mobile devices and workstations to corporate networks, WiFi, and other resources

User Client Authentication for Microsoft Intune
for authentication of users to mobile applications and corporate resources

Preconfigured certificate templates for Microsoft Intune streamline the issuance of digital certificates for user and device authentication.

Certificate Lifecycle Automation

DigiCert Trust Lifecycle Manager automates the certificate lifecycle, reducing administrative overhead and preventing business disruption due to certificate expiration or human error.

Enrollment – Automates certificate issuance via the commonly-used enrollment standard, Simple Certificate Enrollment Protocol (SCEP).

Renewal – Automates renewals based on thresholds that can be set based on remaining certificate validity.

Revocation – Automates certificate revocation from a request queue managed in the Intune portal. Each revocation updates the Certificate Revocation List (CRL) and returns a notification to the Intune portal.

Learn More

Learn more about integrating Trust Lifecycle Manager with Microsoft Intune here.