

UNCLASSIFIED



MICROSOFT INTUNE (DESKTOP) SUPPLEMENTAL PROCEDURES

Version 1, Release 1

24 September 2024

Developed by Microsoft and DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. MICROSOFT INTUNE ENDPOINT MANAGEMENT CLOUD PLATFORM OVERVIEW	1
1.1 Microsoft Intune Architecture	2
1.2 MDM Software Components.....	3
1.3 Microsoft Intune MDM Required Endpoint and Firewall Ports.....	3
1.3.1 Network Endpoints for Microsoft Intune	3
1.3.2 U.S. Government Endpoints for Microsoft Intune.....	3

LIST OF TABLES

	Page
Table 1-1: Microsoft Intune Core Components.....	3

LIST OF FIGURES

	Page
Figure 1-1: Microsoft Intune Architecture.....	2

1. MICROSOFT INTUNE ENDPOINT MANAGEMENT CLOUD PLATFORM OVERVIEW

Microsoft Intune is a 100 percent software-as-a-service (SaaS) cloud-based service. Intune offers mobile device management (MDM) and mobile application management (MAM). Some key tasks include:

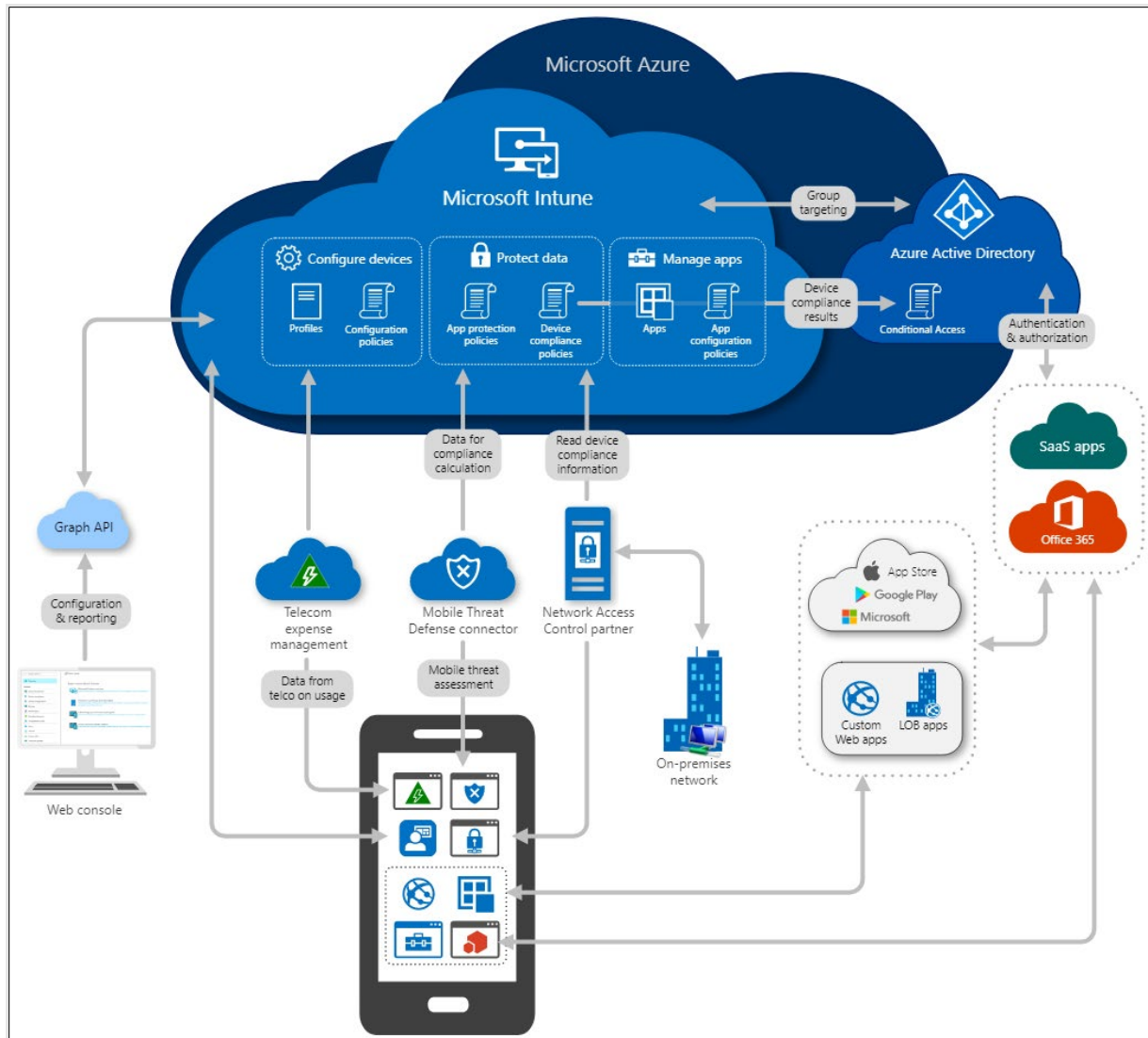
- Ensure devices and apps are compliant with Department of Defense (DOD) organization security requirements.
- Create policies that help keep DOD organization data safe on DOD-owned and personal devices.
- Use a single, unified mobile solution to enforce these policies and help manage devices, apps, users, and groups.
- Protect DOD organization information by helping to control the way the workforce accesses and shares its data.

Intune is part of Microsoft's Enterprise Mobility + Security (EMS) suite. Intune integrates with Entra ID to control who has access and what they can access.

Intune also integrates with Azure Information Protection for data protection. It can be used with the Microsoft 365 suite of products. For example, Microsoft Teams, OneNote, and other Microsoft 365 apps can be deployed to devices. This feature enables those in an organization to be productive on all of their devices while keeping the organization's information protected with policies created.

1.1 Microsoft Intune Architecture

Figure 1-1: Microsoft Intune Architecture



1.2 MDM Software Components

Table 1-1: Microsoft Intune Core Components

Component	Description
Intune Company Portal app	Intune mobile app (Agent) installed on the mobile device to communicate with the Intune cloud service.
Intune SaaS cloud service platform	Intune is a 100 percent SaaS cloud-based MDM and MAM service.
Intune – Microsoft Endpoint Management Console (SaaS Web Console)	Intune web-based administration console. The web console is part of the Intune cloud service platform.
Optional: Intune certificate connectors	Intune certificate connectors can be used to deploy certificates (PKCS imported certificates, PKCS#12, and SCEP certificates) used by mobile devices and apps for authentication to corporate resources through VPN, Wi-Fi, or email profiles.

1.3 Microsoft Intune MDM Required Endpoint and Firewall Ports

As a cloud-only service, Intune does not require on-premises infrastructure such as servers or gateways to enable administrative management of Mobile Operating System (MOS) devices in the DOD.

The following sections outline related Intune network endpoints in the cloud.

1.3.1 Network Endpoints for Microsoft Intune

This page lists IP addresses and port settings needed for firewall/proxy settings in Intune deployments.

- <https://docs.microsoft.com/en-us/mem/intune/fundamentals/intune-endpoints>

1.3.2 U.S. Government Endpoints for Microsoft Intune

This page lists the U.S. Government endpoints needed for firewall/proxy settings in Intune deployments.

- <https://docs.microsoft.com/en-us/mem/intune/fundamentals/intune-us-government-endpoints>