Protected Trust® | Protecting the Privacy of Digital Information Assets

GUIDED MODERN ENDPOINT DEPLOYMENT FOR DESKTOPS

Abstract

Protected Trust proposal for administrative guidance in deploying the advanced features of Microsoft Intune and AutoPilot – Microsoft's endpoint management components of the Modern Workplace. The Modern Workplace allows stakeholders to quickly access information from anywhere at any time while protecting the privacy of their data. Organizations benefit by streamlining their device deployment and management processes while enhancing their security and compliance profiles.

Protected Trust, LLC
199 Ave. B NW, Suite 240
Winter Haven, FL 33881
info@protectedtrust.com
protectedtrust.com

Contents

Guided Modern Endpoint Deployment for Desktops

Project Overview

The Modern Endpoint deployment and management capabilities of Azure Active Directory, Microsoft Endpoint Manager (Intune) and AutoPilot enable organizations to increase their productivity, reduce their administrative costs, enhance their security profiles, and meet their compliance requirements. These cloud-based management tools streamline workstation provisioning, better control endpoint device configurations, and enforce consistent security updates and patching throughout the organization.

Microsoft Endpoint Manager includes the services and tools used to deploy, manage, and monitor desktop computers and mobile devices. This project is specific to desktops and includes two Proof of Concepts, one for Intune and the other for Autopilot. Guided Modern Endpoint Deployment for Mobile Devices like iOS/iPadOS, Android and Android Enterprise is available as a separate project.

The goal of the POCs is to provide Client's IT administrative team with a thorough understanding of Microsoft Endpoint Manager, Active Directory, Azure Directory interaction, different enrollment models, and the pros and cons of each of these models. With this transfer of knowledge, Client's IT administrative team will be able to support the on-going management of Intune and Autopilot and the development of Intune policies.

Intune MDM Proof of Concept (POC)

Services to be provided:

- Proof of concept includes:
  - One to two discovery and scoping calls to understand Client's current environment, discuss POC scope, determine approach and define schedules.
  - Review external dependencies to implement Intune
  - Guidance on how to design and implement Intune
  - Implementation:
    - Configure an Intune subscription
    - Add user groups in Azure AD
    - Assign Intune and Office 365 user licenses
    - Set mobile device management (MDM) authority to Intune
    - Prepare device platforms for enrollment (iOS, Android, Windows)
    - Add and deploy the following:
      - Terms and conditions policies
      - Device configuration policies
      - Resource profiles (Wi-Fi, VPN)
      - Apps
      - Device compliance policies
      - Azure AD Conditional Access policies
    - Enroll up to 50 devices
  - Perform test and validation

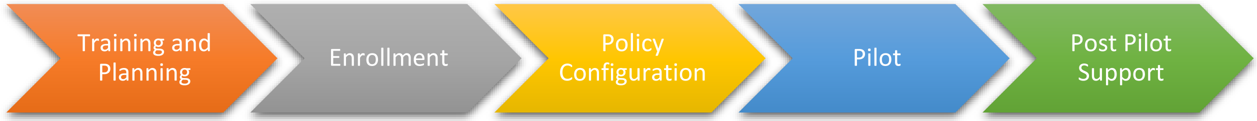
    - Monitor the success of the POC
    - Create action plan to remediate issues
  - Knowledge Transfer and Deployment Support

Windows Autopilot Proof of Concept (POC)

Services to be provided:

- Proof of concept includes:
  - Create Azure AD groups
  - Windows Autopilot and Intune Overview and Design Session
    - Discuss Windows Autopilot scenarios
      - Supporting Azure AD self-service, Hybrid AAD self-service and Self-provisioning AutoPilot scenarios
  - Configure & Enable Windows device management with Intune
    - Intune device configuration policy Creation: Windows 10 administrative template and device restriction policy
    - Assist with auto-enrollment of Windows devices into Intune
    - Provide knowledge transfer to Client's IT administrators
  - Configure VPN and/or Wi-Fi certificate deployment & enable Azure AD conditional access
    - Configure certificate deployment in Intune
    - Configure certificate profile in Intune
    - Deploy device compliance policy for Windows
    - Configure conditional access policy in Azure AD
  - Windows Autopilot Configuration:
    - Configure Windows Autopilot deployment profile
    - Configure Enrollment status page
    - Create Windows Store Apps
    - Deploy apps, device configuration and compliance policies to client devices

Project Plan



Training and Planning

The goal of this phase is to provide Client's IT administrative team with a thorough understanding of the various Active Directory/Azure Directory Hybrid scenarios, different enrollment models, and the pros and cons of those models. This is an important part of understanding how Intune will fit into the existing environment and how policy configuration will flow.

Enrollment

The enrollment phase will address two basic aspects of Intune device enrollment: enrollment of existing machines and devices enrollment going forward. Depending on what Active Directory models exist in the current environment, certain modifications may need to be made to existing OU structure and GPO. If Azure AD Connect has not be established, this will also be setup along with Microsoft Seamless Single Sign-on to facilitate silent enrollment of existing Active Directory joined devices. The manual enrollment process will also be discussed as part of this session. All necessary considerations related to deploying devices using Autopilot will be discussed during this phase including the creation of Dynamic Azure Active Directory groups, enrollment of hardware into Autopilot and the configuration of an Intune Connector for Active Directory if Hybrid AD is desired.

Policy Configuration

Protected Trust will review all major policy areas of Intune and create a basic set of policies for these core areas of Intune to serve as baselines or starter polices use. Areas will include Devices Configuration policies, Windows Update Rings, Device Compliance and App deployment.

Pilot

Once all previous phases have been completed successfully, a pilot group will be selected for initial deployment. Given the scope of Intune capabilities, one specific area of focus will be designated during planning. Completion of this focus area will be the objective for the Pilot. Once all objectives are successfully met, all tested configuration will be applied to the entire organization.

Product Descriptions

The following section describes the components of Microsoft of Endpoint Manager that will be implemented and configured as part of this project:

Microsoft Endpoint Manager

Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint Manager integrates the following services:

Microsoft Intune

As part of Endpoint Manager, use Intune to create and check for compliance, and deploy apps, features, and settings to your devices using the cloud. Intune is a 100% cloud-based mobile device management (MDM) and mobile application management (MAM) provider for your apps and devices. It lets you control features and settings on Windows 10 Pro, Windows 10 Enterprise, macOS, iOS/iPadOS, Android and Android Enterprise devices. It integrates with other services, including Azure Active Directory (AD), mobile threat defenders, ADMX templates, Win32 and custom Line of business (LOB) apps, and more.

If you have on-premises infrastructure, such as Exchange or Active Directory, these Intune connectors are available: 1) the Intune Connector for Active Directory adds entries to your on-premises Active Directory domain for computers that enroll using Windows Autopilot; and 2) the Intune certificate connector processes certificate requests from devices that use certificates for authentication and S/MIME email encryption.

Windows Autopilot

As part of Endpoint Manager, use Autopilot to preconfigure devices, and automatically enroll devices in Intune. You can also integrate Autopilot with Configuration Manager and co-management for more complex device configurations (in preview). Windows Autopilot sets up and pre-configures new devices, getting them ready for use. It's designed to simplify the lifecycle of Windows devices, for both IT and end users, from initial deployment through end of life. Windows Autopilot Deployment allows new, off-the-shelf Windows 10 Pro devices to be delivered to employees without the need for IT setup. This capability is enabled in the Windows 10 Creators Update (1703 or later) in conjunction with a cloud service that prompts the configuration of the Out-of-Box-Experience (OOBE) on Windows 10 Pro devices.

Windows Autopilot Deployment enables the device to join Azure Active Directory (AAD) in Windows 10 OOBE. AAD can then automatically enroll the device into a Mobile Device Management (MDM) service of the customer’s choice (AAD Premium is required for automatic MDM enrollment), allowing the device to take advantage of the most up-to-date Modern IT solutions for the life of the device.

Azure Active Directory (AD)

Azure AD is used by Endpoint Manager for identity of devices, users, groups, and multi-factor authentication (MFA). Azure AD Premium, which may be an additional cost, has additional features to help protect devices, apps, and data, including dynamic groups, auto-enrollment, and conditional access.