Endpoint Administrator

MD-102

TFTEC CLOUD

Module 2: Executar o registro de dispositivo

TFTEC CLOUD

Gerenciar autenticação de dispositivos

TFTEC CLOUD

Introdução

Neste módulo, você aprenderá a importância da autenticação e do gerenciamento de dispositivos ao implementar o Microsoft Entra ID em sua organização. Assim como a autenticação do usuário e a proteção de identidade, proteger identidades de dispositivo é crucial para manter um ambiente de TI seguro e confiável. O Microsoft Entra ID fornece recursos para unir dispositivos baseados no Windows e gerenciá-los usando métodos distintos em comparação com o Active Directory Domain Services

TFTEC CLOUD

Descrever a adesão ao Azure AD (Microsoft Entra Join)

- Windows Pro ou Enterprise Edition podem ingressar no Azure AD (Entra ID) e AD DS
- Os dispositivos ingressados no Azure AD (Entra ID) não podem ser gerenciados com a Política de Grupo
- Cenários típicos para ingressar um dispositivo no Azure AD (Entra ID):
  - Se os aplicativos e recursos que você usa estão principalmente na nuvem
  - Se você deseja separar contas temporárias
  - Se você deseja permitir que os usuários ingressem em seus dispositivos no ambiente corporativo
  - Você deseja fazer a transição para uma infraestrutura baseada em nuvem
  - Você tem filiais remotas com infraestrutura local limitada
- Ingressar dispositivos no Azure AD (Entra ID) durante a configuração inicial ou posteriormente usando as configurações do sistema
- Use o Azure AD híbrido (Entra ID) para registrar automaticamente dispositivos ingressados no domínio local com o Azure AD (Entra ID)

TFTEC CLOUD

Examinar as limitações e benefícios dos pré-requisitos de ingresso no Azure AD (Entra join)

Limitações do Azure AD (Entra ID)

O Azure AD (Entra ID) não faz parte da infraestrutura principal

O Azure AD (Entra ID) não tem os mesmos recursos de gerenciamento que o AD DS

Benefícios do Azure AD (Entra ID)

Logon único (SSO)

Roaming de configurações de usuário entre dispositivos unidos

Suporte do Windows Hello

Restrição de acesso a aplicativos apenas de dispositivos compatíveis

Acesso contínuo a recursos locais

Cenários habilitados usando o Azure AD (Entra ID) com infraestrutura AD local

Facilidade de transição para infraestrutura baseada em nuvem e MDM

Quando a adesão ao domínio local não é possível (tablets, telefones, etc.)

Quando os usuários precisam principalmente acessar o Microsoft 365 ou outros aplicativos SaaS integrados ao Azure AD (Entra ID)

Você deseja gerenciar um grupo de usuários no Azure AD (Entra ID) em vez de no Active Directory

Você deseja fornecer recursos de adesão a funcionários em filiais remotas com infraestrutura local limitada

Ingressar dispositivos no Azure AD (Entra ID)

Ingressar um dispositivo no Microsoft Entra ID não é um procedimento complicado. Você pode fazer isso logo após a instalação do sistema operacional Windows ou pode fazê-lo mais tarde, a qualquer momento

1. Unir um dispositivo ao Azure AD (Entra ID) é um procedimento simples

2. Você pode ingressar no Azure AD (Entra ID) após a instalação do Windows ou mais tarde, a qualquer momento, usando o painel Configurações

3. Você precisa de credenciais do Azure AD (Entra ID) para ingressar o dispositivo no Azure AD (Entra ID)

TFTEC CLOUD

Gerenciar dispositivos associados ao Azure AD (Entra ID)

Política de Grupo ou aplicativos do Microsoft Configuration Manager gerenciam principalmente dispositivos capazes de ingressar no AD DS. Quando você ingressa um dispositivo no Microsoft Entra ID, a Política de Grupo não está disponível, exceto quando você usa o Microsoft Entra Domain Services.

Se você quiser gerenciar dispositivos que ingressam no Microsoft Entra ID, poderá configurar a integração entre o Azure e um mecanismo de gerenciamento de dispositivo móvel, como o Intune. Se você configurar o Intune como um aplicativo no Azure, cada dispositivo que ingressar no Microsoft Entra ID poderá ser configurado para se registrar automaticamente no Intune. Para que isso funcione, você precisa ter uma assinatura ativa do Intune associada ao mesmo locatário do Microsoft Entra em que você configurou a integração desses serviços

Depois que o dispositivo for registrado no Intune, você poderá configurar políticas de segurança e configuração do Intune que serão aplicadas ao usuário ou dispositivo. É importante entender que o gerenciamento por meio de Intune não segue a mesma lógica que o gerenciamento com Política de Grupo, nem tem tantas opções disponíveis.

TFTEC CLOUD

Gerenciar dispositivos associados ao Azure AD (Entra ID)

1. A Política de Grupo gerencia dispositivos que ingressam no AD DS local
2. A Política de Grupo nem sempre está disponível ou suportada para dispositivos que ingressam no Azure AD (Entra ID)
3. O Azure AD (Entra ID) dá suporte à integração com aplicativos de gerenciamento de dispositivos móveis, como o Intune
4. Quando a integração entre o Intune e o Azure AD (Entra ID) é configurada, um dispositivo que ingressa no Azure AD (Entra ID) se inscreve automaticamente no Intune

TFTEC CLOUD

Obrigado

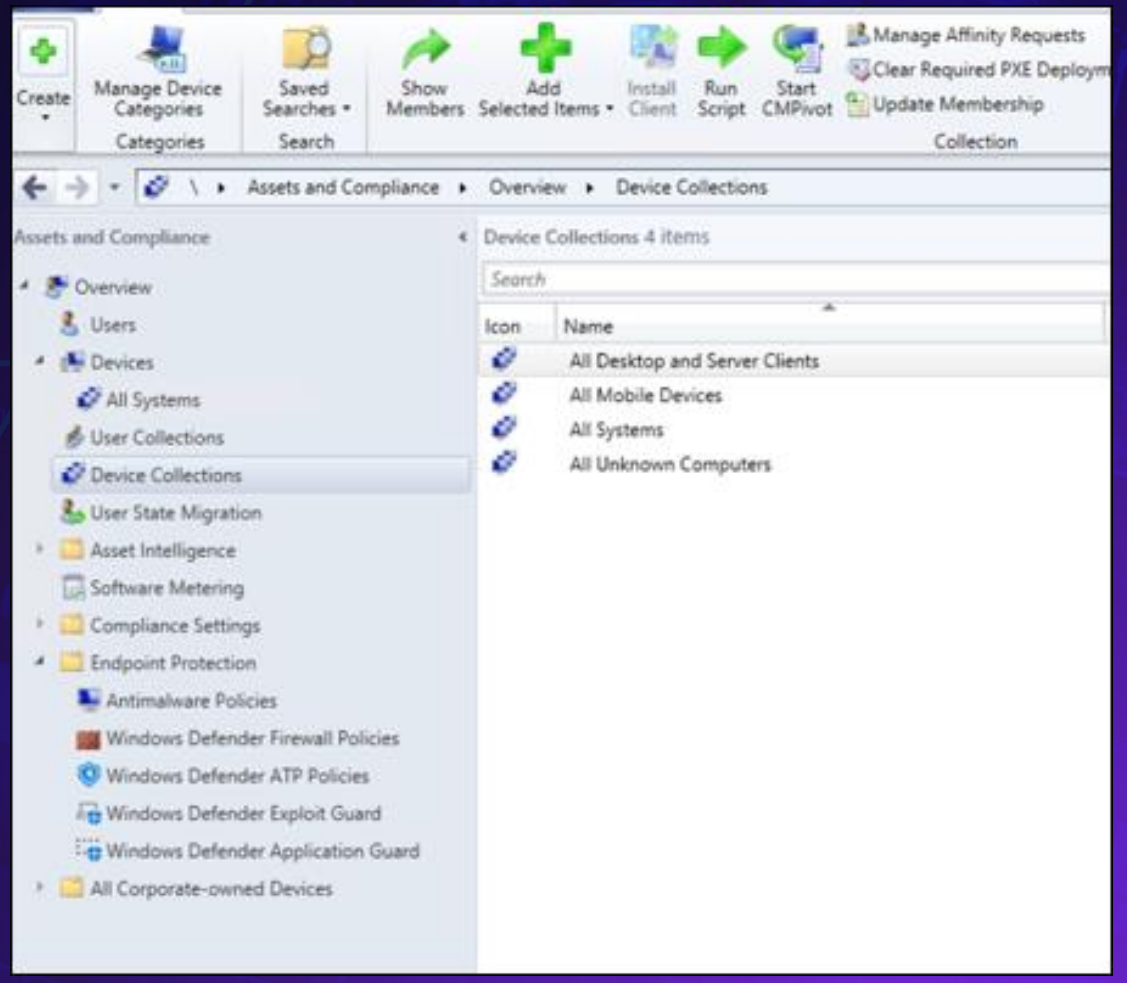
TFTEC CLOUD

Registrar dispositivos usando o Microsoft Configuration Manager

TFTEC CLOUD

Microsoft Configuration Manager

O Microsoft Configuration Manager ajuda a equipe de TI a gerenciar computadores e servidores, mantendo o software atualizado, definindo a configuração e as políticas de segurança e monitorando o status do sistema, além de oferecer aos funcionários acesso a aplicativos corporativos nos dispositivos à escolha deles. Quando o Configuration Manager é integrado ao Microsoft Intune, você pode gerenciar PCs e Macs conectados à empresa junto com dispositivos móveis baseados em nuvem tanto no Windows quanto em dispositivos iOS e Android, tudo em um único console de gerenciamento.



TFTEC CLOUD

Implantar o cliente do Microsoft Configuration Manager

Benefícios do cliente Microsoft Configuration Manager

- Permite o rastreamento de software instalado em um dispositivo cliente
- Fornece informações de inventário de hardware
- Capacidade de gerenciar e implantar o sistema operacional e aplicativos de linha de negócios (LoB)
- Acesso do usuário final ao catálogo de software de autoatendimento

Opções de implantação do cliente

- Client push
- Manual deployment
- OS deployment
- Microsoft Intune

TFTEC CLOUD

Opções de implantação do cliente

Client push

Implanta o cliente Microsoft Configuration Manager diretamente do console do Microsoft Configuration Manager

Descoberta de dispositivos (integração do Active Directory Lightweight Directory Access Protocol (LDAP))

Copia os arquivos para o computador de origem e inicia a instalação automaticamente

O processo de cópia inicial pode aumentar o tráfego de rede

Implantação manual

Implanta os arquivos de origem de instalação do cliente Microsoft Configuration Manager e um arquivo de script contendo os parâmetros de instalação

Executa a partir do arquivo ccmsetup.exe ou do MSI que faz parte dos arquivos do cliente

Pode ser demorado como mecanismo de entrega

OS deployment

Ao instalar e configurar o Windows usando uma sequência de tarefas, insira o cliente do Microsoft Configuration Manager na configuração do Windows e forneça os parâmetros de instalação necessários

Deve ser instalado quando um dispositivo é construído pela primeira vez (ou reconstruído)

Microsoft Intune

O Intune orienta a instalação do cliente do Microsoft Configuration Manager e registra o dispositivo no Cloud Management Gateway

Gerencie cada carga de trabalho respectiva do Intune ou do Microsoft Configuration Manager após a instalação

TFTEC CLOUD

Monitorar o cliente do Microsoft Configuration Manager

1. **Status on-line do cliente.** Online (conectado ao ponto de gerenciamento atribuído) ou offline.
2. **Atividade do cliente.** Active (it has communicated with Microsoft Configuration Manager in the past seven days) or inactive.
3. **Primary User**. O usuário principal deste dispositivo, calculado ao longo de um período de 60 dias das tentativas de login mais frequentes.
4. **Construção do sistema operacional.** Veja a versão do sistema operacional de um dispositivo sem precisar se conectar ou realizar qualquer gerenciamento remoto.
5. **Verificação do cliente.** Estado da avaliação periódica que o cliente Microsoft Configuration Manager executa no dispositivo. A avaliação verifica o dispositivo e pode remediar alguns dos problemas encontrados.

TFTEC CLOUD

Gerenciar o cliente do Microsoft Configuration Manager

- O dispositivo aparece no espaço de trabalho Ativos e Conformidade no nó Dispositivos após a instalação do cliente do Microsoft Configuration Manager e atribuição de site
- Collections
  - Representa dispositivos ou usuários que têm alguns pontos em comum no Microsoft Configuration Manager.
  - Execute tarefas, como direcionar uma implantação ou executar um relatório, em dispositivos de uma coleção.
- As opções de gerenciamento se aplicam a dispositivos em uma coleção ou a dispositivos individuais
  - Inicie o Explorador de Recursos.
  - Inicie a recuperação de política.
  - Adicione a uma coleção.
  - Conjunto de políticas resultante das configurações do cliente (RSOP).

Obrigado

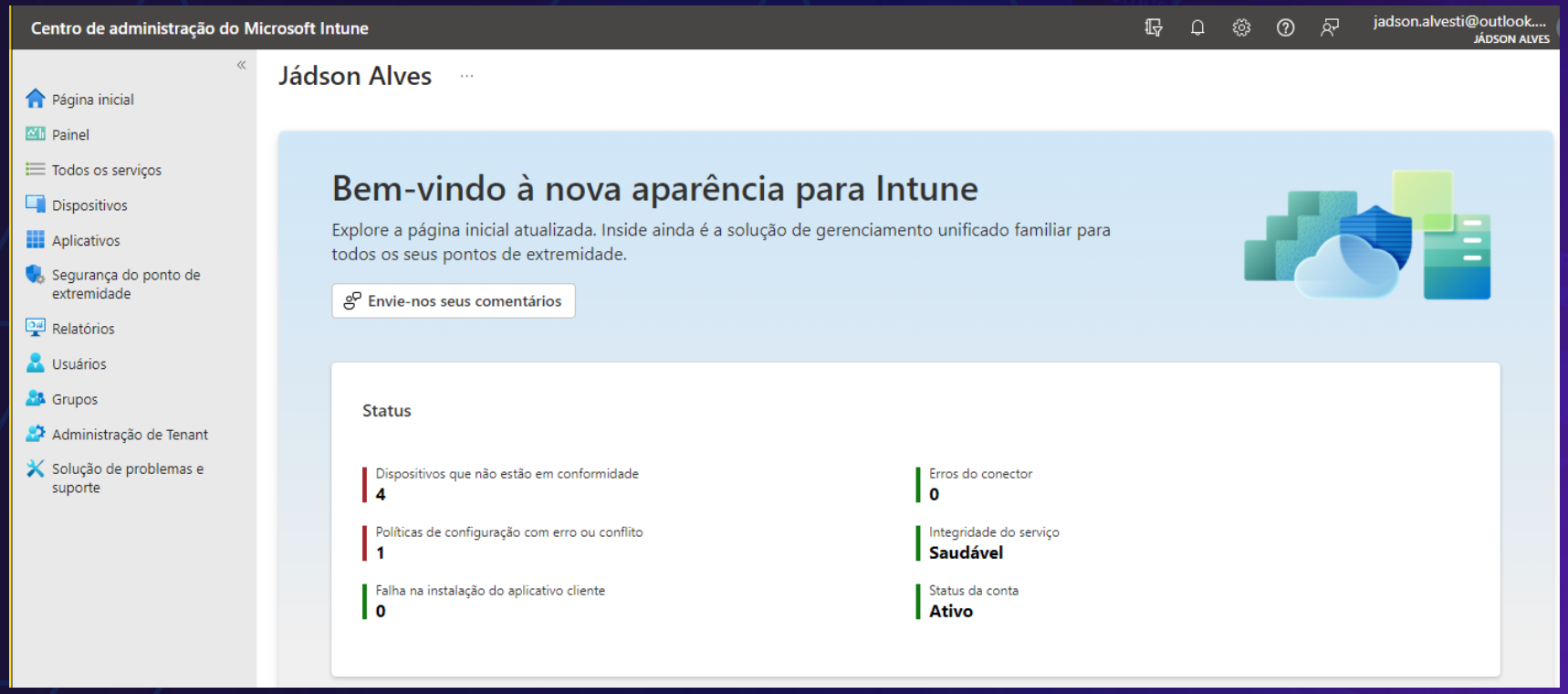
TFTEC CLOUD

Registra dispositivos usando Microsoft Intune

TFTEC CLOUD

Gerenciar dispositivos móveis com o Intune

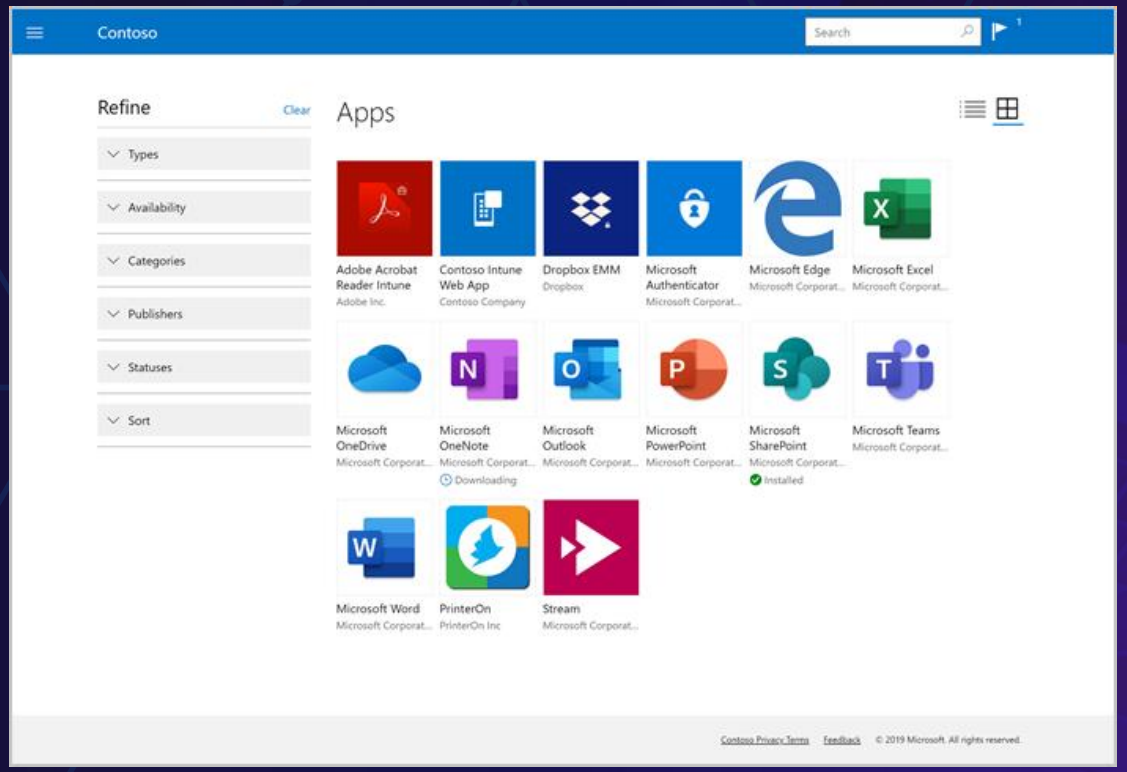
A administração do Intune pode ser acessada usando o *centro de administração do Intune* localizado em https://intune.microsoft.com. Esse console inclui todos os recursos de gerenciamento fornecidos pelo Intune, mas também inclui tarefas comuns de gerenciamento, como gerenciar usuários e grupos. O portal do centro de administração do Intune substitui o console do Intune encontrado anteriormente no portal do Azure.



TFTEC CLOUD

Intune Portal da empresa

O Portal da Empresa está disponível como um aplicativo Web e como um aplicativo para desktops e dispositivos móveis em todas as plataformas. Os usuários usam esse portal para gerenciar automaticamente o registro de dispositivos e também para acessar aplicativos publicados pelo administrador da empresa. Eles o acessam por meio do https://portal.manage.microsoft.com/ ou instalando o aplicativo Portal da Empresa em dispositivos Windows, iOS ou Android.



TFTEC CLOUD

Ciclo de vida do gerenciamento de dispositivo

Como a maioria das atividades de gerenciamento de TI, o gerenciamento de dispositivos móveis segue um ciclo de vida. O ciclo de vida de gerenciamento de dispositivo móvel contém quatro fases:

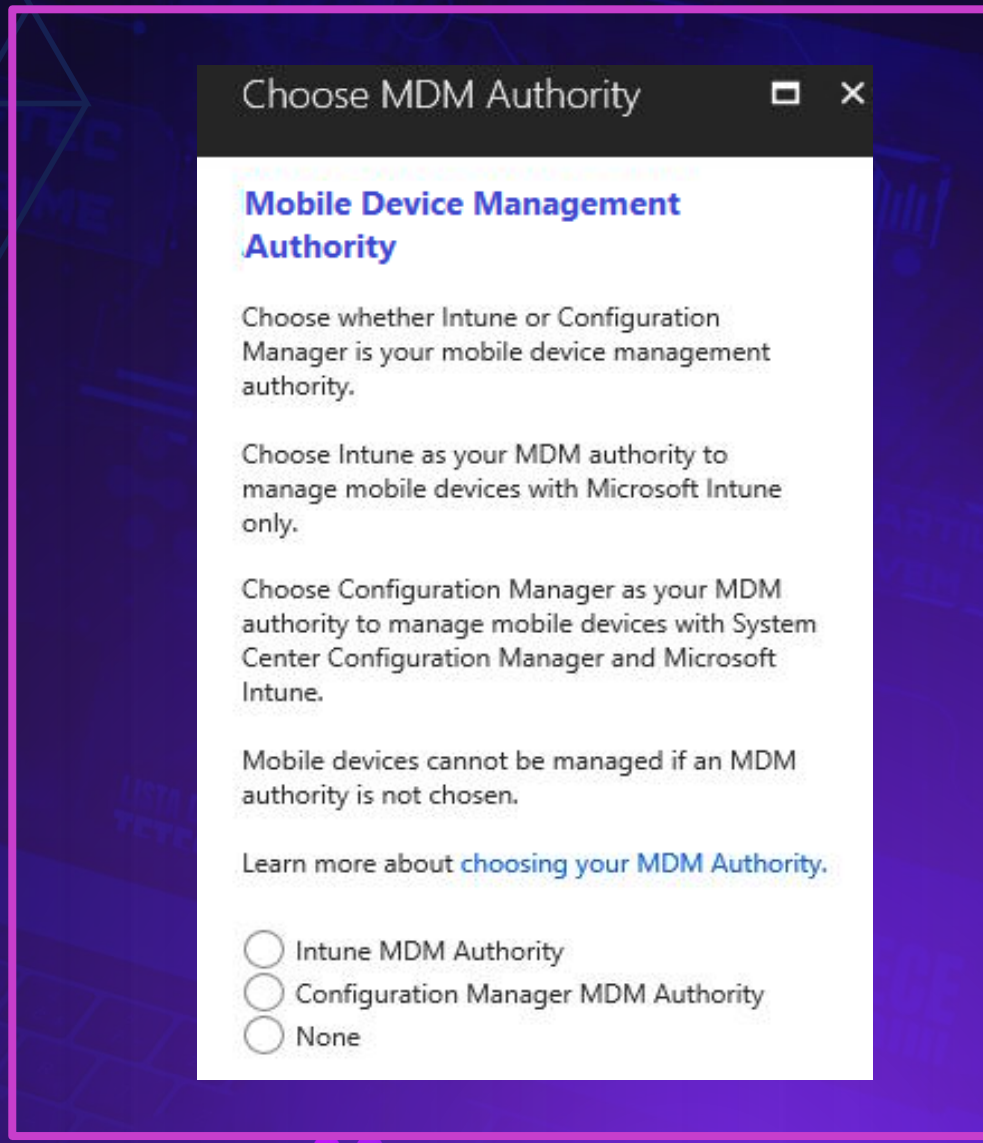
- **Registrar:** na fase Registrar, os dispositivos se registram na solução de gerenciamento de dispositivo móvel. Com o Intune, você pode registrar dispositivos móveis, como telefones e computadores Windows.
- **Configurar:** na fase Configurar, você ajuda a garantir que os dispositivos registrados sejam seguros e estejam em conformidade com qualquer configuração ou política de segurança. Você também pode automatizar tarefas administrativas comuns, como configurar o Wi-Fi.
- **Proteger:** na fase Proteger, a solução de gerenciamento de dispositivo móvel fornece monitoramento contínuo das configurações estabelecidas na fase Configurar. Durante essa fase, você também usa a solução de gerenciamento de dispositivo móvel para ajudar a manter os dispositivos em conformidade por meio do monitoramento e implantação de atualizações de software.
- **Desativar:** quando um dispositivo não é mais necessário, é perdido ou roubado, você deve ajudar a proteger os dados nesse dispositivo. Você pode remover dados redefinindo o dispositivo, executando um apagamento completo ou executando um apagamento seletivo que remove apenas dados de propriedade corporativa do dispositivo.

TFTEC CLOUD

Habilite o gerenciamento de dispositivos móveis

Uma tarefa essencial de qualquer administrador é proteger os recursos e os dados de uma organização. Esse conjunto de tarefas é chamado de gerenciamento de dispositivos. Os usuários têm muitos dispositivos nos quais eles abrem e compartilham arquivos pessoais, visitam sites e instalam aplicativos e jogos. Esses mesmos usuários também são funcionários e querem usar seus dispositivos para acessar os recursos do trabalho, como email e SharePoint. O Gerenciamento de dispositivo permite às organizações proteger os recursos e os dados.

- O gerenciamento de dispositivos móveis (MDM) é um padrão da indústria para gerenciar dispositivos móveis, como smartphones, tablets, laptops e computadores desktop.
- Para permitir a inscrição de dispositivos móveis, a Autoridade MDM deve ser definida na configuração do Intune.
- Por padrão, o Intune permite o registro de dispositivos Windows, Android e Samsung Knox Standard. Para gerenciar dispositivos iOS e macOS, é necessário um certificado push MDM da Apple.



TFTEC CLOUD

Explicar as considerações para o registro do dispositivo

Determinar o método de inscrição

- Política de grupo
- Ingressando no Azure AD
- Manualmente (Configurações, Pacote de Provisão, Aplicativo Portal da Empresa)

Dispositivos suportados

- Windows 10/11 (versões Home, Pro, Education, modo S e Enterprise)
- Computadores em nuvem com Windows 10/11 no Windows 365
- Windows 10 IoT e Windows 10 holográfico
- Windows 10 2019 LTSC
- Windows RT 8.1 e Windows 8.1 (modo de sustentação)
- Apple iOS/iPadOS 13.0 e posterior
- macOS X 10.15 e posterior
- Android 6.0 e posterior, incluindo Samsung Knox 2.4 e posterior e Android for Work

Determine os dispositivos permitidos e os critérios

Determine se a inscrição é opcional ou obrigatória

Gerenciar política de inscrição corporativa

- Seu domínio inicial do Azure AD (Entra ID) seguirá o modelo:
  - your-domain.onmicrosoft.com
- Adicione um ou mais nomes de domínio personalizados, ou seja, Contoso.com (recomendado)
- Adicione nomes de domínio personalizados no portal de gerenciamento do Microsoft 365
- Configurar o registro automático do MDM (recomendado)

  OU

  Crie registros CNAME para simplificar a inscrição e o registro de dispositivos quando não estiver licenciado para Azure AD (Entra ID) Premium

TFTEC CLOUD

Registrar dispositivos Windows no Intune

Muitas maneiras de registrar dispositivos Windows no Microsoft Intune:

- Adicionar conta corporativa ou escolar
- Inscreva-se apenas no MDM (orientado pelo usuário)
- Ingresso no Azure AD (Entra ID) (experiência pronta para uso (OOBE))
- Ingresso no Azure AD (Entra ID) (Autopilot – modo de implantação orientado pelo usuário)
- Ingresso no Azure AD (Entra ID) (modo de autoimplantação do Autopilot)
- Inscreva-se apenas no MDM (Gerenciador de registro de dispositivos)
- Cogerenciamento do Microsoft Configuration Manager
- Ingresso no Azure AD (Entra ID) (inscrição em massa)

TFTEC CLOUD

Registrar dispositivos Android no Intune

O registro de dispositivos Android normalmente é realizado pelo usuário final:

- Baixe o aplicativo Portal da Empresa no Google Play
- Abra o aplicativo Portal da Empresa, entre com uma conta corporativa ou de estudante
- Siga as instruções fornecidas no aplicativo

Android Empresarial

- Perfil de trabalho do Android
- Android Enterprise dedicado
- Android Enterprise totalmente gerenciado

TFTEC CLOUD

Registrar dispositivos iOS no Intune

- Cadastro de dispositivos iOS pode ser feito pelo usuário ou automaticamente
- Para inscrever um dispositivo iOS usando o aplicativo Portal da Empresa
  - Baixe o aplicativo Portal da Empresa na loja de aplicativos da Apple
  - Entre no aplicativo Portal da Empresa com uma conta corporativa ou de estudante e siga as instruções
- Suporte do Intune para métodos de registro de dispositivos iOS de propriedade da empresa
  - Programa de registro de dispositivos da Apple (DEP)
  - Gerente escolar da Apple
  - Inscrição no Assistente de configuração do Apple Configurator
  - Inscrição direta no Configurador Apple
  - Com uma conta de administrador de registro de dispositivos.
- Modo supervisionado

TFTEC CLOUD

Explorar o gerenciador de registro de dispositivos

Os utilizadores existentes do Azure AD podem ser adicionados à conta de utilizador do gestor de inscrição de dispositivos (DEM), permitindo-lhes inscrever até 1000 dispositivos através do Portal da Empresa.

- Limitações de dispositivos registrados usando uma conta DEM
- Permissões para DEM

As funções do Azure AD de Administrador de Serviço Global ou do Intune são necessárias para:

- Conclua tarefas relacionadas à inscrição no DEM no Portal do Administrador
- Acesse todos os usuários do DEM, apesar das permissões de controle de acesso baseado em função (RBAC) estarem listadas e disponíveis na função de usuário personalizada

Monitorar o registro do dispositivo

Usar o centro de administração do Intune

- Informações sobre os dispositivos individuais
- Quantos dispositivos estão usando as diferentes plataformas, incluindo Windows, Android e iOS

Use Azure (Entra) portal

- O centro de administração do Intune mostra apenas dispositivos registrados
- Dispositivos ingressados no Azure-AD (Entra ID)
- Configurações do dispositivo
- Configurar roaming de estado empresarial
- Registros de auditoria

TFTEC CLOUD

Gerencie dispositivos remotamente

Execute ações remotas do dispositivo

- Como retirar, limpar, excluir, bloqueio remoto, reiniciar, sincronizar, verificação rápida e verificação completa, etc..

As ações disponíveis dependem da plataforma do dispositivo e da configuração do dispositivo.

Gerenciar e monitorar informações do dispositivo

- Hardware
- Aplicativos descobertos
- Políticas de conformidade de dispositivos
- Políticas de configuração de dispositivos

TFTEC CLOUD

Obrigado

TFTEC CLOUD

Laboratórios

TFTEC CLOUD

Lab 02

TASK01:

- Criar trial Microsoft Azure
- Criar o trial Office 365
- Ativar o trial Microsoft 365 E5
- Configurar o MDM no Microsoft Azure
- Microsoft Entra Join

TFTEC CLOUD

Lab 02

TASK02:

- Overview Microsoft Intune
- Registro de dispositivos Windows, Android e iOS
- Devices Intune
- Join Device utilizando o Portal da empresa
- Monitorar o registro do dispositivo

TFTEC CLOUD

Obrigado

TFTEC CLOUD