



ESCOLA SUPERIOR DE TECNOLOGIA DA INFORMAÇÃO

Projeto de Bloco

Disciplina: Projeto de Bloco - Arquitetura e Infraestrutura de Aplicações

Aluno: Marcelo Carvalho

Professor: Fabio Campos Chaves

Data: 31/03/2020

1 Introdução

1.1 Cenário

Atualmente a empresa deseja implementar o conceito de BYOD, que significa: **Traga o Seu Próprio Dispositivo**, do inglês **Bring Your Own Device**, para os usuários. Permitindo que utilizem os dispositivos de sua preferência. Assim os colaboradores ficam mais confortáveis com tudo em um só lugar, seja pessoal ou corporativo.

Daí surgem os desafios, pois ao permitir o tráfego e armazenamento de informações sensíveis e confidenciais aumenta o risco de vazamentos de informações ou misturar dados corporativos em aplicativos e ou plataformas inseguras. Portanto é necessária uma solução para permitir administração de políticas de segurança e gerenciamento sem interferir na privacidade ou causar transtornos para os usuários finais. As pesquisas realizadas acerca do tema apresentam números alarmantes:



Fonte imagem:

The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits

<https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>

Os números associados aos riscos de exposição dos dispositivos perdidos ou roubados por ano também são bastante substanciais:



Fonte imagem:

The Rise and Risk of BYOD

www.druva.com/blog/the-rise-and-risk-of-byod/

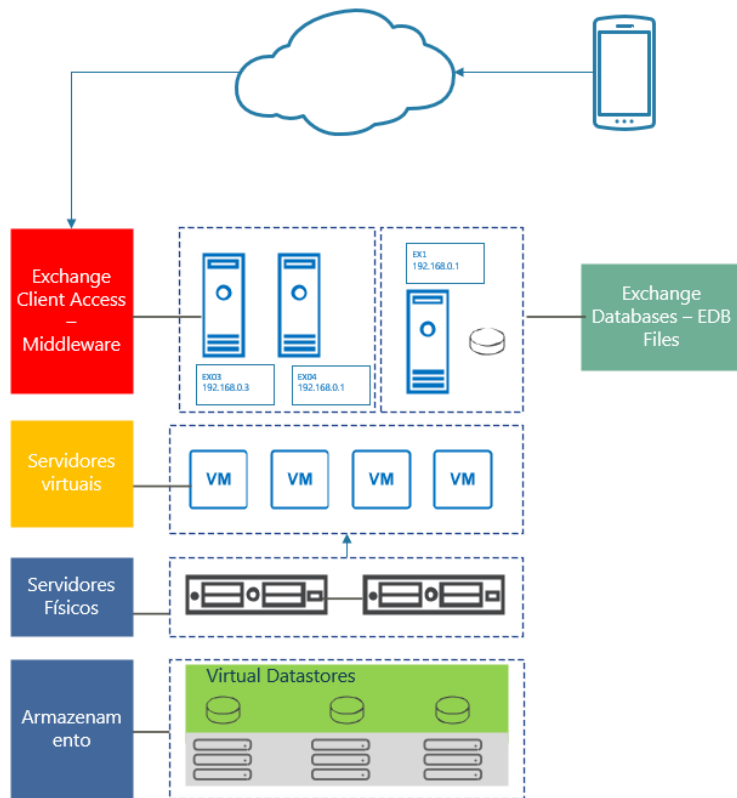
1.2 Necessidades

Dados os fatos do alto volume de usuários que gostariam de utilizarem os dispositivos de sua preferência para fins corporativos e necessidade de manter os dados e o dispositivo protegido a empresa decidiu implementar políticas de Gerenciamento de Dispositivos, de forma que possa aumentar o nível de segurança dos dispositivos

1.3 Proposta da Solução

A solução de gerenciamento de dispositivos ou MDM – Mobile Device Management a ser implementada se baseia na aplicação distribuída do Exchange Server. A solução possui as funcionalidades para endereçar necessidades para o gerenciamento de dispositivos móveis.

A solução será implementada de forma a ser distribuída no ambiente virtual do VMWare e a topologia segue configurada conforme abaixo:



Com a solução as seguintes políticas estão disponíveis no ambiente On-Premises:

geral

▶ **segurança**

- ☐ Pedir uma senha
 - ☒ Permitir senhas simples
 - ☐ Pedir uma senha alfanumérica

A senha deve incluir a seguinte quantidade de conjuntos de caracteres:

1
 - ☐ Solicitar criptografia no dispositivo
 - ☐ Comprimento mínimo da senha:

4
 - ☐ Número de falhas na autenticação antes de o dispositivo ser apagado:

8
 - ☐ Exigir autenticação após o dispositivo ter ficado inativo por (minutos):

15

 minutos
 - ☐ Definir tempo de vida da senha (dias)

90

 dias
- Contagem de reutilização da senha

0

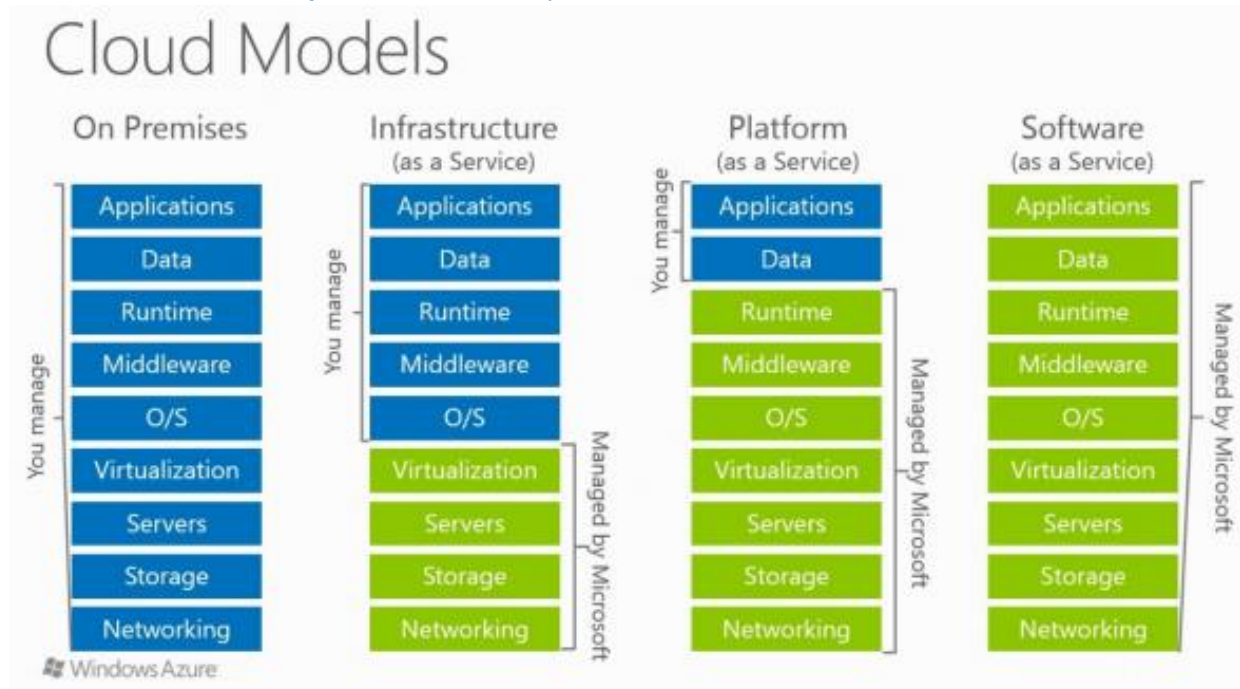
Salvar Cancelar

2 Revisão teórica

2.1 Contexto

Conforme a solução foi sendo implementada e adotada pelo grupo de usuários piloto foram mapeadas necessidades adicionais para um gerenciamento de dispositivos completo e que conseguisse também endereçar políticas de configuração em notebooks, incluindo versões Windows e MacOS. A solução inicial baseada em Exchange Server no ambiente virtual On-Premises possui algumas limitação, portanto a solução adotada será baseada em SaaS – *Software As a Service*. Continua como aplicação distribuída, entretanto, neste modelo todas as camadas são gerenciadas pelo provedor. Cabendo a empresa apenas a gestão e configuração como serviço.

Abaixo uma breve ilustração dos modelos disponíveis em nuvem:



Referencias imagem:

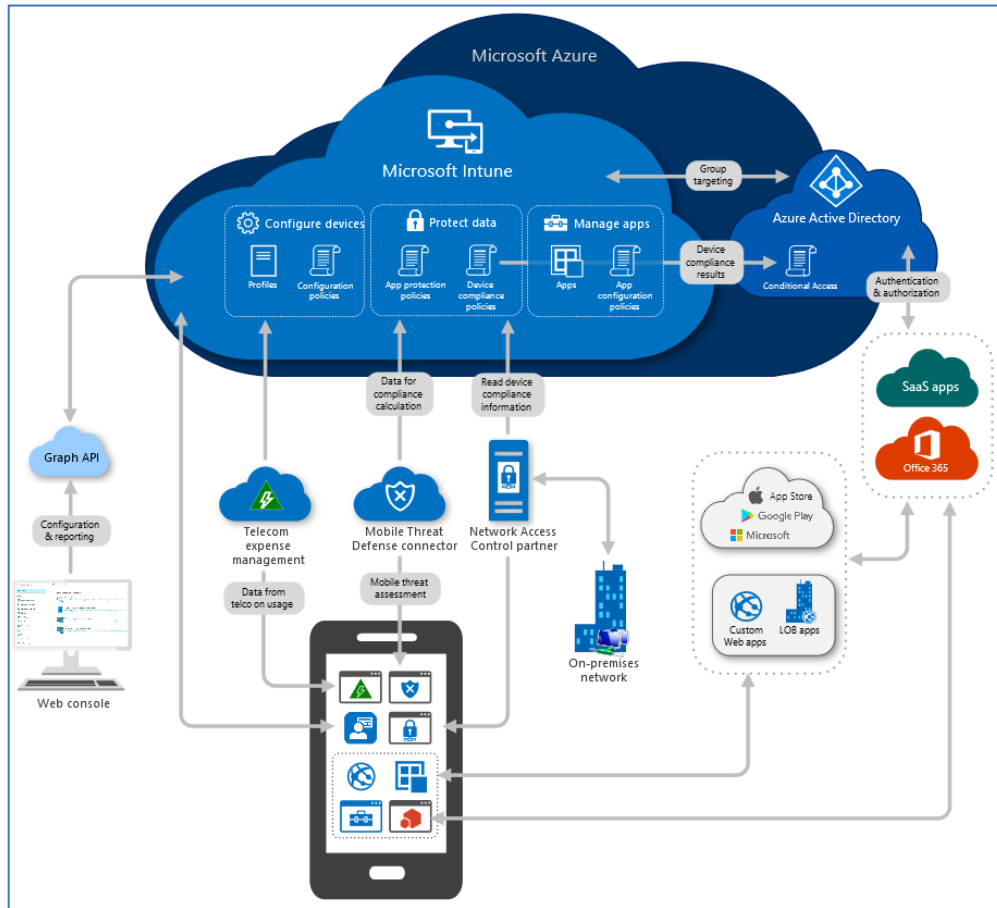
https://www.lambda3.com.br/2017/08/iaas-paas-e-saas-qual-a-diferenca/?doing_wp_cron=1585685064.7924499511718750000000

O Microsoft Intune é uma solução em nuvem, baseada em SaaS, *suportado pelo Microsoft Azure*. Possui licenciamento simplificado e oferece opções de integração com ferramentas internas de gerenciamento, como o *Microsoft System Center*.

O Microsoft Intune é uma solução de gerenciamento de dispositivos ou MDM – Mobile Device Management que permite um gerenciamento de mobilidade completo, a partir de uma única console de gerenciamento e desenvolvida para controlar dispositivos Windows, iOS, Android, MacOS. Através do Intune é possível configurar uma série de parâmetros de segurança, como criptografia, senha de acesso etc., restrições de rede, distribuir aplicativos de forma automatizada e outras funções.

Toda a adoção e configuração da solução exige esforço mínimo e ainda oferece a possibilidade de testar o produto até 90 dias sem custo e ou compromisso.

Abaixo um diagrama da arquitetura da solução:



Referência imagem:

Arquitetura de alto nível para o Microsoft Intune

<https://docs.microsoft.com/pt-br/mem/intune/fundamentals/high-level-architecture>

2.2 Gestão de Código Fonte

A solução do Microsoft Intune é desenvolvida e suportada pela Microsoft e o acesso ao código fonte é vedado ao público. A solução é hospedada na nuvem de serviços da Microsoft, com ambiente altamente redundante e seguro. O fabricante segue normas rígidas, padrões internacionais e melhores práticas para desenvolvimento, homologação, controle e

2.3 Comparação com outras Soluções mesmo segmento

Durante o processo de avaliação, foi avaliada outra solução de MDM, do fabricante VMWare – o AirWatch. Ambas as soluções são excelentes, líderes de mercado e atenderam todas as expectativas das necessidades de negócio da empresa. Abaixo um breve resumo do comparativo das soluções:

Microsoft Intune	VMWare AirWatch MDM
Distribuição de Apps e aplicações	Device Management

Device Management	Políticas de DLP (Data Loss Prevention)
Device Enrollment	Configuração simplificada
Device Compliance	Gerenciamento de políticas e segurança
Monitoramento de aplicações	Device Compliance
Configurações de Acesso Conditional	Gerenciamento de usuários e grupos
Gerenciamento de usuários e grupos	Gerenciamento via MAM (Mobile Application Management)
Controles de usuários baseado em funções (roles)	Device Enrollment
Gerenciamento via MAM (Mobile Application Management)	VMWare TrustPoint
Gerenciamento de políticas e segurança	Remote Commands
Integração com o Microsoft Configuration Manager (Co-Management)	Sistema de gerenciamento de eventos granular
Windows AutoPilot	Dynamic Watermark

Preço por usuário/mês: \$6 (USD)	Preço por usuário/mês: \$10.90 (USD)
---	---

Embora a solução da VMWare seja superior, o critério adotado foi influenciado pelo preço entre as soluções e integração com soluções já implementadas na empresa, como o Microsoft Configuration Manager e o Office 365.

Fonte de informações:

Microsoft Intune Features

<https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune>

Workspace ONE Powered by AirWatch

<https://www.air-watch.com/pricing/>

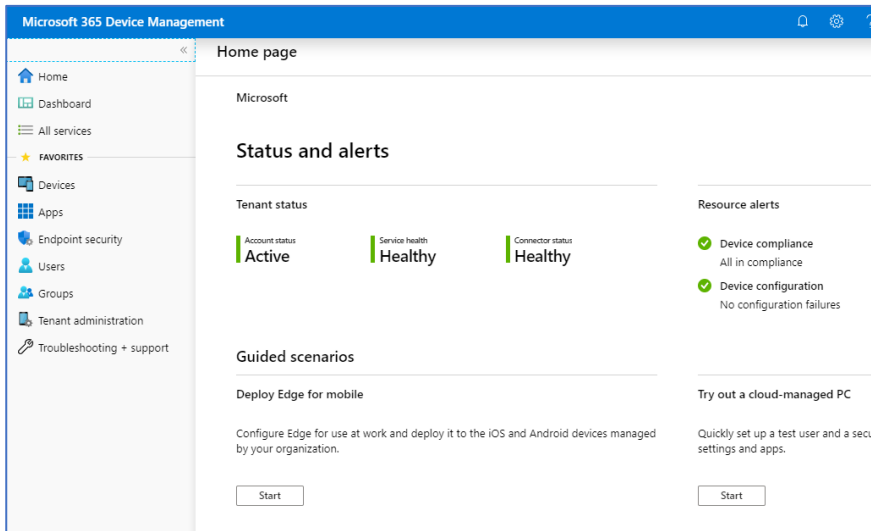
A implementação é feita por meio de assinatura e com base em licenças por número de usuários. Serão adquiridas 800 licenças da solução para atender o cenário da empresa.

2.4 Organização da aplicação

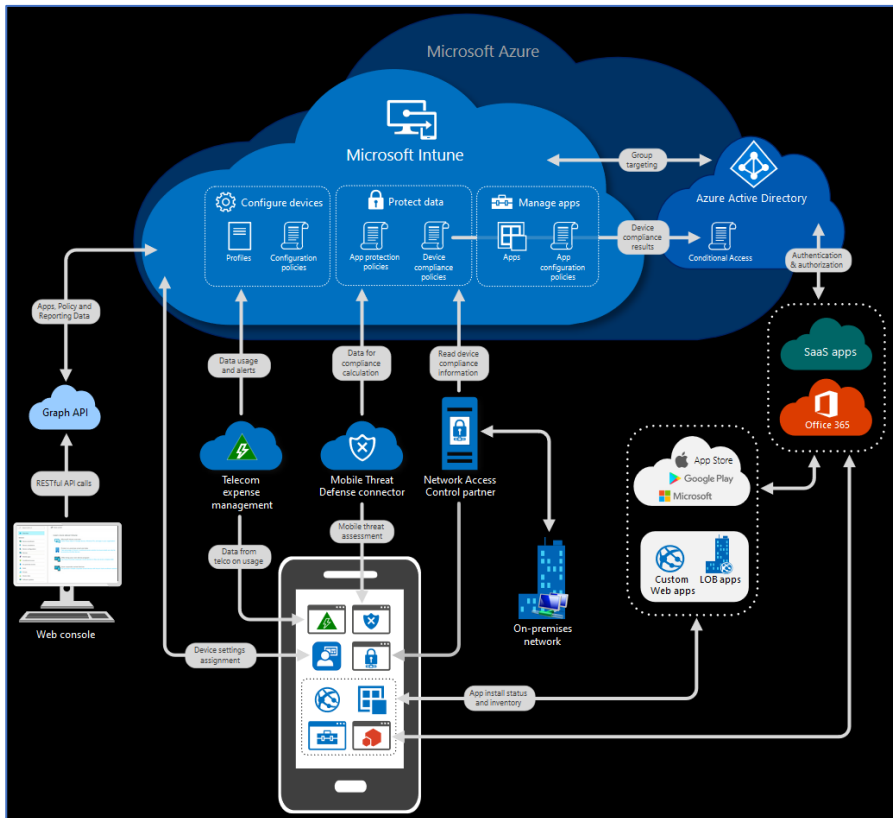
A infraestrutura da solução já é provisionada na nuvem para funcionar de forma elástica, garantindo que consiga suprir as necessidades de acordo que com o número de usuários forem sendo adicionados a solução. Os pré-requisitos também são bastante simplificados, tanto para o lado de infraestrutura, baseado em SaaS quanto pelo lado de adoção por parte dos usuários finais. Os usuários possuem opções bastante simplificadas para realizar o processo de Enrollment (processo de aderir a solução a partir de seus dispositivos). Pode ser feita de instalando um agente específico chamado Portal da Empresa, disponível em qualquer Store online de forma gratuita, ou sem instalar nenhum componente adicional (MAM – Mobile Application Management), o administrador pode especificar políticas em nível de aplicação, como por exemplo para o email corporativo.

A solução possui uma console de gerenciamento web disponível em

<https://devicemanagement.microsoft.com/> e possui a aparência simplificada e fluida conforme abaixo:



Conforme já mencionado anteriormente abaixo uma abordagem de como a infraestrutura da solução do Intune está organizada e como os componentes estão distribuídos:



3 Implementação

3.1 Planejamento e implementação

Abaixo o planejamento macro da implementação da solução:



A implantação será realizada em fases.



Fonte imagem: Intune migration guide

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

1. Fase 1: Setup básico: Nesta etapa as configurações básicas utilizadas na avaliação e homologação da solução serão revisadas;
2. Fase 2: Serão definidas as configurações e políticas de gerenciamento de dispositivos, levando em consideração dispositivos da empresa e dispositivos pessoais (CYOD e BYOD). Também serão definidos os perfis de usuários e respectivas configurações com base nas necessidades de negócio;
3. Fase 3: Configurações de aplicativos: Serão definidas as políticas de uso de aplicativos e informações corporativas nos dispositivos. As configurações para dispositivos no modelo BYOD serão mais restritivas para garantir um nível elevado de segurança em dispositivos que não são gerenciados pela empresa;
4. Fase 4: Plano de comunicação: Os usuários começaram a receber os comunicados com base no plano de comunicação que envolve divulgação da tecnologia, política de uso, suporte do Service Desk, perguntas frequentes, guias, dicas e tutoriais.
5. Fase 5: Fase de adoção: Os usuários começaram a adotar a solução de MDM, com base no dispositivo e perfil de usuário definido na Fase 2;

3.2 Cronograma de implementação

- Cronograma de atividades e o prazo estimado para conclusão da implementação da solução SaaS é de 35 dias:

Projeto Bloco - TP7	35 days
Fase 1:	16 days
Revisão de políticas	8 hrs
Revisão da infraestrutura básica (Rede, internet, usuár	16 hrs
Adquirir e atribuir licenças	8 hrs
Fase 2:	13 days
Definir número de dispositivos que cada usuário reg	8 hrs
Gerenciar configurações de dispositivos (criptografi	8 hrs
Entregar aplicativos, perfis de email, perfis de VPN	24 hrs
Avaliação de critérios no nível do dispositivo para as	24 hrs
Publicar e implantar aplicativos	40 hrs
Fase 3	15 days
Configurar políticas de MAM	16 hrs
Preparar configurações de privacidade e segurança	8 hrs
Configurar políticas de segurança de dispositivo	8 hrs
Testes finais de políticas de MAM	16 hrs
Fase 4	1 day
Plano de comunicação para usuários VIP	3 hrs
Plano de comunicação para usuários Marketing	1 hr
Plano de comunicação para usuários Finanças	1 hr
Plano de comunicação para usuários Administração	1 hr
Plano de comunicação para usuários Vendas	1 hr
Fase 5	5 days
Iniciar campanhas de adoção da solução	2 hrs
Prover workshops periódicos de utilização	16 hrs
Iniciar campanhas de Home Office	24 hrs

A implementação das políticas de gerenciamento foi baseada em 3 pilares:

1. Gerenciamento de dispositivos:

- Gerenciar dispositivos de diferentes plataformas e sistemas operacionais, tais como iOS, MacOS, Linux, Windows.
- Configurar políticas de gerenciamento com base nas políticas de segurança da informação. Bloquear dispositivos que tenham sido desbloqueados (Rooting ou Jailbreaking);
- Permitir que os usuários utilizem dispositivos de sua escolha e ainda assim garantir que os padrões de segurança e facilidades de gerenciamento são mantidos com a mesma qualidade dos dispositivos fornecidos pela empresa;
- Garantir relatórios completos e permitindo a visualização dos dispositivos que estão em conformidade com os padrões da empresa;
- Distribuir configurações personalizadas para os dispositivos, tais como conexões VPN, certificados digitais, configurações e políticas (Exemplo: Bloqueio automático de tela a cada 3 minutos, habilitar criptografia do dispositivo e etc;

- Permitir que o dispositivo seja apagado em caso de perda ou roubo, aumentando a segurança dos dados corporativos.

2. Conformidade e acesso condicional:

- O Intune permite uma integração com o sistema de identidades (AzureAD) para permitir acesso a dados e aplicações corporativas com base em condições do dispositivo do usuário. Por exemplo, o usuário para sincronizar o email corporativo precisa que o dispositivo esteja em conformidade com os políticas definidas pela organização. Se a política determina que o dispositivo para estar em conformidade precisa estar com a criptografia de armazenamento habilitada, somente dispositivos nessa condição conseguirão acessar o email corporativo.

3. Gerenciamento de aplicações:

O Intune possui um conceito de permitir um gerenciamento a nível de aplicações, permitindo proteger os dados corporativos sem misturar com os dados pessoais/privados dos usuários. As principais funcionalidades a serem adotadas:

- Distribuir aplicações com base nas necessidades de negócio, baseado em grupos ou áreas de negócio;
- Permitir a deleção seletiva dos dados, ou seja, em caso de perda, roubo ou desligamento da empresa somente os dados e aplicativos corporativos serão removidos;
- Permitir a gestão das aplicações e dados corporativos sem a necessidade de instalar nenhum agente adicional;

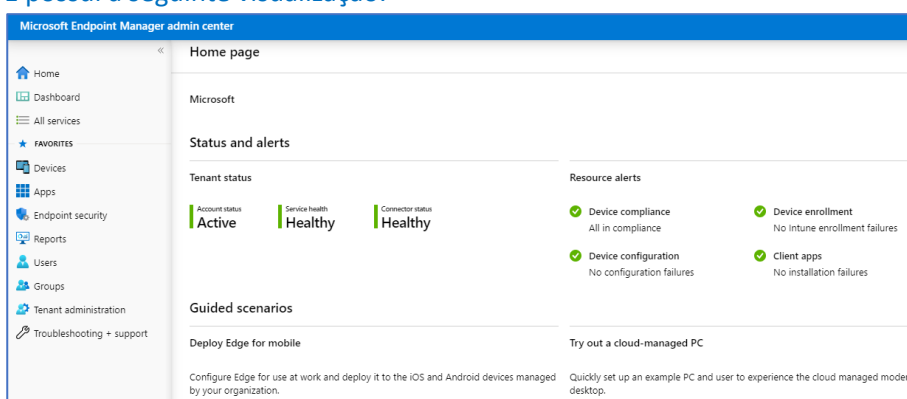
3.3 Referências da aplicação e documentação

Como a solução selecionada é baseada em SaaS (Software As a Service) a plataforma de MDM já contempla todos os componentes necessários para seu funcionamento.

A console de gerenciamento está disponível em:

<https://devicemanagement.microsoft.com>

E possui a seguinte visualização:



3.4 Detalhamento configurações e políticas

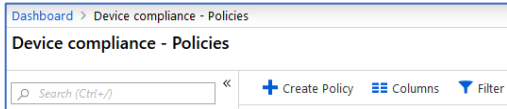
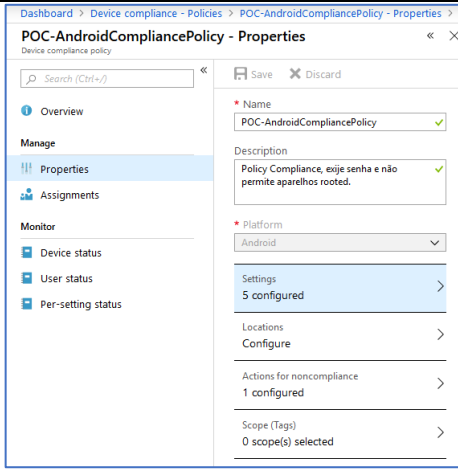
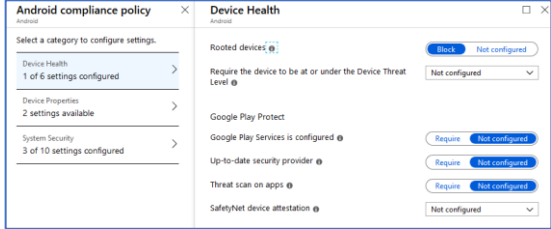
Nesta seção são definidas as configurações básicas de conformidade para os usuários que irão se conectar aos recursos da organização, através de conjuntos de regras que funcionam como requisitos para estes dispositivos, como por exemplo, uma versão mínima de Sistema Operacional, dispositivo sem PIN de acesso. Se os requisitos não são cumpridos o acesso do usuário através do dispositivo que não está em conformidade com a regra é bloqueado.

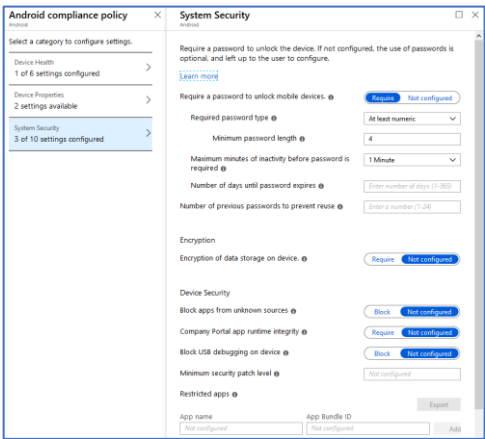
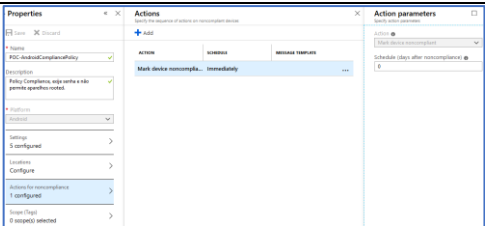
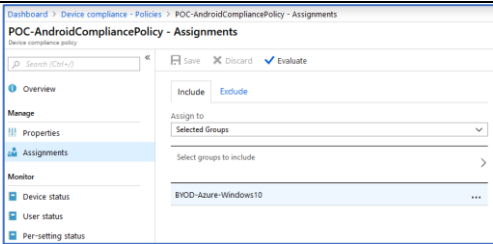
Foram criadas 3 regras básicas para cada plataforma: Android, iOS e Windows 10 conforme abaixo:

+ Create Policy Columns Filter Refresh Export						
<input type="text" value="Search by name"/>						
POLICY NAME	PLATFORM	POLICY TYPE	ASSIGNED	LAST MODIFIED		
POC-AndroidCompliancePolicy	Android	Android compliance policy	Yes	5/16/19, 8:50 PM		
POC-iOS-CompliancePolicy	iOS	iOS compliance policy	Yes	5/14/19, 9:53 PM		
POC-Windows10CompliancePolicy	Windows 10 and later	Windows 10 compliance policy	Yes	5/16/19, 8:51 PM		

Abaixo o detalhamento das regras de conformidade que foram criadas:

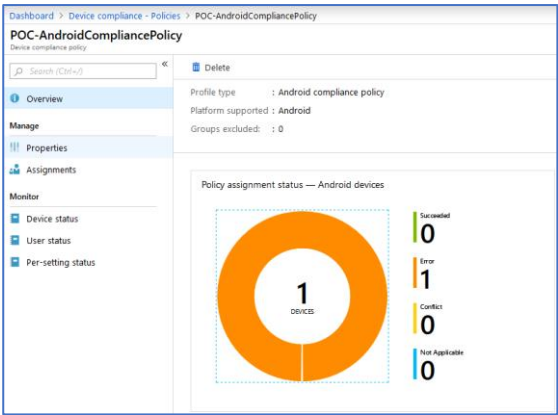
Regra **POC-AndroidCompliancePolicy**

Procedimento	Tela
<p>Acesse o portal https://devicemanagement.microsoft.com > Device compliance policies > Create Policy:</p>  <p>O nome para a política: POC-AndroidCompliancePolicy</p>	
<p>Selecione as políticas conforme desejado em Device Health e System Security:</p>	

	
Na seção Actions for noncompliance é possível especificar se um determinado dispositivo não estiver em conformidade ele pode ser marcado como noncompliant após um determinado período. No caso do piloto a configuração está para marcar imediatamente:	
Depois a regra deve ser associada a um determinado grupo para que possa ser aplicada e entre em vigor para os membros desse determinado grupo. No caso do piloto foi inicialmente adicionado somente o grupo BYOD-Azure-Windows10 . Ou seja, as configurações desta política será aplicada aos membros deste grupo que utilizarem um dispositivo Android:	

Ao final é possível monitorar o status dos dispositivos que foram marcados como fora de conformidade perante as regras de configuração pré-determinadas.

Para acessar os detalhes acesse o Dashboard do Intune > **Device Compliance Policies** e localize o dispositivo que gostaria de obter os detalhes:



Em seguida clique no dispositivo **Device status > Device Compliance** e visualize quais foram os itens do dispositivo que não estão em conformidade:

Dashboard > Device compliance - Policies > POC-AndroidCompliancePolicy > Device status > t3cloud_marcelo.lagden_Android_5/16/2019_10:23 PM - Device compliance > POC-AndroidCompliancePolicy

POC-AndroidCompliancePolicy

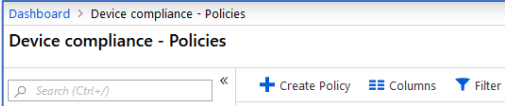
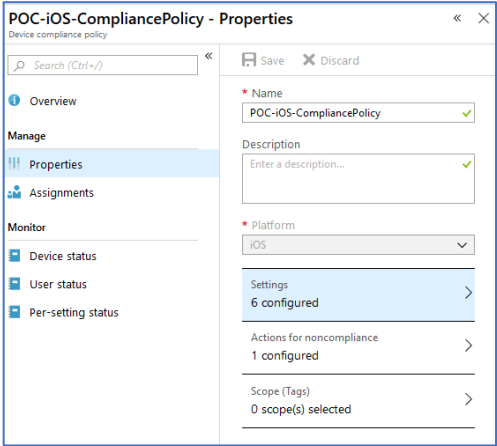
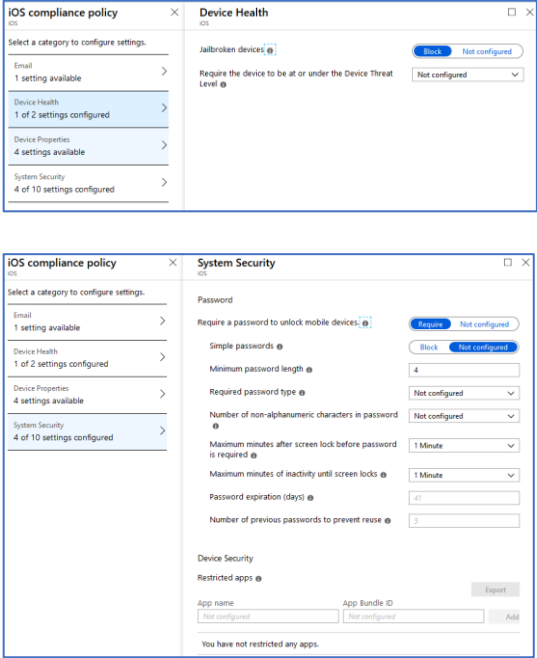
Policy settings

Export

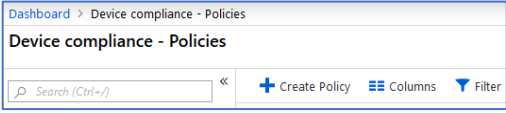
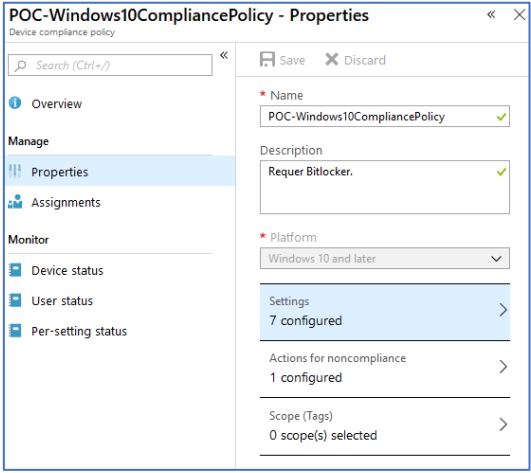
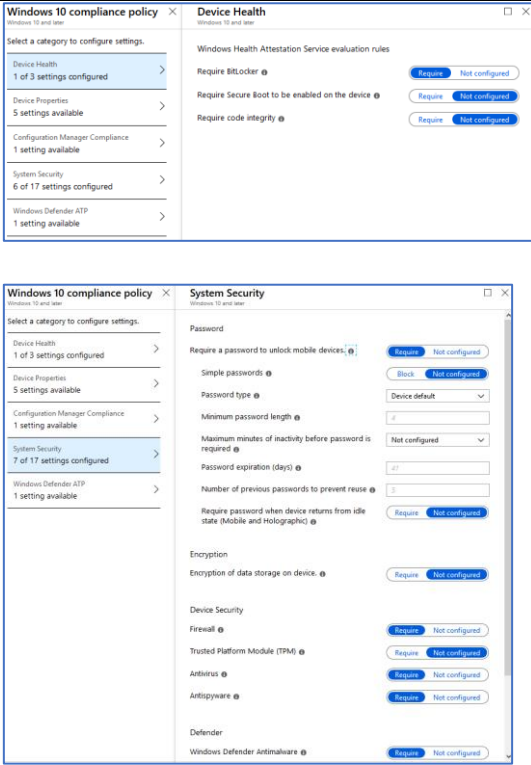
Filter by name

SETTING	STATE	STATE DETAILS
Maximum minutes of inactivity before password is required	Compliant	
Require a password to unlock mobile devices.	Compliant	
Rooted devices	Not Compliant	
Required password type	Error	-2016281112 (Remediation failed)
Minimum password length	Error	-2016281112 (Remediation failed)

Regra POC-iOSCompliancePolicy

Procedimento	Tela
<p>Acesse o portal https://devicemanagement.microsoft.com > Device compliance policies > Create Policy:</p>  <p>O nome para a política: POC-iOSCompliancePolicy</p>	
<p>Selecione as políticas conforme desejado em Device Health e System Security:</p>	

Regra **POC-Windows10CompliancePolicy**

Procedimento	Tela
<p>Acesse o portal https://devicemanagement.microsoft.com > Device compliance policies > Create Policy:</p>  <p>O nome para a política: POC-Windows10CompliancePolicy</p>	
<p>Selecione as políticas conforme desejado em Device Health e System Security:</p>	

3.4.1 Configurações do Azure Conditional Access

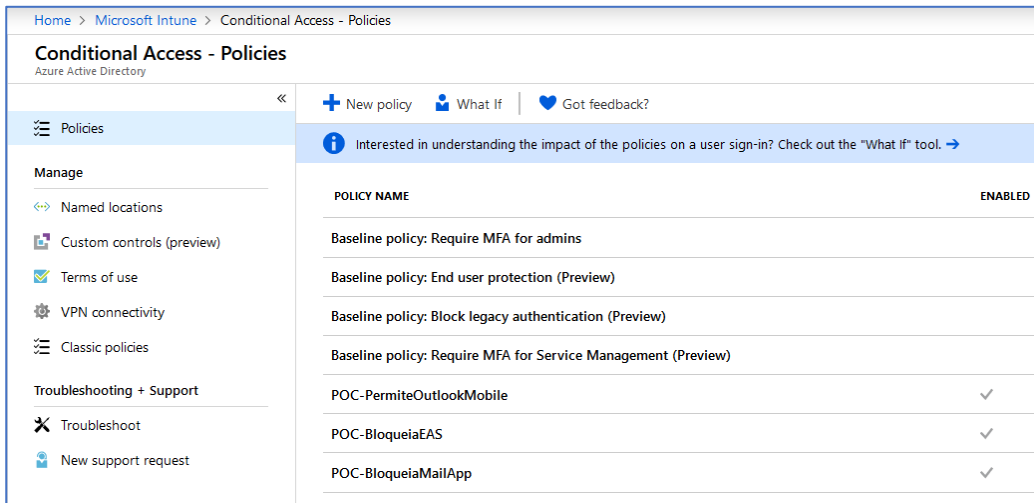
Abaixo estão descritas as configurações realizadas para os testes de Acesso Condicional ao Office 365. As regras criadas bloqueiam o protocolo Exchange ActiveSync sem suporte a *Modern Authentication*.

Foram criadas 3 regras de Acesso Condicional:

- **POC-PermiteOutlookMobile**
- **POC-BloqueiaEAS**

- **POC-BloqueiaMailApp**

Para acessar as regras acesse o portal <https://devicemanagement.microsoft.com> > **Conditional Access:**

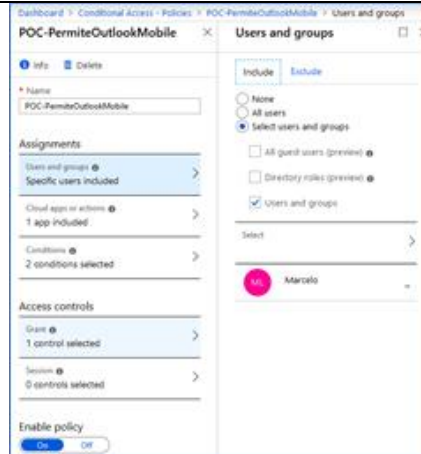


Abaixo o detalhamento das regras de acesso condicional que foram criadas para o piloto:

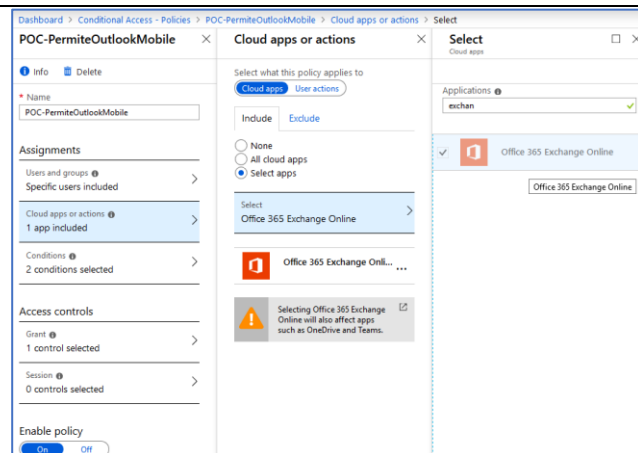
Regra **POC-PermiteOutlookMobile**

Procedimento	Tela
Acesse o portal https://devicemanagement.microsoft.com > Conditional Access:	
Selecione Policies > + New policy	

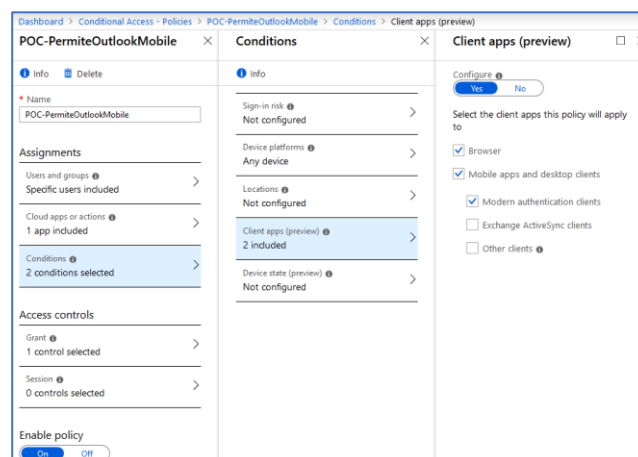
Preencha o nome da regra com **POC-PermiteOutlookMobile** e em seguida clique em **Assignments**. Insira o nome do usuário ou grupo para que receba a política. Se for aplicar para todos os usuários, selecione **All Users**:



Na guia **Cloud Apps** selecione a opção **Office 365 Exchange Online**:



Na guia **Conditions > Client apps** selecione a opção **Configure** para **Yes** e selecione as opções **Browse**, **Modern Apps and desktop clients** e **Modern authentication clients**:



<p>Na guia Access Controls selecione Grant Access e selecione Require device to be marked as compliant. Isso garante que os dispositivos devem estar de acordo com as políticas definidas em Device Compliance (Também no portal do Intune):</p>	
<p>Se certifique a política esta de acordo com o desejado antes de ativa-la na organização. Para habilitar a política basta ativar a opção no botão Enable Policy:</p>	

3.5 Funcionamento da aplicação

Abaixo as evidências sobre a solução de MDM (Mobile Device Management) funcionando sobre os dispositivos, acessando os recursos da empresa.

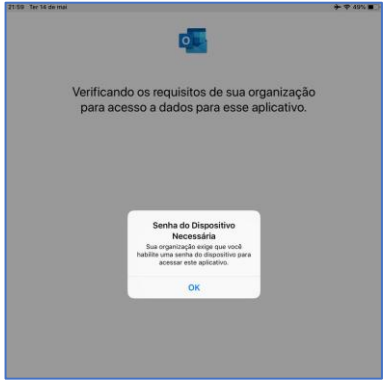
A figura a seguir mostra a mensagem que é exibida ao usuário após o processo de enrollment, aplicando uma política de configuração que exige que o dispositivo tenha um PIN de acesso:



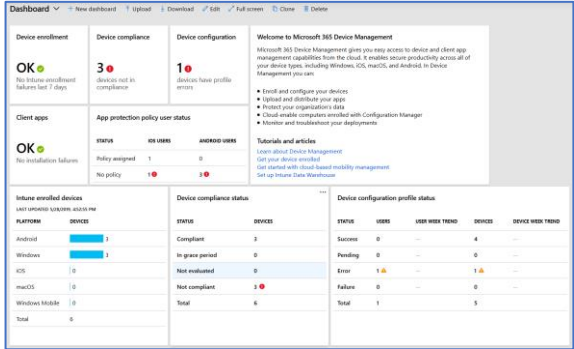
Quando a política MAM é aplicada o usuário é notificado conforme imagem a seguir:



No exemplo de configuração da política de **Access Requirements** utilizada o PIN de acesso é exigido que seja habilitado no dispositivo. Atente que nenhum agente (**Portal da Empresa**) foi instalado no dispositivo:



O Intune oferece relatórios bem completos sob todos os aspectos dos dispositivos que foram habilitados. Acessando o portal <https://devicemanagement.microsoft.com/> já apresenta o Dashboard inicial com uma visão geral dos dispositivos, conformidade, status das políticas e overview de aplicativos e configurações.



4 Conclusão

O mundo mudou e está mais conectado do que nunca. As empresas precisam controlar seus dispositivos móveis para alcançar seus objetivos. Todas as empresa precisam ter maior controle sobre a informação, maior produtividade, segurança e privacidade dos dados, sem contar com a satisfação de seus colaboradores.

Com a solução, passará a ter gestão sobre os dispositivos móveis e ao introduzir essa nova prática na sua empresa, as outras áreas passarão a solicitar novas demandas de mobilidade, ajudando a amadurecer sua gestão sobre a mobilidade corporativa. Ainda a permitir a administração de políticas de segurança e gerenciamento sem interferir na privacidade ou causar transtornos para os usuários finais

As crescentes demandas de mobilidade são cada vez mais exigidas, cabendo a empresa medir se a solução conseguirá acompanhar a essas necessidades.

5 Referências

Visão geral do Microsoft Intune

<https://docs.microsoft.com/pt-br/mem/intune/fundamentals/what-is-intune>

Conceitos básicos do Microsoft Intune

<https://docs.microsoft.com/pt-br/mem/intune/fundamentals/>

Overview PaaS

<https://azure.microsoft.com/pt-br/overview/what-is-saas/>

Arquitetura de alto nível para o Microsoft Intune

<https://docs.microsoft.com/pt-br/mem/intune/fundamentals/high-level-architecture>

Abaixo o link do repositório do GitHub com os documentos entregues

<https://github.com/marcelocarvalho-infnet/infnet>