



ESCOLA SUPERIOR DE TECNOLOGIA DA INFORMAÇÃO

## Teste de Performance 8

**Disciplina:** Projeto de Bloco - Arquitetura e Infraestrutura de Aplicações

**Aluno:** Marcelo Carvalho

**Professor:** Fabio Campos Chaves

**Data:** 20/03/2020

**Faça upload de uma versão inicial do capítulo 3/Implementação de seu Projeto de Bloco. Você deve contemplar:**

- a. Referências dos downloads e/ou versões de todos os componentes da solução implementada.**
- b. Todos os passos/capturas de tela de implementação de sua infraestrutura de virtualização.**
- c. Todos os passos/capturas de tela de configuração de sua aplicação.**
- d. Uma captura de tela de sua aplicação em funcionamento.**

**[A. Referências dos downloads e/ou versões de todos os componentes da solução implementada.]**

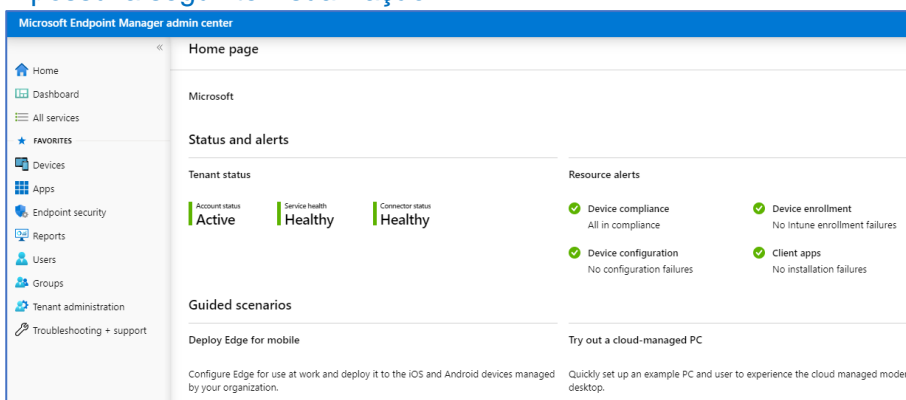
**R:**

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:



**[B. Todos os passos/capturas de tela de implementação de sua infraestrutura de virtualização.]**

**R:**

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.

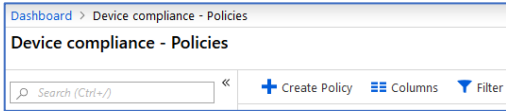
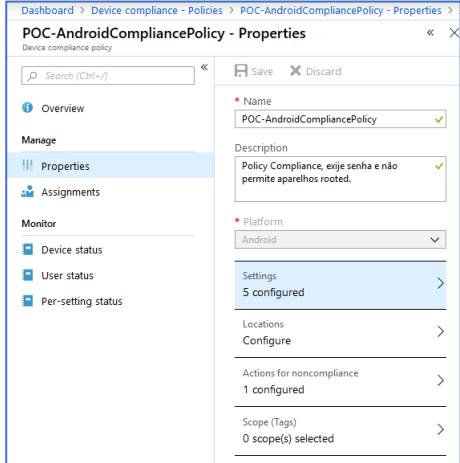

Nesta seção são definidas as configurações básicas de conformidade para os usuários que irão se conectar aos recursos da organização, através de conjuntos de regras que funcionam como requisitos para estes dispositivos, como por exemplo, uma versão mínima de Sistema Operacional, dispositivo sem PIN de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

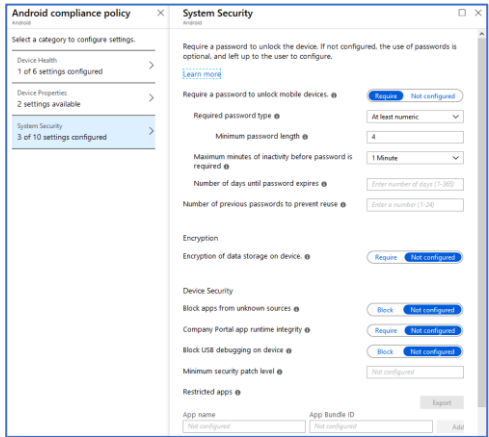
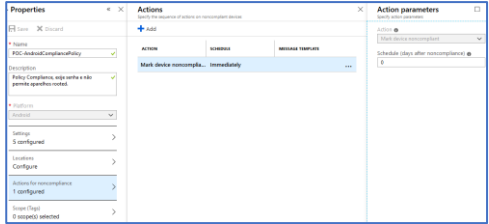
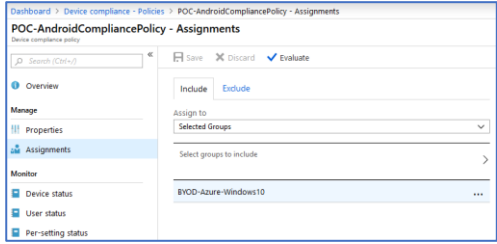
Foram criadas 3 regras básicas para cada plataforma: Android, iOS e Windows 10 conforme abaixo:

<a href="#">+ Create Policy</a> <a href="#">Columns</a> <a href="#">Filter</a> <a href="#">Refresh</a> <a href="#">Export</a>					
<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:

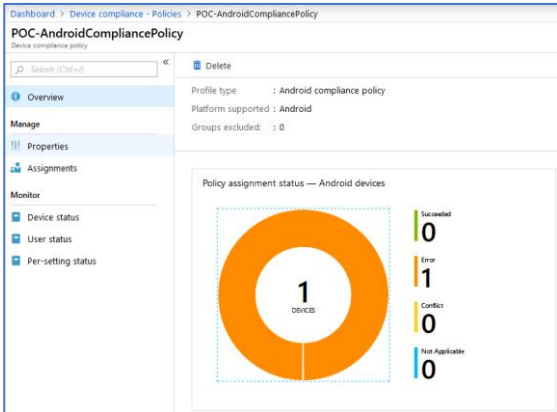
### Regra POC-AndroidCompliancePolicy

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

	
<p>Na seção <b>Actions for noncompliance</b> é possível especificar se um determinado dispositivo não estiver em conformidade ele pode ser marcado como <b>noncompliant</b> após um determinado período. No caso do piloto a configuração está para marcar imediatamente:</p>	
<p>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 <b>BYOD-Azure-Windows10</b>. Ou seja, as configurações desta política será aplicada aos membros deste grupo que utilizarem um dispositivo Android:</p>	

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:



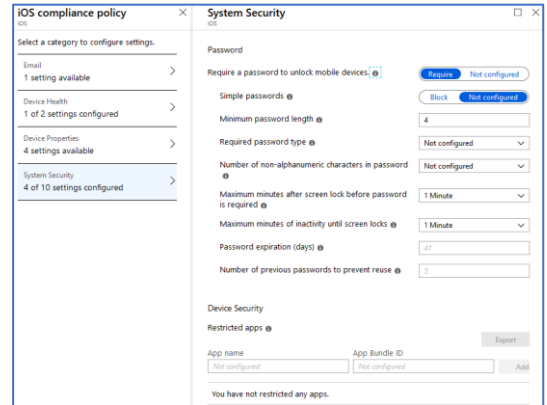
Em seguida clique no dispositivo **Device status > Device Compliance** e visualize quais foram os itens do dispositivo que não estão em conformidade:

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 <a href="https://devicemanagement.microsoft.com">https://devicemanagement.microsoft.com</a> &gt; <b>Device compliance policies &gt; Create Policy:</b></p> <div><div>Dashboard &gt; Device compliance - Policies</div><div>Device compliance - Policies</div><div><div>Search (Ctrl+/)</div><div>Create PolicyColumnsFilter</div></div></div> <p>O nome para a política: <b>POC-iOSCompliancePolicy</b></p>	<div><div>POC-iOS-CompliancePolicy - Properties</div><div>Device compliance policy</div><div><div>Search (Ctrl+/)</div><div>SaveDiscard</div></div><div><div>Overview</div><div>Manage</div><div>Properties</div><div>Assignments</div><div>Monitor</div></div><div><div>Device status</div><div>User status</div><div>Per-setting status</div></div><div><div>Name</div><div>POC-iOS-CompliancePolicy</div></div><div><div>Description</div><div>Enter a description...</div></div><div><div>Platform</div><div>iOS</div></div><div><div>Settings</div><div>6 configured</div></div><div><div>Actions for noncompliance</div><div>1 configured</div></div><div><div>Scope (Tags)</div><div>0 scope(s) selected</div></div></div>

Selecione as políticas conforme desejado em **Device Health** e **System Security**:



## Regra POC-Windows10CompliancePolicy

### Procedimento

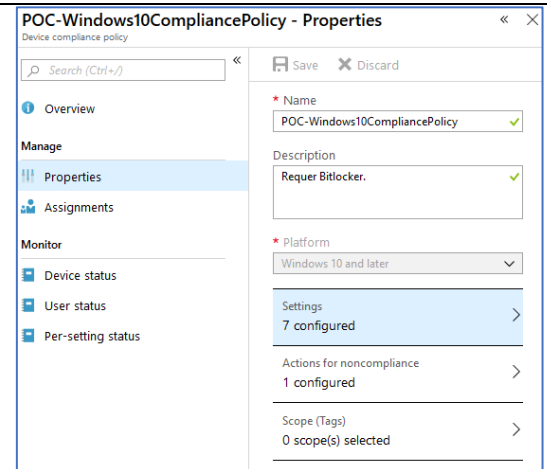
Acesse o portal

<https://devicemanagement.microsoft.com> > **Device compliance policies** > **Create Policy**:

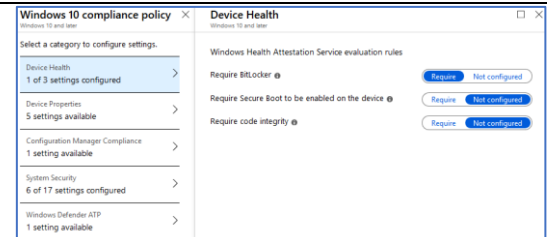


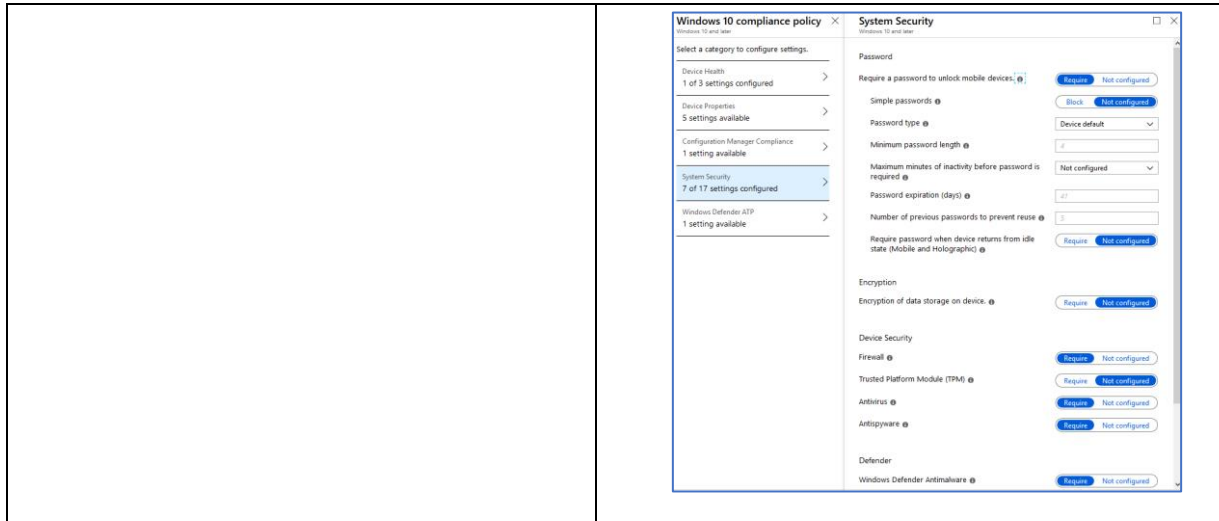
O nome para a política: **POC-Windows10CompliancePolicy**

### Tela



Selecione as políticas conforme desejado em **Device Health** e **System Security**:





## 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:

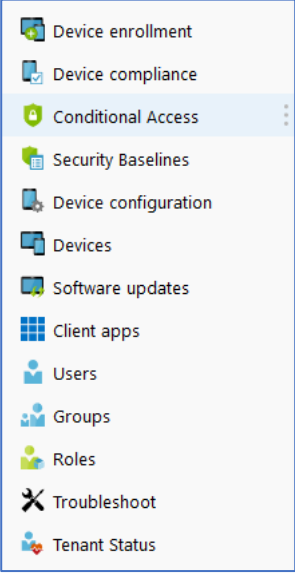
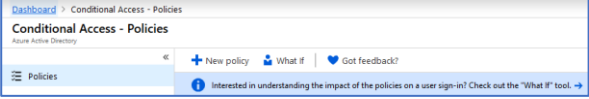
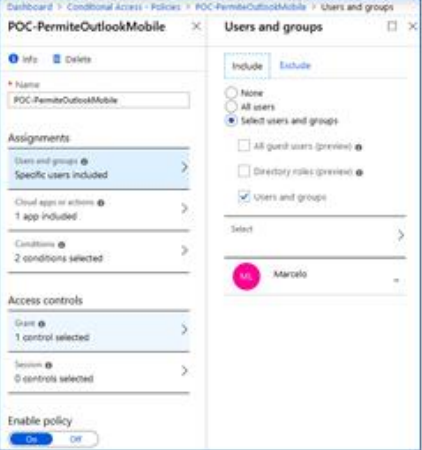
- **POC-PermiteOutlookMobile**
- **POC-BloqueiaEAS**
- **POC-BloqueiaMailApp**

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

Home > Microsoft Intune > Conditional Access - Policies																
Conditional Access - Policies Azure Active Directory																
Policies Manage Named locations Custom controls (preview) Terms of use VPN connectivity Classic policies Troubleshooting + Support Troubleshoot New support request	+ New policy   What If   Got feedback? Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →															
	<table> <thead> <tr> <th>POLICY NAME</th><th>ENABLED</th></tr> </thead> <tbody> <tr> <td>Baseline policy: Require MFA for admins</td><td></td></tr> <tr> <td>Baseline policy: End user protection (Preview)</td><td></td></tr> <tr> <td>Baseline policy: Block legacy authentication (Preview)</td><td></td></tr> <tr> <td>Baseline policy: Require MFA for Service Management (Preview)</td><td></td></tr> <tr> <td>POC-PermiteOutlookMobile</td><td>✓</td></tr> <tr> <td>POC-BloqueiaEAS</td><td>✓</td></tr> <tr> <td>POC-BloqueiaMailApp</td><td>✓</td></tr> </tbody> </table>	POLICY NAME	ENABLED	Baseline policy: Require MFA for admins		Baseline policy: End user protection (Preview)		Baseline policy: Block legacy authentication (Preview)		Baseline policy: Require MFA for Service Management (Preview)		POC-PermiteOutlookMobile	✓	POC-BloqueiaEAS	✓	POC-BloqueiaMailApp
POLICY NAME	ENABLED															
Baseline policy: Require MFA for admins																
Baseline policy: End user protection (Preview)																
Baseline policy: Block legacy authentication (Preview)																
Baseline policy: Require MFA for Service Management (Preview)																
POC-PermiteOutlookMobile	✓															
POC-BloqueiaEAS	✓															
POC-BloqueiaMailApp	✓															

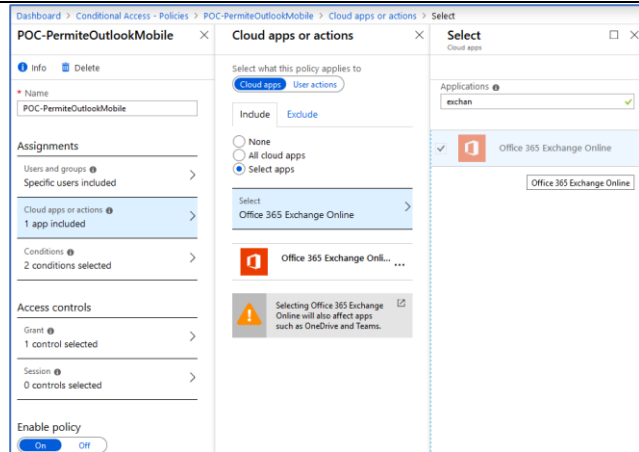
Abaixo o detalhamento das regras de acesso condicional que foram criadas para o piloto:

### Regra **POC-PermiteOutlookMobile**

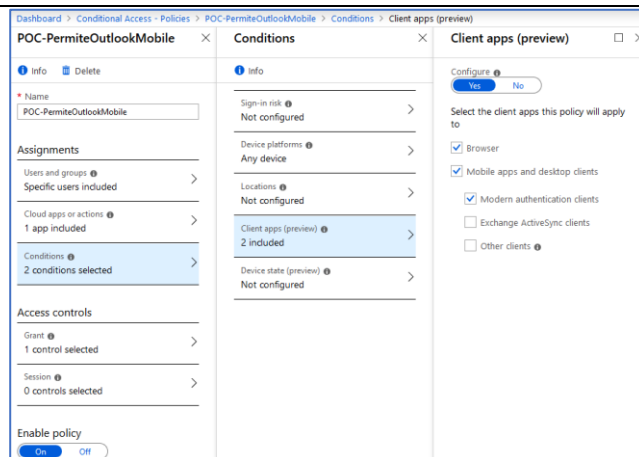
Procedimento	Tela
<p>Acesse o portal <a href="https://devicemanagement.microsoft.com">https://devicemanagement.microsoft.com</a> &gt; <b>Conditional Access:</b></p>	
<p>Selecione <b>Policies &gt; + New policy</b></p>	
<p>Preencha o nome da regra com <b>POC-PermiteOutlookMobile</b> e em seguida clique em <b>Assignments</b>. Insira o nome do usuário ou grupo para que receba a política. Se for aplicar para todos os usuários, selecione <b>All Users</b>:</p>	



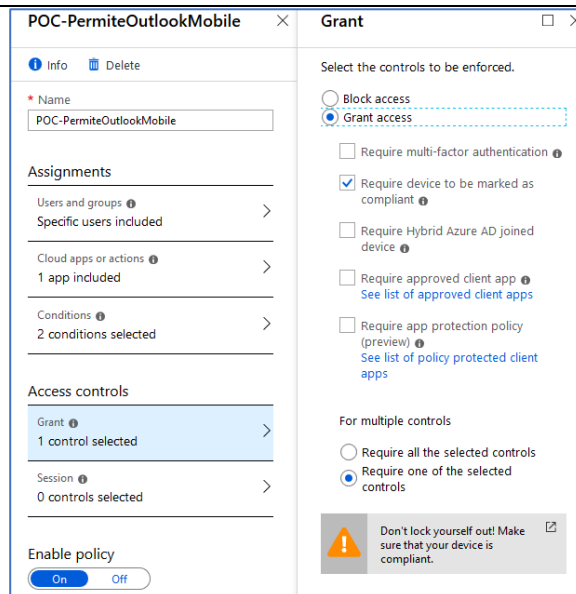
Na guia **Cloud Apps** selecione a opção **Office 365 Exchange Online**:



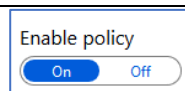
Na guia **Conditions > Client apps** selecione a opção **Configure** para **Yes** e selecione as opções **Browse, Modern Apps and desktop clients** e **Modern authentication clientes**:



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):



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 <b>Enable Policy:</b>	
--	--

**[C. Todos os passos/capturas de tela de configuração de sua aplicação.]**



**R:**

Todas as configurações da aplicação já foram detalhadas no item B.

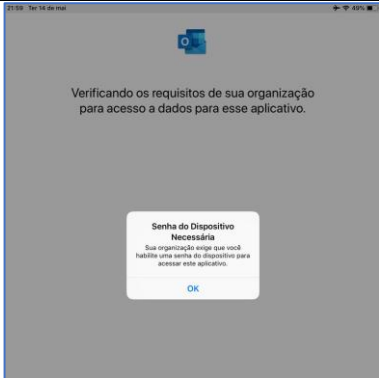
**[D. Uma captura de tela de sua aplicação em funcionamento..]**

**R:**

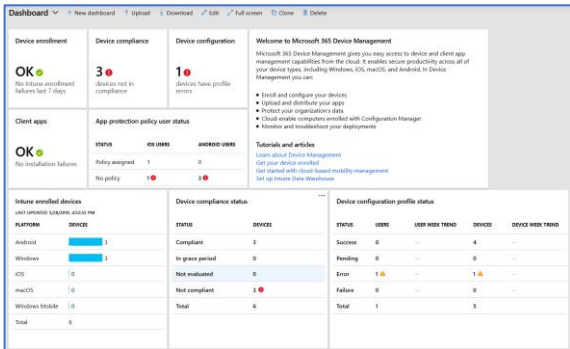
Abaixo as evidências sobre a solução de MDM (Mobile Device Management) funcionando sobre os dispositivos, acessando os recursos da empresa.

<p>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:</p>	
<p>Quando a política MAM é aplicada o usuário é notificado conforme imagem a seguir:</p>	

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.



STATUS	DEVICES
Compliant	3
In grace period	0
Not evaluated	0
Not compliant	1
Total	4

STATUS	USERS	USER WEEK TREND	DEVICES	DEVICE WEEK TREND
Success	0	---	4	---
Pending	0	---	0	---
Error	1	▲	1	▲
Failure	0	---	0	---
Total	1	---	5	---