Guia para implantar o VMware Workspace ONE com o VMware Identity Manager

SETEMBRO DE 2018

VMware Workspace ONE

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

O site da VMware também fornece as atualizações mais recentes de produtos.

Caso tenha comentários sobre esta documentação, envie seu feedback para:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Brasil
Rua Surubim, 504 4º andar CEP 04571-050
Cidade Monções
São Paulo
SÃO PAULO: 04571-050
Brasil
Tel: +55 11 55097200
Fax: + 55. 11. 5509-7224
www.vmware.com/br

Direitos autorais © 2017–2018 VMware, Inc. Todos os direitos reservados. Informações sobre direitos autorais e marca registrada.

Conteúdo

Sobre a implantação do VMware Workspace ONE

O Guia de implantação do VMware Workspace™ ONE™ com o VMware Identity Manager fornece informações sobre a integração do VMware Identity Manager™ e do VMware Workspace ONE UEM™ pela AirWatch para fornecer o Single Sign-On para o gerenciamento de dispositivos no Workspace ONE UEM e no VMware Workspace ONE como um catálogo de aplicativos.

Quando o Workspace ONE UEM e o VMware Identity Manager estão integrados, os usuários com dispositivos inscritos do Workspace ONE UEM podem fazer logon de forma segura nos seus aplicativos habilitados sem inserir várias senhas.

Público-alvo

Estas informações destinam-se a administradores que estejam familiarizados com os serviços do Workspace ONE UEM e do VMware Identity Manager.

A versão de setembro de 2018 se aplica à Nuvem do VMware Identity Manager de setembro de 2018, ao VMware Identity Manager 3.3 e ao Workspace ONE UEM 9.7.

Introdução ao Workspace ONE

1

O VMware Workspace® ONE® é uma plataforma empresarial segura que fornece e gerencia aplicativos em dispositivos iOS, Android e Windows 10. Identidade, aplicação e gerenciamento da mobilidade corporativa estão integrados na plataforma do Workspace ONE.

O VMware Workspace ONE UEM® e o VMware Identity Manager™ estão integrados para fornecer a você o catálogo de aplicativos do Workspace ONE e os serviços de gerenciamento de acesso móvel.

Os serviços do VMware Identity Manager fornecem os componentes relacionados à identidade, incluindo autenticação para os usuários que fazem logon único nos seus recursos. Você cria um conjunto de políticas relacionadas à rede e à autenticação para controlar o acesso a esses recursos.

Os serviços do Workspace ONE UEM fornecem ferramentas de inscrição do dispositivo, distribuição de aplicativos e verificação de conformidade para garantir o cumprimento dos padrões de segurança corporativos pelos dispositivos de acesso remoto. Os usuários dos dispositivos inscritos do Workspace ONE UEM podem fazer login de forma segura nos seus aplicativos habilitados sem inserir várias senhas.

Este capítulo inclui os seguintes tópicos:

Visão geral da arquitetura do Workspace ONE

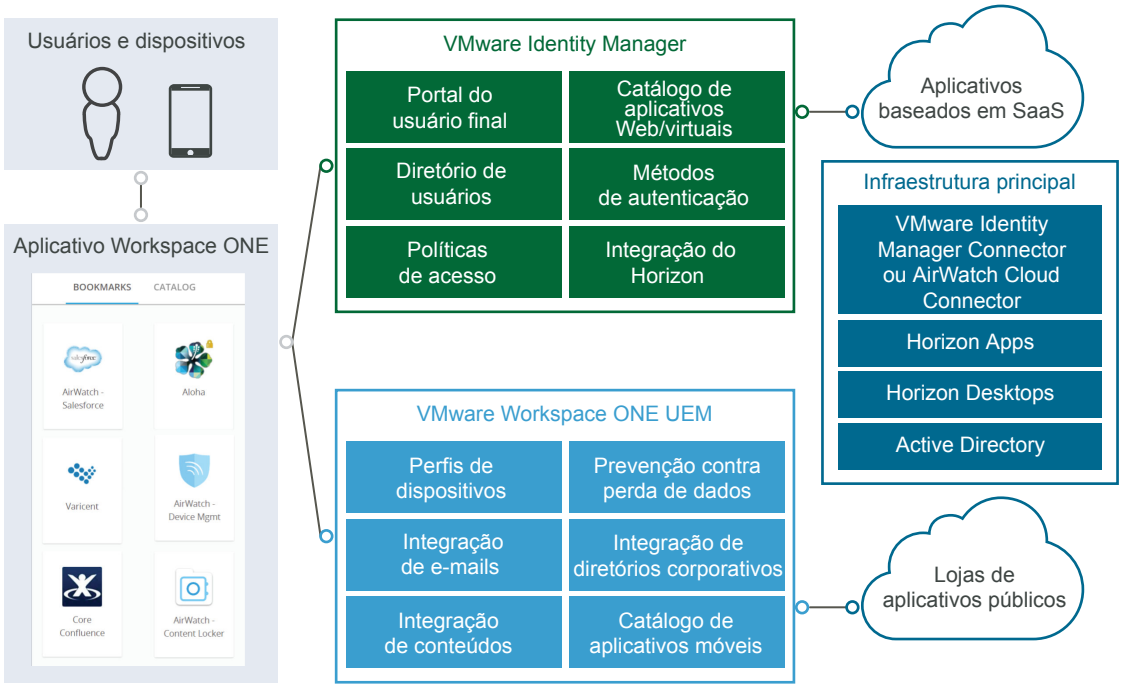
O Workspace ONE fornece aos usuários acesso seguro a aplicativos de nuvem, móveis e do Windows gerenciados de um catálogo unificado. Para acesso ao dispositivo, o aplicativo nativo do Workspace ONE está disponível para dispositivos iOS, Android e Windows 10.

Quando o Workspace ONE é implantado, os serviços a seguir do VMware Identity Manager e do Workspace ONE UEM devem ser implementados.

- Você pode configurar o componente do VMware Identity Manager Connector ou o componente do AirWatch Cloud Connector (ACC).
- Integração do Active Directory da sua empresa com o VMware Identity Manager ou com o Workspace ONE UEM Cloud Connector para sincronizar usuários e grupos do Active Directory ao serviço do Workspace ONE.

- Configure o VMware Identity Manager com as chaves da API do Workspace ONE UEM e com o certificado raiz do administrador, e habilite o Catálogo do Workspace ONE, a verificação de conformidade e a autenticação de senha do usuário por meio do Workspace ONE UEM.

Figura 1-1. Visão geral da arquitetura do Workspace ONE



Requisitos

Os requisitos de sistema do Workspace ONE estão listados abaixo.

Tabela 1-1. Requisitos de sistema do Workspace ONE

Requisitos do Workspace ONE	Detalhes
Active Directory	Windows Server 2008 e 2008 R2 Windows Server 2012 e 2012 R2
Navegador da Web para acesso aos consoles do VMware Identity Manager e do Workspace ONE	Internet Explorer 11 para Windows Google Chrome 4.0 e posterior Mozilla Firefox 40 e posterior Safari 6.2.8 e posterior
VMware Identity Manager Connector ou AirWatch Cloud Connector instalado.	Windows Server 2008 R2 Windows Server 2012 ou 2012 R2 .NET framework 4.6.2 Para obter o guia de instalação do Conector do VMware Identity Manager, consulte o Centro de documentação do VMware Identity Manager. Para obter o guia de instalação do AirWatch Cloud Connector, consulte o Centro de documentação do Workspace ONE UEM.

Detalhes do recurso do Workspace ONE

Os principais recursos do Workspace ONE são descritos abaixo.

Aplicativos Workspace ONE móveis nativos

Os usuários podem instalar o aplicativo Workspace ONE em um dispositivo móvel e usar credenciais corporativas para acesso de logon único (SSO) a aplicativos corporativos, de nuvem e móveis.

Catálogo de aplicativos de autoatendimento para recursos da Web, do Horizon e do Citrix

O Workspace ONE fornece aos usuários acesso a aplicativos de nuvem, móveis e do Windows usando um catálogo unificado. O catálogo contém aplicativos publicados para VMware Identity Manager e VMware Workspace ONE UEM. Os tipos de aplicativos com suporte incluem aplicativo Web interno, SaaS, móvel nativo, móvel desenvolvido internamente, legado e moderno do Windows, Horizon 7, VMware Horizon Cloud Service™, publicado no Citrix e pacotes do ThinApp. A loja de aplicativos também contém desktops virtualizados.

Inicializar aplicativos Web e virtuais com o Single Sign-On

O Workspace ONE fornece logon único (SSO) móvel e implementação de logon com um toque para aplicativos móveis. O SSO móvel está disponível para dispositivos Android, iOS e Windows 10.

Acesso condicional com conformidade do dispositivo

Com o Workspace ONE, você pode aplicar o acesso condicional com base no intervalo de rede, na plataforma e no critério específico do aplicativo para autenticação. Um dispositivo deve provar a conformidade com as regras de segurança antes de autorizar o acesso a um aplicativo. O VMware Identity Manager inclui uma opção de política de acesso que pode ser configurada para verificar no servidor do Workspace ONE UEM o status de conformidade do dispositivo quando os usuários fizerem login no dispositivo.

Autenticação multifator

O Workspace ONE fornece a autenticação multifator por meio do aplicativo VMware Verify. Quando um usuário tenta acessar o catálogo do Workspace ONE ou qualquer aplicativo que requer autenticação forte, o VMware Verify envia uma notificação para o telefone do usuário. Para verificar a tentativa de acesso ao Workspace ONE, o usuário deve tocar em Aceitar para acessar o aplicativo.

Gerenciamento adaptativo

Para aplicativos que exigem apenas um nível básico de segurança, os usuários não são obrigados a inscrever seu dispositivo no Workspace ONE UEM Mobile Device Management™. Os usuários podem baixar o aplicativo móvel Workspace ONE e selecionar os aplicativos que desejam instalar. Para aplicativos que exigem um nível de segurança maior, os usuários podem inscrever seu dispositivo no Workspace ONE UEM diretamente no aplicativo móvel Workspace ONE.

Como começar com o assistente do Workspace ONE

Você pode usar o assistente de Como começar do Workspace ONE para orientá-lo através de várias etapas de configuração para integrar o Workspace ONE UEM e os serviços do VMware Identity Manager para criar o ambiente do Workspace ONE.

O assistente de Como começar não substitui a capacidade de configurar ou editar qualquer configuração individual, mas automatiza significativamente a configuração inicial para a maioria dos clientes.

O assistente de Como começar do Workspace ONE pode ser usado para configurar o seguinte:

- Conector Empresarial e Diretório. O assistente conduz você através das etapas para configurar o VMware Enterprise System Connector e configurar a conexão do Active Directory do Workspace ONE UEM Cloud Connector para importar usuários e grupos do diretório da sua empresa. Consulte o Guia de Configuração Rápida do VMware Workspace ONE para ajudá-lo a configurar o Conector Empresarial.
- Detecção automática. Execute o assistente para registrar seu domínio de e-mail no serviço de detecção automática para que os usuários finais acessem com mais facilidade o portal de aplicativos pelo aplicativo Workspace ONE. Em seguida, os usuários finais podem inserir seu endereço de e-mail em vez da URL da organização.
- Catálogo do Workspace ONE. O assistente de catálogo do Workspace ONE conduz você através das etapas para configurar o catálogo do Workspace ONE. Você também pode usar a etapa de identidade visual personalizada do Workspace ONE para adicionar as informações da marca da empresa ao catálogo do Workspace ONE e ao aplicativo. Consulte o Guia de Configuração Rápida do VMware Workspace ONE para ajudá-lo a configurar o catálogo do Workspace ONE.
- Gerenciamento adaptativo. Configure o gerenciamento adaptativo para restringir determinados aplicativos, exigindo que um perfil seja instalado nos dispositivos do usuário. O perfil garante que os dados e os aplicativos corporativos podem ser removidos se necessário. Você também pode optar por exigir que os aplicativos públicos sejam gerenciados ou usados de forma independente, baixando-os manualmente da loja de aplicativos.

O assistente de Como começar pode alertá-lo se as configurações existentes potencialmente conflitantes já estiverem habilitadas no Workspace ONE UEM ou nos serviços do VMware Identity Manager. Se isso ocorrer, o assistente de Como começar conclui as etapas apenas parcialmente ou os recursos podem ser configurados manualmente. Use este guia para configurar manualmente os serviços do Workspace ONE UEM e VMware Identity Manager para Workspace ONE.

Integrando o Workspace ONE UEM ao VMware Identity Manager

2

Para configurar os serviços de gerenciamento de dispositivos móveis do Workspace ONE UEM para dispositivos com os serviços do VMware Identity Manager de gerenciamento de identidade e logon único para usuários, você deve integrar os serviços.

Quando o Workspace ONE UEM e o VMware Identity Manager estão integrados, os usuários dos dispositivos inscritos do Workspace ONE UEM podem fazer logon no Workspace ONE para acessar seus aplicativos habilitados de forma segura sem inserir várias senhas.

O assistente de Como começar o Workspace ONE pode guiá-lo através de muitas das etapas de configuração para integrar o Workspace ONE UEM e o VMware Identity Manager. Consulte o Guia de Configuração Rápida do VMware Workspace ONE para executar os assistentes do Workspace ONE.

Este capítulo inclui os seguintes tópicos:

Configurar a integração do console do Workspace ONE UEM

Para integrar com os serviços do VMware Identity Manager, defina essas configurações no console do Workspace ONE UEM.

- Chave de administrador da Rest API para comunicação com o serviço do VMware Identity Manager
- Chave da API de usuário inscrito no REST para autenticação de senha do AirWatch Cloud Connector criada no mesmo grupo organizacional onde o VMware Identity Manager está configurado.

- Conta de administrador da API para o VMware Identity Manager e o certificado de autenticação do administrador exportado do Workspace ONE UEM e adicionado às configurações do AirWatch no console do VMware Identity Manager.

Criar as chaves da REST API no Workspace ONE UEM

O acesso de API do administrador REST e o acesso dos usuários inscritos devem ser habilitados no console do Workspace ONE UEM para integrar o VMware Identity Manager ao Workspace ONE UEM. Quando você habilita o acesso à API, gera-se uma chave de API.

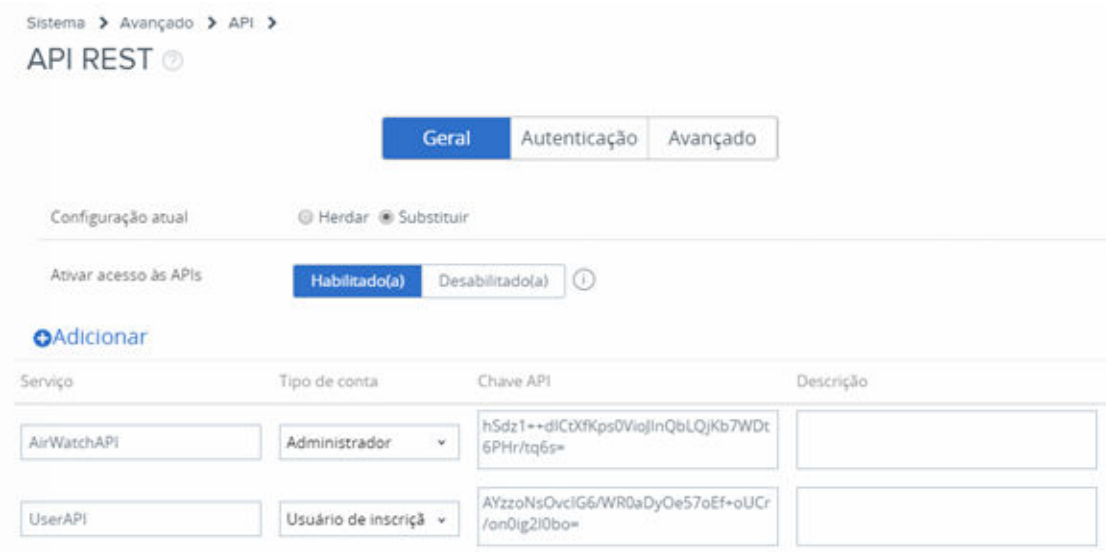
Procedimentos

1. No console do Workspace ONE UEM, selecione o Global > Grupo organizacional de nível de cliente e navegue para **Grupos e Configurações > Todas as Configurações > Sistema > Avançado > API > Rest API**.
2. Na guia Geral, clique em **Adicionar** para gerar a chave de API a ser usada no serviço do VMware Identity Manager. O tipo de conta deve ser **Administrador**.

   Forneça um nome de serviço exclusivo. Adicione uma descrição, como `API do AirWatch para IDM`.
3. Para gerar a chave de API do usuário de inscrição, clique em **Adicionar**.
4. No menu suspenso Tipo de Conta, selecione **Usuário de Inscrição**.

   Forneça um nome de serviço exclusivo. Adicione uma descrição, como `API do Usuário para IDM`.
5. Copie as duas chaves de API e as salve em um arquivo.

   Você adiciona essas chaves ao configurar o Workspace ONE UEM (AirWatch) no console do VMware Identity Manage.



6. Clique em **Salvar**.

Exportar o certificado-raiz de administrador do VMware Workspace ONE UEM

Após a criação da chave de API do administrador, adicione uma conta de administrador e configure uma autenticação de certificado no console do Workspace ONE UEM.

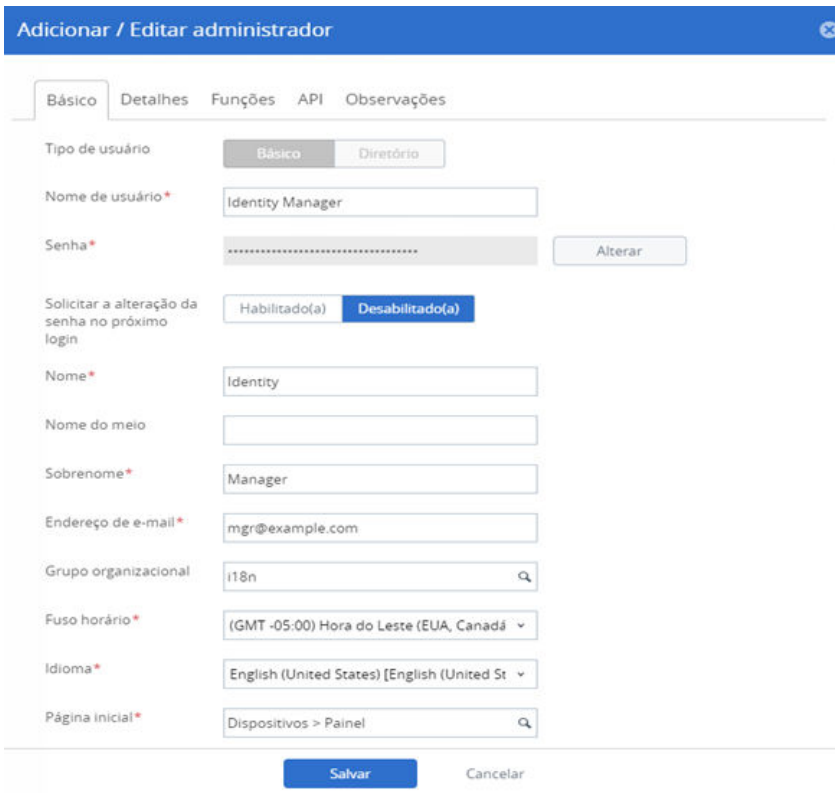
Para a autenticação baseada em certificado da REST API, gera-se um certificado de nível de usuário a partir do console do Workspace ONE UEM. O certificado usado é um certificado Workspace ONE UEM, autoassinado e gerado a partir do certificado-raiz de administrador do Workspace ONE UEM.

Pré-requisitos

A chave de API do administrador REST do Workspace ONE UEM é criada.

Procedimentos

1. No console do Workspace ONE UEM, selecione Global > Grupo organizacional a nível de cliente e navegue para **Contas > Administradores > Modo de Exibição de Lista**.
2. Clique em **Adicionar > Adicionar administrador**.
3. Na guia Básico, digite o nome de usuário e a senha do administrador do certificado nos devidos campos.



4. Selecione a guia Funções e escolha o grupo organizacional atual, clique no segundo campo e selecione **Administrador do AirWatch**.
5. Selecione a guia API e, no campo Autenticação, selecione **Certificados**.

6 Digite a senha do certificado. A senha é a mesma senha inserida para o administrador na guia Básico.

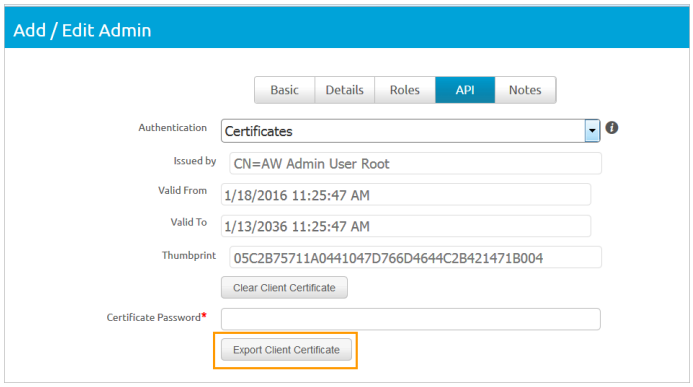
7 Clique em **Salvar**.

A nova conta de administrador e o certificado de cliente são criados.

8 Na página Visualização da lista, selecione o administrador que você criou e abra novamente a guia API.

A página de certificados exibe informações sobre o certificado.

9 Digite a senha definida no campo Senha do certificado, clique em **Exportar certificado do cliente** e salve o arquivo.



O certificado de cliente é salvo como um tipo de arquivo .p12.

Próximo passo

Defina suas configurações de URL do Workspace ONE UEM no console do VMware Identity Manager.

Configuração de uma instância do Workspace ONE UEM no VMware Identity Manager

Após definir as configurações no console do Workspace ONE UEM, na página Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, insira a URL do Workspace ONE UEM, os valores de chave de API e o certificado. Quando as configurações do Workspace ONE UEM estiverem definidas, você poderá habilitar as opções de recurso disponíveis para o Workspace ONE.

Adicionar configurações do Workspace ONE UEM ao VMware Identity Manager

Defina as configurações do Workspace ONE UEM no VMware Identity Manager para integrar o Workspace ONE UEM ao VMware Identity Manager e habilitar as opções de integração do recurso do Workspace ONE UEM. A chave de API do Workspace ONE UEM e o certificado são adicionados para a autorização do VMware Identity Manager com o Workspace ONE UEM.

Pré-requisitos

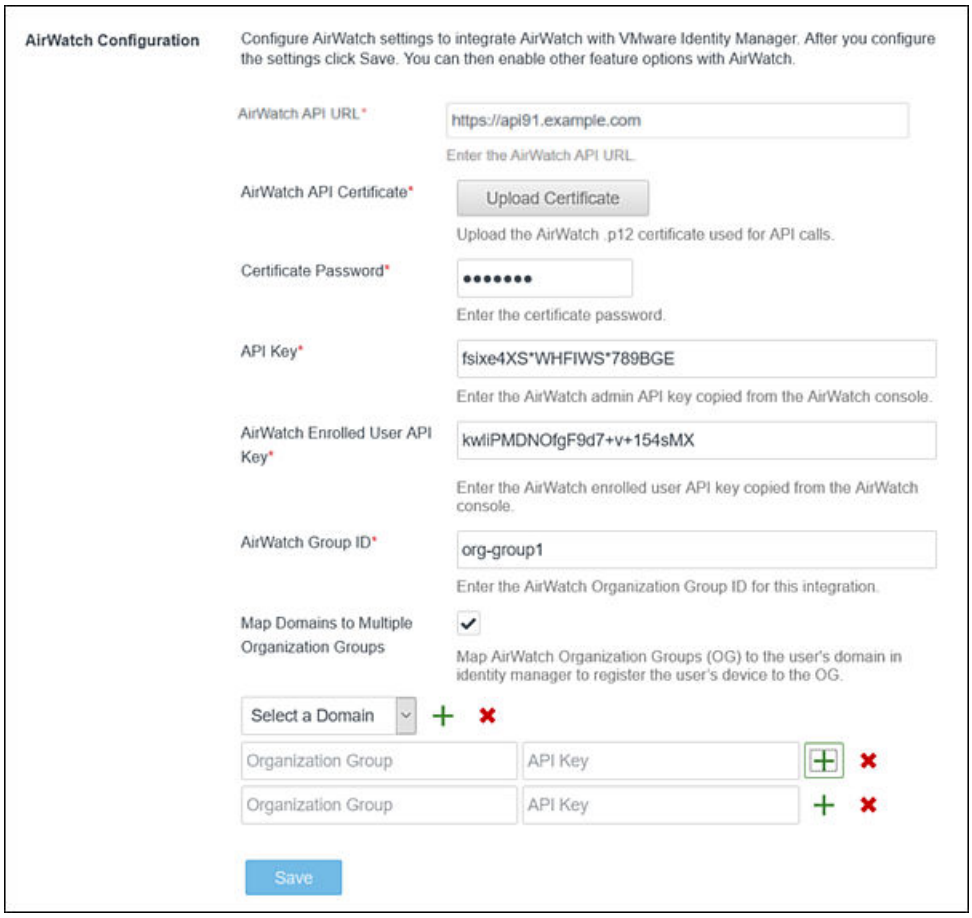
- A URL do servidor do Workspace ONE UEM que o administrador utiliza para fazer login no console do Workspace ONE UEM.
- A chave de API de administrador do Workspace ONE UEM que é usada para fazer solicitações de API do VMware Identity Manager para o servidor do Workspace ONE UEM, a fim de configurar a integração.
- O arquivo de certificado do Workspace ONE UEM usado para fazer chamadas API e a senha do certificado. O arquivo de certificado deve estar no formato de arquivo .p12.
- Chave de API de usuário inscrito do Workspace ONE UEM.
- A ID do grupo do Workspace ONE UEM para o seu inquilino, que é o identificador do tenant no Workspace ONE UEM.

Procedimentos

1. No console do VMware Identity Manager, guia Gerenciamento de Identidade e Acesso, clique em **Configuração > AirWatch**.
2. Insira as configurações de integração do Workspace ONE UEM nos seguintes campos.

Campo	Descrição
URL de API do AirWatch	Insira a URL do Workspace ONE UEM. Por exemplo, `https://myco.ws1uem.com`
Certificado de API do AirWatch	Faça upload do arquivo de certificado usado para fazer chamadas API.
Senha do Certificado	Digite a senha do certificado.
Chave de API do administrador do AirWatch	Digite o valor da chave de API do administrador. Exemplo de um valor de chave de API `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
Chave de API de usuário inscrito do AirWatch	Digite o valor da chave de API do usuário inscrito.
ID de Grupo do AirWatch.	Digite a ID de grupo do Workspace ONE UEM para o grupo organizacional em que a conta de administrador e a chave de API foram criados.

3 Clique em **Salvar**.



Próximo passo

Habilite a opção de recurso Catálogo do Workspace ONE para mesclar os aplicativos configurados com o catálogo do Workspace ONE UEM ao catálogo do Workspace ONE.

- Ativar a Verificação de Conformidade para verificar se os dispositivos gerenciados pelo Workspace ONE UEM obedecem às políticas de conformidade do Workspace ONE UEM.

Consulte Habilitando a verificação de conformidade para dispositivos gerenciados do Workspace ONE UEM.

Mapeando domínios do VMware Identity Manager para vários grupos organizacionais no Workspace ONE UEM

Ao configurar usuários e dispositivos no Workspace ONE UEM, o Workspace ONE UEM usa grupos organizacionais (GO) para organizar e agrupar usuários para estabelecer permissões. Quando o Workspace ONE UEM está integrado ao VMware Identity Manager, as chaves da REST API do usuário de inscrição e administrador podem somente ser configuradas no grupo organizacional do Workspace ONE UEM de tipo Cliente.

Nos ambientes do Workspace ONE UEM configurados para vários inquilinos, muitos grupos organizacionais são criados para usuários e dispositivos. Os dispositivos se tornam registrados ou inscritos em um grupo organizacional. Os grupos organizacionais podem ser definidos em configurações exclusivas em um ambiente de vários tenants. Por exemplo, grupos organizacionais por geografias, departamentos ou casos de uso separados.

Você pode vincular domínios configurados no VMware Identity Manager Identity Manager a grupos organizacionais específicos no Workspace ONE UEM para gerenciar o registro do dispositivo através do Workspace ONE. Quando os usuários fazem login no Workspace ONE, um evento de registro do dispositivo é acionado no VMware Identity Manager. Durante o registro do dispositivo, uma solicitação é enviada para que o Workspace ONE UEM efetue o pull de todos os aplicativos aos quais a combinação de usuário e dispositivo tem direito.

Os grupos organizacionais do dispositivo devem ser identificados quando o Workspace ONE UEM está integrado ao VMware Identity Manager para que o Identity Manager possa localizar o usuário e registrar com sucesso o dispositivo no grupo organizacional apropriado.

Ao definir as configurações do Workspace ONE UEM no serviço do VMware Identity Manager, você pode digitar IDs de grupos organizacionais de dispositivos e chaves da API para mapear vários GOs para um domínio. Quando os usuários fazem login no Workspace ONE dos seus dispositivos, os registros dos usuários são verificados e o dispositivo é registrado no grupo organizacional apropriado no Workspace ONE UEM.

Para saber mais sobre como configurar vários grupos organizacionais, consulte Estratégias de implantação para configurar vários grupos organizacionais do Workspace ONE UEM.

Observação Quando o Workspace ONE UEM estiver integrado ao VMware Identity Manager e vários grupos organizacionais do Workspace ONE UEM estiverem configurados, a opção de Catálogo Global do Active Directory não pode ser configurada para uso com o serviço do VMware Identity Manager.

Habilitar o catálogo do Workspace ONE para Workspace ONE UEM

Ao configurar o VMware Identity Manager com sua instância do Workspace ONE UEM, você pode ativar o Catálogo do Workspace ONE para incluir os aplicativos do Catálogo do Workspace ONE UEM. Os usuários finais veem no portal do Workspace ONE todos os aplicativos aos quais têm direito.

Procedimentos

1. No console do VMware Identity Manager, guia Gerenciamento de Identidade e Acesso, clique em **Configuração > AirWatch** e navegue até a seção Catálogo do Workspace ONE.
2. Para incluir aplicativos do AirWatch com aplicativos no catálogo do Identity Manager, ative **Obter do IDM** e **Obter do Airwatch**.

   Ao usar o Catálogo do Workspace ONE em dispositivos móveis sem o serviço do VMware Identity Manager configurado, selecione apenas **Obter do AirWatch**.

   O padrão é a opção **Obter do IDM** ativada.

3 Clique em **Salvar**.

Próximo passo

Notifique os usuários finais do Workspace ONE UEM sobre como acessar o catálogo e visualizar o portal do Workspace ONE.

Habilitando a verificação de conformidade para dispositivos gerenciados do Workspace ONE UEM

Quando os usuários inscrevem seus dispositivos, as amostras que contêm os dados utilizados para a avaliação de conformidade são enviadas com base em uma programação. A avaliação desses dados de amostra garante que o dispositivo respeite as regras de conformidade estabelecidas pelo administrador no console do Workspace ONE UEM (UEM). Se o dispositivo não estiver em conformidade com essas regras, serão tomadas as ações correspondentes configuradas no console do UEM.

O serviço do VMware Identity Manager inclui uma opção de políticas de acesso que pode ser configurada para verificar o servidor do Workspace ONE UEM para o status de conformidade do dispositivo quando os usuários fazem login no dispositivo. A verificação de conformidade garante que os usuários serão impedidos de fazer logon ou de usar o single sign-on no portal do Workspace ONE se o dispositivo não estiver em conformidade. Quando o dispositivo estiver em conformidade novamente, restaura-se a capacidade de login.

O aplicativo do Workspace ONE faz logoff e bloqueia automaticamente o acesso aos aplicativos se o dispositivo estiver comprometido. Se o dispositivo tiver sido inscrito através do gerenciamento adaptativo, um comando de limpeza de dados corporativos (enterprise wipe) emitido através do console do UEM cancelará a inscrição do dispositivo e removerá os aplicativos gerenciados do dispositivo. Os aplicativos não gerenciados não são removidos.

Para obter mais informações sobre as políticas de conformidade do Workspace ONE UEM, consulte o Guia de Gerenciamento de Dispositivos Móveis do VMware Workspace ONE UEM, nas páginas de Documentação do VMware Workspace ONE UEM.

Habilitar a autenticação de senha do usuário pelo Workspace ONE UEM

Para implementar a autenticação com o AirWatch Cloud Connector, você deve habilitar a autenticação de senha por meio do recurso do Workspace ONE UEM.

Pré-requisitos

- Workspace ONE UEM configurado no VMware Identity Manager.
- AirWatch Cloud Connector instalado e ativado.
- Serviços de diretório do Workspace ONE UEM integrados ao Active Directory.

Procedimentos

1 No console do VMware Identity Manager, guia Gerenciamento de Identidade e Acesso, clique em **Configuração > AirWatch**.

2 Na seção Autenticação de senha do usuário pelo AirWatch, selecione **Habilitar**.

3 Clique em **Salvar**.

Próximo passo

Consulte Implementando a autenticação com o AirWatch Cloud Connector para usar a autenticação do AirWatch Cloud Connector.

Configurar regras de verificação de conformidade

Após a habilitação da verificação de conformidade, crie uma regra de política de acesso que requer a verificação de conformidade de dispositivo e autenticação para os dispositivos gerenciados do Workspace ONE UEM.

A regra de política de verificação de conformidade funciona em uma cadeia de autenticação com o SSO móvel para iOS, SSO móvel para Android e implantação em nível do Certificado. Ao configurar a regra, o método de autenticação a ser usado deve preceder o método de conformidade do dispositivo.

Pré-requisitos

Métodos de autenticação configurados e associados a um provedor de identidade interno.

Verificação de conformidade habilitada na página do VMware Identity Manager AirWatch.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, selecione **Gerenciar > Políticas**.

2 Clique em **Editar Política Padrão**.

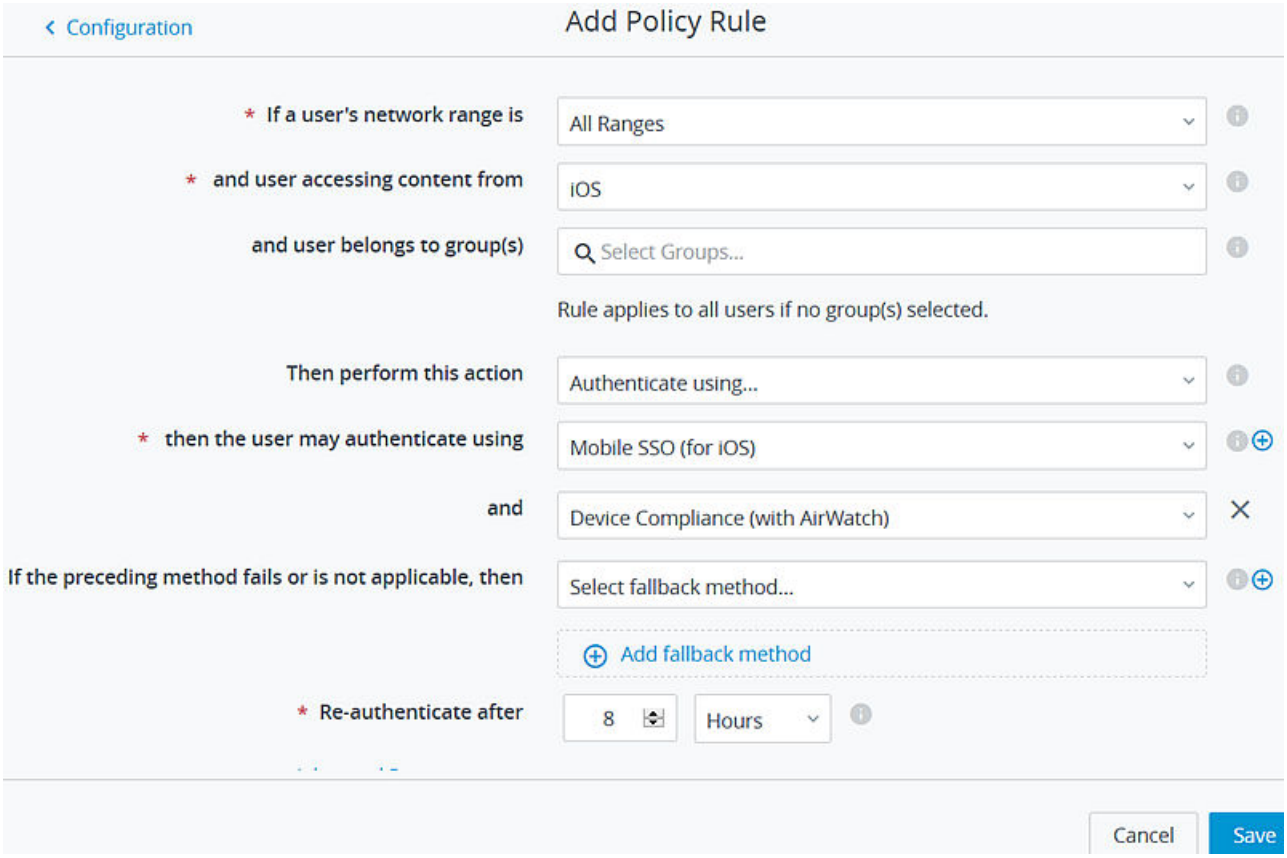
3 Clique em **Avançar**.

4 Clique em **Adicionar Regra de Política** para adicionar uma regra, ou selecione uma regra a ser editada.

Opção	Descrição
Caso um intervalo de rede de usuário seja	Verifique se o intervalo de rede está correto, se você adicionar uma regra, selecione o intervalo de rede.
e usuário acessando conteúdo de	Selecione o tipo de dispositivo móvel.
e o usuário pertence a grupos	Se essa regra de acesso for aplicada a grupos específicos, pesquise os grupos na caixa de pesquisa. Se não for selecionado nenhum grupo, a política de acesso se aplicará a todos os usuários.
Em seguida, execute esta ação	Selecione **Autenticar usando....**

Opção	Descrição
em seguida, o usuário pode autenticar usando	Selecione o método de autenticação de dispositivo móvel a ser aplicado. Clique em + e, no menu suspenso, selecione **Conformidade do Dispositivo (com AirWatch)**.
Se os métodos anteriores falharem ou não forem aplicáveis,	Configure o método de autenticação de fallback, se necessário.
Reautenticar após	Selecione a duração da sessão, após a qual os usuários deverão autenticar novamente.

5 Clique em **Salvar**.



Atualizando o VMware Identity Manager após a atualização do Workspace ONE UEM

Ao atualizar o Workspace ONE UEM para uma nova versão, você deve atualizar as opções de Catálogo do Workspace ONE e de Autenticação de Senha do Usuário na página de configuração da AirWatch no console do VMware Identity Manager.

Quando você salva essas opções após o upgrade do Workspace ONE UEM, as configurações do AirWatch no serviço do VMware Identity Manager são atualizadas com a nova versão do Workspace ONE UEM.

Procedimentos

1. Após a atualização do Workspace ONE UEM, faça login no console do VMware Identity Manager.
2. Na guia Gerenciamento de Identidade e Acesso, clique em **Configuração > AirWatch**.
3. Role a página para baixo até a seção **Catálogo do Workspace ONE** e clique em **Salvar**.
4. Role a página até a seção **Autenticação da senha de usuário por meio do AirWatch** e clique em **Salvar**.

A configuração do Workspace ONE UEM é atualizada com a nova versão no serviço do VMware Identity Manager.

Implementando a autenticação com o AirWatch Cloud Connector

O componente do AirWatch Cloud Connector (ACC) do VMware Enterprise Systems Connector está integrado ao VMware Identity Manager para autenticação de senha do usuário no Workspace ONE.

Observação Você instala o ACC e configura o componente do ACC no Workspace ONE UEM. Consulte no guia Instalação e configuração do VMware Enterprise Systems Connector as informações sobre como instalar e configurar o AirWatch Cloud Connector. Após a instalação e a configuração do ACC, integre os serviços de diretório do Workspace ONE UEM ao Active Directory. Consulte o Guia de Serviços de Diretório do VMware Workspace ONE UEM para obter informações sobre como habilitar os serviços de diretório.

Para implementar a autenticação do AirWatch Cloud Connector para o Workspace ONE, no console do VMware Identity Manager, o método de autenticação de Senha (Workspace ONE UEM Connector) é associado a um provedor de identidade integrado.

Você pode habilitar o suporte just-in-time no Workspace ONE UEM para adicionar novos usuários ao diretório do VMware Identity Manager quando os usuários fizerem logon pela primeira vez. Quando o suporte just-in-time estiver habilitado, os usuários não precisarão esperar pela próxima sincronização agendada do servidor do Workspace ONE UEM para acessar o Workspace ONE. Além disso, os novos usuários fazem logon no portal do Workspace ONE, de um dispositivo iOS ou Android ou de um computador desktop, e digitam o respectivo nome de usuário e senha do Active Directory. O serviço do VMware Identity Manager autentica as credenciais do Active Directory através do AirWatch Cloud Connector e adiciona o perfil do usuário ao diretório.

Depois de associar os métodos de autenticação no provedor de identidade interno, crie políticas de acesso a serem aplicadas a esse método de autenticação.

Observação A autenticação de nome de usuário e senha é integrada à implantação do AirWatch Cloud Connector. Para autenticar usuários usando outros métodos de autenticação com suporte pelo VMware Identity Manager, o conector do VMware Identity Manager deve ser configurado.

Gerenciando o mapeamento de atributos do usuário

Você pode configurar o mapeamento de atributos do usuário entre o diretório do Workspace ONE UEM e o diretório do VMware Identity Manager.

A página Atributos de Usuário na guia Gerenciamento de Identidade e Acesso do VMware Identity Manager, lista os atributos de diretório padrão que são mapeados para os atributos do Diretório do Workspace ONE UEM. Os atributos obrigatórios são marcados com um asterisco. Os usuários que deixarem algum atributo sem preencher em seu perfil não serão sincronizados com o serviço do VMware Identity Manager.

Tabela 2-1. Mapeamento padrão dos atributos do diretório do Workspace ONE UEM

Nome do atributo de usuário do VMware Identity Manager	Mapeamento padrão para o atributo de usuário do Workspace ONE UEM
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	Domínio
desativado (usuário externo desativado)	desabilitado
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
e-mail	Email*
userName	username*

Sincronizar usuários e grupos do diretório do Workspace ONE UEM para o VMware Identity Manager

Você pode definir as configurações do VMware Identity Manager no console do Workspace ONE UEM para estabelecer uma conexão entre sua instância do grupo organizacional do diretório do Workspace ONE UEM e VMware Identity Manager. Essa conexão é usada para sincronizar os usuários e os grupos com um diretório criado no serviço do VMware Identity Manager.

Usuários e grupos sincronizam inicialmente com o diretório do VMware Identity Manager manualmente. A agenda de sincronização do Workspace ONE UEM determina quando os usuários e os grupos são sincronizados com o diretório do VMware Identity Manager.

Quando um usuário ou um grupo é adicionado ou excluído no servidor do Workspace ONE UEM, a alteração tem reflexo imediato no serviço do VMware Identity Manager.

Pré-requisitos

- Nome de administrador local e senha do VMware Identity Manager.

- Identifique os valores do atributo para fazer o mapeamento a partir do diretório do Workspace ONE UEM. Consulte Gerenciando o mapeamento de atributos do usuário.

Procedimentos

1. No console do Workspace ONE UEM, página Grupos e Configurações, Todas as Configurações, selecione Global > Grupo organizacional de nível de cliente e navegue para **Sistema > Integração Empresarial** >**VMware Identity Manager**.
2. Na seção Servidor, clique em **Configurar**.

   Observação O botão de configuração só fica disponível quando os Serviços de diretório também estão configurados para o mesmo grupo organizacional. Se o botão Configurar não estiver visível, você não está no grupo organizacional correto. Você pode alterar o grupo organizacional no menu suspenso Global.

3. Insira as configurações do VMware Identity Manager.

Opção	Descrição
URL	Insira sua URL de tenant da VMware. Por exemplo, `https://myco.identitymanager.com`.
Nome de usuário de administrador	Insira o nome de usuário administrador local do VMware Identity Manager.
Senha de administrador	Insira a senha do usuário administrador local do VMware Identity Manager.

4. Clique em **Avançar**.
5. Habilite o mapeamento personalizado para configurar o mapeamento de atributos do usuário do Workspace ONE UEM para o serviço do VMware Identity Manager.
6. Clique em **Testar Conexão** para verificar se as configurações estão corretas.
7. Clique em **Sincronizar Agora** para sincronizar manualmente todos os usuários e grupos com o serviço do VMware Identity Manager.

   Observação Para se controlar a carga do sistema, a sincronização manual só pode ser realizada quatro horas após uma sincronização anterior.

Um diretório do Workspace ONE UEM é criado no serviço do VMware Identity Manager e os usuários e grupos são sincronizados com um diretório no VMware Identity Manager.

Próximo passo

Veja a guia Usuários e Grupos do console de administração do VMware Identity Manager para verificar se os nomes de usuário e grupo estão sincronizados.

Gerenciando a configuração de autenticação de senha para o Workspace ONE UEM

Você pode revisar e gerenciar a configuração de Senha (AirWatch Connector) que foi configurada quando você instalou o Workspace ONE UEM e adicionou o serviço do VMware Identity Manager.

O método de autenticação de Senha (AirWatch Connector) é gerenciado a partir da página Gerenciamento de Identidade e Acesso > Métodos de Autenticação e está associado ao provedor de identidade interno na página Provedores de Identidade.

Importante Quando o software do AirWatch Cloud Connector for atualizado, certifique-se de atualizar a configuração do Workspace ONE UEM na página do AirWatch do console do VMware Identity Manager.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, selecione **Métodos de Autenticação**.

2 Na coluna **Senha (AirWatch Connector)** Configurar, clique no ícone de lápis.

3 Verifique a configuração.

Opção	Descrição
Habilitar a autenticação de senha no AirWatch	Essa caixa de seleção permite a autenticação de senha no Workspace ONE UEM.
URL do console de administração do AirWatch	Preenchida automaticamente com a URL do Workspace ONE UEM.
Chave da API do AirWatch	Pré-preenchida com a chave da API de administrador do Workspace ONE UEM.
Certificado Usado para Autenticação	Pré-preenchida com o certificado do Workspace ONE UEM Cloud Connector.
Senha do Certificado	Preenchida automaticamente com a senha para o certificado do Workspace ONE UEM Cloud Connector.
ID de Grupo do AirWatch	Pré-preenchida com a ID do grupo organizacional.
Número de tentativas de autenticação permitidas	O número máximo de tentativas de login falhas durante o uso da senha no Workspace ONE UEM para autenticação. Não são permitidas mais tentativas de login após os logins com falha atingirem esse número. O serviço do VMware Identity Manager tentará usar o método de autenticação de fallback se ele estiver configurado. O padrão é de cinco tentativas.
JIT Ativado	Se o JIT não estiver habilitado, marque essa caixa de seleção para habilitar o provisionamento just-in-time dos usuários no serviço do VMware Identity Manager dinamicamente quando fizerem o login pela primeira vez.

4 Clique em **Salvar**.

Configurar os provedores de identidade integrados

Você pode configurar vários provedores de identidade incorporados e associar métodos de autenticação que foram configurados em Gerenciamento de Identidade e Acesso Gerenciar > Métodos de Autenticação.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso, vá a **Gerenciar > Provedores de Identidade**.

2 Clique em **Adicionar Provedor de Identidade** e selecione **Criar IDP Integrado**.

Opção	Descrição
Nome do provedor de identidade	Insira um nome para esta instância do provedor de identidade integrado.
Usuários	Selecione os usuários para autenticação. Os diretórios configurados são listados.
Rede	Os intervalos de rede existente configurados no serviço são listados. Selecione os intervalos de rede para os usuários com base nos endereços IP que você deseja direcionar a essa instância do provedor de identidade para autenticação.
Métodos de autenticação	Os métodos de autenticação configurados no serviço são exibidos. Marque a caixa de seleção dos métodos de autenticação a serem associados a esse provedor de identidade integrado. Para Conformidade do Dispositivo (com o Workspace ONE UEM) e Senha (AirWatch Connector), certifique-se de que a opção esteja habilitada na página de configuração do AirWatch.

3 Clique em **Adicionar**.

Próximo passo

Configure a regra de políticas de acesso padrão para adicionar a política de autenticação à regra. Consulte Configurar regras de verificação de conformidade

Implementando a autenticação do Single Sign-On móvel para dispositivos iOS gerenciados pelo Workspace ONE UEM

3

Para a autenticação de dispositivo iOS, o VMware Identity Manager usa um provedor de identidade integrado ao serviço do VMware Identity Manager para fornecer acesso à autenticação do SSO móvel.

Esse método de autenticação para dispositivos iOS usa um Centro de Distribuição de Chave (KDC) sem o uso de um conector ou de um sistema de terceiros. A autenticação Kerberos fornece aos usuários, que fizeram logon com sucesso no domínio, acesso ao portal de aplicativos do Workspace ONE sem avisos de credenciais adicionais.

Este capítulo inclui os seguintes tópicos:

Visão geral da implementação para configurar o SSO móvel para iOS

A implementação da autenticação do SSO móvel para dispositivos iOS 9 ou posteriores gerenciados pelo Workspace ONE UEM requer as seguintes etapas de configuração.

- Faça download do certificado do emissor para configurar o SSO móvel para iOS
  - Se você estiver usando os Active Directory Certificate Services, configure um modelo de autoridade de certificação para a distribuição de certificado Kerberos nos Active Directory Certificate Services. Em seguida, configure o Workspace ONE UEM para usar a autoridade de certificação do Active Directory. Adicione o modelo de certificado ao console do Workspace ONE UEM. Faça download do certificado do emissor para configurar o SSO móvel para iOS.
  - Se você estiver usando a autoridade de certificação do Workspace ONE UEM, habilite Certificados na página Integrações do VMware Identity Manager. Faça download do certificado do emissor para configurar o SSO móvel para iOS.
- Estabeleça o Centro de Distribuição de Chave (KDC) a ser usado.
- Configure o perfil do dispositivo iOS e habilite o single sign-on a partir do console do Workspace ONE UEM.
- Configurar o método de autenticação SSO Móvel para iOS
- Configure o provedor de identidade integrado e associe a autenticação do SSO móvel para iOS no console do VMware Identity Manager.

Configurar a autoridade de certificação do Active Directory no Workspace ONE UEM

Para configurar a autenticação de single sign-on para os dispositivos móveis iOS 9 gerenciados do Workspace ONE UEM, você pode configurar uma relação de confiança entre o Active Directory e o Workspace ONE UEM, bem como habilitar o método de autenticação SSO móvel para iOS no VMware Identity Manager.

Depois de configurar a autoridade de certificação e o modelo de certificado para a distribuição de certificado Kerberos nos Active Directory Certificate Services, habilite o Workspace ONE UEM à solicitação do certificado usado para a autenticação e adicione a autoridade de certificação ao console do Workspace ONE UEM.

Procedimentos

1. No menu principal do console do Workspace ONE UEM, navegue para **Dispositivos > Certificados > Autoridades de Certificação**.
2. Clique em **Adicionar**.

3 Configure o seguinte na página Autoridade de Certificação.

Observação Certifique-se de que o Microsoft AD CS está selecionado como o Tipo de Autoridade antes de começar a preencher esse formulário.

Opção	Descrição
Nome	Digite um nome para a nova Autoridade de Certificação.
Tipo de Autoridade	Garanta que a opção **Microsoft ADCS** esteja selecionada.
Protocolo	Selecione **ADCS** como o protocolo.
Nome do Host do Servidor	Insira a URL do servidor. Insira o nome do host neste formato `https://{servername.com}/certsrv.adcs/`. O site pode ser http ou https, dependendo de como está configurado. A URL deve incluir `/` à direita. **Observação** Se a conexão falhar ao testar a URL, remova http:// ou https:// do endereço e teste a conexão novamente.
Nome da Autoridade	Digite o nome da autoridade de certificação à qual o endpoint do ADCS está conectado. Esse nome pode ser encontrado por meio da inicialização do aplicativo da Autoridade de Certificação no servidor da autoridade de certificação.
Autenticação	Garanta que a opção **Conta do Serviço** esteja selecionada.
Usuário e senha	Digite o nome de usuário e a senha da conta de administrador do AD CS com acesso suficiente para permitir que o Workspace ONE UEM solicite e emita certificados.

4 Clique em **Salvar**.

Próximo passo

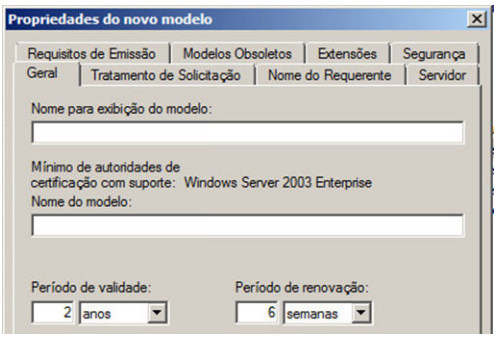
Configure o modelo de certificado no Workspace ONE UEM.

Configurando o Workspace ONE UEM para usar a autoridade de certificação do Active Directory

Seu modelo de autoridade de certificação deve ser devidamente configurado para a distribuição de certificado Kerberos. Nos Active Directory Certificate Services (AD CS), você pode duplicar o modelo existente de autenticação Kerberos para configurar um novo modelo de autoridade de certificação para a autenticação Kerberos para iOS.

Quando você duplica o modelo de autenticação Kerberos a partir do AD CS, é necessário configurar as seguintes informações na caixa de diálogo Propriedades do Novo Modelo.

Figura 3-1. Propriedades dos Certificate Services do Active Directory da caixa de diálogo Novo Modelo



- Guia **Geral**. Digite o nome de exibição e o nome do modelo. Por exemplo, iOSKerberos. Esse é o nome de exibição mostrado nos snap-ins Modelos de Certificado, Certificados e Autoridade de Certificação.
- Guia **Tratamento de Solicitação** . Habilite **Permitir que a chave privada seja exportada**.
- Guia **Nome da Entidade**. Selecione o botão de opções **Fornecer na solicitação**. O nome da entidade é fornecido pelo Workspace ONE UEM quando o Workspace ONE UEM solicita o certificado.
- Guia **Extensões**. Defina as políticas de aplicativo.
  - Selecione Políticas de Aplicativos e clique em Editar para adicionar uma nova política de aplicativos. Nomeie esta política como Autenticação de cliente Kerberos.
  - Adicione o identificador de objeto (OID) da seguinte maneira: 1.3.6.1.5.2.3.4. Não altere.
  - Na lista Descrição das políticas de aplicativo, exclua todas as políticas listadas, exceto a política de Autenticação de cliente Kerberos e a política de Autenticação por cartão inteligente.
- Guia **Segurança**. Adicione a conta Workspace ONE UEM à lista de usuários que podem usar o certificado. Defina as permissões para a conta. Escolha Controle Total para permitir que a entidade de segurança modifique todos os atributos de um modelo de certificado, incluindo as permissões para o modelo de certificado. Caso contrário, defina as permissões de acordo com os requisitos da organização.

Salve as alterações. Adicione o modelo à lista de modelos utilizados pelo Autoridade de certificação do Active Directory.

No Workspace ONE UEM, configure a autoridade de certificação e adicione o modelo de certificado.

Adicionar um modelo de certificado no Workspace ONE UEM

Você adiciona o modelo de certificado que associa a autoridade de certificação usada para gerar a certificação de usuário.

Pré-requisitos

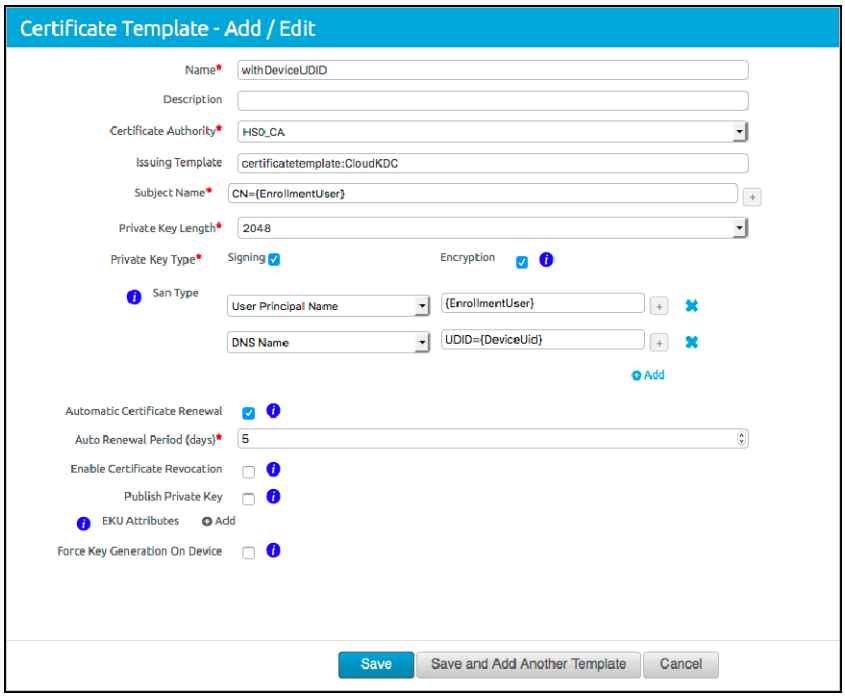
Configure a autoridade de certificação no Workspace ONE UEM.

Procedimentos

1. No console do Workspace ONE UEM, navegue para **Sistema > Integração Empresarial > Autoridades de Certificação**.
2. Selecione a guia **Modelo de Solicitação** e clique em **Adicionar**.
3. Configure o seguinte na página de modelo de certificado.

Opção	Descrição
Nome	Digite o nome do novo modelo de solicitação no Workspace ONE UEM.
Autoridade de certificação	No menu suspenso, selecione a autoridade de certificação que foi criada.
Emitindo o modelo	Digite o nome do modelo de certificado para o Microsoft CA conforme você criou no AD CS. Por exemplo, **`iOSKerberos`**.
Nome da Entidade	Insira o nome da Entidade para o modelo. Você pode clicar em + para selecionar um valor de pesquisa na lista. Certifique-se de que o valor seja inserido após **CN=** na caixa de texto. Se você selecionar o tipo de pesquisa DeviceUid, insira dois pontos (:) após o valor e selecione o valor de pesquisa na lista. Por exemplo, **CN={DeviceUid}:{lookupvalue}**, onde a caixa de texto {} é o valor de pesquisa do Workspace ONE UEM. Certifique-se de incluir os dois pontos (:). O texto inserido nessa caixa de texto é a Entidade do certificado, que pode ser usada para determinar quem ou qual dispositivo recebeu o certificado.
Comprimento da chave privada	Esse comprimento da chave privada corresponde à configuração do modelo de certificado que está sendo usado pelo AD CS. Normalmente corresponde a 2048.
Tipo de chave privada	Marque as caixas de seleção para **Assinatura** e **Criptografia**.
Tipo de SAN	Clique em **+Adicionar**. Para o Nome alternativo da entidade, selecione **Nome Principal do Usuário**. O valor deve ser **`{EnrollmentUser}`**. Quando a verificação de conformidade do dispositivo estiver configurada com a autenticação Kerberos, se você não tiver configurado o DeviceUid como o valor de pesquisa do Nome da Entidade, adicione um segundo tipo de SAN para incluir o identificador exclusivo do dispositivo (UDID). Selecione o tipo de SAN **Nome do DNS**. O valor deve ser **UDID={DeviceUid}**.
Renovação automática de certificado	Marque a caixa de seleção para ter certificados que usam esse modelo automaticamente renovado antes da data de expiração.
Período de autorrenovação (dias)	Especifique a autorrenovação em dias.
Habilitar a revogação do certificado	Marque a caixa de seleção para ter certificados revogados automaticamente quando os dispositivos aplicáveis são cancelados ou excluídos, ou se o perfil aplicável for removido.
Publicar chave privada	Marque esta caixa de seleção para publicar a chave privada.
Destino da chave privada	Serviço de diretório ou serviço da Web personalizado

4 Clique em **Salvar**.



Próximo passo

No console do VMware Identity Provider, configure o provedor de identidade integrado com o método de autenticação SSO móvel para iOS.

Usando a Autoridade de Certificação do Workspace ONE UEM para a Autenticação Kerberos

Você pode usar a Autoridade de Certificação do Workspace ONE UEM em vez da Autoridade de Certificação do Active Directory para configurar o single sign-on com a autenticação Kerberos incorporada para dispositivos móveis do iOS 9 gerenciados do Workspace ONE UEM. Você pode habilitar a Autoridade de Certificação do Workspace ONE UEM no console do Workspace ONE UEM e exportar o certificado do emissor da Autoridade de Certificação para uso no serviço do VMware Identity Manager.

A Autoridade de Certificação do Workspace ONE UEM foi criada para seguir o SCEP (Simple Certificate Enrollment Protocol - Protocolo de Inscrição de Certificado Simples) e é usada com dispositivos gerenciados do Workspace ONE UEM que suportam o SCEP. A integração do VMware Identity Manager com o Workspace ONE UEM usa a Autoridade de Certificação do Workspace ONE UEM para emitir certificados para dispositivos móveis do iOS 9 como parte do perfil.

O certificado-raiz do emissor da Autoridade de Certificação do Workspace ONE UEM também é o certificado de autenticação do OCSP.

Habilitar e exportar a autoridade de certificação do Workspace ONE UEM

Quando o VMware Identity Manager estiver habilitado no Workspace ONE UEM, você poderá gerar o certificado raiz do emissor do Workspace ONE UEM e exportar o certificado para uso com a autenticação do SSO móvel para iOS em dispositivos móveis iOS 9 gerenciados.

Procedimentos

1. No console do Workspace ONE UEM, navegue até **Sistema > Integração Empresarial** > **VMware Identity Manager**.

   Para habilitar a Autoridade de Certificação do Workspace ONE UEM, o tipo de grupo organizacional deve ser Cliente.

Dica Para visualizar ou alterar o tipo de grupo, navegue para Grupos e Configurações, **Grupos > Grupos Organizacionais**> **Detalhes do Grupo Organizacional**.

2. Clique em **Configuração**.
3. Na seção CERTIFICADO, clique em **Habilitar**.

   A página exibe os detalhes do certificado raiz do emissor.
4. Clique em **Exportar** e salve o arquivo.

Próximo passo

No console de administração do VMware Identity Manager, configure a autenticação Kerberos no provedor de identidade integrado e adicione o certificado do emissor de autoridade de certificação.

Usando um Centro de Distribuição de Chave para autenticação de dispositivos iOS

Para dispositivos iOS, você integra o serviço ao Kerberos. A autenticação Kerberos fornece aos usuários, que fizeram logon com sucesso no domínio, acesso ao portal de aplicativos sem avisos de credenciais adicionais. Esse método de autenticação para dispositivos iOS usa um Centro de Distribuição de Chave (KDC) sem o uso de um conector ou de um sistema de terceiros.

Os tenants da Nuvem do VMware Identity Manager não precisam gerenciar ou configurar o KDC.

Para implantações no local, duas opções de serviço do KDC estão disponíveis.

- KDC integrado. O KDC interno requer a inicialização do KDC no serviço e a criação de entradas DNS públicas para permitir que os clientes Kerberos encontrem o KDC. Para obter mais informações sobre como habilitar o KDC integrado, consulte o guia de Administração do VMware Identity Manager.

- KDC como um serviço hospedado na nuvem do VMware Identity Manager. O uso do KDC na nuvem requer a seleção do nome de território apropriado na página do adaptador de autenticação iOS.

Observação Quando o VMware Identity Manager está instalado e configurado com o Workspace ONE UEM em um ambiente do Windows, o método de autenticação de iOS móvel deve ser configurado para usar o serviço do KDC hospedado na nuvem do VMware Identity Manager.

Usando o serviço do KDC hospedado na nuvem

A fim de oferecer suporte ao uso da autenticação Kerberos para SSO Móvel para iOS, o VMware Identity Manager fornece um serviço do KDC hospedado na nuvem.

O serviço do KDC hospedado na nuvem deve ser usado quando o serviço do VMware Identity Manager for implantado com o Workspace ONE UEM em um ambiente do Windows.

Para usar o KDC gerenciado no appliance do VMware Identity Manager, consulte o tópico Preparando-se para usar a autenticação Kerberos em dispositivos iOS no *Guia de instalação e configuração do VMware Identity Manager*.

Ao configurar a autenticação SSO móvel para iOS, você configura o nome do território para o serviço do KDC hospedado na nuvem. O território é o nome da entidade administrativa que mantém os dados de autenticação. Quando você clica em Salvar, o serviço do VMware Identity Manager é registrado no serviço do KDC hospedado na nuvem. Os dados armazenados no serviço do KDC baseiam-se na sua configuração do método de autenticação SSO móvel para iOS, que inclui o certificado da CA, o certificado de assinatura OCSP e as informações da configuração da solicitação OCSP.

Os registros de log são armazenados no serviço de nuvem. As informações de identificação pessoal (PII) nos registros de log incluem o nome principal do Kerberos a partir do perfil do usuário, os valores de SAN de e-mail e UPN e DN de sujeito, a ID de dispositivo do certificado do usuário e o FQDN do serviço IDM que o usuário está acessando.

Para usar o serviço do KDC hospedado na nuvem, o VMware Identity Manager deve ser configurado da seguinte maneira.

- O FQDN do serviço do VMware Identity Manager deve ser acessível pela Internet. O certificado SSL/TLS usado pelo VMware Identity Manager deve ser assinado publicamente.
- Uma porta 88 (UDP) e uma porta 443 (HTTPS/TCP) de solicitação/resposta de saída devem estar acessíveis a partir do serviço do VMware Identity Manager.
- Se você habilitar o OCSP, o respondedor OCSP deverá ser acessível pela Internet.

Configurar autenticação do SSO móvel para iOS

Você configura o método de autenticação SSO móvel para iOS na página Métodos de Autenticação no console do VMware Identity Manager. Selecione o método de autenticação SSO móvel (para iOS) no provedor de identidade integrado.

Pré-requisitos

- Arquivo PEM e DER da autoridade de certificação usado para emitir certificados para os usuários no tenant do Workspace ONE UEM.
- Para a verificação de revogação, o certificado de autenticação do respondente do OCSP.
- Para o serviço do KDC, selecione o nome do território do serviço do KDC. Se você estiver usando o serviço do KDC incorporado, o KDC deverá ser inicializado. Consulte Instalando e configurando o VMware Identity Manager para obter os detalhes do KDC integrado.

Procedimentos

1. Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, vá para **Gerenciar > Métodos de Autenticação**.
2. Na coluna Configurar para **SSO Móvel (para iOS)**, clique no ícone de lápis.
3. Configure o método de autenticação Kerberos.

Opção	Descrição
Habilitar Autenticação KDC	Marque essa caixa de seleção para permitir que os usuários façam login usando dispositivos iOS que suportam a autenticação Kerberos.
Território	Para as implantações de tenant na nuvem, o valor do território é somente leitura. O nome do território exibido é o nome do território do Identity Manager para seu tenant. Em implantações locais, se você estiver usando o KDC hospedado na nuvem, insira o nome de território compatível predefinido que foi fornecido a você. O texto desse parâmetro deve ser inserido em letras maiúsculas. Por exemplo, OP.VMWAREIDENTITY.COM. Se você estiver usando o KDC integrado, aparecerá o nome de território que você configurou quando inicializou o KDC.
Certificados de autoridade de certificação intermediária e raiz	Faça upload do arquivo de certificado do emissor da autoridade de certificação. O formato de arquivo pode ser PEM ou DER.
DNs da Entidade de Certificação CA Carregados	O conteúdo do arquivo de certificado carregado aparece aqui. É possível carregar mais de um arquivo, e quaisquer certificados incluídos serão adicionados à lista.
Habilitar OCSP	Marque a caixa de seleção para usar o protocolo de validação de certificado do Protocolo de status de certificado online (OCSP) para obter o status de revogação de um certificado.
Enviar nonce do OCSP	Marque essa caixa de seleção se você desejar que o identificador único da solicitação de OCSP seja enviado na resposta.
Certificado de autenticação do respondente do OCSP	Faça upload do certificado do OCSP para o respondente. Quando você estiver usando a autoridade de certificação do Workspace ONE UEM, o certificado do emissor é usado como o certificado OCSP. Carregue o certificado do Workspace ONE UEM aqui também.
DN da entidade do certificado de autenticação do respondente do OCSP	O arquivo de certificado OCSP carregado está listado aqui.
Mensagem de Cancelamento	Crie uma mensagem de login personalizada que aparece quando a autenticação está demorando muito. Se você não criar uma mensagem personalizada, a mensagem padrão é `Attempting to authenticate your credentials`.

Opção	Descrição
Habilitar Link de Cancelamento	Quando a autenticação está demorando muito, dê aos usuários a capacidade de clicar em Cancelar para interromper a tentativa de autenticação e cancelar o login. Quando o link Cancelar estiver ativado, aparecerá a palavra Cancelar no fim da mensagem de erro de autenticação exibida.
URL do Servidor de Gerenciamento de Dispositivo Corporativo	Insira a URL do servidor de Gerenciamento de Dispositivos Móveis (MDM) para redirecionar os usuários quando o acesso é negado porque o dispositivo não está inscrito no Workspace ONE UEM para o gerenciamento de MDM. Essa URL é exibida na mensagem de erro de falha de autenticação. Se você não inserir uma URL aqui, será exibida a mensagem de Acesso Negado genérica.

4 Clique em **Salvar**.

Próximo passo

- Associe o método de autenticação de SSO móvel (para iOS) no provedor de identidade integrado.

Configurar o provedor de identidade integrado para autenticação do SSO móvel para iOS

Configure o provedor de identidade integrado e associe o método de autenticação do SSO móvel para iOS que foi configurado na página Gerenciamento de Identidade e Acesso > Gerenciar > Métodos de Autenticação.

Pré-requisitos

Autenticação do SSO móvel (para iOS) configurada na página Métodos de Autenticação.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso, vá a **Gerenciar > Provedores de Identidade**.

2 Clique em **Adicionar Provedor de Identidade** e selecione **Criar IDP Integrado**.

Opção	Descrição
Nome do provedor de identidade	Insira um nome para esta instância do provedor de identidade integrado.
Usuários	Selecione os usuários para autenticação. Os diretórios configurados são listados.
Rede	Os intervalos de rede existente configurados no serviço são listados. Selecione os intervalos de rede para os usuários com base nos endereços IP que você deseja direcionar a essa instância do provedor de identidade para autenticação.
Métodos de autenticação	Os métodos de autenticação configurados no serviço são exibidos. Marque a caixa de seleção dos métodos de autenticação de iOS a serem associados a esse provedor de identidade integrado. Adicione outros métodos de autenticação. Para Conformidade do Dispositivo (com o Workspace ONE UEM) e Senha (Workspace ONE UEM Connector), certifique-se de que a opção esteja ativada na página de configuração do Workspace ONE UEM.

3 Na seção Exportação de Certificado KDC, clique em **Baixar Certificado**. Salve esse certificado em um arquivo que pode ser acessado do console do Workspace ONE UEM.

   Você carrega esse certificado ao configurar o perfil do dispositivo iOS no Workspace ONE UEM.

4 Clique em **Adicionar**.

Próximo passo

- Configure a regra de política de acesso padrão para a autenticação Kerberos para dispositivos iOS. Certifique-se de que esse método de autenticação seja o primeiro método criado na regra.
- Vá ao console do Workspace ONE UEM, configure o perfil do dispositivo iOS no Workspace ONE UEM e adicione o certificado do emissor do certificado do servidor KDC a partir do VMware Identity Manager.

Configurar o perfil iOS da Apple no Workspace ONE UEM usando o modelo de certificado e a autoridade de certificação do Active Directory

Crie e implante o perfil do dispositivo iOS da Apple no Workspace ONE UEM para enviar por push as configurações do Provedor de Identidade ao dispositivo. Esse perfil contém as informações necessárias para o dispositivo conectar-se ao VMware Identity Provider e ao certificado que o dispositivo usou para a autenticação. Habilite o single sign-on para permitir acesso contínuo sem a necessidade de autenticação em cada aplicativo.

Pré-requisitos

- O SSO móvel para iOS está configurado no VMware Identity Manager.
- O arquivo da autoridade de certificação Kerberos de iOS salvo em um computador que pode ser acessado do console de administração do Workspace ONE UEM.
- Seu modelo de certificado e autoridade de certificação estão devidamente configurados no Workspace ONE UEM.
- Lista de URLs e IDs de pacote de aplicativos que usam o SSO móvel para a autenticação de iOS em dispositivos iOS.

Procedimentos

1 No console do Workspace ONE UEM, navegue para **Dispositivos > Perfis e Recursos > Perfis** .

2 Selecione **Adicionar > Adicionar Perfil** e selecione **Apple iOS**.

3 Insira o nome como **`iOSKerberos`** e defina as configurações **Geral**.

4 No painel de navegação à esquerda, selecione **Credenciais > Configurar** para configurar a credencial.

Opção	Descrição
Origem da Credencial	Selecione **Autoridade de Certificação Definida** no menu suspenso.
Autoridade de certificação	Selecione a autoridade de certificação da lista no menu suspenso.
Modelo de Certificado	Selecione o modelo de solicitação que faz referência à autoridade de certificação a partir do menu suspenso. Esse é o modelo de certificado criado em Adicionando o modelo de certificado no Workspace ONE UEM.

5 Clique em **+** no canto inferior direito da página novamente e crie uma segunda credencial.

6 No menu suspenso **Origem da Credencial**, selecione **Carregar**.

7 Insira um nome de credencial.

8 Clique em **Carregar** para fazer upload do certificado raiz do servidor KDC baixado da página Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidades > Provedor de Identidade Integrado.

9 No painel de navegação à esquerda, selecione **Single Sign-On** e clique em **Configuração**.

10 Insira informações de conexão.

Opção	Descrição
Nome da Conta	Insira `Kerberos`.
Nome Principal do Kerberos	Clique em **+** e selecione **{EnrollmentUser}**.
Território	Para implantações de tenant na nuvem, insira o nome do território do Identity Manager do seu tenant. O texto desse parâmetro deve estar em letras maiúsculas Por exemplo, `VMWAREIDENTITY.COM`. Nas implantações locais, insira o nome do território que você usou quando inicializou o KDC no appliance do VMware Identity Manager. Por exemplo, `EXEMPLO.COM`
Certificado de Renovação	Selecione **Certificate#1** no menu suspenso. Esse é o certificado da autoridade de certificação do Active Directory que foi configurado primeiro com credenciais.
Prefixos de URL	Insira os prefixos de URL que devem corresponder para se usar essa conta para a autenticação Kerberos por HTTP. Para implantações de tenant na nuvem, insira a URL do servidor do VMware Identity Manager como `https://<tenant>.vmwareidentity.<region>`. Para implantações locais, insira a URL do servidor do VMware Identity Manager como `https://myco.example.com`.
Aplicativos	Insira a lista das identidades de aplicativos que têm permissão para usar esse sign-on. Para executar o single sign-on usando navegador Safari integrado para iOS, digite a primeira ID de pacote de aplicativos como `com.apple.mobilesafari`. Continue a inserir as IDs de pacote de aplicativos. Os aplicativos listados devem oferecer suporte à autenticação SAML.

11 Clique em **Salvar e Publicar**.

Próximo passo

Atribua o perfil de dispositivo a um grupo inteligente. Grupos inteligentes são grupos personalizáveis que determinam quais dispositivos de plataforma e usuários recebem um aplicativo atribuído, um livro, uma política de conformidade, um perfil de dispositivo ou uma provisão.

Configurar o perfil iOS da Apple no Workspace ONE UEM usando a autoridade de certificação do Workspace ONE UEM

Crie e implante o perfil do dispositivo iOS da Apple no Workspace ONE UEM para enviar por push as configurações do Provedor de Identidade ao dispositivo. Esse perfil contém as informações necessárias para o dispositivo conectar-se ao VMware Identity Provider e ao certificado que o dispositivo usa para a autenticação.

Pré-requisitos

- Kerberos integrado configurado no VMware Identity Manager.
- O arquivo de certificado raiz do servidor KDC do VMware Identity Manager salvo em um computador que pode ser acessado do console do Workspace ONE UEM.
- Certificado habilitado e baixado da página Sistema > Integração Empresarial > VMware Identity Manager do console do Workspace ONE UEM.
- Lista de URLs e IDs de pacote de aplicativos que usam a autenticação Kerberos integrada em dispositivos iOS.

Procedimentos

1. No console do Workspace ONE UEM, navegue para **Dispositivos > Perfis e Recursos > Perfil > Adicionar Perfil** e selecione **Apple iOS**.
2. Defina as configurações de **Geral** do perfil e digite o nome do dispositivo como `iOSKerberos`.
3. No painel de navegação à esquerda, selecione **SCEP > Configurar** para configurar a credencial.

Opção	Descrição
Origem da Credencial	Selecione **AirWatch Certificate Authority** no menu suspenso.
Autoridade de certificação	Selecione **AirWatch Certificate Authority** no menu suspenso.
Modelo de Certificado	Selecione **Single Sign On** para definir o tipo de certificado emitido pela AirWatch Certificate Authority.

4. Clique em **Credenciais > Configurar** e crie uma segunda credencial.
5. No menu suspenso **Origem da Credencial**, selecione **Carregar**.
6. Digite o nome da credencial Kerberos de iOS.
7. Clique em **Carregar** para fazer upload do certificado raiz do servidor KDC do VMware Identity Manager baixado da página Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidades > Provedor de Identidade Integrado.

8 No painel de navegação à esquerda, selecione **Single Sign-On**.

9 Insira informações de conexão.

Opção	Descrição
Nome da Conta	Insira **Kerberos**.
Nome Principal do Kerberos	Clique em **+** e selecione **{EnrollmentUser}**.
Território	Para implantações de tenant na nuvem, insira o nome do território do VMware Identity Manager do seu tenant. O texto desse parâmetro deve estar em letras maiúsculas Por exemplo, **VMWAREIDENTITY.COM**. Nas implantações locais, insira o nome do território que você usou quando inicializou o KDC na máquina do VMware Identity Manager. Por exemplo, **EXEMPLO.COM**.
Certificado de Renovação	Em dispositivos iOS 8 e posteriores, selecione o certificado usado para reautenticar o usuário automaticamente sem necessidade de interação do usuário quando a sessão de single sign-on do usuário expirar.
Prefixos de URL	Insira os prefixos de URL que devem corresponder para se usar essa conta para a autenticação Kerberos por HTTP. Para implantações de tenant na nuvem, insira a URL do servidor do VMware Identity Manager como **https://<tenant>.vmwareidentity.<região>**. Para implantações locais, insira a URL do servidor do VMware Identity Manager como **https://myco.exemplo.com**.
Aplicativos	Insira a lista das identidades de aplicativos que têm permissão para usar esse sign-on. Para executar o single sign-on usando navegador Safari integrado para iOS, digite a primeira ID de pacote de aplicativos como **com.apple.mobilesafari**. Continue a inserir as IDs de pacote de aplicativos. Os aplicativos listados devem oferecer suporte à autenticação SAML.

10 Clique em **Salvar e Publicar**.

Quando o perfil iOS é enviado por push com êxito para os dispositivos dos usuários, estes podem fazer logon no VMware Identity Manager utilizando o método de autenticação Kerberos integrado sem inserir suas credenciais.

Próximo passo

Atribua o perfil de dispositivo a um grupo inteligente. Grupos inteligentes são grupos personalizáveis que determinam quais dispositivos de plataforma e usuários recebem um aplicativo atribuído, um livro, uma política de conformidade, um perfil de dispositivo ou uma provisão.

Atribuir um perfil de dispositivo do Workspace ONE UEM

Depois de criar um perfil de dispositivo, você atribui o perfil a um grupo inteligente.

Grupos inteligentes são grupos personalizáveis que determinam quais dispositivos de plataformas e usuários recebem um aplicativo atribuído, uma política de conformidade, um perfil de dispositivo ou uma provisão. Consulte o Guia de Gerenciamento de dispositivos móveis do Workspace ONE UEM.

Procedimentos

1. No console do Workspace ONE UEM, navegue até **Dispositivos > Perfis e Recursos** > **Perfis**.
2. Selecione o perfil de dispositivo que deseja atribuir ao grupo inteligente.
3. Na guia Geral, clique na caixa de texto de **Grupos Atribuídos** e selecione **Criar Grupo de Atribuição**.
4. Na página Criar Novo Grupo Inteligente, digite o nome para o grupo inteligente.
5. Selecione **Plataforma e Sistema Operacional** e selecione o sistema operacional e a versão corretos nos menus suspensos.
6. Clique em **Salvar e Publicar**.

Depois de atribuir um grupo inteligente à opção do dispositivo, os usuários podem fazer logon no Workspace ONE e acessar aplicativos do catálogo.

Implementando a autenticação do Single Sign-On móvel para dispositivos Android gerenciados

4

O Single Sign-On Móvel (SSO) para Android é uma implementação do método de autenticação de certificados para dispositivos Android gerenciados pelo Workspace ONE UEM. O SSO móvel permite que os usuários entrem no seu dispositivo e acessem com segurança seus aplicativos Workspace ONE sem precisar reinserir uma senha.

O aplicativo móvel VMware Tunnel® está instalado no dispositivo Android para adicionar informações de certificados e de ID do dispositivo em fluxos de autenticação. As configurações do Tunnel são definidas no Workspace ONE UEM Console para acessar o serviço do VMware Identity Manager para autenticação, e o serviço obtém o certificado do dispositivo para autenticação.

No Workspace ONE UEM Console, você define as seguintes configurações.

- Perfil de VPN Android. Usa-se esse perfil para a habilitação dos recursos de encapsulamento por aplicativo para Android.
- Habilite o VPN para cada aplicativo que usa a funcionalidade de encapsulamento de aplicativo a partir do Workspace ONE UEM Console.
- Crie regras de tráfego de rede com uma lista de todos os aplicativos configurados para o VPN por aplicativo, os detalhes do servidor proxy e a URL do VMware Identity Manager.

Ao implementar o SSO móvel para Android com o serviço do VMware Identity Manager no local, você configura o serviço de proxy de certificado na máquina do VMware Identity Manager. Depois que o serviço de proxy de certificado for configurado, você pode configurar a autenticação de certificado no provedor de identidade integrado do VMware Identity Manager no console do VMware Identity Manager.

Ao implementar o SSO móvel para Android com o serviço do VMware Identity Manager na nuvem, você pode configurar a autenticação de certificado no provedor de identidade integrado do VMware Identity Manager no console do VMware Identity Manager. O serviço de proxy de certificado é gerenciado para você.

Consulte a publicação *Single Sign-On móvel de Android para o VMware Workspace ONE* no Centro de documentação do Workspace ONE para obter informações detalhadas sobre como configurar o SSO móvel do Android.

Suporte para dispositivo Android

O Android 5.1 ou posterior é suportado.

Aplicativos acessados a partir de um dispositivo Android devem suportar SAML ou outra norma de federação com suporte para single sign-on.

Direcionar inscrição usando o aplicativo Workspace ONE 5

A inscrição direta por meio do Workspace ONE requer que os usuários inscrevam seus dispositivos para que possam acessar recursos no aplicativo Workspace ONE.

Após fazer a inscrição direta pelo aplicativo Workspace ONE, você poderá instruir todos os usuários a ir à loja de aplicativos apropriada, baixar o aplicativo Workspace ONE, inserir o endereço de e-mail e, em seguida, seguir os prompts para começar a usar o Workspace ONE nos dispositivos.

Dispositivos compatíveis

- Apple iOS 9.0 e posterior
- Android Enterprise (anteriormente conhecido como Android for Work) 5.1 e posteriores
- Android Legacy 4.1 e posteriores

  Um dispositivo Android Legacy é qualquer dispositivo Android não compatível com o Android Enterprise, ou um dispositivo compatível com o Android Enterprise que se conecta a uma instância do Workspace ONE UEM que não tem o Android Enterprise habilitado.

Este capítulo inclui os seguintes tópicos:

Habilitar o Workspace ONE para a inscrição direta

Você habilita a inscrição de dispositivo direta por meio do Workspace ONE na página Inscrição > Restrição do console do Workspace ONE UEM para o seu grupo organizacional (GO).

Quando o Workspace ONE está habilitado para inscrição direta, os dispositivos qualificados que fazem logon pela primeira vez são inscritos diretamente. Os dispositivos que não se qualificarem para a inscrição direta terão acesso de somente gerenciamento de aplicativos móveis em um estado registrado do Workspace ONE.

Procedimentos

1 No console do Workspace ONE UEM, selecione o grupo organizacional para habilitar a Inscrição Direta para o Workspace ONE.

2 Navegue para **Grupos e Configurações > Todas as Configurações > Dispositivo e Usuários > Geral > Inscrição** e selecione a guia **Restrições**.

3 Para Configurações Atuais, selecione **Substituir**, se necessário.

4 Role para baixo até Requisitos de Gerenciamento do Workspace ONE e selecione as opções de configuração.

Configuração	Descrição
Exigir o MDM para o Workspace ONE	Quando essa opção está habilitada, os usuários e dispositivos qualificados são solicitados a se inscreverem imediatamente após o logon no Workspace ONE.
Grupo de Usuários Atribuído	O grupo de usuários padrão é Todos os Usuários. Você pode selecionar um grupo de usuários específico a ser incluído no processo de inscrição direta.
iOS	Habilite para incluir dispositivos iOS. Os dispositivos iOS não serão elegíveis para a inscrição direta se essa opção estiver desativada. Se essa opção estiver desativada, os dispositivos ainda poderão ser registrados no Workspace ONE UEM em um estado não gerenciado.
Android Legacy	Habilite para incluir os dispositivos Android Legacy. Os dispositivos Android Legacy não serão elegíveis para a inscrição direta se essa opção estiver desativada. Se essa opção estiver desativada, os dispositivos ainda poderão ser registrados no Workspace ONE UEM em um estado não gerenciado.
Android Enterprise	Habilite para incluir os dispositivos Android Enterprise. Os dispositivos Android Enterprise não serão elegíveis para a inscrição direta se essa opção estiver desativada. Se essa opção estiver desativada, os dispositivos ainda poderão ser registrados no Workspace ONE UEM em um estado não gerenciado.

5 Clique em **Salvar**.

6 Continue para configurar as guias de inscrição com as opções de inscrição suportadas no Workspace ONE. Consulte Opções de configuração de inscrição direta do Workspace ONE.

Para obter mais informações sobre como configurar a inscrição direta para o Workspace ONE, consulte o Guia do VMware AirWatch Mobile Device Management, capítulo Inscrição de dispositivo.

Opções de configuração de inscrição direta do Workspace ONE

Configure a inscrição direta com o Workspace ONE no console do Workspace ONE UEM. Navegue para **Grupos e Configurações > Todas as Configurações > Dispositivo e Usuários/Geral/Inscrição**. A Tabela de Opções de Inscrição de Dispositivo do Workspace ONE lista os itens de menu que podem ser configurados.

A página de Configurações de inscrição permite configurar opções relacionadas às inscrições de dispositivos e usuários. A página é dividida em guias que são descritas abaixo. Veja informações detalhadas sobre como configurar a inscrição de dispositivo no guia do VMware Workspace ONE UEM Gerenciamento de Dispositivo Móvel.

Figura 5-1. Página de inscrição do console do Workspace ONE UEM

Tabela 5-1. Itens de menu configuráveis de inscrição direta do Workspace ONE

Guia Inscrição	Itens de menu configuráveis para a inscrição direta no Workspace ONE
Autenticação	Há suporte para usuários de diretório. Além disso, há suporte para usuários de SAML mais Active Directory "quando necessário". Há suporte para os usuários de SAML sem LDAP quando há o registro de usuário no Workspace ONE UEM no momento do login inicial. Para Mod de Inscrição de Dispositivos, somente há suporte para **Inscrição Aberta**. Não há suporte para Somente Dispositivos Registrados.
Termos de Uso	Os termos de uso podem ser criados para exigir que os usuários os aceitem antes de prosseguirem com o processo de inscrição direta.
Agrupamento	Todas as opções do menu de agrupamento são compatíveis com a inscrição direta do Workspace ONE. A opção **Sincronizar Grupos de Usuários em Tempo Real para o Workspace ONE** é ativada por padrão. Quando um dispositivo está se inscrevendo, o Workspace ONE UEM faz uma chamada em tempo real para o Active Directory para sincronizar os grupos de usuários do usuário. Se o usuário não existir no Workspace ONE UEM, o console do Workspace ONE UEM primeiro sincroniza o usuário e, em seguida, sincroniza os grupos de usuários em tempo real. Se este recurso não estiver ativado, o console do Workspace ONE UEM não sincronizará os grupos de usuários. **Observação** Este recurso está com uso intensivo de CPU. Se os grupos de usuários não estiverem mudando com frequência ou se os grupos de usuários já existirem no Workspace ONE UEM, desative essa configuração para melhorar o desempenho e evitar problemas de latência ao iniciar o aplicativo Workspace ONE. Consulte a seção Colocar dispositivos no grupo organizacional correto em Estratégias de implantação para configurar vários grupos organizacionais do Workspace ONE UEM.

Restrições	■ No **Controle de Acesso do Usuário**, você pode selecionar tanto Limitar a Inscrição aos Usuários Conhecidos quanto Limitar a Inscrição aos Grupos Configurados.
	■ Há suporte ao limite máximo de dispositivos.
	■ Há suporte parcial à **Configuração de política**.
	  ■ **Tipos de propriedade permitidos**. O Workspace ONE só exibe alerta para Propriedade do Funcionário e Corporativo - Dedicado.
	  Observação Não há suporte para o tipo de inscrição Permitir Contêiner.

Tabela 5-1. Itens de menu configuráveis de inscrição direta do Workspace ONE (Continuação)

Guia Inscrição	Itens de menu configuráveis para a inscrição direta no Workspace ONE
Alerta opcional	Os dois alertas opcionais que podem ser habilitados são **Solicitar Tipo de Propriedade** e **Habilitar a Solicitação pelo Número de Ativo do Dispositivo**. A solicitação para inserir o número de ativo só é feita quando o tipo de propriedade for Propriedade da Empresa.
Personalização	Há suporte para as opções do menu de personalização. ■ URL de entrada após a inscrição (somente iOS) ■ Mensagem de perfil de MDM (somente iOS) ■ Usar aplicativos de MDM personalizados É possível habilitar a opção Usar um modelo de mensagem específico para cada plataforma, mas os modelos de mensagem específicos do Workspace ONE não estão disponíveis para o Workspace ONE 3.2.

Experiência do usuário durante a inscrição direta no Workspace ONE UEM com o Workspace ONE

Quando o gerenciamento de dispositivos móveis é implementado por meio do Workspace ONE, os usuários baixam o aplicativo Workspace ONE, autenticam-se com o Workspace ONE UEM e inscrevem seus dispositivos. Depois que o dispositivo estiver inscrito, os usuários poderão usar o Workspace ONE para adicionar e usar seus recursos autorizados imediatamente.

O processo pelo qual os usuários passam ao usar o Workspace ONE para inscrever seus dispositivos é semelhante para dispositivos iOS e Android Enterprise. A inscrição do Android Legacy é redirecionada para o AirWatch Agent para a inscrição. O AirWatch Agent entrega automaticamente o controle de volta ao Workspace ONE quando a inscrição é concluída. Os usuários podem acessar o Workspace ONE em todas as essas variações.

Inscrição direta por meio do Workspace ONE em dispositivos iOS

Instrua os usuários a baixar, instalar e executar o aplicativo Workspace ONE na App Store da Apple.

Procedimentos

1 Os usuários abrem o aplicativo, inserem o endereço de e-mail e a URL do servidor e se autenticam de acordo com a configuração de seus ambientes.

2 Aparece a **tela É necessário configuração adicional por sua empresa**.

Figura 5-2. Notificação de configuração da inscrição do dispositivo

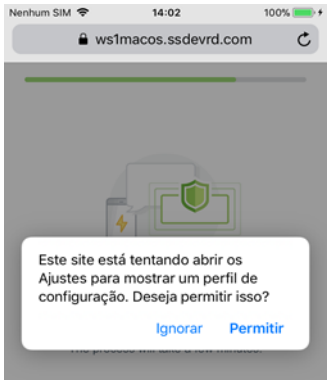
3 Se os termos de uso estiverem configurados, os usuários terão de aceitá-los antes de prosseguirem.

4 Se você configurar os avisos opcionais para mostrar o tipo de propriedade do dispositivo e solicitar o número de ativo do dispositivo, essas informações serão exibidas.

Figura 5-3. Seleção de propriedade do dispositivo

5 O Safari abre e os usuários clicam em **Permitir** para abrir a página de configurações.

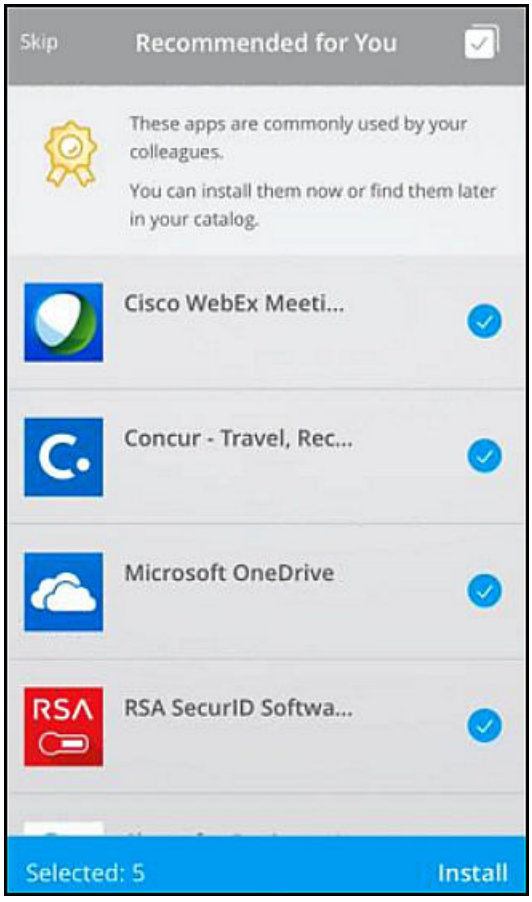
Figura 5-4. Permitir as definições de perfil de configuração



O Workspace Services e o perfil de configuração são configurados no dispositivo.

O dispositivo agora está inscrito no Workspace ONE UEM e o Workspace ONE foi inicializado. A tela Recomendado para Você abre.

Figura 5-5. Tela Aplicativos recomendados



6 Os usuários podem selecionar os aplicativos que desejam instalar ou podem pular essa etapa por enquanto.

O dispositivo agora é gerenciado pelo Workspace ONE UEM MDM. Caso tenha sido selecionada a instalação dos aplicativos recomendados, os usuários começarão a receber notificações por push para esses aplicativos.

Inscrição direta usando o Workspace ONE em dispositivos Android Enterprise

Instrua os usuários a baixar, instalar e executar o aplicativo Workspace ONE no Google Play ou no repositório.

Procedimentos

1 Os usuários inserem o endereço de e-mail e a URL do servidor e se autenticam de acordo com a configuração de seus ambientes.

2 Aparece a tela **É necessário configuração adicional por sua empresa**. O usuário clica em **Continuar**.

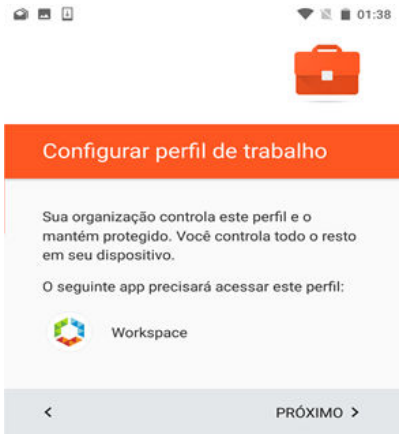
Figura 5-6. Notificação de configuração da inscrição do dispositivo

3 Se os termos de uso estiverem configurados, os usuários terão de aceitá-los antes de prosseguirem.

4 Se você configurar os avisos opcionais para mostrar o tipo de propriedade do dispositivo e solicitar o número de ativo do dispositivo, essas informações serão exibidas.

5 O Workspace Services e o perfil de trabalho são configurados no dispositivo.

Figura 5-7. Configurar a notificação de perfil de trabalho

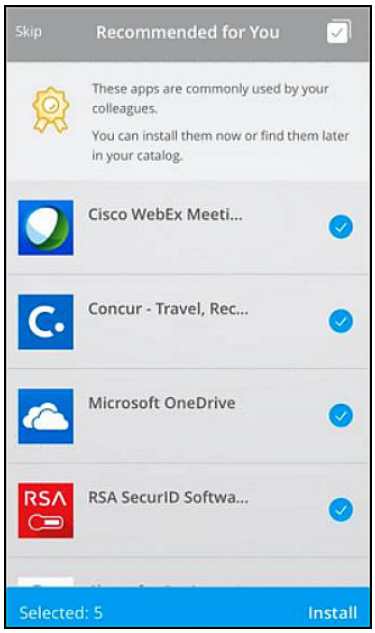


Os usuários veem uma mensagem que descreve o controle do gerenciamento de dispositivos com o perfil de trabalho e clicam em **OK**.

O aplicativo Workspace ONE está instalado e a conta do Android Work registrada.

6 O dispositivo agora está inscrito no Workspace ONE UEM e o Workspace ONE foi inicializado. A tela Recomendado para você abre.

Figura 5-8. Tela Aplicativos recomendados



7 Os usuários podem selecionar os aplicativos que desejam instalar ou pular essa etapa por enquanto.

O dispositivo agora é gerenciado pelo Workspace ONE UEM MDM. Caso tenha sido selecionada a instalação dos aplicativos recomendados, esses aplicativos começarão a ser instalados com um ícone de maleta do Android Enterprise.

Inscrição de dispositivo para dispositivos Android Legacy

A inscrição de dispositivo para os dispositivos Android Legacy redireciona ao AirWatch Agent onde é feita a inscrição. O AirWatch Agent entrega automaticamente o controle de volta ao Workspace ONE quando se conclui a inscrição.

Os usuários diretos vão à loja de aplicativos para fazer o download do Workspace ONE.

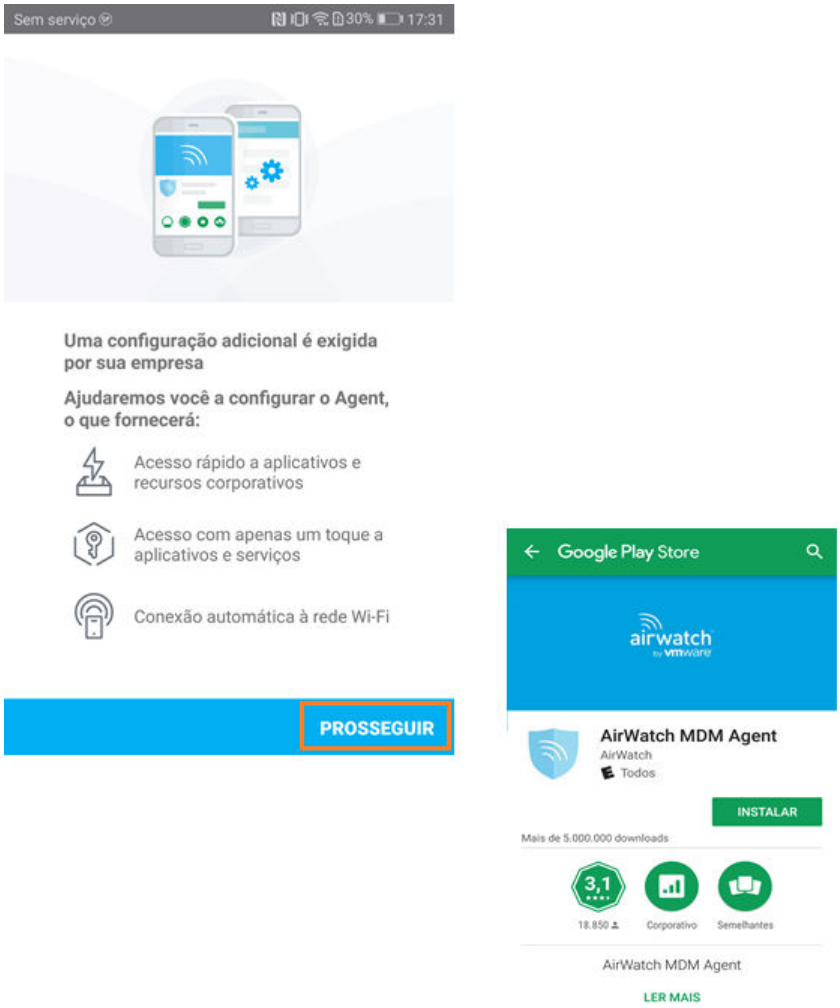
Procedimentos

1 Os usuários abrem o aplicativo, inserem a URL do servidor ou o endereço de e-mail e inserem o nome de usuário e a senha para fazerem o logon.

   Nesse ponto, o aplicativo Workspace ONE pode detectar que o dispositivo não está habilitado para o Android Enterprise e se o dispositivo requer a inscrição direta antes de se acessar os recursos do Workspace ONE.

2 Aparece a **tela É necessário configuração adicional por sua empresa** e quando os usuários clicam em **Prosseguir**, são redirecionados para o aplicativo AirWatch Agent no Google Play.

Figura 5-9. Pedido de download do aplicativo AirWatch Agent



3 Os usuários baixam o aplicativo AirWatch Agent.

Observação Se o aplicativo AirWatch Agent já estiver instalado no dispositivo, o Workspace ONE o iniciará automaticamente. Eles não são redirecionados para a loja de aplicativos.

Os detalhes de autenticação que foram inseridos para o Workspace ONE são passados para o aplicativo AirWatch Agent para que os usuários não reinsiram essas informações.

O aplicativo AirWatch Agent é iniciado. Durante a inscrição de dispositivo com o AirWatch Agent, os usuários selecionam o tipo de propriedade e inserem o número de ativo do dispositivo, se configurado.

4 Quando aparece a opção **Permitir que o AirWatch Agent faça e gerencie telefonemas**, os usuários clicam em **Permitir**.

O AirWatch Agent valida a inscrição, autentica o usuário e concede as permissões à AirWatch nesse dispositivo.

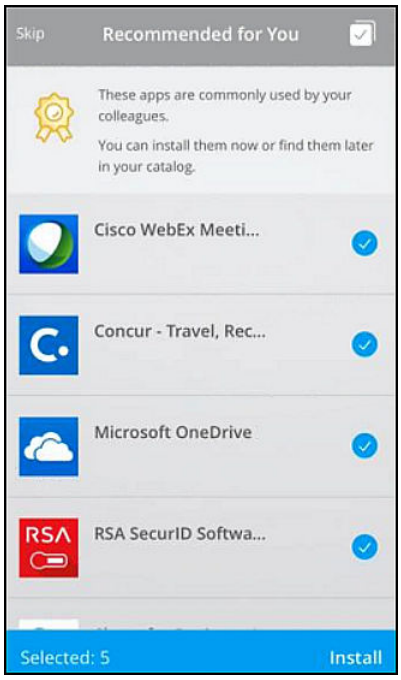
5 Quando aparece a tela **Ativar aplicativo de administração de dispositivos?**, os usuários clicam em **Ativar este aplicativo de administração de dispositivos**.

Figura 5-10. Ativar o aplicativo de administração de dispositivos

6 Os usuários são solicitados a conceder permissão de acesso a diversos recursos de dispositivo.

O dispositivo agora está inscrito no Workspace ONE UEM e o Workspace ONE foi inicializado. A tela Aplicativos recomendados abre.

Figura 5-11. Tela Aplicativos recomendados



7 Os usuários podem selecionar os aplicativos que desejam instalar ou podem pular essa etapa por enquanto.

O dispositivo agora é gerenciado pelo Workspace ONE UEM MDM. Caso se tenha selecionado a instalação dos aplicativos recomendados, os usuários começarão a receber notificações para esses aplicativos.

Aplicando o Workspace ONE para oferecer suporte à integração do programa de inscrição de dispositivo da Apple

6

O Programa de inscrição de dispositivo da Apple (Apple Device Enrollment Program, DEP) não oferece suporte a cenários em que um cliente está usando o SAML para a autenticação do usuário. No entanto, o Workspace ONE implementou uma maneira exclusiva de oferecer suporte a esse caso de uso.

Por meio da preparação de dispositivo do Workspace ONE UEM, os administradores podem atribuir o dispositivo a um usuário de preparação de vários dispositivos e permitir que o Workspace ONE reatribua o dispositivo ao usuário apropriado quando ele entrar no aplicativo Workspace ONE.

O aplicativo Workspace ONE deve ser instalado no dispositivo como parte da inscrição de usuário de preparação. Quando os usuários fazem login no Workspace ONE pela primeira vez, o Workspace ONE autentica o usuário por meio do provedor SAML configurado. Após a autenticação do usuário, a propriedade do dispositivo mudará do usuário de preparação de vários dispositivos para o usuário de diretório autenticado.

Pré-requisito

O usuário de diretório deve existir no Workspace ONE UEM quando o usuário faz login no aplicativo Workspace ONE. Você pode pré-carregar os usuários em um carregamento em massa por meio de CSV ou aplicar a seguinte API para gerar os usuários conforme necessário.

Observação O valor de Tipo de Segurança deve ser igual ao diretório.

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

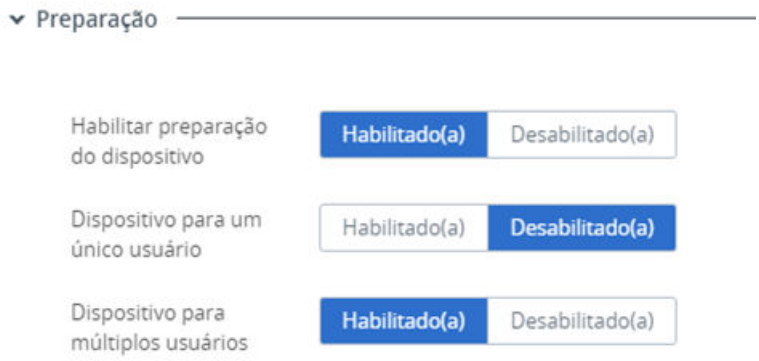
Fluxo do suporte do Workspace ONE da integração do DEP

As tarefas a seguir devem ser concluídas para implementar o suporte do DEP da Apple usando o Workspace ONE.

- Instale o aplicativo Workspace ONE nos dispositivos iOS.
- Certifique-se de que exista um usuário de preparação com a seguinte configuração de preparação no console do Workspace ONE UEM.
  a Navegue até **Contas > Usuários > Exibição em Lista** e selecione a conta de usuário para a qual você deseja habilitar a preparação do dispositivo para a edição.

b Na página **Adicionar/Editar** Usuário, selecione a guia **Avançado**. Role para baixo até a seção **Preparação** e habilite **Preparação do dispositivo** e **Dispositivos para múltiplos usuários**.

Figura 6-1. Configuração de dispositivos para múltiplos usuários no Workspace ONE UEM



- Atribua o dispositivo ao usuário de preparação no portal do DEP da Apple e ofereça o dispositivo ao usuário final.

  Para obter mais informações sobre o Programa de inscrição de dispositivo da Apple, consulte o guia de Inscrição de dispositivo da Apple.

Como funciona a integração

Quando o usuário liga o dispositivo pela primeira vez, o dispositivo é inscrito e atribuído ao usuário de preparação de vários dispositivos. O usuário inicializa o aplicativo Workspace ONE que está disponível na tela inicial e faz logon. O Workspace ONE autentica o usuário por meio do provedor SAML configurado.

Após a autenticação do usuário, a propriedade do dispositivo mudará do usuário de preparação de vários dispositivos para o usuário de diretório autenticado. Os aplicativos, perfis e recursos atribuídos ao usuário autenticado são enviados por push ao dispositivo.

Observação O grupo organizacional do dispositivo não muda. Este recurso não oferece suporte ao mapeamento de grupo de usuário (ou à seleção manual do usuário com base no menu suspenso) localizado na seção Configuração de Inscrição do console do Workspace ONE UEM.

Implantando o aplicativo móvel VMware Workspace ONE

7

Quando o aplicativo VMware Workspace ONE estiver instalado em dispositivos móveis, os usuários poderão acessar os recursos que você autorizou que eles usem.

Os usuários podem acessar seus aplicativos autorizados usando a funcionalidade de logon único quando suas identidades são gerenciadas com o VMware Identity Manager. Eles também podem acessar um catálogo de aplicativos onde podem adicionar outros aplicativos.

A interface do aplicativo Workspace ONE oferece experiência e opções semelhantes em qualquer telefone, tablet ou computador desktop.

Se o dispositivo estiver inscrito no Gerenciamento de Dispositivos Móveis (MDM), você poderá enviar por push o aplicativo Workspace ONE como um aplicativo público.

Este capítulo inclui os seguintes tópicos:

Opções de gerenciamento de dispositivos no Workspace ONE UEM para aplicativos públicos e internos para Workspace ONE

Você pode configurar para implantar aplicativos públicos e internos com base no status de gerenciamento de dispositivos. Qualquer dispositivo pode acessar aplicativos que estão configurados como acesso aberto. Somente dispositivos com permissão, habilitados através do Workspace Services ou da Inscrição de Agente, podem acessar aplicativos que estão configurados para acesso gerenciado.

A tabela descreve funcionalidades para cenários gerenciados e não gerenciados.

Tipo de acesso	Recursos	Descrição	Usos sugeridos
Acesso aberto (não gerenciado)	■ Catálogo de aplicativos de autoatendimento para recursos da Web, do Horizon e do Citrix ■ Inicializar aplicativos Web/virtuais com inicialização de logon único (SSO) ■ Proteção de aplicativos com Touch ID/PIN ■ Detecção de jailbreak de dispositivos ■ Suporte para acesso condicional do VMware Identity Manager, incluindo políticas de autenticação e dispositivos de bloqueio. ■ Acesso de aplicativo nativo. ■ Distribuição de aplicativo SDK e aplicativo interno	Os usuários acessam recursos no seu dispositivo sem conceder permissão de administradores para acessar seu dispositivo. Os aplicativos com acesso aberto estão disponíveis para dispositivos independentemente do seu status gerenciado. Os administradores não podem remover aplicativos nativos sistematicamente quando estão definidos para Acesso aberto.	■ Forneça acesso de aplicativos aos usuários finais imediatamente após o logon, sem permissões de segurança elevadas. ■ Recomenda-se o uso de um aplicativo sem exigir que o aplicativo seja instalado. Os usuários podem instalar o aplicativo em seu dispositivo quando quiserem. ■ Os aplicativos não contêm dados corporativos sensíveis e não acessam recursos corporativos protegidos. ■ Para distribuir aplicativos para pessoal auxiliar sem o perfil MDM do Workspace ONE UEM.
Acesso gerenciado	■ Catálogo de aplicativos de autoatendimento para recursos da Web, do Horizon e do Citrix ■ Inicializar aplicativos Web/virtuais com inicialização de logon único (SSO) ■ Proteção de aplicativos com Touch ID/PIN ■ Detecção de jailbreak de dispositivos ■ Suporte para acesso condicional do VMware Identity Manager, incluindo políticas de autenticação e dispositivos de bloqueio. ■ Instalação direta e gerenciada de Aplicativos nativos ■ Gerenciamento de aplicativo SDK e aplicativo interno ■ Suporte para configuração de aplicativo ■ VPN Por Aplicativo ■ SSO com um toque para aplicativos nativos habilitados por SAML	Os usuários instalam um perfil de gerenciamento no seu dispositivo para conceder permissão de administradores para acessar seu dispositivo. Aplicativos com acesso gerenciado estão disponíveis para dispositivos que o Workspace ONE UEM gerencia. Se o Workspace ONE UEM não gerenciar o dispositivo, o Workspace ONE solicitará ao usuário no dispositivo que se inscreva com o Workspace ONE UEM. Se o dispositivo estiver inscrito, o usuário poderá usar o dispositivo para acessar o aplicativo através do Workspace ONE.	■ Para remover dados corporativos sensíveis dos dispositivos quando os usuários deixam a organização ou perdem seu dispositivo. ■ Exija o tunelamento de aplicativos para autenticação e comunicação seguras com recursos internos de back-end quando os aplicativos acessam a Intranet. ■ Habilite o logon único para aplicativos. ■ Acompanhe a adoção de usuário e o status de instalação para aplicativos. ■ Implante o aplicativo automaticamente após a inscrição.

Tipo de acesso	Recursos	Descrição	Usos sugeridos
	■ Perfis de dispositivos ■ Mecanismo de conformidade do Workspace ONE UEM		

Para obter informações sobre como configurar opções de acesso gerenciado para aplicativos internos ou como adicionar aplicativos públicos para implantação através do Workspace ONE, consulte o Guia de Gerenciamento de Aplicativos Móveis (MAM) do Workspace ONE UEM.

Plataformas com suporte para acesso aberto e gerenciado

Configure o tipo de acesso para aplicativos públicos e internos com base na plataforma.

	Acesso gerenciado	Acesso aberto
APLICATIVOS INTERNOS		
Android	X	X
iOS	X	X
Windows 10 Desktop	X	-
Telefone Windows 10	X	-
APLICATIVOS PÚBLICOS		
Android	X	X
iOS	X	X
Windows 10 Desktop	-	X
Telefone Windows 10	-	X

Gerenciando acesso a aplicativos

Um usuário único pode ter autorização a uma combinação de acesso aberto ou gerenciado a aplicativos nativos. A abordagem de gerenciamento adaptativo permite que os usuários finais usem aplicativos de acesso aberto sem exigir gerenciamento. Quando os usuários solicitam um aplicativo nativo que requer gerenciamento, o gerenciamento adaptativo fornece a segurança e o controle adicionais necessários para gerenciar esse aplicativo nativo.

Quando os aplicativos são gerenciados, os usuários devem habilitar o Workspace Services para instalar e usar os aplicativos gerenciados. Quando você carrega um aplicativo no console do Workspace ONE UEM, o estado de acesso é exibido como aberto ou gerenciado com base na configuração para esse aplicativo. Por exemplo, se a opção **Enviar a Configuração de Aplicativo** for selecionada, um aplicativo será configurado para exigir o gerenciamento.

Os aplicativos que requerem que o gerenciamento exiba um ícone de estrela quando visualizados em um estado não gerenciado no catálogo. Os usuários devem selecionar a habilitação do Workspace Services através do processo de gerenciamento adaptativo para usar o aplicativo. Quando os usuários tentam baixar um aplicativo que exibe um ícone de estrela, é apresentada uma mensagem que solicita que os usuários habilitem o Workspace Services. Os usuários podem clicar no link de aviso de privacidade para ver o impacto sobre a privacidade das suas informações pessoais caso optem por continuar com o processo de gerenciamento adaptativo. O aviso de privacidade puxa automaticamente as configurações do ambiente do Workspace ONE UEM em que os usuários estão prestes a se inscrever. Depois de analisar as informações de configuração de privacidade, os usuários podem prosseguir para habilitar o Workspace Services ou voltar e continuar a usar o aplicativo Workspace ONE de forma não gerenciada no seu dispositivo. Quando os usuários habilitam o Workspace Services, o ícone de estrela é removido de todos os aplicativos gerenciados.

Removendo o acesso em dispositivos gerenciados

Os usuários podem desativar o aplicativo Workspace ONE em seu dispositivo gerenciado através da opção Remover Conta. A remoção da conta executa uma limpeza de dados corporativos do dispositivo, removendo o acesso corporativo e retornando o usuário para a tela de logon. Os administradores podem executar uma limpeza de dados corporativos a partir do console do Workspace ONE UEM para desativar os serviços do Workspace ONE.

A execução de uma ação de Remover Conta em dispositivos gerenciados revoga o acesso concedido através do aplicativo Workspace ONE e cancela a inscrição do dispositivo do Workspace ONE UEM. Os aplicativos que exigiam gerenciamento são removidos do dispositivo e o acesso aos aplicativos de produtividade do Workspace ONE UEM, como o Boxer, o Browser e o Content Locker, é revogado.

Solicitando termos de uso para o acesso ao catálogo do Workspace ONE

Você pode escrever os próprios termos de uso do Workspace ONE de sua organização e garantir que o usuário final aceite esses termos de uso antes de usarem o Workspace ONE.

Os termos de uso são exibidos após o usuário entrar no Workspace ONE. Os usuários devem aceitar os termos de uso antes de prosseguirem para o catálogo do Workspace ONE.

O recurso Termos de Uso inclui as seguintes opções de configuração.

- Crie versões dos termos de uso existentes.
- Edite os termos de uso.
- Crie vários termos de uso que podem ser exibidos com base no tipo de dispositivo.
- Crie cópias dos termos de uso específicas a certos idiomas.

As políticas de termos de uso que você configura estão listadas na guia Gerenciamento de Identidade e Acesso. Você pode editar a política de termos de uso para fazer uma correção da política existente ou criar uma nova versão da política. A adição de uma nova versão dos termos de uso substitui os termos de uso existentes. A edição de uma política não cria uma versão dos termos de uso.

Você pode ver o número de usuários que aceitaram ou recusaram os termos de uso na página de termos de uso. Clique no número de aceitações ou recusas para ver uma lista de usuários e seu status.

Configurar e habilitar os termos de uso

Na página Termos de Uso, você adiciona a política de termos de uso e configura os parâmetros de uso. Após a adição dos termos de uso, habilite a opção de Termo de Uso. Quando os usuários fazem logon no Workspace ONE, eles devem aceitar os termos de uso para acessar o catálogo.

Pré-requisitos

O texto da política de termos de uso formatado em HTML a ser copiado e colado na caixa de texto do conteúdo Termos de Uso. Você pode adicionar termos de uso em inglês, alemão, espanhol, francês, italiano e holandês.

Procedimentos

1. Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, selecione **Configuração > Termos de Uso**.
2. Clique em **Adicionar Termos de Uso**.
3. Insira um nome descritivo para os termos de uso.
4. Selecione **Qualquer um**, se a política de termos de uso for para todos os usuários. Para usar as políticas de termos de uso por tipo de dispositivo, selecione **Plataformas de Dispositivos Selecionados** e selecione os tipos de dispositivo que exibem essa política de termos de uso.
5. Por padrão, o idioma dos termos de uso que será exibido primeiro baseia-se nas configurações de preferência de idioma do navegador. Insira o conteúdo dos termos de uso para o idioma padrão na caixa de texto.
6. Clique em **Salvar**.

   Para adicionar uma política de termos de uso em outro idioma, clique em **Adicionar Idioma** e selecione outro idioma. A caixa de texto do conteúdo dos Termos de Uso é atualizada, e você pode adicionar o texto à caixa de texto.

   Você pode arrastar o nome do idioma para estabelecer a ordem em que os termos de uso serão exibidos.
7. Para começar a usar os termos de uso, clique em **Habilitar Termos de Uso** na página exibida.

Próximo passo

Se você tiver selecionado um tipo de dispositivo específico para os termos de uso, poderá criar termos de uso adicionais para os outros tipos de dispositivo.

Visualizar o status da aceitação dos termos de uso

As políticas de termos de uso listadas na página Identidade e Gerenciamento > Termos de Uso mostram o número de usuários que aceitaram ou recusaram a política.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, selecione **Configuração > Termos de Uso**.

2 Na coluna Aceito/Recusado, clique no número Aceito à esquerda ou no número Recusado à direita.

Uma página de status exibe a ação tomada, aceitação ou recusa, com o nome do usuário, a ID do dispositivo, a versão da política visualizada, a plataforma usada e a data.

3 Clique em **Cancelar** para fechar a visualização.

Obtendo e distribuindo o aplicativo Workspace ONE

Os usuários podem fazer download do aplicativo VMware Workspace ONE da loja de aplicativos do dispositivo, ou os administradores podem configurar o Workspace ONE UEM para enviar por push o aplicativo Workspace ONE como um aplicativo gerenciado aos dispositivos.

Você implanta o aplicativo Workspace ONE a partir do console do Workspace ONE UEM em grupos e usuários específicos na sua organização. Depois que os usuários fizerem login no aplicativo do Workspace ONE em seus dispositivos, eles poderão acessar os aplicativos Web e de SaaS autorizados a eles.

As seguintes etapas servem para enviar por push o aplicativo móvel Workspace ONE como um aplicativo gerenciado a partir do console do Workspace ONE UEM. Você também pode executar o assistente de Como começar do Workspace ONE para enviar o aplicativo por push.

Observação Para obter informações detalhadas sobre a configuração de aplicativos gerenciados no Workspace ONE UEM, consulte o Guia do Gerenciamento de Aplicativos Móveis (MAM) do VMware Workspace ONE UEM, disponível no Portal de Recursos em https://resources.air-watch.com.

Pré-requisitos

Se você estiver planejando enviar por push o aplicativo móvel Workspace ONE a partir de um console do Workspace ONE UEM, prepare os Grupos Inteligentes de usuários finais autorizados para o aplicativo.

Procedimentos

1 No console do Workspace ONE UEM, vá para **Aplicativos e Livros > Aplicativos** > **Exibição em Lista > Público** e selecione **Adicionar Aplicativo**.

2 Selecione a plataforma, que pode ser iOS, Android ou Windows.

3 Selecione **Procurar na Loja de Aplicativos** e na caixa de texto **Nome**, insira `Workspace ONE` como a palavra-chave para localizar o VMware Workspace ONE na Loja de Aplicativos.

4 Escolha **Avançar** e use **Selecionar** para carregar o aplicativo Workspace ONE a partir da página Resultados da Loja de Aplicativos.

5 Configure as opções de atribuição e de implantação para usuários do Workspace ONE nas seguintes configurações de guia.

Guia	Descrição
Informações	Insira e visualize as informações sobre os modelos de dispositivo, classificações e categorias suportados.
Atribuição	Atribua o aplicativo móvel Workspace ONE a grupos inteligentes de usuários finais que podem usar o aplicativo em seu dispositivo.
Implantação	Configure recursos de enterprise mobility management (EMM) avançados e de disponibilidade, se aplicável. Para configurar automaticamente os aplicativos gerenciados, habilite **Enviar a Configuração de Aplicativo** e insira os pares chave-valor do App Configuration for Enterprise (ACE). Consulte Configuração do aplicativo do Workspace ONE UEM para pares de chave-valor da empresa.
Termos de Uso	(Opcional) Habilite **Termos de Uso** para usar o aplicativo Workspace ONE.

6 Selecione **Salvar e Publicar** para disponibilizar o aplicativo para os usuários.

Conclua essas etapas para cada plataforma suportada.

Configuração do aplicativo do Workspace ONE UEM para pares de chave-valor da empresa

Ao implantar o aplicativo Workspace ONE como um aplicativo gerenciado no Workspace ONE UEM e habilitar a opção Enviar Configurações do Aplicativo ao enviar por push o aplicativo Workspace ONE no console do Workspace ONE UEM, você pode predefinir as configurações do Workspace ONE que são aplicadas quando os usuários instalam e inicializam o aplicativo Workspace ONE.

Quando o aplicativo Workspace ONE é carregado para o console do Workspace ONE UEM como um aplicativo móvel gerenciado, é possível fazer a configuração da URL do servidor do VMware Workspace ONE, do valor de UID do dispositivo e da exigência da autenticação do certificado nos dispositivos Android.

Tabela 7-1. Opções de configuração no dispositivo gerenciado do Workspace ONE no console do Workspace ONE UEM

Plataforma	Chave de configuração	Tipo de valor	Valor de configuração	Explicação
Tudo	`AppServiceHost`	Cadeia de caracteres	**<URL do Servidor do VMware Workspace ONE >**	Configura a URL do servidor do VMware Workspace ONE em dispositivos.
iOS	`deviceUDID`	Cadeia de caracteres	**{DeviceUid}** Digite o valor de UID do dispositivo. Não use a função Inserir Valor de Localização.	Rastreia os dispositivos usados para autenticar o ambiente do VMware Identity Manager.

Tabela 7-1. Opções de configuração no dispositivo gerenciado do Workspace ONE no console do Workspace ONE UEM (Continuação)

Plataforma	Chave de configuração	Tipo de valor	Valor de configuração	Explicação
iOS	SkipDiscoveryScreen	Booliano	**true**	A partir da versão 3.1 do aplicativo Workspace ONE, a chave de configuração SkipDiscoveryScreen pode ser configurada. Quando definido como True, o Workspace ONE tenta passar pela tela de endereço de e-mail/URL do servidor. Quando usado com a chave de configuração do AppServiceHost, os usuários são imediatamente levados para a tela de autenticação. Se o SSO móvel também for usado, os administradores poderão fornecer aos usuários finais uma experiência perfeita ao iniciar o Workspace ONE e começar imediatamente a carregar o aplicativo Workspace ONE.
Android e iOS	RemoveAccountSignOut	Inteiro	0 - A opção Remover Conta aparece 1 - A opção Remover Conta não aparece Se o valor não estiver definido, a opção Remover Conta aparecerá.	Quando o valor é definido como 1, a opção Remover Conta não aparece na página Configurações do Workspace ONE dos usuários. Os usuários não podem remover a conta do Workspace ONE do dispositivo. Quando esse valor é definido como 0 ou nenhum valor for definido, a opção Remover Conta aparece. Se os usuários clicarem em Remover Conta, o Workspace ONE UEM executará um

Tabela 7-1. Opções de configuração no dispositivo gerenciado do Workspace ONE no console do Workspace ONE UEM (Continuação)

Plataforma	Chave de configuração	Tipo de valor	Valor de configuração	Explicação
				apagamento dos dados corporativos do dispositivo e cancelará a inscrição do dispositivo no Workspace ONE UEM.

Registrando domínios de e-mail para a descoberta automática

Você pode registrar seu domínio de e-mail no serviço de detecção automática no para que os usuários finais acessem com mais facilidade o portal de aplicativos pelo aplicativo Workspace ONE. Os usuários finais inserem seu endereço de e-mail em vez da URL da organização.

Quando o domínio de e-mail da organização é registrado para a descoberta automática, os usuários finais só precisam inserir seu endereço de e-mail na página de login para acessar o portal de aplicativos. Por exemplo, eles inserem **nomedousuário@minhaemp.com**.

Quando não se usa a descoberta automática, na primeira vez que os usuários finais abrirem o aplicativo Workspace One, eles deverão fornecer a URL completa da organização. Por exemplo, eles inserem **minhaemp.vmwareidentity.com**.

Configurar a descoberta automática no VMware Identity Manager

Para registrar um domínio, insira seu domínio de e-mail e endereço de e-mail na página Detecção Automática do console do VMware Identity Manager.

Uma mensagem de e-mail com um token de ativação é enviada ao seu endereço de e-mail no domínio. Para ativar o registro de domínio, insira o token na página Descoberta Automática e verifique se o domínio registrado é o seu domínio.

Observação Para configurar a descoberta automática para as implantações locais do VMware Identity Manager, você deve fazer login no console do VMware Identity Manager como administrador local. Digite a ID e a senha do Workspace ONE UEM criadas no site do Workspace ONE UEM, https://secure.air-watch.com/register.

Procedimentos

1 Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, clique em **Configuração > Detecção Automática**.

2 (Apenas implantações locais). Configure a URL da descoberta automática do Workspace ONE UEM.

Opção	Descrição
URL do Auto Discovery	Digite a URL de acordo com https://discovery.awmdm.com.
ID do AirWatch	Digite o endereço de e-mail que você registrou no Workspace ONE UEM para fazer login no site.
Senha	Digite a senha associada à conta do Workspace ONE UEM.

3 Na caixa de texto **Domínio de E-mail**, insira o domínio de e-mail da sua organização a ser registrado.

4 Na caixa de texto **Confirmação do Endereço de E-mail**, insira um endereço de e-mail nesse domínio de e-mail para receber o token de verificação.

5 Clique em **OK**.

O status deste registro de domínio de e-mail está marcado Pendente. Você pode ter apenas um domínio de e-mail pendente por vez.

6 Navegue até o e-mail e copie o token de ativação que está na mensagem.

7 Retorne à página **Gerenciamento de Identidade e Acesso > Descoberta Automática** e cole o token na caixa de texto Token de Ativação

8 Clique em **Verificar** para registrar o domínio.

O domínio de e-mail é registrado e adicionado à lista de domínios de e-mail registrados na página Descoberta Automática.

Os usuários finais já podem inserir seu endereço de e-mail no aplicativo do Workspace ONE para acessar seu portal de aplicativos.

Próximo passo

Se você tiver mais de um domínio de e-mail, adicione outro domínio de e-mail a ser registrado.

Configuração de autenticação de sessão

O serviço do VMware Identity Manager possui uma política de acesso padrão que controla o acesso do usuário aos recursos do VMware Identity Manager.

A duração da sessão de autenticação configurada nas regras da política determina a quantidade máxima de tempo que os usuários têm, desde o seu último evento de autenticação, para acessar a página do inicializador de aplicativos ou para inicializar um aplicativo Web específico. O padrão é de oito horas. Após a autenticação dos usuários, eles têm oito horas para inicializar um aplicativo da Web, a menos que eles inicializem outro evento de autenticação que estenda o tempo.

Você pode editar a política padrão para alterar a duração da sessão do console do VMware Identity Manager, guia Gerenciamento de Identidade e Acesso, Gerenciar > Políticas. Consulte o guia Administração do VMware Identity Manager, Gerenciando políticas de acesso.

Habilitando a verificação de conformidade para dispositivos gerenciados do Workspace ONE UEM

Quando os usuários inscrevem seus dispositivos, as amostras que contêm os dados utilizados para a avaliação de conformidade são enviadas com base em uma programação. A avaliação desses dados de amostra garante que o dispositivo respeite as regras de conformidade estabelecidas pelo administrador no console do Workspace ONE UEM (UEM). Se o dispositivo não estiver em conformidade com essas regras, serão tomadas as ações correspondentes configuradas no console do UEM.

O serviço do VMware Identity Manager inclui uma opção de políticas de acesso que pode ser configurada para verificar o servidor do Workspace ONE UEM para o status de conformidade do dispositivo quando os usuários fazem login no dispositivo. A verificação de conformidade garante que os usuários serão impedidos de fazer logon ou de usar o single sign-on no portal do Workspace ONE se o dispositivo não estiver em conformidade. Quando o dispositivo estiver em conformidade novamente, restaura-se a capacidade de login.

O aplicativo do Workspace ONE faz logoff e bloqueia automaticamente o acesso aos aplicativos se o dispositivo estiver comprometido. Se o dispositivo tiver sido inscrito através do gerenciamento adaptativo, um comando de limpeza de dados corporativos (enterprise wipe) emitido através do console do UEM cancelará a inscrição do dispositivo e removerá os aplicativos gerenciados do dispositivo. Os aplicativos não gerenciados não são removidos.

Para obter mais informações sobre as políticas de conformidade do Workspace ONE UEM, consulte o Guia de Gerenciamento de Dispositivos Móveis do VMware Workspace ONE UEM, nas páginas de Documentação do VMware Workspace ONE UEM.

Estratégias de implantação para configurar vários grupos organizacionais do Workspace ONE UEM

O Workspace ONE UEM usa grupos organizacionais (GO) para identificar usuários e estabelecer permissões. Quando o Workspace ONE UEM está integrado ao VMware Identity Manager, as chaves da REST API do usuário de inscrição e administrador são configuradas no tipo de grupo organizacional do Workspace ONE UEM chamado Cliente.

Quando os usuários fazem logon no Workspace ONE de um dispositivo, um evento de registro do dispositivo é acionado no VMware Identity Manager. Uma solicitação é enviada para o Workspace ONE UEM para efetuar pull de todos os aplicativos que a combinação de usuário e dispositivo tem direito. A solicitação é enviada usando a REST API para localizar o usuário no Workspace ONE UEM e para colocar o dispositivo no grupo organizacional apropriado.

Para gerenciar grupos organizacionais, é possível configurar duas opções no VMware Identity Manager.

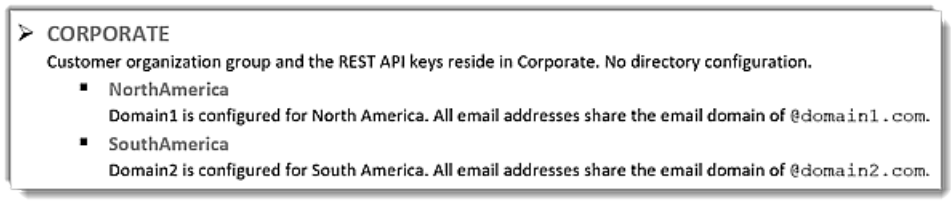
- Habilitar a detecção automática do Workspace ONE UEM.
- Mapeie os grupos organizacionais do Workspace ONE UEM para domínios no serviço do VMware Identity Manager.

Se nenhuma dessas duas opções estiver configurada, o Workspace ONE tentará localizar o usuário no grupo organizacional onde a chave da REST API foi criada. Esse é o grupo Cliente.

Usando a detecção automática do Workspace ONE UEM

Configure a Detecção Automática quando um único diretório estiver configurado em um grupo herdeiro para o Grupo organizacional do cliente ou quando vários diretórios estiverem configurados abaixo do grupo Cliente com domínios de e-mail exclusivos.

Figura 7-1. Exemplo 1



No exemplo 1, o domínio de e-mail da organização está registrado para detecção automática. Os usuários digitam apenas seu endereço de e-mail na página de logon do Workspace ONE.

Neste exemplo, quando os usuários no domínio NorthAmerica fazem logon no Workspace ONE, eles digitam o endereço de e-mail completo como user1@domain1.com. O aplicativo procura o domínio e verifica se o usuário existe ou pode ser criado com uma chamada de diretório no grupo organizacional NorthAmerica. O dispositivo pode ser registrado.

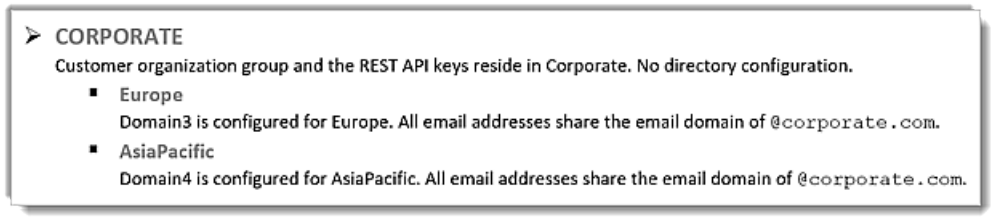
Usando mapeamento de grupo organizacional do Workspace ONE UEM para domínios do VMware Identity Manager

Configure o serviço do VMware Identity Manager para o mapeamento do grupo organizacional do Workspace ONE UEM quando vários diretórios são configurados com o mesmo domínio de e-mail. Você habilita **Mapear Domínios para Vários Grupos de Organizações** na página de configuração da AirWatch no console do VMware Identity Manager.

Quando a opção Mapear Domínios para Vários Grupos de Organizações está habilitada, os domínios configurados no VMware Identity Manager podem ser mapeados para os IDs de grupos organizacionais do Workspace ONE UEM. A chave da REST API de administrador também é necessária.

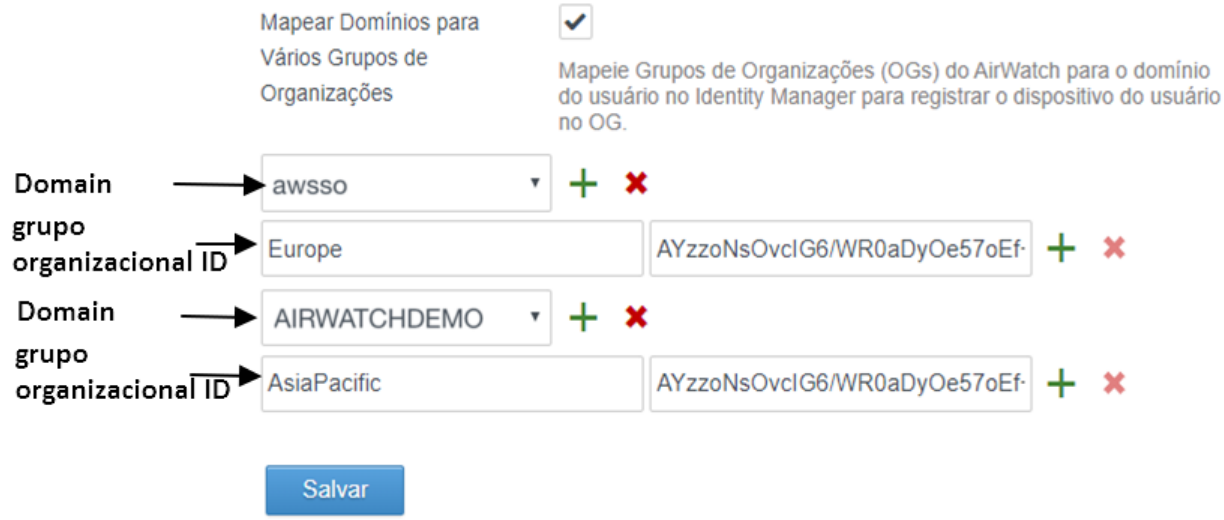
No exemplo 2, dois domínios são mapeados para diferentes grupos organizacionais. É necessária uma chave da REST API de administrador. A mesma chave da REST API de administrador é usada para ambas as IDs do grupo organizacional.

Figura 7-2. Exemplo 2



Na página de configuração da AirWatch no console do VMware Identity Manager, configure um ID específico do grupo organizacional do Workspace ONE UEM para cada domínio.

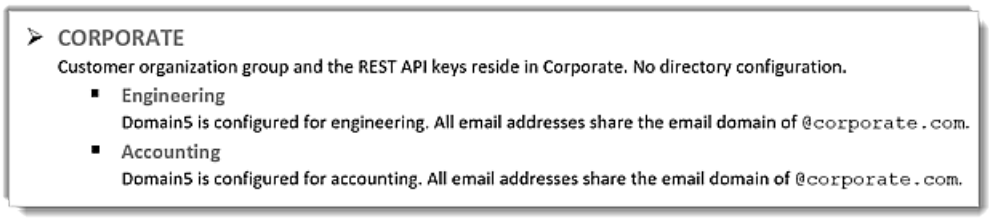
Figura 7-3. Exemplo 2: Configuração do grupo organizacional



Com esta configuração, quando os usuários fazem logon no Workspace ONE do seu dispositivo, a solicitação de registro do dispositivo tenta localizar usuários do Domain3 no grupo organizacional Europe e usuários do Domain4 no grupo organizacional AsiaPacific.

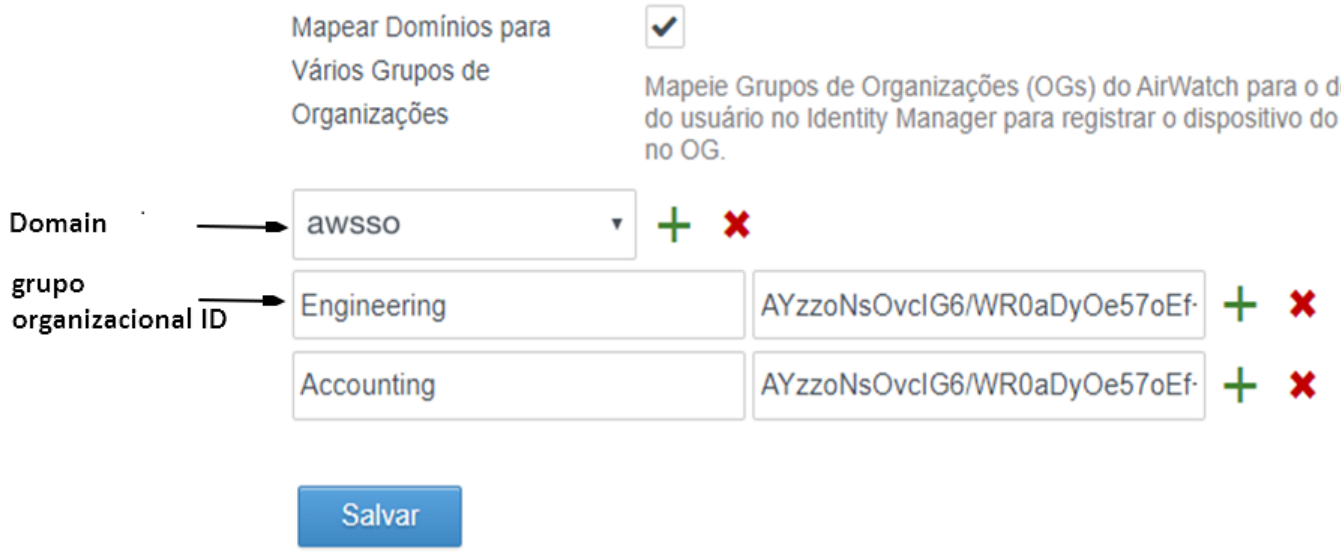
No exemplo 3, um domínio é mapeado para vários grupos organizacionais do Workspace ONE UEM. Ambos os diretórios compartilham o domínio de e-mail. O domínio aponta para o mesmo grupo organizacional do Workspace ONE UEM.

Figura 7-4. Exemplo 3



Nesta configuração, quando os usuários fazem logon no Workspace ONE, o aplicativo solicita que os usuários selecionem o grupo em que eles desejam se registrar. Neste exemplo, os usuários podem selecionar Engenharia ou Contabilidade.

Figura 7-5. Grupos organizacionais onde os diretórios compartilham o mesmo domínio



Colocando os dispositivos no grupo organizacional correto

Quando um registro de usuário é localizado com êxito, o dispositivo é adicionado ao grupo organizacional apropriado. O **Modo de Atribuição de ID de Grupo** da configuração de inscrição do Workspace ONE UEM determina o grupo organizacional a colocar o dispositivo. Essa configuração está na página Configurações do Sistema > Dispositivo e Usuários > Geral > Inscrição > Agrupamento no Workspace ONE UEM Console.

Figura 7-6. Inscrição do grupo do Workspace ONE UEM para dispositivos

No exemplo 4, todos os usuários estão no nível do grupo organizacional Corporação.

Figura 7-7. Exemplo 4

A colocação do dispositivo depende da configuração selecionada para o Modo de Atribuição de ID de Grupo no grupo organizacional Corporação.

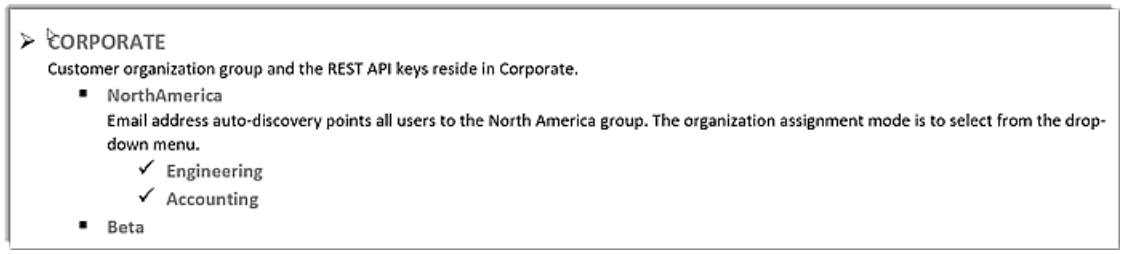
- Se Padrão for selecionado, o dispositivo será colocado no mesmo grupo onde o usuário está localizado. Para o exemplo 4, o dispositivo é colocado no grupo Corporação.
- Se a opção Avisar Usuário para Selecionar ID de Grupo for selecionada, os usuários serão solicitados a selecionar qual grupo registrar seu dispositivo. Para o exemplo 4, os usuários veem um menu suspenso no aplicativo Workspace ONE com Engenharia e Contabilidade como opções.
- Se a opção Selecionado Automaticamente com Base no Grupo de Usuários for selecionada, os dispositivos serão colocados em Engenharia ou Contabilidade com base na atribuição do grupo de usuários e no mapeamento correspondente no console do Workspace ONE UEM.

Entendendo o conceito de um grupo oculto

No exemplo 4, quando os usuários são solicitados a selecionar um grupo organizacional para se registrar, os usuários também podem digitar um valor de ID de grupo que não esteja na lista apresentada no aplicativo Workspace ONE. Este é o conceito de um grupo oculto.

No exemplo 5, na estrutura do grupo organizacional Corporação, América do Norte e Beta são configurados como grupos em Corporação.

Figura 7-8. Exemplo 5



No exemplo 5, os usuários digitam seu endereço de e-mail no Workspace ONE. Após a autenticação, os usuários mostram uma lista que exibe Engenharia e Contabilidade para escolher. Beta não é uma opção exibida. Se os usuários conhecem a ID do grupo organizacional, eles poderão digitar manualmente Beta na caixa de texto da seleção do grupo e registrar com êxito seu dispositivo em Beta.

Trabalhando no portal do Workspace ONE

8

Quando um aplicativo Workspace ONE é instalado em dispositivos, os usuários podem fazer logon no Workspace ONE para acessar com segurança um catálogo de aplicativos que a sua organização habilitou para eles. Quando o aplicativo é configurado com o single sign-on, os usuários não precisam reinserir as credenciais de login quando inicializarem o aplicativo.

A interface do usuário do Workspace ONE funciona de forma semelhante em telefones, tablets e desktops. A página Catálogo no Workspace ONE mostra os recursos que foram enviados por push para o Workspace ONE. Os usuários podem tocar ou clicar para pesquisar, adicionar, marcar e atualizar aplicativos. Eles podem clicar com o botão direito do mouse em um aplicativo para removê-lo da página Marcado e ir para a página Catálogo para adicionar recursos com autorização.

Este capítulo inclui os seguintes tópicos:

Trabalhando com aplicativos no Workspace ONE

O portal do usuário do Workspace ONE é composto por uma guia Catálogo e uma guia Indicadores. Quando os usuários fazem login no seu portal do Workspace ONE pela primeira vez, a guia Catálogo é exibida se a guia Indicadores está vazia.

Após a primeira inicialização, os usuários são levados diretamente para a última guia visitada. Se os usuários preferirem inicializar a partir da guia Catálogo, eles poderão usar a exibição Catálogo.

Você pode ocultar a guia Catálogo ou Indicadores no portal do Workspace ONE para fornecer uma experiência de usuário específica às suas necessidades. Você pode alterar a configuração do portal na página Catálogo > Configurações > Configuração do Portal do Usuário do console do VMware Identity Manager.

Figura 8-1. Visualização inicial da página de Indicadores

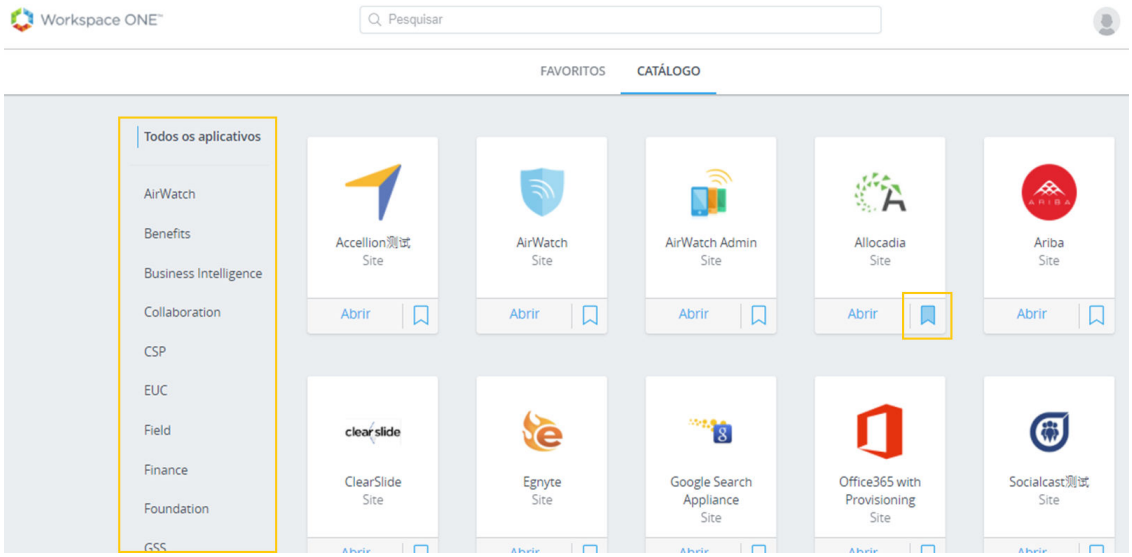
No catálogo, os usuários podem instalar os aplicativos Web, móveis e virtuais autorizados. Os aplicativos Web e virtuais podem ser abertos diretamente da página Catálogo ou Favoritos no aplicativo Workspace ONE.

Aplicativos nativos, como iOS e Android, não podem ser adicionados aos favoritos ou inicializados a partir das páginas do Workspace ONE. Esses aplicativos são inicializados a partir do springboard iOS ou Android.

Na página Catálogo, você pode organizar os aplicativos em categorias lógicas para facilitar para os usuários localizarem os recursos necessários. Uma categoria, chamada Recomendado, está listada por padrão. Quando você categoriza aplicativos como Recomendado, pode ativar a opção **Mostrar aplicativos recomendados na guia Indicadores** para preencher a página Indicadores com esses aplicativos.

Com essa configuração, os usuários terão acesso imediato a aplicativos recomendados quando eles fazem login pela primeira vez no portal do Workspace ONE.

Figura 8-2. Página Catálogo do Workspace ONE



Observação Os aplicativos móveis não estão disponíveis nos navegadores do desktop.

Os usuários podem inicializar aplicativos Web da seguinte forma:

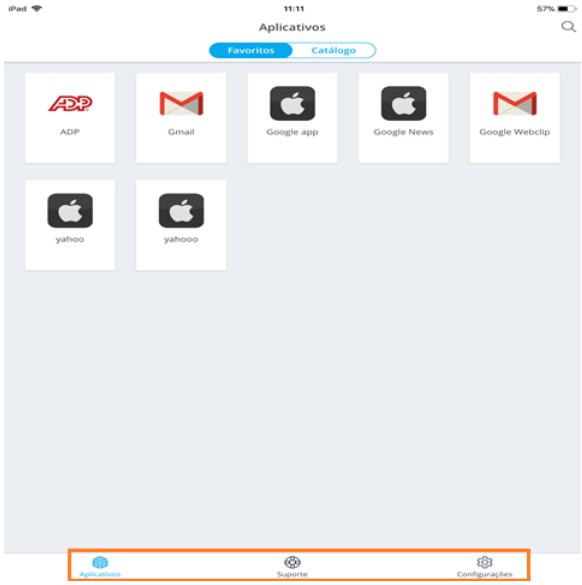
- Na guia Indicadores. Os usuários clicam no ícone do aplicativo para inicializá-lo.
- Na guia Catálogo. Os usuários clicam na caixa com o ícone de seta para abrir o aplicativo.
- Na Pesquisa em Destaque ou na Pesquisa no Workspace ONE. Na Pesquisa em Destaque em dispositivos iOS, os usuários selecionam o ícone do aplicativo na lista. Na pesquisa no Workspace ONE, os usuários clicam na caixa com o ícone de seta para abrir o aplicativo.

Os usuários podem acessar as configurações do Workspace ONE na seta suspensa ao lado do nome.

- Conta. As informações de perfil do usuário, incluindo seu nome, nome de usuário e endereço de e-mail.
- Dispositivos. A lista de dispositivos que fizeram logon no aplicativo Workspace ONE e a última data e hora de logon.
- Dicas de aplicativo. Dicas sobre como navegar no Workspace ONE a partir do dispositivo do usuário.
- Sobre. Informações de direitos autorais, patentes e licenças do Workspace ONE.
- Preferências. A configuração de inicialização padrão, quando os aplicativos remotos do Horizon são acessados, visualiza o aplicativo do Horizon Client ou de um navegador.

Os usuários tocam no ícone do aplicativo Workspace ONE em seus dispositivos para fazer logon no portal dos seus aplicativos. Se eles tiverem marcados aplicativos, a página Indicadores será exibida. O aplicativo Workspace ONE em dispositivos inclui links para Suporte e para Configurações.

Figura 8-3. Visualização do dispositivo no portal do Workspace ONE



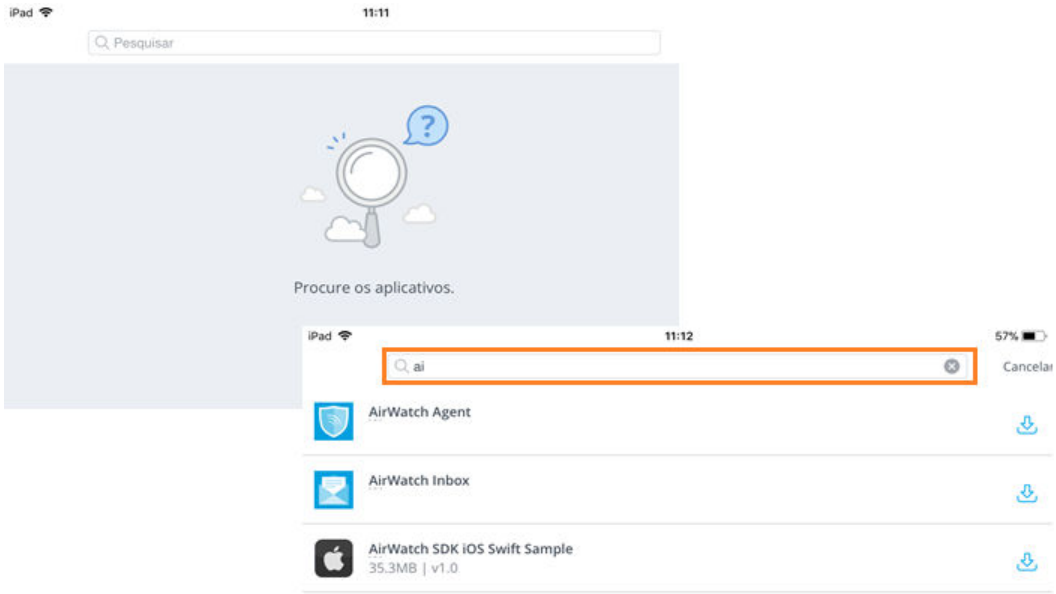
- A página de Suporte inclui um link para Dispositivos e para Enviar Relatório. A página Dispositivos mostra quando eles fizeram o último logon no dispositivo. A opção Enviar Relatório oferece ao usuário uma forma de enviar informações de diagnóstico ou outros comentários para você. Os usuários podem desativar ou ativar esse recurso nas configurações do dispositivo.
- A página Configurações mostra a versão do aplicativo Workspace ONE e a política de privacidade do VMware Workspace. Os usuários podem remover a conta da página Configurações para sair do aplicativo Workspace ONE.

Usando a pesquisa no Workspace ONE

Os usuários podem usar a pesquisa no Workspace ONE para encontrar aplicativos por nome ou por categoria.

À medida que os usuários digitam na caixa de texto de pesquisa, os aplicativos que correspondem à entrada são exibidos.

Figura 8-4. Pesquisar mostrando os resultados



Os usuários podem iniciar um aplicativo Web ou baixar um aplicativo nativo diretamente dos resultados da pesquisa.

Nos dispositivos iOS, os usuários podem usar Destaque para procurar aplicativos que estejam no portal do Workspace ONE. Na tela inicial do dispositivo iOS, toque na tela e arraste para baixo para revelar o campo de pesquisa Destaque. Quando os usuários digitam um nome de aplicativo que está no seu portal do Workspace ONE, o Workspace ONE abre e o aplicativo é iniciado.

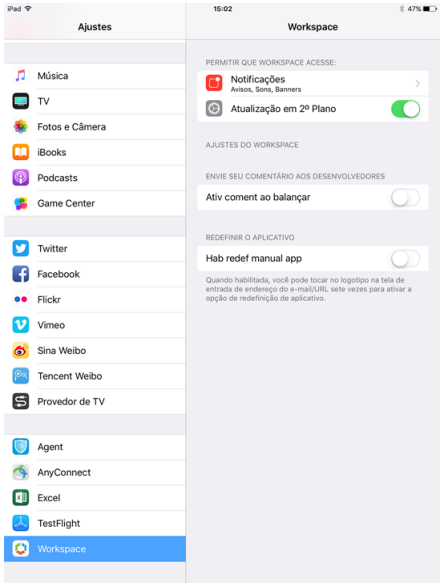
Ajudar os usuários a relatar problemas de dispositivos iOS

Para dispositivos iOS, o recurso Rage Shake pode ser usado para enviar logs para desenvolvedores de aplicativos iOS.

Por padrão, os usuários agitam seu dispositivo e ele registra seu estado atual e envia detalhes em uma mensagem de e-mail aos desenvolvedores de aplicativos do Workspace ONE. Os usuários podem digitar manualmente outro e-mail para enviar as informações para outro endereço.

Os usuários podem ativar o recurso Habilitar Comentários no recurso Agitar na página Configurações > Espaço de Trabalho no seu dispositivo. Os usuários podem usar o Rage Shake de qualquer tela no portal do Workspace ONE para enviar um relatório.

Figura 8-5. Habilitar comentários no recurso Agitar



Quando um dispositivo iOS recebe uma mensagem de erro que é semelhante a `este dispositivo está registrado para outro usuário ou ambiente`, a opção Redefinição de Aplicativo Manual pode ser usada para apagar todos os dados do aplicativo armazenados localmente no dispositivo.

Configurar códigos de acesso para o aplicativo Workspace ONE

Os usuários devem habilitar o recurso de código de acesso de bloqueio em seus dispositivos. Se ele não estiver habilitado, na primeira vez que o aplicativo do Workspace ONE for inicializado, os usuários são convidados a criar um código de acesso. Este código de acesso é inserido sempre que os usuários acessam o Workspace ONE dos seus dispositivos.

Se o recurso de código de acesso não for usado, os usuários serão solicitados a criar um código de acesso antes que eles possam acessar o aplicativo Workspace ONE. Depende da plataforma o nível em que o código de acesso é definido. Para dispositivos Android, o código de acesso é definido no nível do aplicativo. Para dispositivos de área de trabalho do Windows e para dispositivos iOS que usam o Workspace ONE 3.2 ou anterior, o código de acesso é definido no nível do dispositivo.

Observação Os dispositivos iOS e Android também oferecem suporte à funcionalidade de detecção de impressões digitais Touch ID.

O Workspace ONE pode detectar possíveis problemas de segurança nos dispositivos. Se os usuários desativarem o código de acesso no dispositivo, na próxima vez que acessarem o aplicativo Workspace ONE, eles serão convidados a definir um código de acesso antes que possam acessar o Workspace ONE Se um código de acesso no nível de aplicativo estiver ativado, os usuários finais não poderão desativar o seu código de acesso no nível de aplicativo.

Códigos de acesso de aplicativo em dispositivos iOS

Você pode criar códigos de acesso mais complexos do que o código de acesso do dispositivo com no mínimo quatro dígitos. O código de acesso de aplicativo pode ser compartilhado com outros aplicativos de produtividade, por exemplo, o VMware Boxer.

Você pode designar o requisito de código de acesso local para um aplicativo no console do Workspace ONE UEM. Vá a Grupos e Configurações > Todas as Configurações > Aplicativos > Configurações e Políticas > Políticas de Segurança > Tipo de Autenticação.

Quando a autenticação de código de acesso estiver configurada, será solicitado que os usuários definam um código de acesso de aplicativo, se não houver outros aplicativos de produtividade, ou será solicitado que eles insiram o código de acesso compartilhado com outros aplicativos de produtividade.

Se a autenticação do código de acesso não estiver configurada, será preciso um código de acesso do dispositivo nos dispositivos iOS.

Adicionando aplicativos nativos

Os aplicativos nativos são programas de aplicativo desenvolvidos para um dispositivo móvel específico. Os usuários conseguem ver os aplicativos nativos autorizados do Workspace ONE UEM na página Catálogo do Workspace ONE. Por exemplo, caso um usuário esteja visualizando o catálogo em um dispositivos iOS, serão exibidos apenas os aplicativos iOS autorizados ao usuário.

Na página Catálogo, os usuários tocam em Instalar para instalar o aplicativo em seus dispositivos. Ao tocar em Instalar, aparece um pop-up para permitir que o usuário saiba o acontecerá em seguida. As informações exibidas são baseadas no tipo de aplicativo e na plataforma. Os aplicativos que exibem um ícone de cadeado exigem que o dispositivo seja gerenciado pelo Workspace ONE UEM. Quando um usuário final tenta baixar um aplicativo com um ícone de cadeado, ele recebe uma mensagem que diz `Installation of this app requires enablement of Workspace Services`.

Usando o VMware Verify para autenticação de usuário

Quando o serviço do VMware Verify estiver habilitado como o segundo método de autenticação para autenticação de dois fatores para fazer logon no Workspace ONE do seu dispositivo, os usuários devem baixar o aplicativo VMware Verify da loja de aplicativos do dispositivo.

A primeira vez que os usuários fizerem logon no aplicativo Workspace ONE, eles devem digitar seu nome de usuário e senha. Quando o nome de usuário e a senha são verificados, os usuários são solicitados a digitar o número de telefone do dispositivo para se inscreverem no serviço do VMware Verify.

Ao clicarem em **Inscrever**, o número de telefone do dispositivo é registrado no serviço do VMware Verify. Se não baixaram o aplicativo VMware Verify, eles serão solicitados a baixar o aplicativo.

Quando o aplicativo é instalado, os usuários são solicitados a inserir o mesmo número de telefone que foi inserido antes e a selecionar um método de notificação para receber um código de registro único. O código de registro é inserido na página do pin de registro.

Depois que o número de telefone do dispositivo estiver registrado, os usuários poderão usar uma senha única baseada em tempo exibida no aplicativo VMware Verify para entrar no Workspace ONE. A senha é um número exclusivo que é gerado no dispositivo e está em constante mudança.

Os usuários podem registrar mais de um dispositivo. A senha do VMware Verify é sincronizada automaticamente com cada um dos dispositivos registrados.

Enviar alertas para usuários do Workspace ONE

Os administradores podem notificar os usuários do Workspace ONE sobre as futuras inatividades do sistema e o status de conformidade para solicitar ações ou enviar alertas. As notificações são enviadas por meio do console do Workspace ONE UEM.

Os usuários gerenciam como eles recebem notificações de seus dispositivos.

Trabalhando com o Workspace ONE para dispositivos Android

Os seguintes tipos de aplicativos podem ser ativados através do aplicativo Workspace ONE no Android.

- Aplicativos Web
- Aplicativos remotos habilitados no serviço do VMware Identity Manager. Por exemplo, aplicativos virtuais do Horizon, do Citrix XenApp e do ThinApp.
- Aplicativos nativos, gerenciados e não gerenciados. Aplicativos nativos são aplicativos Android desenvolvidos para plataforma Android. Estão disponíveis dois tipos.
  - Aplicativos públicos que são distribuídos do Google Play Store.
  - Aplicativos internos que são distribuídos de forma privada através do Workspace ONE UEM e não estão disponíveis no Google Play Store.

  Aplicativos Web abertos em um navegador. Os usuários podem acessar aplicativos virtuais através do VMware Horizon Client ou do Citrix Receiver.

Registrando o aplicativo Workspace ONE de dispositivos Android

Fazer login no aplicativo Workspace ONE com credenciais e URL de servidor válidas permite aos usuários acessar o catálogo unificado do Workspace ONE. No catálogo unificado, os usuários podem visualizar todos os aplicativos atribuídos.

Os usuários devem se registrar no aplicativo Workspace ONE para acessar os aplicativos. No estado registrado do Workspace ONE, os usuários podem usar aplicativos Web e virtuais que são habilitados através do VMware Identity Manager, aplicativos de produtividade do Workspace ONE UEM e aplicativos SDK sem gerenciamento.

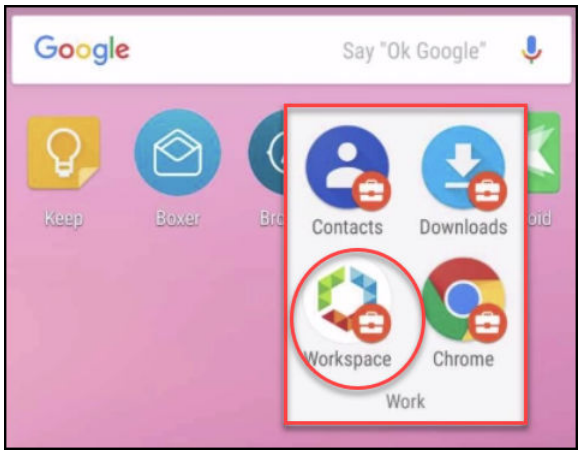
Observação Os aplicativos SDK são contidos e gerenciados através do Workspace ONE UEM SDK e não exigem que o dispositivo seja gerenciado.

Os usuários podem iniciar o gerenciamento adaptativo, que habilita o Android for Work no dispositivo e permite perfis, políticas e distribuição de aplicativos melhorada para o dispositivo.

Gerenciando o Android for Work com o Workspace ONE

Habilitar o Android for Work em dispositivos separa dados pessoais dos dados de trabalho a nível do sistema operacional. O Android for Work cria uma clara separação entre aplicativos pessoais e de trabalho. O Android for Work cria os aplicativos de trabalho com um selo distinto de trabalho do Android.

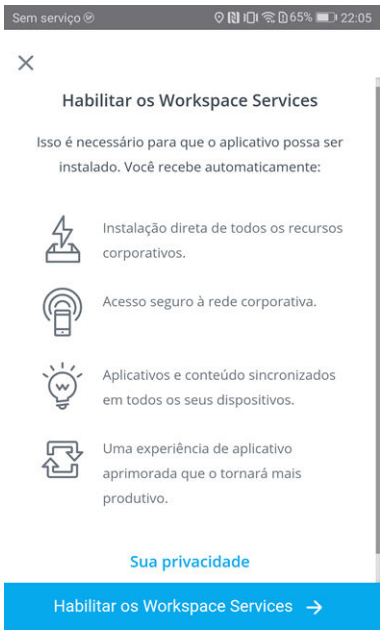
Figura 8-6. Android para conteúdo de trabalho



Os administradores determinam quais aplicativos no catálogo exigem que um dispositivo seja gerenciado antes que o aplicativo possa ser acessado. Os aplicativos no catálogo que exigem gerenciamento exibem um símbolo de estrela distinto ao lado do botão de download.

Quando os usuários tentam baixar um desses aplicativos, eles recebem uma mensagem de que o aplicativo exige que o dispositivo seja gerenciado. É exibida uma tela que descreve os recursos e os benefícios do gerenciamento de dispositivos.

Figura 8-7. Página de introdução do Workspace Services



Quando os usuários concordam em habilitar o gerenciamento do Android for Work, eles são guiados pelo processo para configurar o gerenciamento. Depois que o dispositivo é gerenciado, o contêiner do Android for Work é criado no dispositivo.

Usando o catálogo do Workspace ONE

9

Quando Workspace ONE UEM e VMware Identity Manager são integrados, o catálogo de aplicativos do Workspace ONE é o repositório de todos os recursos que você pode autorizar aos usuários. Os usuários podem acessar aplicativos empresariais que você gerencia no catálogo do Workspace ONE com base nas configurações estabelecidas para o aplicativo.

Os aplicativos na Nuvem, Móveis e Windows podem ser acessados do catálogo. Os aplicativos nativos desenvolvidos internamente ou que estão publicamente disponíveis em lojas de aplicativos poderão ser disponibilizados para seus usuários finais pelo portal do Workspace ONE.

Nas páginas de Catálogo do Workspace ONE, você pode realizar as seguintes tarefas:

- Adicionar novos recursos ao seu catálogo
- Visualizar os recursos aos quais você pode autorizar os usuários atualmente
- Acessar informações sobre cada recurso em seu catálogo

Alguns aplicativos Web podem ser adicionados ao seu catálogo diretamente das páginas de Catálogo. Outros tipos de recursos exigem que você aja fora do console administrativo. Consulte o guia Configurando recursos do VMware Identity Manager para obter informações sobre como configurar recursos.

Gerenciando recursos no Catálogo

Antes de poder autorizar um recurso específico aos usuários, você deve preencher o seu catálogo com esse recurso. O método utilizado para o preenchimento do seu catálogo com um recurso depende do tipo de recurso.

Os tipos de recursos que você pode definir em seu catálogo para qualificação e distribuição aos usuários são aplicativos Web, aplicativos Windows capturados como pacotes do VMware ThinApp, pools de desktops do Horizon Client e aplicativos virtuais do Horizon ou aplicativos com base no Citrix.

Para integrar e ativar pools de áreas de trabalho e aplicativos do Horizon Client, recursos publicados Citrix ou aplicativos empacotados do ThinApp, use o recurso Coleção de Aplicativos Virtuais disponível no menu suspenso da guia Catálogo.

Para obter informações, requisitos, instalação e configuração desses recursos, consulte *Configurando recursos no VMware Identity Manager*.

Adicionando aplicativos Web ao catálogo da sua organização

Você pode adicionar aplicativos Web ao seu catálogo selecionando-os no catálogo de aplicativos da nuvem ou criando novos.

O catálogo de aplicativos da nuvem contém aplicativos Web empresariais comumente usados. Esses aplicativos são configurados parcialmente e você deve fornecer informações adicionais para concluir o registro do aplicativo. Também é possível que você precise trabalhar com seus representantes de conta de aplicativo da Web para completar outras configurações que se façam necessárias.

Muitos dos aplicativos no catálogo de aplicativos da nuvem usam SAML 2.0 ou 1.1 para trocar dados de autenticação e autorização para permitir single sign-on do Workspace ONE no aplicativo Web.

Quando você cria um aplicativo, precisa inserir todas as informações de configuração do aplicativo. A configuração varia de acordo com o tipo de aplicativo que você está adicionando. Para aplicativos sem um protocolo de federação, solicite apenas uma URL de Destino.

Os aplicativos de quaisquer provedores de identidade de terceiros que você configurou como origens do aplicativo no VMware Identity Manager são adicionados como novos aplicativos.

Ao adicionar um aplicativo, você também pode selecionar uma política de acesso para controlar o acesso do usuário ao aplicativo. Uma política de acesso padrão está disponível, e você também pode criar novas políticas na página Gerenciamento de Identidade e Acesso > Gerenciar > Políticas. Consulte *Administração do VMware Identity Manager* para obter informações sobre as políticas de acesso.

Agrupando recursos em categorias

Você pode organizar os recursos em categorias lógicas para facilitar para os usuários a localização do recurso necessário no seu portal Workspace ONE.

Ao criar categorias, considere a estrutura da sua organização, a função de trabalho dos recursos e o tipo de recurso. Você pode atribuir mais de uma categoria a um recurso. Por exemplo, você pode criar uma categoria chamada Associado de Vendas e outra categoria chamada Recursos de Vendas da Equipe. Atribua Associado de Vendas a todos os recursos de vendas no seu catálogo. Atribua também Recursos de Vendas da Equipe a recursos de vendas específicos que são compartilhados apenas com os associados da equipe.

Após ter criado uma categoria, você poderá aplicar essa categoria a qualquer um dos recursos do catálogo. É possível aplicar várias categorias ao mesmo recurso.

Quando os usuários fazem logon no portal Workspace ONE, eles veem as categorias que você habilitou para exibição.

Consulte o guia Administração do VMware Identity Manager, Gerenciando o catálogo.

Identidade visual personalizada para serviços do VMware Identity Manager

10

Você pode personalizar os logotipos, as fontes e o plano de fundo que aparecem no console do VMware Identity Manager, nas telas de logon do usuário e do administrador, na exibição da Web do portal de aplicativos do Workspace ONE e na exibição da Web do aplicativo Workspace ONE em dispositivos móveis.

Você pode usar a ferramenta de personalização para que as interfaces reflitam a aparência das cores, dos logotipos e do design de sua empresa.

Este capítulo inclui os seguintes tópicos:

Personalizar a identidade visual no serviço do VMware Identity Manager

Você pode adicionar o nome da sua empresa, o nome do produto e o favicon à barra de endereço do console de administração e do portal do usuário. Você também pode personalizar a página de login para definir as cores do plano de fundo para corresponder às cores da sua empresa e ao design do logotipo.

Procedimentos

1. Na guia Gerenciamento de Identidade e Acesso do console do VMware Identity Manager, selecione **Configuração > Identidade Visual Personalizada**.
2. Edite as seguintes configurações no formulário, conforme apropriado.

Campo do formulário	Descrição
	Guia Nomes e Logos
Nome da Empresa	Nome da Empresa aplica-se tanto aos dispositivos móveis quanto aos de desktop. Você pode adicionar o nome da sua empresa como o título que aparece na guia do navegador. Digite o novo nome de empresa por cima do nome existente para alterá-lo.
Nome do produto	Nome do Produto aplica-se tanto aos dispositivos móveis quanto aos de desktop. O nome do produto aparece após o nome da empresa na guia do navegador.

Campo do formulário	Descrição
Favicon	Um favicon é um ícone associado a um URL que é exibido na barra de endereços do navegador. O tamanho máximo da imagem do favicon é 16 x 16 px. O formato pode ser JPEG, PNG, GIF ou ICO. Clique em **Carregar** para carregar uma nova imagem que substituirá o favicon atual. Você será solicitado a confirmar a alteração. A alteração é realizada imediatamente.
	Guia Tela de Logon
Logotipo	Clique em **Carregar** para carregar um novo logotipo que substituirá o logotipo atual nas telas de login. Assim que você clicar em **Confirmar**, a alteração é realizada imediatamente. Recomenda-se que o tamanho mínimo da imagem a ser carregada seja 350 x 100 px. Se você carregar imagens maiores que 350 x 100 px, elas serão dimensionadas para o tamanho 350 x 100 px. O formato pode ser JPEG, PNG ou GIF.
Cor do Plano de Fundo	A cor que aparece no plano de fundo da tela de login. Digite o código de cor hexadecimal de seis dígitos por cima do código existente para mudar a cor do plano de fundo.
Cor do Plano de Fundo da Caixa	A cor da caixa da tela de login pode ser personalizada. Digite o código de cor hexadecimal de seis dígitos por cima do código existente.
Cor do plano de fundo do botão de logon	A cor do botão de login pode ser personalizada. Digite o código de cor hexadecimal de seis dígitos por cima do código existente.
Cor do texto do botão de logon	A cor do texto que aparece no botão de login pode ser personalizada. Digite o código de cor hexadecimal de seis dígitos por cima do código existente.

Após personalizar a tela de login, você poderá ver as alterações no painel de Visualização antes de salvá-las.

3 Clique em **Salvar**.

As atualizações de identidade visual personalizada no console do VMware Identity Manager e nas páginas de logon são aplicadas dentro de cinco minutos após você clicar em Salvar.

Próximo passo

Verifique a aparência das alterações de identidade visual nas diversas interfaces.

Atualize a aparência do portal Workspace ONE e das exibições Móvel e Tablet do usuário final. Consulte Personalizar a identidade visual do portal do usuário

Personalizar a identidade visual do portal do usuário

Você pode adicionar um logotipo, alterar as cores do plano de fundo e adicionar imagens para personalizar o portal Workspace ONE.

Procedimentos

1 Na guia Catálogos do console do VMware Identity Manager, selecione **Configurações > Identidade Visual do Portal do Usuário**.

2 Edite as configurações no formulário, conforme apropriado.

Item do formulário	Descrição
Logotipo	Adicione um logotipo na manchete para ser a faixa na parte superior das páginas da Web do portal Workspace ONE e do console do VMware Identity Manager. O tamanho máximo da imagem é 220 x 40 px. O formato pode ser JPEG, PNG ou GIF.
	Portal
Cor do plano de fundo da manchete	Digite o código de cor hexadecimal de seis dígitos por cima do código existente para mudar a cor do plano de fundo da manchete. A cor do plano de fundo muda na tela de visualização do portal de aplicativos quando se digita um novo código de cor.
Cor do texto da manchete	Digite o código de cor hexadecimal de seis dígitos por cima do código existente para mudar a cor do texto da manchete.
Cor do Plano de Fundo	A cor que aparece no plano de fundo da tela do portal da Web. Digite um novo código de cor hexadecimal de seis dígitos por cima do código existente para mudar a cor do plano de fundo. A cor do plano de fundo muda na tela de visualização do portal de aplicativos quando se digita um novo código de cor. Selecione **Realce de Plano de Fundo** para acentuar a cor do plano de fundo. Se o Realce do plano de fundo for habilitado, os navegadores que suportam múltiplas imagens de plano de fundo mostrarão a sobreposição nas páginas do inicializador e do catálogo. Selecione **Padrão do Plano de Fundo** para definir o padrão de triângulo pré-concebido na cor do plano de fundo.
Cor do Plano de Fundo do Ícone	Insira um código de cor hexadecimal de seis dígitos para alterar a caixa de cor do plano de fundo que circunda os ícones de aplicativo.
Opacidade do Plano de Fundo do Ícone	Para definir uma transparência, mova o controle deslizante na barra.
Cor do nome e do ícone	Você pode selecionar a cor do texto para os nomes listados sob os ícones nas páginas do portal de aplicativos. Digite um código de cor hexadecimal por cima do código existente para mudar a cor da fonte.
Efeito de rótulo	Selecione o tipo de rótulo a ser usado para o texto nas telas do portal Workspace ONE.
Realce de Plano de Fundo	Se estiver habilitado, em navegadores que permitem várias imagens de plano de fundo, a sobreposição de plano de fundo será exibida nas páginas de catálogo e de indicadores.
Padrão do Plano de Fundo	Se estiver habilitado, em navegadores que permitem várias imagens de plano de fundo, as sobreposições de plano de fundo serão exibidas nas páginas de catálogo e de indicadores.
Imagem (opcional)	Para adicionar uma imagem ao plano de fundo da tela do portal de aplicativos em vez de uma cor, faça upload de uma imagem.

3 Clique em **Salvar**.

As atualizações de identidade visual são renovadas a cada 24 horas para o portal do usuário. Para enviar por push as alterações mais brevemente, como administrador, abra uma nova guia e digite essa URL, substituindo seu nome de domínio por minhaemp.exemplo.com. `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

Próximo passo

Verifique a aparência das alterações de identidade visual nas diferentes interfaces.

Como acessar outros documentos

11

Ao configurar o Workspace ONE, talvez seja necessário consultar a documentação para o VMware Identity Manager e o VMware Workspace ONE UEM.

Documentações adicionais podem ser encontradas nestes centros de documentação

- VMware Workspace ONE
- VMware Workspace ONE UEM
- VMware Identity Manager