Guida alla distribuzione di VMware Workspace ONE con VMware Identity Manager

SET 2018

VMware Workspace ONE

vmware®

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:
https://docs.vmware.com/it/
Il sito Web di VMware fornisce, inoltre, gli ultimi aggiornamenti di prodotto.
In caso di commenti sulla presente documentazione, inviare un messaggio all'indirizzo:
docfeedback@vmware.com

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

VMware, Inc.
Centro Leoni Palazzo A
Via Spadolini 5
Ground Floor
Milan, MI 20121
tel: +39 02 30412700
fax: +39 02 30412701
www.vmware.com/it

Sommario

Informazioni sulla distribuzione di VMware Workspace ONE

La guida alla distribuzione di VMware Workspace™ ONE™ con VMware Identity Manager fornisce informazioni sull'integrazione di VMware Identity Manager™ e VMware Workspace ONE UEM™ mediante AirWatch per offrire il protocollo Single Sign-On a Workspace ONE, la gestione dei dispositivi in Workspace ONE UEM e VMware Workspace ONE come catalogo di applicazioni.

Quando Workspace ONE UEM e VMware Identity Manager sono integrati, gli utenti dei dispositivi registrati in Workspace ONE UEM possono accedere in modo sicuro alle applicazioni per cui sono autorizzati senza dover inserire più password.

Destinatari

Queste informazioni sono destinate agli amministratori che hanno familiarità con i servizi Workspace ONE UEM e VMware Identity Manager.

La versione di settembre 2018 si applica a VMware Identity Manager Cloud di settembre 2018, VMware Identity Manager 3.3 e Workspace ONE UEM 9.7.

Introduzione a Workspace ONE

1

VMware Workspace® ONE® è una piattaforma aziendale sicura che invia e gestisce applicazioni su dispositivi iOS, Android e Windows 10. Nella piattaforma Workspace ONE sono integrati gestione di identità, applicazioni e mobilità aziendale.

VMware Workspace ONE UEM® e VMware Identity Manager™ si integrano per fornire il catalogo di applicazioni e i servizi di gestione degli accessi mobile di Workspace ONE.

I servizi di VMware Identity Manager offrono i componenti correlati all'identità, inclusa l'autenticazione per gli utenti con accesso di tipo SSO alle proprie risorse. È possibile creare un insieme di criteri correlati alla rete e all'autenticazione per controllare gli accessi a queste risorse.

I servizi di Workspace ONE UEM forniscono iscrizione dei dispositivi, distribuzione delle applicazioni e strumenti di verifica della conformità per garantire il rispetto degli standard di sicurezza aziendale da parte dei dispositivi che accedono da remoto. Gli utenti dei dispositivi registrati in Workspace ONE UEM possono accedere in modo sicuro alle applicazioni per cui sono autorizzati senza dover inserire più password.

Questo capitolo include i seguenti argomenti:

Panoramica dell'architettura di Workspace ONE

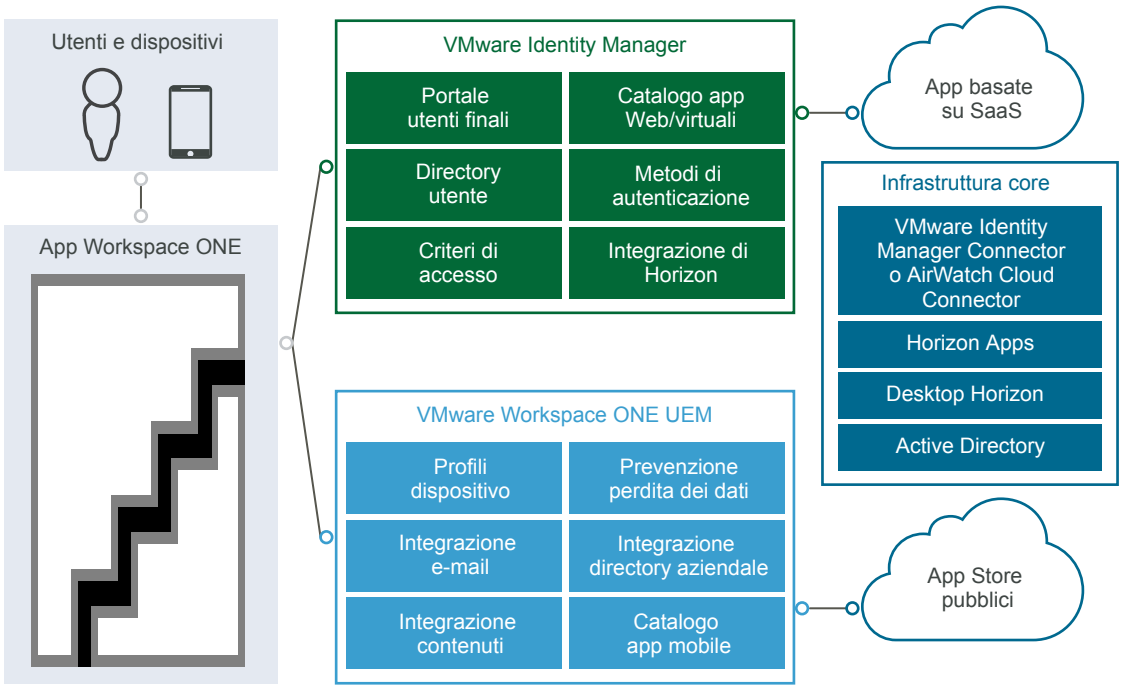
Workspace ONE fornisce agli utenti l'accesso sicuro ad applicazioni cloud, mobile e Windows gestite da un catalogo unificato. Per l'accesso del dispositivo, l'applicazione nativa Workspace ONE è disponibile per dispositivo iOS, Android e Windows 10.

Quando si distribuisce Workspace ONE, è necessario implementare i seguenti servizi di VMware Identity Manager e Workspace ONE UEM.

- È possibile configurare il componente Connettore VMware Identity Manager o il componente AirWatch Cloud Connector (ACC).

- Integrazione di Active Directory dell'azienda con VMware Identity Manager o con Workspace ONE UEM Cloud Connector per sincronizzare utenti e gruppi da Active Directory al servizio di Workspace ONE.
- Configurazione di VMware Identity Manager con le chiavi API di Workspace ONE UEM e il certificato root dell'amministratore e abilitazione del catalogo di Workspace ONE, del controllo della conformità e dell'autenticazione della password dell'utente tramite Workspace ONE UEM.

Figura 1-1. Panoramica dell'architettura di Workspace ONE



Requisiti

Di seguito sono riportati i requisiti di sistema di Workspace ONE.

Tabella 1-1. Requisiti di sistema di Workspace ONE

Requisiti di Workspace ONE	Dettagli
Active Directory	Windows Server 2008 e 2008 R2 Windows Server 2012 e 2012 R2
Browser Web per accedere alle console di VMware Identity Manager e Workspace ONE	Internet Explorer 11 per Windows Google Chrome 4.0 e versioni successive Mozilla Firefox 40 e versioni successive Safari 6.2.8 e versioni successive
VMware Identity Manager Connector o AirWatch Cloud Connector installato.	Windows Server 2008 R2 Windows Server 2012 o 2012 R2 .NET Framework 4.6.2 Per la guida all'installazione di VMware Identity Manager Connector, vedere il Centro documentazione di VMware Identity Manager. Per la Guida all'installazione di AirWatch Cloud Connector, consultare il Centro documentazione di Workspace ONE UEM.

Dettagli sulle funzionalità di Workspace ONE

Di seguito sono descritte le funzionalità principali presenti in Workspace ONE.

Applicazioni mobili native di Workspace ONE

Gli utenti possono installare l'applicazione Workspace ONE su un dispositivo mobile e utilizzare le credenziali dell'azienda per accedere mediante il protocollo Single Sign-On (SSO) alle applicazioni dell'azienda, cloud e mobile.

Catalogo di app self-service per risorse Web, Horizon e Citrix

Workspace ONE fornisce agli utenti l'accesso ad applicazioni cloud, mobile e Windows utilizzando un catalogo unificato. Il catalogo contiene applicazioni pubblicate in VMware Identity Manager e VMware Workspace ONE UEM. I tipi di applicazioni supportate includono interne, Web, SaaS, mobile native, mobile sviluppate internamente, Windows legacy e moderne, Horizon 7, VMware Horizon Cloud Service™, pubblicate Citrix e pacchetti ThinApp. Lo store di applicazioni contiene anche desktop virtualizzati.

Avvio di app Web e virtuali con Single Sign-On

Workspace ONE offre un'implementazione di accesso Single Sign-On (SSO) mobile alle applicazioni mobile, richiamabile con un singolo tocco. SSO mobile è disponibile per dispositivi Android, iOS e Windows 10.

Accesso condizionale con conformità del dispositivo

Con Workspace ONE, è possibile applicare l'accesso condizionale basato su criteri di autenticazione per intervallo di rete, piattaforma e specifici delle applicazioni. Un dispositivo deve comprovare la conformità con le regole di sicurezza prima di essere autorizzato ad accedere a un'applicazione.
VMware Identity Manager dispone di un'opzione per i criteri di accesso che può essere configurata per controllare lo stato di conformità del dispositivo nel server Workspace ONE UEM quando gli utenti accedono dal dispositivo.

Autenticazione multifattore

Workspace ONE fornisce l'autenticazione multifattore tramite l'applicazione VMware Verify. Quando un utente tenta di accedere al catalogo di Workspace ONE o a qualsiasi applicazione che richiede un'autenticazione complessa, VMware Verify invia una notifica al telefono dell'utente. Per confermare il tentativo di accesso a Workspace ONE, l'utente deve scorrere su Accetta per accedere all'applicazione.

Gestione adattiva

Per le applicazioni che richiedono solo un livello di sicurezza di base, agli utenti non viene richiesto di registrare il proprio dispositivo in Workspace ONE UEM Mobile Device Management™. Gli utenti possono scaricare l'applicazione mobile di Workspace ONE e selezionare le applicazioni che desiderano installare. Per le applicazioni che richiedono un livello di sicurezza più elevato, gli utenti possono registrare il proprio dispositivo in Workspace ONE UEM direttamente dall'applicazione mobile Workspace ONE.

Introduzione guidata di Workspace ONE

È possibile utilizzare l'Introduzione guidata di Workspace ONE per ricevere le istruzioni in modalità guidata per molte procedure di configurazione atte a integrare i servizi di Workspace ONE UEM e VMware Identity Manager e a creare l'ambiente Workspace ONE.

L'introduzione guidata non sostituisce la possibilità di configurare o modificare le singole impostazioni, ma automatizza significativamente la configurazione iniziale per la maggior parte dei clienti.

L'introduzione guidata di Workspace ONE può essere utilizzata per configurare i seguenti aspetti.

- Connector e directory dell'azienda. La procedura guidata conduce l'utente nelle operazioni da eseguire per configurare VMware Enterprise System Connector e la connessione ad Active Directory da Workspace ONE UEM Cloud Connector per importare utenti e gruppi dalla directory in uso nell'azienda. Fare riferimento alla Guida alla configurazione rapida di VMware Workspace ONE per ulteriori informazioni su come configurare il connector dell'azienda.
- Auto Discovery. Eseguire la procedura guidata per registrare il dominio di posta elettronica nel servizio di individuazione automatica e agevolare così l'accesso da parte degli utenti finali al loro portale di app tramite l'applicazione Workspace ONE. Gli utenti finali possono quindi immettere il proprio indirizzo e-mail anziché l'URL dell'organizzazione.

- Catalogo di Workspace ONE. La procedura guidata del catalogo di Workspace ONE conduce l'utente nelle operazioni necessarie per configurare il catalogo di Workspace ONE. È possibile eseguire anche il branding personalizzato di Workspace ONE per aggiungere le informazioni sul brand dell'azienda all'applicazione e al catalogo di Workspace ONE. Fare riferimento alla Guida alla configurazione rapida di VMware Workspace ONE per ulteriori informazioni su come configurare il catalogo di Workspace ONE.
- Gestione adattiva. Configurare la gestione adattiva per impedire a determinate applicazioni di richiedere l'installazione di un profilo sui dispositivi degli utenti. Il profilo garantisce la possibilità di rimuovere le applicazioni e i dati dell'azienda, se necessario. Si può anche scegliere di richiedere la gestione o l'uso di applicazioni pubbliche in maniera indipendente scaricandole manualmente dall'App Store.

L'introduzione guidata può avvisare l'utente se sono già presenti configurazioni potenzialmente in conflitto in Workspace ONE UEM o nei servizi di VMware Identity Manager. Se si verifica questa situazione, o se l'introduzione guidata completa solo parzialmente i passaggi, le funzionalità possono essere configurate manualmente. Utilizzare questa guida per configurare manualmente Workspace ONE UEM e i servizi di VMware Identity Manager per Workspace ONE.

Integrazione di Workspace ONE UEM con VMware Identity Manager

2

Per configurare i servizi di gestione mobile di Workspace ONE UEM per i dispositivi con i servizi di VMware Identity Manager per l'autenticazione Single Sign-On e la gestione dell'identità per gli utenti, è necessario integrare i servizi.

Quando Workspace ONE UEM e VMware Identity Manager sono integrati, gli utenti dei dispositivi registrati in Workspace ONE UEM possono accedere in modo sicuro a Workspace ONE per accedere alle applicazioni per cui sono autorizzati senza dover inserire più password.

L'introduzione guidata di Workspace ONE guida l'utente nei molti passaggi della procedura di configurazione per integrare Workspace ONE UEM e VMware Identity Manager. Consultare la Guida alla configurazione rapida di VMware Workspace ONE per l'esecuzione delle procedure guidate di Workspace ONE.

Questo capitolo include i seguenti argomenti:

Configurazione dell'integrazione dalla console di Workspace ONE UEM

Per l'integrazione con i servizi di VMware Identity Manager, configurare queste impostazioni nella console di Workspace ONE UEM.

- Chiave amministratore REST API per la comunicazione con il servizio VMware Identity Manager
- Chiave API utente registrato REST per l'autenticazione con password di AirWatch Cloud Connector creata nello stesso gruppo di organizzazioni in cui è configurato VMware Identity Manager.

- Account amministratore API per VMware Identity Manager e per il certificato di autenticazione amministratore esportato da Workspace ONE UEM e aggiunto alle impostazioni di AirWatch nella console di VMware Identity Manager.

Creazione di chiavi REST API in Workspace ONE UEM

L'accesso dell'API di amministrazione REST e l'accesso degli utenti registrati devono essere abilitati nella console di Workspace ONE UEM per l'integrazione di VMware Identity Manager con Workspace ONE UEM. Quando si attiva l'accesso API viene generata una chiave API.

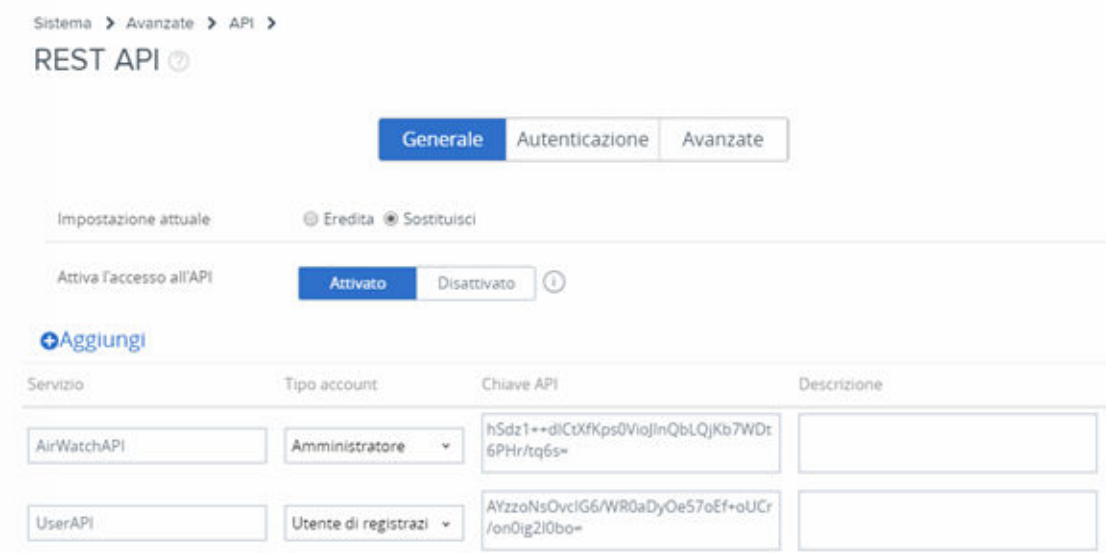
Procedura

1. Nella console di Workspace ONE UEM, selezionare Globale > Gruppo di organizzazioni a livello di cliente e passare a **Gruppi e impostazioni > Tutte le impostazioni > Sistema> Avanzate > API > REST API**.
2. Nella scheda Generale, fare clic su **Aggiungi** per generare la chiave API da utilizzare nel servizio VMware Identity Manager. Il tipo di account deve essere **Amministratore**.

   Immettere un nome di servizio univoco. Aggiungere una descrizione, come ad esempio **`AirWatchAPI for IDM`**.
3. Per generare la chiave API utente di registrazione, fare nuovamente clic su **Aggiungi**.
4. Selezionare **Utente di registrazione** dal menu a discesa Tipo account.

   Immettere un nome di servizio univoco. Aggiungere una descrizione, come ad esempio **`UserAPI per IDM`**.
5. Copiare le due chiavi API e salvare le chiavi in un file.

   Aggiungere queste chiavi quando si configura Workspace ONE UEM (AirWatch) nella console di VMware Identity Manage.



6. Fare clic su **Salva**.

Esportazione del certificato root dell'amministratore di VMware Workspace ONE UEM

Dopo aver creato la chiave dell'API di amministrazione, è possibile aggiungere un account amministratore e impostare l'autenticazione del certificato nella console di Workspace ONE UEM.

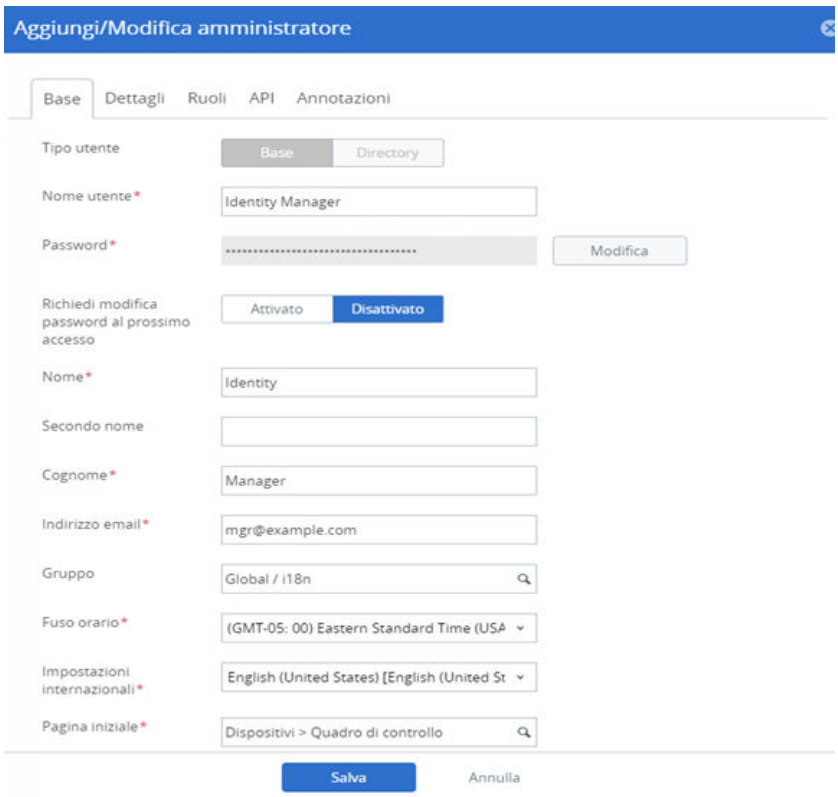
Per l'autenticazione basata su certificato di REST API, viene generato un certificato a livello di utente dalla console di Workspace ONE UEM. Il certificato utilizzato è un certificato di Workspace ONE UEM autofirmato generato dal certificato root di amministrazione di Workspace ONE UEM.

Prerequisiti

La chiave dell'API di amministrazione REST di Workspace ONE UEM deve essere stata creata.

Procedura

1. Nella console di Workspace ONE UEM, selezionare Globale > Gruppo di organizzazioni a livello di cliente e passare a **Account > Amministratori > Visualizzazione elenco**.
2. Fare clic su **Aggiungi > Aggiungi amministratore**.
3. Nella scheda Base, immettere il nome utente e la password dell'amministratore del certificato nelle caselle di testo corrispondenti.



4. Selezionare la scheda Ruoli, scegliere il gruppo organizzazione corrente, fare clic sulla seconda casella di testo e selezionare **Amministratore di AirWatch**.
5. Fare clic sulla scheda API e selezionare **Certificati** nella casella di testo Autenticazione.

6 Immettere la password del certificato. La password coincide con la password immessa per l'amministratore nella scheda Base.

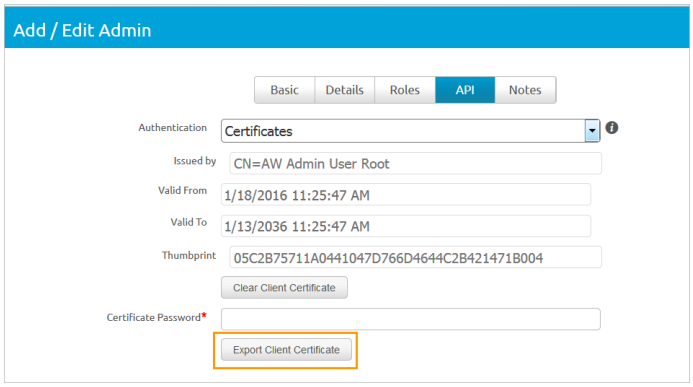
7 Fare clic su **Salva**.

Vengono creati il nuovo account amministrativo e il certificato client.

8 Nella pagina Vista elenco, selezionare l'amministratore creato e aprire nuovamente la scheda API.

La pagina dei certificati visualizza informazioni sul certificato.

9 Immettere la password impostata nella casella di testo Password certificato, fare clic su **Esporta certificato client** e salvare il file.



Il certificato del client viene salvato come tipo di file .p12.

Operazioni successive

Configurare le impostazioni dell'URL di Workspace ONE UEM nella console di VMware Identity Manager.

Configurazione di un'istanza di Workspace ONE UEM in VMware Identity Manager

Dopo aver configurato le impostazioni nella console di Workspace ONE UEM, nella pagina Gestione identità e accessi della console di VMware Identity Manager, è necessario specificare l'URL di Workspace ONE UEM, i valori delle chiavi API e il certificato. Una volta configurate le impostazioni di Workspace ONE UEM, è possibile abilitare le opzioni delle funzionalità disponibili per Workspace ONE.

Aggiunta di impostazioni di Workspace ONE UEM a VMware Identity Manager

Configurare le impostazioni di Workspace ONE UEM in VMware Identity Manager per integrare Workspace ONE UEM con VMware Identity Manager e attivare le opzioni di integrazione della funzionalità Workspace ONE UEM. Vengono aggiunti il certificato e la chiave dell'API di Workspace ONE UEM per l'autorizzazione di VMware Identity Manager con Workspace ONE UEM.

Prerequisiti

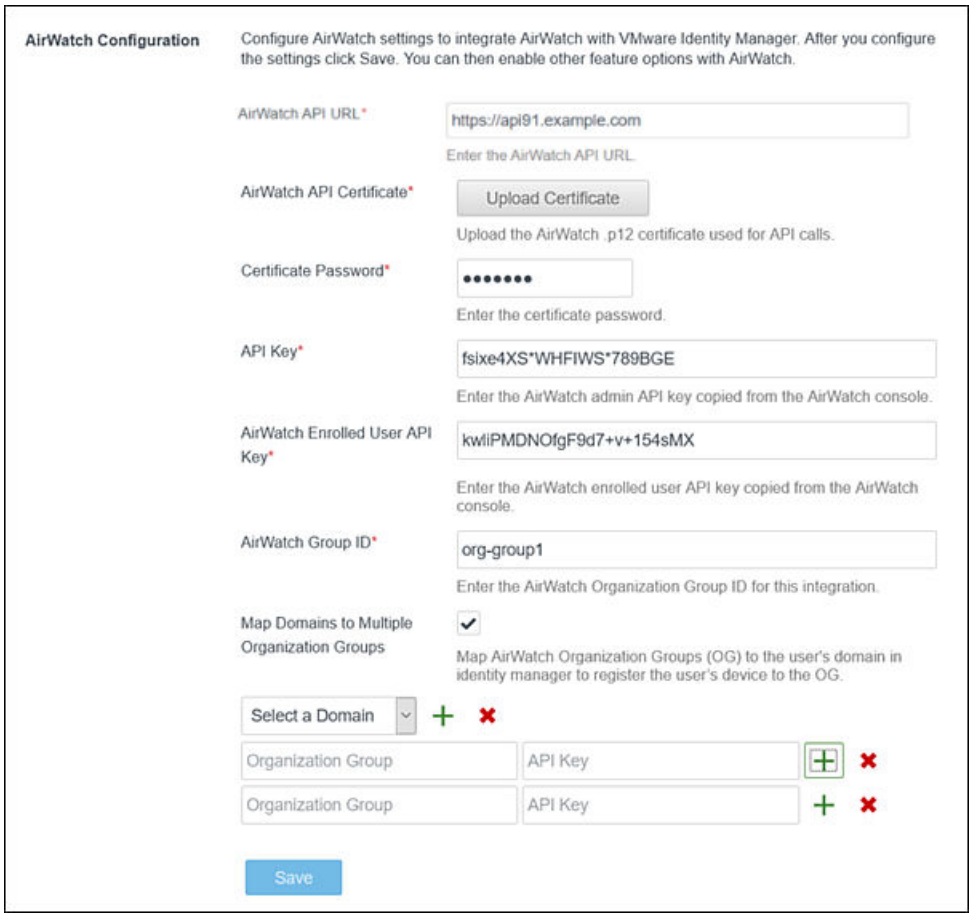
- URL del server di Workspace ONE UEM utilizzato dall'amministratore per accedere alla console di Workspace ONE UEM.
- Chiave dell'API di amministrazione di Workspace ONE UEM utilizzata per creare richieste di API da VMware Identity Manager al server di Workspace ONE UEM per configurare l'integrazione.
- File del certificato di Workspace ONE UEM utilizzato per effettuare chiamate API e password del certificato. Il file del certificato deve essere in formato .p12.
- Chiave API utente registrato di Workspace ONE UEM.
- ID del gruppo di Workspace ONE UEM per il tenant, ovvero l'identificatore del tenant in Workspace ONE UEM.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager selezionare **Configurazione > AirWatch**.
2. Specificare le impostazioni di integrazione di Workspace ONE UEM nei seguenti campi.

Campo	Descrizione
URL API di AirWatch	Immettere l'URL di Workspace ONE UEM. Ad esempio, `https://myco.ws1uem.com`
Certificato API di AirWatch	Caricare il file del certificato utilizzato per effettuare chiamate API.
Password certificato	Immettere la password del certificato.
Chiave API di amministrazione di AirWatch	Immettere il valore della chiave dell'API di amministrazione. Un esempio di valore di chiave API è `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
Chiave API utente registrato di AirWatch	Immettere la chiave API dell'utente registrato.
ID Gruppo di AirWatch	Immettere l'ID di Workspace ONE UEM relativo al gruppo di organizzazioni in cui sono stati creati la chiave API e l'account di amministrazione.

3 Fare clic su **Salva**.



Operazioni successive

Abilitare l'opzione della funzionalità Catalogo Workspace ONE per unire al catalogo di Workspace ONE le app configurate con il catalogo di Workspace ONE UEM.

- Attivare il controllo della conformità per verificare che i dispositivi gestiti Workspace ONE UEMsi attengano alla politica di conformità di Workspace ONE UEM.

Vedere Abilitazione del controllo di conformità per i dispositivi gestiti di Workspace ONE UEM.

Mappatura dei domini di VMware Identity Manager a più gruppi di organizzazioni in Workspace ONE UEM

Quando si configurano utenti e dispositivi in Workspace ONE UEM, Workspace ONE UEM utilizza i gruppi di organizzazioni per organizzare e raggruppare gli utenti e stabilire le autorizzazioni. Quando Workspace ONE UEM è integrato con VMware Identity Manager, le chiavi REST API dell'utente di amministrazione e registrazione possono essere configurate solo nel gruppo di organizzazioni di Workspace ONE UEM di tipo Cliente.

Negli ambienti Workspace ONE UEM configurati per tenancy multipla, vengono creati molti gruppi di organizzazioni per utenti e dispositivi. I dispositivi vengono registrati in un gruppo di organizzazioni. È possibile impostare gruppi di organizzazioni in configurazioni uniche in un ambiente a tenancy multipla. Ad esempio gruppi di organizzazioni per aree geografiche, reparti o casi d'uso differenti.

È possibile collegare domini configurati in VMware Identity Manager a gruppi di organizzazioni specifici in Workspace ONE UEM per gestire la registrazione dei dispositivi tramite Workspace ONE. Quando gli utenti accedono a Workspace ONE, in VMware Identity Manager viene attivato un evento di registrazione. Durante la registrazione del dispositivo, viene inviata una richiesta a Workspace ONE UEM per effettuare il pull di tutte le applicazioni per le quali la combinazione utente/dispositivo è autorizzata.

I gruppi di organizzazioni del dispositivo devono essere identificati quando Workspace ONE UEM viene integrato con VMware Identity Manager, in modo che Identity Manager sia in grado di individuare l'utente e registrare correttamente il dispositivo nel gruppo di organizzazioni appropriato.

Quando si configurano le impostazioni di Workspace ONE UEM nel servizio VMware Identity Manager, è possibile specificare gli ID dei gruppi di organizzazioni del dispositivo e le chiavi API per mappare più gruppi di organizzazioni a un dominio. Quando gli utenti accedono a Workspace ONE dai loro dispositivi, i record degli utenti vengono verificati e i dispositivi vengono registrati nel gruppo di organizzazioni appropriato in Workspace ONE UEM.

Per ulteriori informazioni su come configurare gruppi di organizzazioni multipli, vedere Strategie di distribuzione per l'impostazione di gruppi di organizzazioni di Workspace ONE UEM multipli.

Nota Quando Workspace ONE UEM è integrato con VMware Identity Manager e sono configurati più gruppi di organizzazioni Workspace ONE UEM, l'opzione Catalogo globale di Active Directory non può essere configurata per l'utilizzo con il servizio VMware Identity Manager.

Abilitazione del catalogo di Workspace ONE per Workspace ONE UEM

Quando si configura VMware Identity Manager con l'istanza di Workspace ONE UEM, è possibile abilitare il catalogo di Workspace ONE per includere le app del catalogo di Workspace ONE UEM. Gli utenti finali possono visualizzare tutte le applicazioni per cui sono autorizzati dal proprio portale Workspace ONE.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager, fare clic su **Configura > AirWatch** e passare alla sezione Catalogo Workspace ONE.
2. Per includere le app del catalogo di AirWatch con le app del catalogo di Identity Manager, abilitare **Recupera da IDM** e **Recupera da Airwatch**.

   Quando si utilizza il catalogo di Workspace ONE in dispositivi mobili in cui non è configurato il servizio VMware Identity Manager, selezionare solo **Recupera da AirWatch**.

   Per impostazione predefinita, l'opzione **Recupera da IDM** è abilitata.
3. Fare clic su **Salva**.

Operazioni successive

Indicare agli utenti finali di Workspace ONE UEM come accedere al catalogo e visualizzare il proprio portale Workspace ONE.

Abilitazione del controllo di conformità per i dispositivi gestiti di Workspace ONE UEM

Quando gli utenti registrano i propri dispositivi, a scadenze regolari programmate vengono inviati dati campione che vengono utilizzati per valutare conformità. La valutazione di questi dati di esempio consente di verificare che il dispositivo soddisfi le regole di conformità impostate dall'amministratore nella console di Workspace ONE UEM (UEM). Se il dispositivo non rispetta la conformità, vengono intraprese le azioni corrispondenti configurate nella console di UEM.

Il servizio VMware Identity Manager include un'opzione dei criteri di accesso che può essere configurata per controllare lo stato di conformità del dispositivo nel server Workspace ONE UEM quando gli utenti accedono dal dispositivo. Grazie al controllo di conformità, è possibile impedire agli utenti di accedere a un'applicazione o di utilizzare Single Sign-On nel portale di Workspace ONE se il dispositivo non rispetta la conformità. La possibilità di accedere viene ripristinata quando il dispositivo rispetta nuovamente la conformità.

Se il dispositivo è compromesso, l'applicazione Workspace ONE si disconnette automaticamente e blocca l'accesso alle applicazioni. Se il dispositivo è stato registrato tramite la gestione adattiva, con un comando di rimozione dei dati aziendali emesso dalla console UEM è possibile annullare la registrazione del dispositivo e rimuovere le applicazioni gestite dal dispositivo. Le applicazioni non gestite non vengono rimosse.

Per ulteriori informazioni sui criteri di conformità di Workspace ONE UEM, consultare la guida VMware Workspace ONE UEM Mobile Device Management, nelle pagine della documentazione di VMware Workspace ONE UEM.

Abilitazione dell'autenticazione della password utente tramite Workspace ONE UEM

Per implementare l'autenticazione con AirWatch Cloud Connector, è necessario abilitare l'autenticazione con password tramite la funzionalità Workspace ONE UEM.

Prerequisiti

- Workspace ONE UEM configurato in VMware Identity Manager.
- AirWatch Cloud Connector installato e attivato.
- Servizi directory di Workspace ONE UEM integrati con Active Directory.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager selezionare **Configurazione > AirWatch**.

2 Nella sezione Autenticazione password utente tramite AirWatch, selezionare **Attiva**.

3 Fare clic su **Salva**.

Operazioni successive

Per utilizzare l'autenticazione di AirWatch Cloud Connector, vedere Implementazione dell'autenticazione con AirWatch Cloud Connector.

Configurazione delle regole di controllo di conformità

Quando il controllo di conformità è abilitato, si crea una regola dei criteri di accesso che richiede autenticazione e verifica della conformità per i dispositivi gestiti da Workspace ONE UEM.

La regola del criterio di controllo conformità opera in una catena di autenticazione con SSO mobile per iOS, SSO mobile per Android e Certificato (distribuzione cloud). Quando si configura la regola, il metodo di autenticazione da utilizzare deve precedere il metodo di conformità del dispositivo.

Prerequisiti

Metodi di autenticazione configurati e associati a un provider di identità integrato.

Controllo di conformità abilitato nella pagina AirWatch di VMware Identity Manager.

Procedura

1 Nella scheda Gestione identità e accessi della console di VMware Identity Manager, selezionare **Gestione > Criteri**.

2 Fare clic su **Modifica criterio predefinito**.

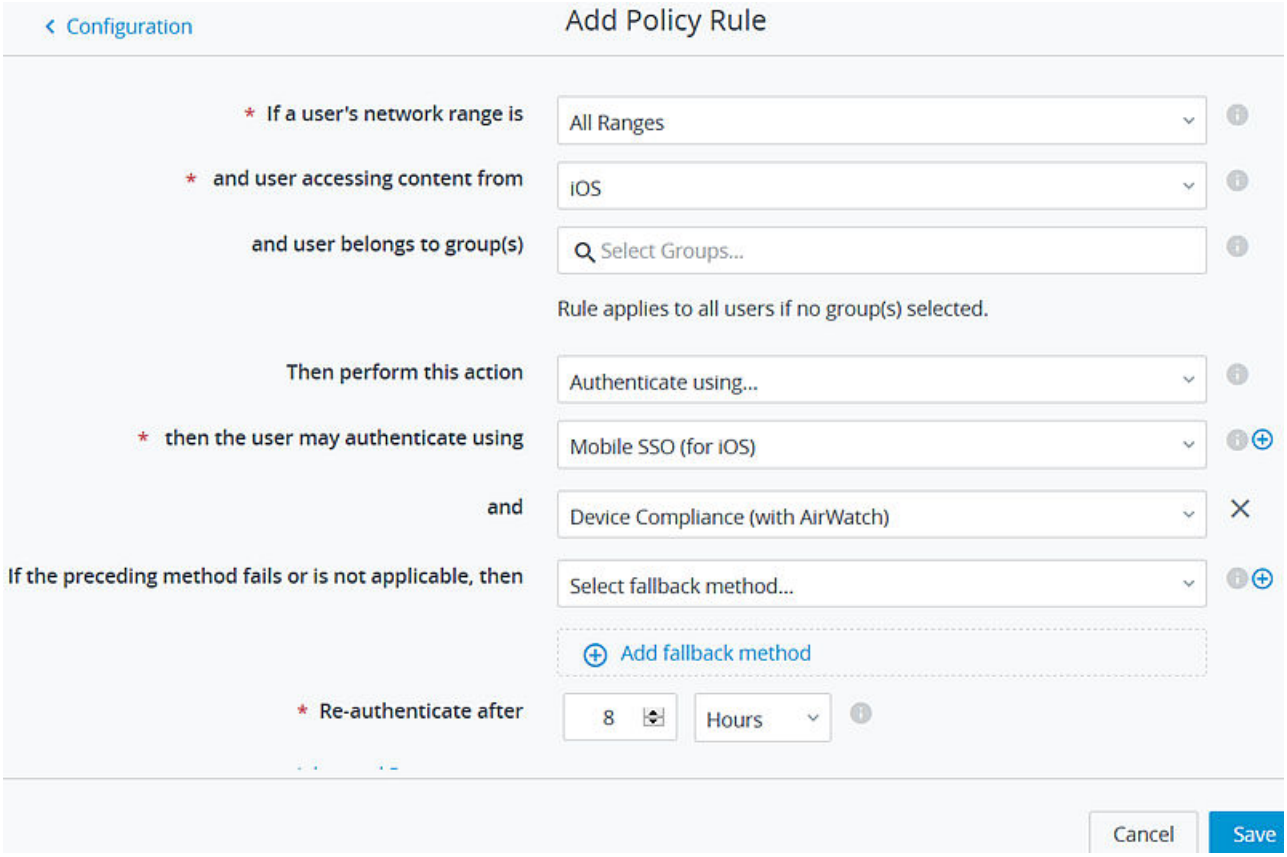
3 Fare clic su **Avanti**.

4 Fare clic su **Aggiungi regola criterio** per aggiungere una regola o selezionare una regola da modificare.

Opzione	Descrizione
Se l'intervallo di rete di un utente è	Verificare che l'intervallo di rete sia corretto. Se si sta aggiungendo una regola, selezionare l'intervallo di rete.
e l'utente accede al contenuto da	Selezionare il tipo di dispositivo mobile.
e l'utente appartiene al gruppo o ai gruppi	Se questa regola di accesso verrà applicata a gruppi specifici, cercare i gruppi nella casella di ricerca. Se non si seleziona alcun gruppo, il criterio di accesso viene applicato a tutti gli utenti.
Eseguire questa azione	Selezionare **Esegui autenticazione mediante...**
l'utente può eseguire l'autenticazione mediante	Selezionare il metodo di autenticazione del dispositivo mobile da applicare. Fare clic su + e nel menu a discesa selezionare **Conformità dispositivo (con AirWatch)**.

Opzione	Descrizione
Se il metodo precedente non riesce o non è applicabile,	Configurare il metodo di autenticazione di fallback, se necessario.
Nuova autenticazione dopo	Selezionare la durata della sessione, trascorsa la quale gli utenti dovranno eseguire nuovamente l'autenticazione.

5 Fare clic su **Salva**.



Aggiornamento di VMware Identity Manager dopo l'aggiornamento di Workspace ONE UEM

Quando si aggiorna Workspace ONE UEM a una nuova versione, è necessario aggiornare le opzioni Catalogo Workspace ONE e Autenticazione password utente nella pagina di configurazione di AirWatch della console di VMware Identity Manager.

Quando si salvano queste opzioni dopo l'aggiornamento di Workspace ONE UEM, le impostazioni di AirWatch nel servizio VMware Identity Manager vengono aggiornate con la nuova versione di Workspace ONE UEM.

Procedura

1 Dopo aver aggiornato Workspace ONE UEM, accedere alla console di VMware Identity Manager.

2 Nella scheda Gestione identità e accessi, fare clic su **Configura > AirWatch**.

3 Scorrere la pagina verso il basso fino alla sezione **Catalogo Workspace ONE** e fare clic su **Salva**.

4 Scorrere verso il basso fino alla sezione **Autenticazione password utente tramite AirWatch** e fare clic su **Salva**.

La configurazione di Workspace ONE UEM viene aggiornata con la nuova versione nel servizio VMware Identity Manager.

Implementazione dell'autenticazione con AirWatch Cloud Connector

Il componente AirWatch Cloud Connector (ACC) di VMware Enterprise Systems Connector è integrato con VMware Identity Manager per l'autenticazione della password dell'utente in Workspace ONE.

Nota Installare ACC e configurare il componente ACC in Workspace ONE UEM. Per informazioni sull'installazione e la configurazione di AirWatch Cloud Connector, vedere la guida all'installazione e alla configurazione di VMware Enterprise Systems Connector. Dopo aver installato e configurato ACC, integrare i servizi directory di Workspace ONE UEM con Active Directory. Per informazioni sull'abilitazione dei servizi directory, vedere la guida ai servizi directory di VMware Workspace ONE UEM.

Per implementare l'autenticazione di AirWatch Cloud Connector per Workspace ONE, nella console di VMware Identity Manager, associare il metodo di autenticazione Password (Workspace ONE UEM Connector) a un provider di identità integrato.

È possibile abilitare il supporto Just-in-Time in Workspace ONE UEM per aggiungere i nuovi utenti alla directory di VMware Identity Manager quando accedono per la prima volta. Quando il supporto Just-in-Time è abilitato, gli utenti non devono attendere la sincronizzazione pianificata successiva dal server Workspace ONE UEM per accedere a Workspace ONE. È sufficiente che i nuovi utenti accedano al portale Workspace ONE, da un dispositivo iOS o Android oppure dal computer desktop, e immettano nome utente e password di Active Directory. Il servizio VMware Identity Manager esegue l'autenticazione delle credenziali di Active Directory tramite AirWatch Cloud Connector e aggiunge il profilo utente alla directory.

Dopo aver associato il metodo di autenticazione nel provider di identità integrato, creare criteri di accesso da applicare a tale metodo di autenticazione.

Nota L'autenticazione con nome utente e password è integrata nella distribuzione di AirWatch Cloud Connector. Per autenticare gli utenti che utilizzano altri metodi di autenticazione supportati da VMware Identity Manager, è necessario configurare il connettore di VMware Identity Manager.

Gestione della mappatura degli attributi dell'utente

È possibile configurare la mappatura degli attributi utente tra la directory di Workspace ONE UEM e la directory di VMware Identity Manager.

La pagina Attributi utente della scheda Gestione identità e accessi di VMware Identity Manager, include gli attributi predefiniti della directory mappati agli attributi della directory di Workspace ONE UEM. Gli attributi obbligatori sono contrassegnati con un asterisco. Gli utenti nel cui profilo manca un attributo obbligatorio non vengono sincronizzati con il servizio VMware Identity Manager.

Tabella 2-1. Mappatura degli attributi predefiniti della directory Workspace ONE UEM

Nome attributo utente VMware Identity Manager	Mappatura predefinita all'attributo utente Workspace ONE UEM
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	Dominio
disabled (utente esterno disabilitato)	disabilitato
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Email*
userName	username*

Sincronizzazione di utenti e gruppi dalla directory Workspace ONE UEM alla directory VMware Identity Manager

Configurare le impostazioni di VMware Identity Manager nella console di Workspace ONE UEM per stabilire una connessione tra l'istanza del gruppo di organizzazioni della directory di Workspace ONE UEM e VMware Identity Manager. Questa connessione viene utilizzata per sincronizzare utenti e gruppi in una directory creata nel servizio VMware Identity Manager.

Utenti e gruppi vengono inizialmente sincronizzati manualmente nella directory di VMware Identity Manager. La pianificazione della sincronizzazione di Workspace ONE UEM determina quando gli utenti e i gruppi vengono sincronizzati con la directory di VMware Identity Manager.

Quando un utente o un gruppo viene aggiunto o eliminato nel server Workspace ONE UEM, la modifica viene immediatamente applicata nel servizio VMware Identity Manager.

Prerequisiti

- Nome e password dell'amministratore locale di VMware Identity Manager.
- Identificare i valori di attributo da mappare dalla directory di Workspace ONE UEM. Vedere Gestione della mappatura degli attributi dell'utente.

Procedura

1. Nella pagina Gruppi e impostazioni > Tutte le impostazioni della console di Workspace ONE UEM, selezionare Globale > Gruppo di organizzazioni a livello di cliente e passare a **Sistema > Integrazione aziendale** >**VMware Identity Manager**.

2 Nella sezione Server, fare clic su **Configura**.

Nota Il pulsante di configurazione è disponibile solo se anche il servizio di directory è configurato per lo stesso gruppo dell'organizzazione. Se il pulsante Configura non è visibile, significa che non ci si trova nel gruppo dell'organizzazione corretto. È possibile cambiare il gruppo dell'organizzazione nel menu a discesa Globale.

3 Immettere le impostazioni di VMware Identity Manager.

Opzione	Descrizione
URL	Immettere l'URL VMware del tenant. Ad esempio `https://myco.identitymanager.com`.
Nome utente amministratore	Immettere il nome utente amministratore locale di VMware Identity Manager.
Password amministratore	Immettere la password dell'utente amministratore locale di VMware Identity Manager.

4 Fare clic su **Avanti**.

5 Abilitare la mappatura personalizzata per configurare la mappatura degli attributi utente da Workspace ONE UEM al servizio VMware Identity Manager.

6 Fare clic su **Test della connessione** per verificare che le impostazioni siano corrette.

7 Fare clic su **Sincronizza ora** per sincronizzare manualmente tutti gli utenti e i gruppi con il servizio VMware Identity Manager.

Nota Per controllare il carico del sistema, la sincronizzazione manuale può essere eseguita solo quattro ore dopo la sincronizzazione precedente.

Viene creata una directory Workspace ONE UEM nel servizio VMware Identity Manager e gli utenti e i gruppi vengono sincronizzati in una directory in VMware Identity Manager.

Operazioni successive

Controllare la scheda Utenti e gruppi della console di VMware Identity Manager per verificare che i nomi degli utenti e dei gruppi siano sincronizzati.

Gestione della configurazione dell'autenticazione con password per Workspace ONE UEM

È possibile esaminare e gestire la configurazione Password (AirWatch Connector) che è stata impostata durante l'installazione di Workspace ONE UEM e l'aggiunta del servizio VMware Identity Manager.

Il metodo di autenticazione Password (AirWatch Connector) viene gestito dalla pagina Gestione identità e accessi > Metodi di autenticazione e viene associato al provider di identità integrato nella pagina Provider di identità.

Importante Quando si aggiorna il software AirWatch Cloud Connector, assicurarsi di aggiornare la configurazione di Workspace ONE UEM nella pagina AirWatch della console di VMware Identity Manager.

Procedura

1 Nella scheda Gestione identità e accessi della console di VMware Identity Manager, selezionare **Metodi di autenticazione**.

2 Nella colonna Configura di **Password (AirWatch Connector)**, fare clic sull'icona a forma di matita.

3 Esaminare la configurazione.

Opzione	Descrizione
Abilita autenticazione con password di AirWatch	Questa casella di controllo consente di abilitare l'autenticazione con password di Workspace ONE UEM.
URL console di gestione di AirWatch	Campo già popolato con l'URL di Workspace ONE UEM.
Chiave dell'API di AirWatch	Campo già popolato con la chiave dell'API di amministrazione di Workspace ONE UEM.
Certificato utilizzato per l'autenticazione	Campo già popolato con il certificato di Workspace ONE UEM Cloud Connector.
Password per il certificato	Campo già popolato con la password per il certificato di Workspace ONE UEM Cloud Connector.
ID Gruppo di AirWatch	Campo già popolato con l'ID del gruppo di organizzazioni.
Numero di tentativi di autenticazione consentiti	Numero massimo di tentativi di accesso non riusciti quando si utilizza l'autenticazione con password di Workspace ONE UEM. Quando viene raggiunto questo numero, non sono consentiti altri tentativi di accesso. Il servizio VMware Identity Manager tenta di utilizzare il metodo di autenticazione fallback se è configurato. Il valore predefinito è cinque tentativi.
JIT abilitato	Se JIT non è abilitato, selezionare questa casella di controllo per abilitare il provisioning JIT dinamico degli utenti nel servizio VMware Identity Manager quando accedono per la prima volta.

4 Fare clic su **Salva**.

Configurazione di provider di identità integrati

È possibile configurare più provider di identità integrati e associare i metodi di autenticazione configurati nella pagina Gestione identità e accessi > Metodi di autenticazione.

Procedura

1 Nella scheda Gestione identità e accessi, andare a **Gestione > Provider di identità**.

2 Fare clic su **Aggiungi provider di identità** e selezionare **Crea provider di identità integrato**.

Opzione	Descrizione
Nome del provider di identità	Immettere il nome per l'istanza di questo provider di identità integrato.
Utenti	Selezionare gli utenti per cui eseguire l'autenticazione. Vengono elencate le directory configurate.
Rete	Sono elencati gli intervalli di rete esistenti configurati nel servizio. Selezionare gli intervalli di rete per gli utenti in base agli indirizzi IP che si desidera indirizzare a questa istanza del provider di identità per l'autenticazione.
Metodi di autenticazione	Vengono visualizzati i metodi di autenticazione configurati nel servizio. Selezionare le caselle di controllo relative ai metodi di autenticazione da associare a questo provider di identità integrato. Per Conformità dispositivo (con Workspace ONE UEM) e Password (AirWatch Connector), assicurarsi che l'opzione sia abilitata nella pagina di configurazione di AirWatch.

3 Fare clic su **Aggiungi**.

Operazioni successive

Configurare la regola dei criteri di accesso predefinita per aggiungere i criteri di autenticazione alla regola. Vedere Configurazione delle regole di controllo di conformità

Implementazione dell'autenticazione SSO mobile per dispositivi iOS gestiti da Workspace ONE UEM

3

Per l'autenticazione di dispositivi iOS, VMware Identity Manager utilizza un provider di identità integrato nel servizio di VMware Identity Manager per fornire accesso all'autenticazione SSO mobile.

Questo metodo di autenticazione per dispositivi iOS utilizza un Centro distribuzione chiavi senza l'impiego di un connettore o di un sistema di terze parti. Grazie all'autenticazione Kerberos, gli utenti che hanno effettuato l'accesso al loro dominio, possono accedere al proprio portale di app Workspace ONE senza dover immettere altre credenziali.

Questo capitolo include i seguenti argomenti:

Panoramica dell'implementazione per la configurazione di SSO mobile per iOS

L'implementazione dell'autenticazione SSO mobile per i dispositivi iOS 9 o versione successiva gestiti da Workspace ONE UEM richiede i passaggi di configurazione seguenti.

- Scaricare il certificato dell'emittente per configurare SSO mobile per iOS
  - Se si utilizzano i Servizi certificati Active Directory, configurare un modello di CA per la distribuzione di certificati Kerberos nei Servizi certificati Active Directory. Quindi configurare Workspace ONE UEM per utilizzare la CA di Active Directory. Aggiungere il modello di certificato nella console di Workspace ONE UEM. Scaricare il certificato dell'emittente per configurare SSO mobile per iOS.
  - Se si utilizza Workspace ONE UEM Certificate Authority, attivare Certificati nella pagina delle integrazioni di VMware Identity Manager. Scaricare il certificato dell'emittente per configurare SSO mobile per iOS.
- Stabilire il centro distribuzione chiavi (KDC) da utilizzare.
- Configurare il profilo del dispositivo iOS e attivare Single Sign-On dalla console di Workspace ONE UEM.
- Configurare il metodo di autenticazione SSO mobile (iOS)
- Configurare il provider di identità integrato e associare l'autenticazione SSO mobile per iOS nella console di VMware Identity Manager.

Configurazione dell'autorità di certificazione di Active Directory in Workspace ONE UEM

Per impostare l'autenticazione SSO (Single Sign-On) in dispositivi mobili iOS 9 gestiti da Workspace ONE UEM, è possibile configurare una relazione di attendibilità tra Active Directory e Workspace ONE UEM e abilitare il metodo di autenticazione SSO mobile per iOS in VMware Identity Manager.

Dopo aver configurato l'autorità di certificazione e il modello di certificato per la distribuzione del certificato Kerberos in Servizi certificati Active Directory, abilitare la richiesta del certificato utilizzato per l'autenticazione in Workspace ONE UEM e aggiungere l'autorità di certificazione nella console di Workspace ONE UEM.

Procedura

1. Nel menu principale della console di Workspace ONE UEM, passare a **Dispositivi > Certificati > Autorità di certificazione**.
2. Fare clic su **Aggiungi**.

3 Configurare le opzioni seguenti nella pagina Autorità di certificazione.

Nota Assicurarsi che come Tipo autorità sia selezionata Microsoft ADCS prima di iniziare a compilare il modulo.

Opzione	Descrizione
Nome	Immettere il nome della nuova autorità di certificazione.
Tipo di autorità	Assicurarsi che sia selezionata l'opzione **Microsoft ADCS**.
Protocollo	Selezionare il protocollo **ADCS**.
Nome host del server	Immettere l'URL del server. Immettere il nome host nel formato `https://{servername.com}/certsrv.adcs/`. L'indirizzo può iniziare con http o https in base alla configurazione del sito. L'URL deve includere una barra / finale. **Nota** Se la connessione non riesce quando si verifica l'URL, rimuovere http:// o https:// dall'indirizzo e verificare di nuovo la connessione.
Nome autorità	Immettere il nome dell'autorità di certificazione a cui è connesso l'endpoint di ADCS. È possibile conoscere questo nome avviando l'applicazione Certification Authority sul server dell'autorità di certificazione.
Autenticazione	Assicurarsi che sia selezionata l'opzione **Account servizio**.
Nome utente e password	Immettere il nome utente e la password per l'account amministrativo di Servizi certificati Active Directory che dispone di privilegi di accesso sufficienti per consentire a Workspace ONE UEM di richiedere ed emettere certificati.

4 Fare clic su **Salva**.

Operazioni successive

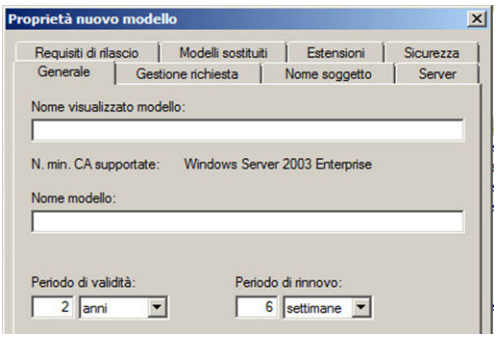
Configurare il modello di certificato in Workspace ONE UEM.

Configurazione di Workspace ONE UEM in modo che utilizzi l'autorità di certificazione di Active Directory

Il modello dell'autorità di certificazione deve essere configurato correttamente per la distribuzione di certificati Kerberos. Nei servizi certificati Active Directory (AD CS) è possibile duplicare il modello di autenticazione Kerberos per configurare un nuovo modello di autorità di certificazione per l'autenticazione iOS Kerberos.

Quando si duplica il modello di autenticazione Kerberos da AD CS, è necessario configurare le seguenti informazioni nella finestra di dialogo Proprietà nuovo modello.

Figura 3-1. Proprietà dei servizi certificati Active Directory della finestra di dialogo Nuovo modello



- Scheda **Generale**. Immettere il nome visualizzato del modello e il nome del modello, ad esempio iOSKerberos. Si tratta del nome visualizzato mostrato nello snap-in Modelli di certificato, nello snap-in Certificati e nello snap-in Autorità di certificazione.
- Scheda **Gestione richiesta** . Abilitare **Consenti chiave privata da esportare**.
- Scheda **Nome oggetto**. Selezionare il pulsante di opzione **Inserisci nella richiesta**. Il nome dell'oggetto viene fornito da Workspace ONE UEM quando Workspace ONE UEM richiede il certificato.
- Scheda **Estensione**. Definire i criteri dell'applicazione.
  - Selezionare Criteri di applicazione e fare clic su Modifica per aggiungere un nuovo criterio di applicazione. Denominare questo criterio Autenticazione client Kerberos.
  - Aggiungere l'identificatore di oggetto (OID) come segue: 1.3.6.1.5.2.3.4. Non modificare.
  - Nell'elenco Descrizione dei criteri di applicazione, elencare tutti i criteri elencati tranne il criterio Autenticazione client Kerberos e il criterio Autenticazione smart card.
- Scheda **Sicurezza**. Aggiungere l'account Workspace ONE UEM all'elenco di utenti che possono utilizzare il certificato. Impostare i permessi per l'account. Impostare Controllo completo per consentire all'entità di sicurezza di modificare tutti gli attributi di un modello di certificato, compresi i permessi per il modello di certificato. In caso contrario, impostare i permessi in base ai requisiti dell'organizzazione.

Salvare le modifiche. Aggiungere il modello all'elenco di modelli utilizzati dall'autorità di certificazione Active Directory.

In Workspace ONE UEM, configurare l'autorità di certificazione e aggiungere il modello di certificato.

Aggiunta di un modello di certificato in Workspace ONE UEM

È possibile aggiungere un modello di certificato che associ la CA (Certificate Authority, autorità di certificazione) utilizzata per generare il certificato dell'utente.

Prerequisiti

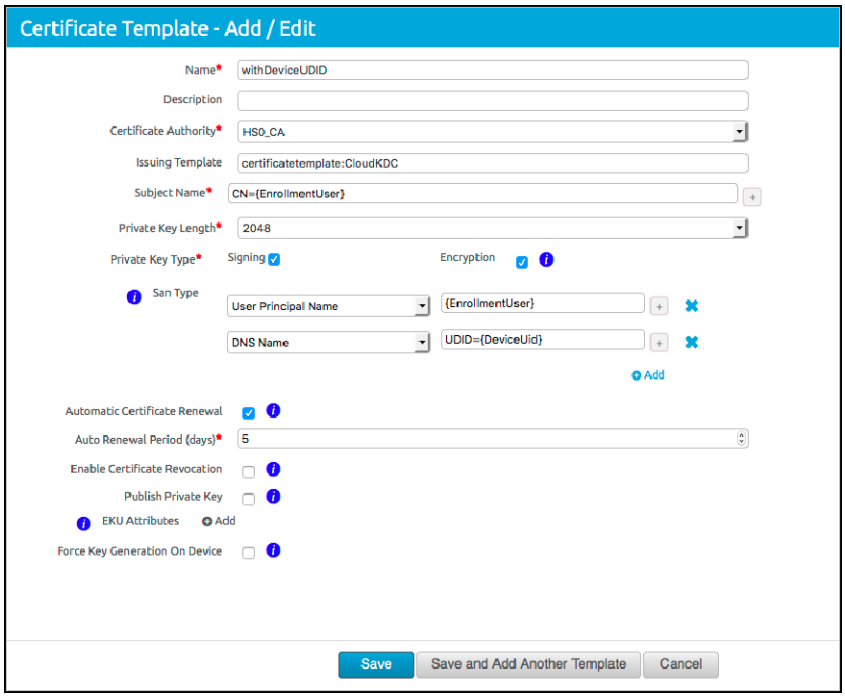
Configurare l'autorità di certificazione in Workspace ONE UEM.

Procedura

1. Nella console di Workspace ONE UEM, passare a **Sistema > Integrazione aziendale > Autorità di certificazione**.
2. Selezionare la scheda **Modello di richiesta** e fare clic su **Aggiungi**.
3. Configurare le opzioni seguenti nella pagina dei modelli di certificato.

Opzione	Descrizione
Nome	Immettere il nome del nuovo modello di richiesta in Workspace ONE UEM.
Autorità di certificazione	Selezionare l'autorità di certificazione creata dal menu a discesa.
Modello emittente	Immettere il nome del modello di certificato CA di Microsoft esattamente come creato in AD CS. Ad esempio `iOSKerberos`.
Nome oggetto	Immettere il nome dell'oggetto per il modello. È possibile fare clic su + per selezionare un valore di ricerca dall'elenco. Assicurarsi che il valore venga immesso dopo **CN=** nella casella di testo. Se si seleziona il tipo di ricerca DeviceUid, immettere un segno di due punti (:) dopo il valore e selezionare il valore di ricerca dall'elenco. Ad esempio, **CN={DeviceUid}:{valorericerca}**, dove la casella di testo {} è il valore di ricerca di Workspace ONE UEM. Assicurarsi di includere il segno di due punti (:). Il testo immesso in questa casella di testo corrisponde all'oggetto del certificato, che può essere utilizzato per determinare chi o quale dispositivo ha ricevuto il certificato.
Lunghezza chiave privata	Questa lunghezza della chiave privata corrisponde all'impostazione del modello di certificato utilizzato da AD CS. In genere è pari a 2048.
Tipo chiave privata	Selezionare le caselle di controllo **Firma** e **Crittografia**.
Tipo di SAN	Fare clic su **+Aggiungi**. Per il SAN (Subject Alternate Name, nome alternativo dell'oggetto), selezionare **Nome principale utente**. Il valore deve essere `{EnrollmentUser}`. Quando il controllo di conformità dei dispositivi è configurato con l'autenticazione Kerberos, se non si configura il DeviceUid come valore di ricerca del nome dell'oggetto, aggiungere un secondo tipo di SAN per includere l'identificatore univoco del dispositivo (UDID). Selezionare il **Nome DNS** del tipo di SAN. Il valore deve essere **UDID={DeviceUid}**.
Rinnovo automatico certificati	Selezionare la casella di controllo per far sì che i certificati che utilizzano questo modello vengano rinnovati automaticamente prima della rispettiva data di scadenza.
Periodo di rinnovo automatico (in giorni)	Specificare il periodo di rinnovo automatico, espresso in giorni.
Consenti la revoca dei certificati	Selezionare la casella di controllo per far sì che i certificati vengano revocati automaticamente quando vengono eliminati i dispositivi applicabili o ne viene annullata la registrazione, oppure se viene rimosso il profilo applicabile.
Pubblica chiave privata	Selezionare questa casella di controllo per pubblicare la chiave privata.
Destinazione chiave privata	Servizio di directory o servizio Web personalizzato

4 Fare clic su **Salva**.



Operazioni successive

Nella console di VMware Identity Provider, configurare il provider di identità integrato con il metodo di autenticazione SSO mobile (per iOS).

Utilizzo dell'autorità di certificazione di Workspace ONE UEM per l'autenticazione Kerberos

È possibile utilizzare l'autorità di certificazione di Workspace ONE UEM anziché quella di Active Directory per configurare SSO con l'autenticazione Kerberos integrata nei dispositivi mobili iOS 9 gestiti da Workspace ONE UEM. È possibile abilitare Autorità di certificazione Workspace ONE UEM nella console di Workspace ONE UEM ed esportare il certificato dell'emittente CA per l'utilizzo nel servizio VMware Identity Manager.

L'autorità di certificazione di Workspace ONE UEM è progettata per seguire il protocollo SCEP (Simple Certificate Enrollment Protocol) e viene utilizzata con i dispositivi gestiti da Workspace ONE UEM che supportano SCEP. L'integrazione di VMware Identity Manager con Workspace ONE UEM utilizza l'Autorità di certificazione di Workspace ONE UEM per emettere certificati per i dispositivi mobili iOS 9 come parte del profilo.

Il certificato root dell'emittente dell'autorità di certificazione di Workspace ONE UEM è anche il certificato di firma OCSP.

Abilitazione ed esportazione dell'autorità di certificazione di Workspace ONE UEM

Quando si abilita VMware Identity Manager in Workspace ONE UEM, è possibile generare il certificato root dell'emittente di Workspace ONE UEM ed esportare il certificato per utilizzarlo nell'autenticazione SSO mobile per iOS su dispositivi mobili iOS 9 gestiti.

Procedura

1 Nella console di Workspace ONE UEM, passare a **Sistema > Integrazione aziendale** > **VMware Identity Manager**.

Per abilitare l'autorità di certificazione di Workspace ONE UEM, il gruppo deve essere di tipo Cliente.

Suggerimento Per visualizzare o cambiare il tipo del gruppo, passare a Gruppi e impostazioni, **Gruppi > Gruppi**> **Dettagli gruppo**.

2 Fare clic su **Configurazione**.

3 Nella sezione CERTIFICATO, fare clic su **Attiva**.

La pagina mostra i dettagli del certificato root dell'emittente.

4 Fare clic su **Esporta** e salvare il file.

Operazioni successive

Nella console di VMware Identity Manager, configurare l'autenticazione Kerberos nel provider di identità integrato e aggiungere il certificato dell'emittente dell'autorità di certificazione.

Utilizzo di un centro di distribuzione chiavi (KDI) per l'autenticazione da dispositivi iOS

Nel dispositivo iOS, è necessario integrare il servizio con Kerberos. Grazie all'autenticazione Kerberos, gli utenti che hanno effettuato l'accesso al loro dominio, possono accedere al portale dell'applicazione senza dover immettere altre credenziali. Questo metodo di autenticazione per dispositivi iOS utilizza un Centro distribuzione chiavi senza l'impiego di un connettore o di un sistema di terze parti.

I tenant del Cloud VMware Identity Manager non devono gestire o configurare KDC.

Per le distribuzioni in locale, sono disponibili due opzioni relative al servizio KDC.

- KDC integrato. Il servizio KDC integrato richiede l'inizializzazione di KDC nell'appliance e la creazione di voci DNS pubbliche per consentire ai client Kerberos di individuare KDC. Per ulteriori informazioni sull'attivazione del KDC integrato, vedere la guida di amministrazione di VMware Identity Manager.

- KDC come servizio ospitato nel cloud di VMware Identity Manager. Se si utilizza KDC nel cloud, è necessario selezionare il nome dell'area di autenticazione appropriato nella pagina dell'adattatore di autenticazione di iOS.

Nota Se VMware Identity Manager è installato e configurato con Workspace ONE UEM in un ambiente Windows, è necessario configurare il metodo di autenticazione per i dispositivi iOS mobili in modo che utilizzino il cloud di VMware Identity Manager ospitato nel servizio del KDC.

Utilizzo del servizio KDC ospitato nel cloud

Per supportare l'utilizzo dell'autenticazione Kerberos per SSO mobile per iOS, VMware Identity Manager offre un servizio KDC ospitato nel cloud.

È necessario utilizzare il servizio KDC ospitato nel cloud quando il servizio VMware Identity Manager viene distribuito con Workspace ONE UEM in un ambiente Windows.

Per utilizzare il servizio KDC gestito nell'appliance di VMware Identity Manager, vedere la sezione relativa alla preparazione per l'utilizzo dell'autenticazione Kerberos nei dispositivi iOS della *guida all'installazione e alla configurazione di VMware Identity Manager*.

Se si configura l'autenticazione SSO mobile per iOS, è necessario configurare il nome dell'area di autenticazione per il servizio KDC ospitato nel cloud. L'area di autenticazione è il nome dell'entità amministrativa che gestisce i dati di autenticazione. Quando si fa clic su Salva, il servizio VMware Identity Manager viene registrato nel servizio KDC ospitato nel cloud. I dati archiviati nel servizio KDC si basano sulla configurazione del metodo di autenticazione SSO mobile per iOS, che include il certificato CA, il certificato di firma OCSP e i dettagli di configurazione della richiesta OCSP.

I record di accesso vengono archiviati nel servizio cloud. Le informazioni personali incluse nei record di accesso includono il nome dell'entità Kerberos del profilo utente, i valori DN, UPN e e-mail SAN dell'oggetto, l'ID dispositivo che si trova nel certificato dell'utente, nonché il nome di dominio completo del servizio IDM a cui l'utente sta accedendo.

Per utilizzare il servizio KDC ospitato nel cloud, VMware Identity Manager deve essere configurato nel modo seguente.

- Il nome di dominio completo del servizio VMware Identity Manager deve essere raggiungibile da Internet. Il certificato SSL/TLS utilizzato da VMware Identity Manager deve essere firmato pubblicamente.
- La porta 88 (UDP) di richiesta/risposta in uscita e la porta 443 (HTTPS/TCP) devono essere accessibili dal servizio VMware Identity Manager.
- Se si abilita OCSP, il risponditore OCSP deve essere raggiungibile da Internet.

Configurazione di SSO mobile per l'autenticazione iOS

È possibile configurare il metodo di autenticazione SSO mobile per iOS dalla pagina Metodi di autenticazione della console di VMware Identity Manager. Selezionare il metodo di autenticazione SSO mobile (per iOS) da utilizzare nel provider di identità integrato.

Prerequisiti

- File PEM o DER dell'autorità di certificazione utilizzato per emettere certificati per gli utenti nel tenant di Workspace ONE UEM.
- Per il controllo della revoca, il certificato della firma del risponditore OCSP.
- Per il servizio KDC selezionare il nome dell'area di autenticazione del servizio KDC. Se si utilizza il servizio KDC integrato, è necessario inizializzare KDC. Per dettagli relativi al servizio KDC integrato, vedere Installazione e configurazione di VMware Identity Manager.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager, passare a **Gestione > Metodi di autenticazione**.
2. Nella colonna Configura di**SSO Mobile (per iOS)**, fare clic sull'icona a forma di matita.
3. Configurare il metodo di autenticazione Kerberos.

Opzione	Descrizione
Abilita autenticazione KDC	Selezionare questa casella di controllo per attivare l'accesso degli utenti dotati di dispositivi iOS che supportano l'autenticazione Kerberos.
Area di autenticazione	Per le distribuzioni tenant nel cloud, il valore dell'area di autenticazione è sola lettura. Il nome dell'area di autenticazione visualizzato è il nome dell'area di autenticazione di Identity Manager per il tenant. In distribuzioni in locale, se si utilizza il servizio KDC ospitato nel cloud, immettere il nome dell'area di autenticazione supportata predefinita che viene fornito. Il testo di questo parametro deve essere tutto maiuscolo. Ad esempio, OP.VMWAREIDENTITY.COM. Se si utilizza il servizio KDC integrato, viene visualizzato il nome dell'area di autenticazione configurato durante l'inizializzazione di KDC.
Certificati CA intermedi e root	Caricare il file del certificato della CA emittente. I formati file supportati sono PEM e DER.
DN oggetto certificato CA caricati	Il contenuto del file del certificato caricato viene visualizzato qui. È possibile caricare più di un file e all'elenco vengono aggiunti tutti i certificati inclusi.
Abilita OCSP	Selezionare la casella di controllo per utilizzare il protocollo di convalida del certificato OCSP (Online Certificate Status Protocol) per ottenere lo stato della revoca di un certificato.
Invia nonce OCSP	Selezionare questa casella di controllo se si desidera inviare l'identificativo univoco della richiesta OCSP nella risposta.
Certificato di firma risponditore OCSP	Caricare il certificato OCSP per il risponditore. Quando si utilizza l'autorità di certificazione di Workspace ONE UEM, come certificato OCSP viene utilizzato il certificato dell'emittente. Caricare qui anche il certificato di Workspace ONE UEM.
DN oggetto certificato di firma risponditore OCSP	Qui viene mostrato il file del certificato OCSP caricato.
Messaggio di annullamento	Creare un messaggio di accesso personalizzato che verrà visualizzato nel caso in cui l'autenticazione stia impiegando troppo tempo. Se non si crea un messaggio personalizzato, il messaggio predefinito è `Attempting to authenticate your credentials`.

Opzione	Descrizione
Abilita collegamento per annullamento	Quando l'autenticazione impiega troppo tempo, questa opzione offre agli utenti la possibilità di fare clic su Annulla per interrompere il tentativo di autenticazione e annullare l'accesso. Quando è abilitato il collegamento Annulla, alla fine del messaggio di errore dell'autenticazione visualizzato è presente la parola Annulla.
URL server gestione dispositivi aziendali	Immettere l'URL del server Mobile Device Management (MDM) per reindirizzare gli utenti quando l'accesso viene negato perché il dispositivo non è registrato in Workspace ONE UEM per la gestione di MDM. Questo URL viene visualizzato nel messaggio di errore di autenticazione non riuscita. Se non si immette un URL qui, viene visualizzato il messaggio di accesso negato generico.

4 Fare clic su **Salva**.

Operazioni successive

- Associare il metodo di autenticazione SSO mobile (per iOS) nel provider di identità integrato.

Configurazione del provider di identità integrato per l'autenticazione SSO mobile di iOS

Configurare il provider di identità integrato e associare il metodo di autenticazione SSO mobile per iOS configurato nella pagina Gestione identità e accessi > Metodi di autenticazione.

Prerequisiti

L'autenticazione SSO mobile (per iOS) configurata nella pagina Metodi di autenticazione.

Procedura

1 Nella scheda Gestione identità e accessi, andare a **Gestione > Provider di identità**.

2 Fare clic su **Aggiungi provider di identità** e selezionare **Crea provider di identità integrato**.

Opzione	Descrizione
Nome del provider di identità	Immettere il nome per l'istanza di questo provider di identità integrato.
Utenti	Selezionare gli utenti per cui eseguire l'autenticazione. Vengono elencate le directory configurate.
Rete	Sono elencati gli intervalli di rete esistenti configurati nel servizio. Selezionare gli intervalli di rete per gli utenti in base agli indirizzi IP che si desidera indirizzare a questa istanza del provider di identità per l'autenticazione.
Metodi di autenticazione	Vengono visualizzati i metodi di autenticazione configurati nel servizio. Selezionare la casella di controllo relativa al metodo di autenticazione di iOS da associare a questo provider di identità integrato. Aggiungere eventuali altri metodo di autenticazione. Per Conformità dispositivo (con Workspace ONE UEM) e Password (Workspace ONE UEM Connector), assicurarsi che l'opzione sia abilitata nella pagina di configurazione di Workspace ONE UEM.

3 Nella sezione Esportazione certificato KDC, fare clic su **Scarica certificato**. Salvare questo certificato in un file accessibile dalla console di Workspace ONE UEM.

   Caricare questo certificato durante la configurazione del profilo del dispositivo iOS in Workspace ONE UEM.

4 Fare clic su **Aggiungi**.

Operazioni successive

- Configurare la regola del criterio di accesso predefinito per l'autenticazione Kerberos per i dispositivi iOS. Assicurarsi che questo metodo di autenticazione sia il primo metodo impostato nella regola.
- Passare alla console di Workspace ONE UEM e configurare il profilo del dispositivo iOS in Workspace ONE UEM e aggiungere il certificato dell'emittente di certificati del server KDC da VMware Identity Manager.

Configurazione del profilo Apple iOS in Workspace ONE UEM utilizzando autorità di certificazione Active Directory e modello di certificato

Creare e distribuire il profilo di dispositivo Apple iOS in Workspace ONE UEM per inserire le impostazioni del provider di identità nel dispositivo. Questo profilo contiene le informazioni necessarie al dispositivo per connettersi al provider di identità di VMware e il certificato utilizzato dal dispositivo stesso per l'autenticazione. Attivare Single Sign-On per consentire un accesso rapido e integrato senza richiedere l'autenticazione in ogni app.

Prerequisiti

- SSO mobile per iOS è configurato in VMware Identity Manager.
- File dell'autorità di certificazione iOS Kerberos salvato su un computer a cui sia possibile accedere dalla console di amministrazione di Workspace ONE UEM.
- Configurazione corretta in Workspace ONE UEM della propria autorità di certificazione e del modello di certificato.
- Elenco degli URL e degli ID dei pacchetti applicazione che utilizzano l'autenticazione SSO mobile per iOS sui dispositivi iOS.

Procedura

1 Nella console di Workspace ONE UEM, passare a **Dispositivi > Profili e risorse > Profili**.

2 Selezionare **Aggiungi > Aggiungi profilo** e selezionare **Apple iOS**.

3 Immettere il nome `iOSKerberos` e configurare le impostazioni in **Generale**.

4 Nel riquadro di navigazione di sinistra, selezionare **Credenziali > Configura** per configurare la credenziale.

Opzione	Descrizione
Origine credenziali	Selezionare **Autorità di certificazione definita** dal menu a discesa.
Autorità di certificazione	Selezionare l'autorità di certificazione nell'elenco del menu a discesa.
Modello di certificato	Selezionare il modello di richiesta che fa riferimento all'autorità di certificazione dal menu a discesa. Questo è il modello di certificato creato in Aggiunta del modello di certificato in Workspace ONE UEM.

5 Fare di nuovo clic sul **+** nell'angolo inferiore destro della pagina e creare una seconda credenziale.

6 Dal menu a discesa **Origine credenziali**, selezionare **Carica**.

7 Immettere il nome della credenziale.

8 Fare clic su **Carica** per caricare il certificato root del server KDC scaricato dalla pagina Gestione identità e accessi > Gestione > Provider di identità > Provider di identità integrato.

9 Nel riquadro di navigazione a sinistra, selezionare **Single Sign-On** e fare clic su **Configura**.

10 Immettere le informazioni di connessione.

Opzione	Descrizione
Nome account	Inserire `Kerberos`.
Nome principale Kerberos	Fare clic su **+** e scegliere **{EnrollmentUser}**.
Area di autenticazione	Per le distribuzioni tenant nel cloud, immettere il nome dell'area di autenticazione di Identity Manager per il tenant. Il testo di questo parametro deve essere in maiuscolo. Ad esempio, `VMWAREIDENTITY.COM`. Per distribuzioni in locale, immettere il nome dell'area di autenticazione utilizzato durante l'inizializzazione del KDC nell'appliance VMware Identity Manager. Ad esempio, `EXAMPLE.COM`
Certificati di rinnovo	Selezionare **Certificato 1** dal menu a discesa. Questo è il certificato della CA di Active Directory che è stato configurato per primo con le credenziali.
Prefissi URL	Immettere i prefissi di URL che devono corrispondere per poter utilizzare questo con autenticazione Kerberos su HTTP. Per le distribuzioni tenant nel cloud, immettere l'URL del server VMware Identity Manager nella forma `https://<tenant>.vmwareidentity.<region>`. Per distribuzioni in locale, immettere l'URL del server VMware Identity Manager nella forma `https://myco.example.com`.
Applicazioni	Inserire l'elenco di identificatori di applicazione a cui è consentito l'uso di questo accesso. Per eseguire un singolo accesso utilizzando il browser Safari integrato in iOS, immettere il primo ID di pacchetto applicazione nella forma `com.apple.mobilesafari`. Continuare l'immissione degli altri ID di pacchetti applicazione. Le applicazioni elencate devono supportare l'autenticazione SAML.

11 Fare clic su **Salva e pubblica**.

Operazioni successive

Assegnare il profilo dispositivo a un gruppo smart. I gruppi smart sono gruppi personalizzabili che determinano quali piattaforme, dispositivi e quali utenti riceveranno un'applicazione, una rubrica, un criterio di conformità, un profilo dispositivo o un provisioning assegnato.

Configurazione del profilo Apple iOS in Workspace ONE UEM mediante l'autorità di certificazione di Workspace ONE UEM

Creare e distribuire il profilo di dispositivo Apple iOS in Workspace ONE UEM per inserire le impostazioni del provider di identità nel dispositivo. Questo profilo contiene le informazioni necessarie al dispositivo per connettersi al provider di identità di VMware e il certificato utilizzato dal dispositivo stesso per l'autenticazione.

Prerequisiti

- Kerberos incorporato configurato in VMware Identity Manager.
- File del certificato root del server KDC di VMware Identity Manager salvato in un computer accessibile dalla console di Workspace ONE UEM.
- Certificato abilitato e scaricato dalla pagina Sistema > Integrazione aziendale > VMware Identity Manager della console di Workspace ONE UEM.
- Elenco degli URL e degli ID dei pacchetti applicazione che utilizzano l'autenticazione Kerberos integrata sui dispositivi iOS.

Procedura

1. Nella console di Workspace ONE UEM passare a **Dispositivi > Profili e risorse > Profilo > Aggiungi profilo** e selezionare **Apple iOS**.
2. Configurare le impostazioni della sezione **Generale** del profilo e specificare `iOSKerberos` come nome del dispositivo.
3. Nel riquadro di navigazione di sinistra, selezionare **SCEP > Configura** per configurare la credenziale.

Opzione	Descrizione
Origine credenziali	Selezionare **AirWatch Certificate Authority** dal menu a discesa.
Autorità di certificazione	Selezionare la **AirWatch Certificate Authority** dal menu a discesa.
Modello di certificato	Selezionare **Single Sign On** per impostare il tipo di certificato emesso dalla CA di AirWatch.

4. Fare clic su **Credenziali > Configura** e creare una seconda credenziale.
5. Dal menu a discesa **Origine credenziali**, selezionare **Carica**.
6. Immettere il nome della credenziale iOS Kerberos.

7 Fare clic su **Carica** per caricare il certificato root del server KDC di VMware Identity Manager scaricato dalla pagina Gestione identità e accessi > Gestione > Provider di identità > Provider di identità integrato.

8 Nel riquadro di navigazione di sinistra, selezionare **Single Sign-On**.

9 Immettere le informazioni di connessione.

Opzione	Descrizione
Nome account	Inserire **`Kerberos`**.
Nome principale Kerberos	Fare clic su **+** e scegliere **{EnrollmentUser}**.
Area di autenticazione	Per le distribuzioni tenant nel cloud, immettere il nome dell'area di autenticazione di VMware Identity Manager per il tenant. Il testo di questo parametro deve essere in maiuscolo. Ad esempio, **`VMWAREIDENTITY.COM`**. Per distribuzioni in locale, immettere il nome dell'area di autenticazione utilizzato durante l'inizializzazione del KDC nella macchina VMware Identity Manager. Ad esempio **`EXAMPLE.COM`**.
Certificati di rinnovo	Nei dispositivi iOS 8 o versione successiva, selezionare il certificato utilizzato per eseguire nuovamente l'autenticazione dell'utente in modo automatico senza alcuna interazione da parte dell'utente quando la sessione Single Sign-On dell'utente scade.
Prefissi URL	Immettere i prefissi di URL che devono corrispondere per poter utilizzare questo con autenticazione Kerberos su HTTP. Per le distribuzioni tenant nel cloud, immettere l'URL del server VMware Identity Manager nella forma **`https://<tenant>.vmwareidentity.<region>`**. Per distribuzioni in locale, immettere l'URL del server VMware Identity Manager nella forma **`https://myco.example.com`**.
Applicazioni	Inserire l'elenco di identificatori di applicazione a cui è consentito l'uso di questo accesso. Per eseguire un singolo accesso utilizzando il browser Safari integrato in iOS, immettere il primo ID di pacchetto applicazione **`com.apple.mobilesafari`**. Continuare l'immissione degli altri ID di pacchetti applicazione. Le applicazioni elencate devono supportare l'autenticazione SAML.

10 Fare clic su **Salva e pubblica**.

Dopo aver inserito il profilo iOS nei dispositivi degli utenti, questi possono accedere a VMware Identity Manager utilizzando il metodo di autenticazione Kerberos integrato senza dover immettere le proprie credenziali.

Operazioni successive

Assegnare il profilo dispositivo a un gruppo smart. I gruppi smart sono gruppi personalizzabili che determinano quali piattaforme, dispositivi e quali utenti riceveranno un'applicazione, una rubrica, un criterio di conformità, un profilo dispositivo o un provisioning assegnato.

Assegnazione di un profilo dispositivo di Workspace ONE UEM

Dopo aver creato un profilo dispositivo, assegnare il profilo a un gruppo smart.

I gruppi smart sono gruppi personalizzabili che determinano quali piattaforme, dispositivi e quali utenti riceveranno un'applicazione, un criterio di conformità, un profilo dispositivo o un provisioning assegnato. Vedere la guida di Workspace ONE UEM Mobile Device Management.

Procedura

1. Nella console di Workspace ONE UEM, passare a **Dispositivi > Profili e risorse** > **Profili**.
2. Selezionare il profilo dispositivo da assegnare al gruppo smart.
3. Nella scheda Generale, fare clic sulla casella di testo **Gruppi assegnati** e selezionare **Crea gruppo di assegnazione**.
4. Nella pagina Crea nuovo gruppo smart, inserire il nome del gruppo smart.
5. Selezionare **Piattaforma e sistema operativo** e selezionare il sistema operativo e la versione corretti dal menu a discesa.
6. Fare clic su **Salva e pubblica**.

Dopo aver assegnato un gruppo smart all'opzione di dispositivo, gli utenti possono registrarsi in Workspace ONE e accedere alle applicazioni dal catalogo.

Implementazione dell'autenticazione Single Sign-On mobile per dispositivi Android gestiti

4

Single Sign-on (SSO) mobile per Android è un'implementazione del metodo di autenticazione del certificato per i dispositivi Android gestiti da Workspace ONE UEM. SSO mobile consente agli utenti di accedere al proprio dispositivo ed effettuare l'accesso sicuro alle proprie app di Workspace ONE senza dover reimmettere una password.

L'app mobile VMware Tunnel® è installata sul dispositivo Android per aggiungere informazioni sul certificato e l'ID dispositivo nei flussi di autenticazione. Le impostazioni di Tunnel sono configurate in Workspace ONE UEM Console per accedere al servizio VMware Identity Manager per l'autenticazione, è quindi il servizio che si occupa di recuperare il certificato dal dispositivo per l'autenticazione.

Nella Workspace ONE UEM Console è possibile configurare anche le impostazioni seguenti.

- Profilo VPN per Android. Questo profilo è utilizzato per attivare le funzionalità di tunneling per app per Android.
- Abilitare la VPN per ogni app che utilizza la funzionalità di tunnel dell'app in Workspace ONE UEM Console.
- Creare regole del traffico di rete con un elenco di tutte le applicazioni configurate per la VPN per app, i dettagli del server proxy e l'URL di VMware Identity Manager.

Quando si implementa SSO mobile per Android con il servizio VMware Identity Manager in locale, si configura il servizio proxy certificato nella macchina VMware Identity Manager. Dopo aver configurato il servizio proxy certificato, è possibile configurare l'autenticazione del certificato nel provider di identità integrato VMware Identity Manager dalla console di VMware Identity Manager.

Durante l'implementazione di SSO mobile per Android con il servizio VMware Identity Manager nel cloud, è possibile configurare l'autenticazione del certificato nel provider di identità integrato di VMware Identity Manager dalla console di VMware Identity Manager. Il servizio proxy certificato viene gestito per l'utente.

Vedere la pubblicazione *Android Mobile Single Sign-on a VMware Workspace One* nel Centro documentazione di Workspace ONE per informazioni dettagliate sulla configurazione di SSO Mobile per Android.

Dispositivo Android supportato

È supportato Android 5.1 o versioni successive.

Le applicazioni a cui si accede da un dispositivo Android devono supportare SAML o un altro standard di federazione supportato per il Single Sign-On.

Registrazione diretta tramite l'app Workspace ONE

5

La registrazione diretta tramite Workspace ONE richiede che gli utenti registrino i propri dispositivi prima di poter accedere alle risorse dell'applicazione Workspace ONE.

Quando la registrazione diretta avviene tramite l'applicazione Workspace ONE, è possibile richiedere a tutti gli utenti di accedere allo store delle applicazioni appropriato, scaricare l'app Workspace ONE, immettere il proprio indirizzo e-mail e seguire le istruzioni per iniziare a utilizzare Workspace ONE sui loro dispositivi.

Dispositivi supportati

- Apple iOS 9.0 e versioni successive
- Android Enterprise (precedentemente denominato Android for Work) 5.1 e versioni successive
- Android Legacy 4.1 e versioni successive

  Un dispositivo Android Legacy è qualsiasi dispositivo Android che non supporta Android Enterprise, oppure un dispositivo in grado di supportare Android Enterprise connesso a un'istanza di Workspace ONE UEM in cui Android Enterprise non è abilitato.

Questo capitolo include i seguenti argomenti:

Abilitazione di Workspace ONE per la registrazione diretta

È possibile abilitare la registrazione diretta del dispositivo tramite Workspace ONE dalla pagina Registrazione > Restrizione della console di Workspace ONE UEM per il proprio gruppo di organizzazioni.

Quando Workspace ONE è abilitato per la registrazione diretta, i dispositivi idonei che effettuano la registrazione per la prima volta vengono registrati direttamente. I dispositivi non idonei per la registrazione diretta possono accedere alle sole funzioni di gestione dell'applicazione mobile in uno stato registrato di Workspace ONE.

Procedura

1. Nella console di Workspace ONE UEM, selezionare il gruppo di organizzazioni per abilitare la registrazione diretta per Workspace ONE.
2. Passare a **Gruppi e impostazioni > Tutte le impostazioni > Dispositivi e utenti > Generale > Registrazione** e selezionare la scheda **Restrizioni**.
3. Per Impostazioni correnti, selezionare **Sostituisci** se necessario.
4. Scorrere verso il basso fino a raggiungere Requisiti di gestione per Workspace ONE e selezionare le opzioni di configurazione.

Impostazione	Descrizione
Richiedi MDM per Workspace ONE	Quando questa opzione è attivata, agli utenti e ai dispositivi idonei viene richiesto di registrarsi immediatamente dopo l'accesso a Workspace ONE.
Gruppo utenti assegnato	Tutti gli utenti è il gruppo utenti predefinito. È possibile selezionare un gruppo utenti specifico da includere nel processo di registrazione diretta.
iOS	Abilitare questa opzione per includere i dispositivi iOS. I dispositivi iOS non saranno idonei per la registrazione diretta se questa opzione è disabilitata. Se l'opzione è disabilitata, i dispositivi potranno effettuare comunque la registrazione in Workspace ONE UEM in uno stato non gestito.
Android Legacy	Abilitare questa opzione per includere i dispositivi Android Legacy. I dispositivi Android Legacy non sono idonei per la registrazione diretta se questa opzione è disabilitata. Se l'opzione è disabilitata, i dispositivi potranno effettuare comunque la registrazione in Workspace ONE UEM in uno stato non gestito.
Android Enterprise	Abilitare questa opzione per includere i dispositivi Android Enterprise. I dispositivi Android Enterprise non sono idonei per la registrazione diretta se questa opzione è disabilitata. Se l'opzione è disabilitata, i dispositivi potranno effettuare comunque la registrazione in Workspace ONE UEM in uno stato non gestito.

5. Fare clic su **Salva**.
6. Continuare a configurare le schede relative alla registrazione con le opzioni di registrazione supportate per Workspace ONE. Vedere Opzioni di configurazione della registrazione diretta di Workspace ONE.

   Per ulteriori informazioni sulla configurazione della registrazione diretta per Workspace ONE, vedere la Guida di VMware AirWatch Mobile Device Management nel capitolo sulla registrazione del dispositivo.

Opzioni di configurazione della registrazione diretta di Workspace ONE

Configurare la registrazione diretta in Workspace ONE nella console di Workspace ONE UEM. Passare a **Gruppi e impostazioni > Tutte le impostazioni > Dispositivo e utenti/Generale/Registrazione**. La tabella delle opzioni di registrazione del dispositivo di Workspace ONE include l'elenco delle voci di menu che possono essere configurate.

La pagina delle impostazioni di registrazione consente di configurare le opzioni relative alla registrazione di dispositivi e utenti. La pagina è suddivisa nelle schede descritte di seguito. Per informazioni dettagliate sulla configurazione della registrazione del dispositivo, vedere la guida VMware Workspace ONE UEM Mobile Device Management.

Figura 5-1. Pagina di registrazione console di Workspace ONE UEM

Tabella 5-1. Voci di menu configurabili della registrazione diretta di Workspace ONE

Scheda Registrazione	Voci di menu configurabili per la registrazione diretta a Workspace ONE
Autenticazione	Gli utenti della directory sono supportati. Sono inoltre supportati gli utenti di SAML e Active Directory "al volo". Un utente SAML senza LDAP è supportato quando il record dell'utente è presente in Workspace ONE UEM al momento dell'accesso iniziale. Per la mod di registrazione dispositivi, è supportata solo la **registrazione aperta** . Solo dispositivi registrati non è supportata.
Condizioni d'uso	È possibile creare condizioni d'uso che gli utenti dovranno accettare prima di poter procedere con il processo di registrazione diretta.
Raggruppamento	Tutte le opzioni del menu Raggruppamento sono compatibili con la registrazione diretta di Workspace ONE. L'opzione **Sincronizza utenti e gruppi in tempo reale per Workspace ONE** è abilitata per impostazione predefinita. Quando un dispositivo è in fase di registrazione, Workspace ONE UEM effettua una chiamata in tempo reale ad Active Directory per sincronizzare i gruppi di utenti dell'utente. Se l'utente non esiste in Workspace ONE UEM, la console di Workspace ONE UEM sincronizza innanzitutto l'utente e quindi sincronizza i gruppi di utenti in tempo reale. Se questa funzionalità non è abilitata, la console di Workspace ONE UEM non sincronizza i gruppi di utenti. **Nota** Questa funzionalità determina un utilizzo elevato della CPU. Se i gruppi di utenti non vengono modificati di frequente o esistono già in Workspace ONE UEM, disabilitare questa impostazione per migliorare le prestazioni ed evitare problemi di latenza quando si avvia l'app Workspace ONE. Vedere la sezione sull'inserimento dei dispositivi nel gruppo di organizzazioni corretto in Strategie di distribuzione per l'impostazione di gruppi di organizzazioni di Workspace ONE UEM multipli.

Tabella 5-1. Voci di menu configurabili della registrazione diretta di Workspace ONE (Continua)

Scheda Registrazione	Voci di menu configurabili per la registrazione diretta a Workspace ONE
Restrizioni	■ In **Controllo dell'accesso dell'utente** è possibile selezionare sia Limita la registrazione agli utenti conosciuti sia Limita la registrazione solo ai gruppi configurati. ■ È supportato il limite del numero massimo di dispositivi. ■ L'**Impostazione dei criteri** è parzialmente supportata. ■ **Tipi di proprietà consentiti**. Workspace ONE richiede Personale e Aziendale (dedicato). **Nota** Il tipo di registrazione Container non è supportato.
Richieste facoltative	Le due richieste facoltative che possono essere abilitate sono **Richiedi tipo di proprietà** e **Attiva messaggio di richiesta del numero dell'asset**. La richiesta di immettere il numero dell'asset viene presentata solo quando il tipo di proprietà è Aziendale.
Personalizzazione	Opzioni del menu di personalizzazione supportate. ■ URL di destinazione dopo la registrazione (solo iOS) ■ Messaggio profilo MDM (solo iOS) ■ Utilizzo di applicazioni MDM personalizzate L'utilizzo di un modello di messaggio specifico per ogni piattaforma può essere abilitato, ma non sono disponibili modelli di messaggio Workspace ONE specifici per Workspace ONE 3.2.

Esperienza utente durante la registrazione diretta in Workspace ONE UEM con Workspace ONE

Quando la gestione dei dispositivi mobili è implementata tramite Workspace ONE, gli utenti scaricano l'applicazione Workspace ONE, effettuano l'autenticazione in Workspace ONE UEM e registrano il dispositivo. Dopo la registrazione del dispositivo, gli utenti possono utilizzare Workspace ONE per aggiungere e utilizzare immediatamente le proprie risorse idonee.

Il processo che gli utenti sperimentano quando si utilizzano Workspace ONE per registrare i dispositivi è simile per i dispositivi iOS e per i dispositivi Android Enterprise. La registrazione Android Legacy viene reindirizzata ad AirWatch Agent per la registrazione. AirWatch Agent restituisce automaticamente il controllo a Workspace ONE una volta completata la registrazione. Gli utenti possono accedere a Workspace ONE in ciascuna di queste varianti.

Registrazione diretta tramite Workspace ONE su dispositivi iOS

Indicare agli utenti di scaricare, installare ed eseguire l'applicazione Workspace ONE dall'App Store di Apple.

Procedura

1 Gli utenti aprono l'app, immettono il proprio indirizzo e-mail e URL del server e si autenticano a seconda della configurazione per il proprio ambiente.

2 Viene visualizzata la **schermata configurazione aggiuntiva richiesta dall'azienda**.

Figura 5-2. Notifica della configurazione della registrazione del dispositivo

3 Se Condizioni d'uso è configurato, agli utenti viene chiesto di accettare le condizioni d'uso prima di procedere.

4 Se le richieste facoltative sono impostate in modo che venga visualizzato il tipo di proprietà del dispositivo e la richiesta di specificare il numero di asset del dispositivo, tali informazioni vengono visualizzate.

Figura 5-3. Selezione delle proprietà del dispositivo

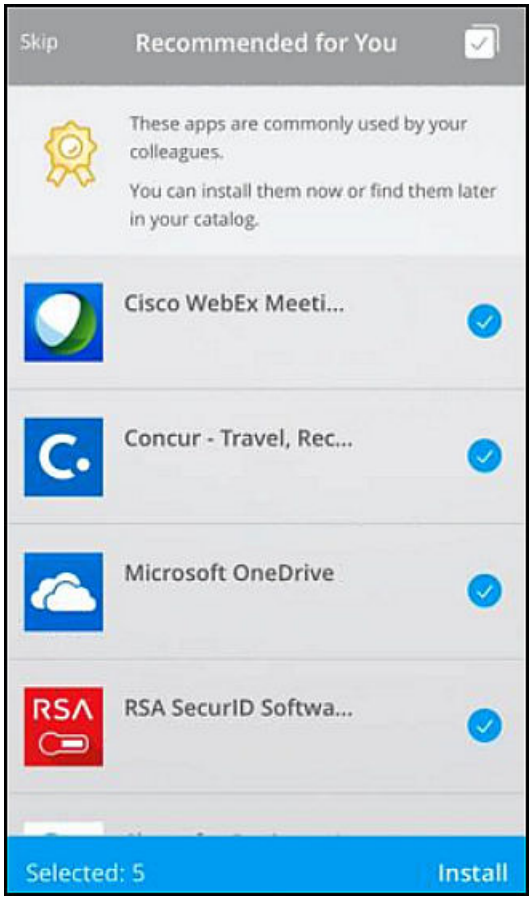
5 Viene aperto Safari e gli utenti fanno clic su **Consenti** per aprire la pagina Impostazioni.

Figura 5-4. Consenti impostazioni del profilo di configurazione

I Servizi area di lavoro e il profilo di configurazione sono configurati sul dispositivo.

Ora il dispositivo è registrato in Workspace ONE UEM e Workspace ONE viene avviato. Viene visualizzata la schermata Consigliata per te.

Figura 5-5. Schermata delle applicazioni consigliate



6 Gli utenti possono selezionare le applicazioni che desiderano installare oppure saltare temporaneamente questo passaggio.

Ora il dispositivo è gestito da Workspace ONE UEM MDM. Se sono state selezionate applicazioni consigliate da installare, gli utenti iniziano a ricevere notifiche push per tali applicazioni.

Registrazione diretta tramite Workspace ONE sui dispositivi Android aziendali

Indica agli utenti di scaricare, installare ed eseguire l'applicazione Workspace ONE da Google App Store o dal repository.

Procedura

1 Gli utenti immettono il proprio indirizzo e-mail e URL del server e si autenticano a seconda della configurazione per il proprio ambiente.

2 Viene visualizzata la **schermata configurazione aggiuntiva richiesta dall'azienda**. L'utente fa clic su **Continua**.

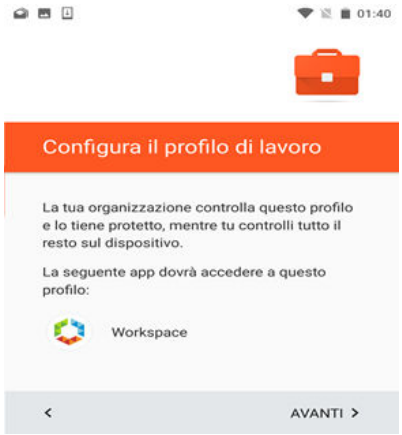
Figura 5-6. Notifica della configurazione della registrazione del dispositivo

3 Se Condizioni d'uso è configurato, agli utenti viene chiesto di accettare le condizioni d'uso prima di procedere.

4 Se le richieste facoltative sono impostate in modo che venga visualizzato il tipo di proprietà del dispositivo e la richiesta di specificare il numero di asset del dispositivo, tali informazioni vengono visualizzate.

5 I servizi area di lavoro e il profilo di lavoro vengono configurati sul dispositivo.

Figura 5-7. Impostazione della notifica del profilo di lavoro

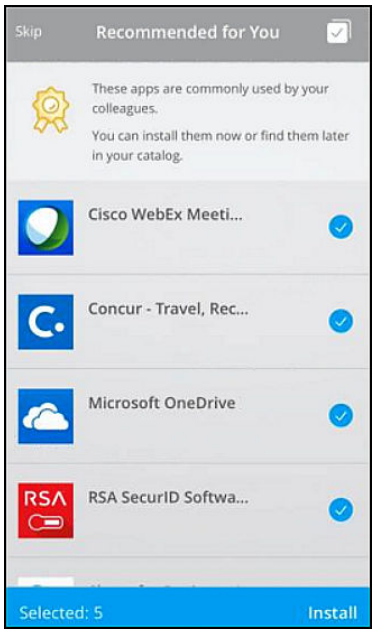


Gli utenti visualizzano un messaggio che descrive il controllo della gestione del dispositivo per il profilo di lavoro corrente e fanno clic su **OK**.

L'applicazione Workspace ONE viene installata e l'Account Android Work viene registrato.

6 Ora il dispositivo è registrato in Workspace ONE UEM e Workspace ONE viene avviato. Viene visualizzata la schermata Consigliata per te.

Figura 5-8. Schermata delle applicazioni consigliate



7 Gli utenti possono selezionare le applicazioni che desiderano installare oppure saltare temporaneamente questo passaggio.

Ora il dispositivo è gestito da Workspace ONE UEM MDM. Se si è scelto di installare applicazioni consigliate, ha inizio l'installazione delle applicazioni e in loro corrispondenza viene mostrata un'icona contrassegnata Android Enterprise a forma di valigetta.

Registrazione del dispositivo per i dispositivi Android legacy

Registrazione del dispositivo per i dispositivi Android Legacy reindirizza ad AirWatch Agent per la registrazione. AirWatch Agent automaticamente restituisce il controllo a Workspace ONE una volta completata la registrazione.

Indicare agli utenti di accedere all'archivio di applicazioni per il download di Workspace ONE.

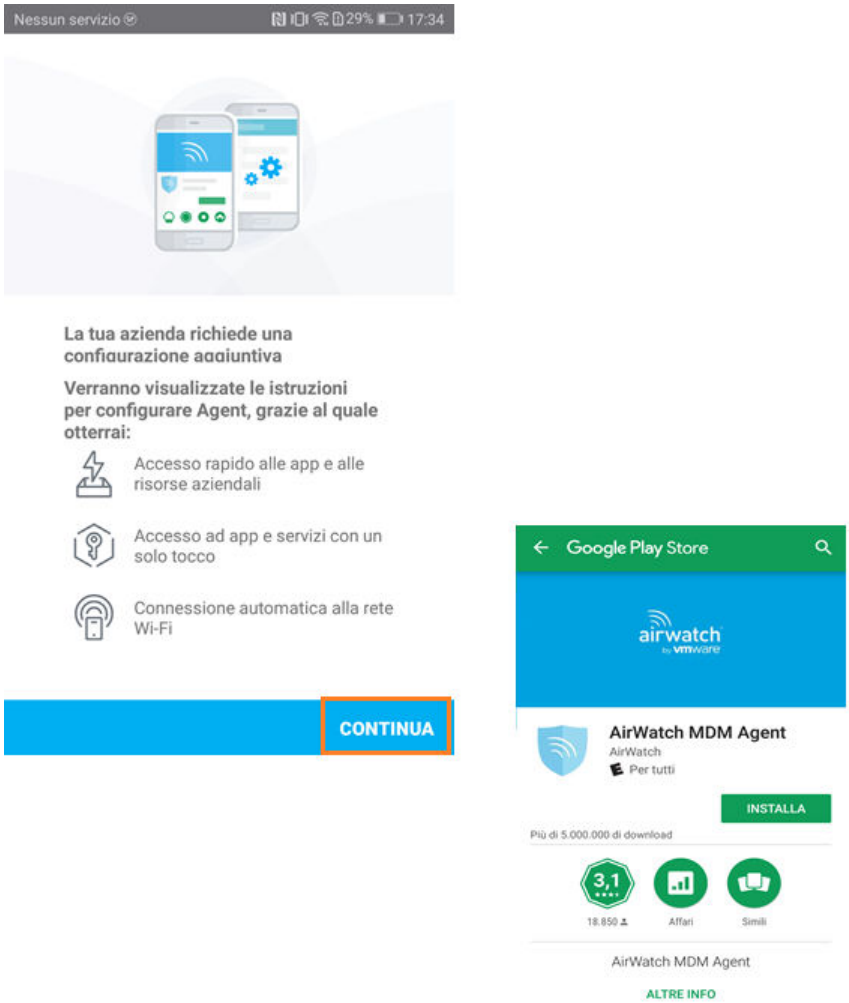
Procedura

1 Gli utenti aprono l'app, immettono gli URL del server o l'indirizzo e-mail e il nome utente e la password per accedere.

   A questo punto, l'applicazione Workspace ONE può rilevare che il dispositivo non è abilitato per Android Enterprise e se il dispositivo richiede la registrazione diretta prima che sia possibile accedere alle risorse su Workspace ONE.

2 Viene visualizzato **La tua azienda richiede una configurazione aggiuntiva** e quando gli utenti fanno clic su **Continua** vengono reindirizzati all'applicazione AirWatch Agent in Google Play Store.

Figura 5-9. Richiesta di download dell'applicazione AirWatch Agent



3 Gli utenti eseguono il download dell'applicazione AirWatch Agent.

Nota Se l'applicazione AirWatch Agent è già installata sul dispositivo, Workspace ONE automaticamente avvia l'applicazione. Non vengono reindirizzati all'app store.

I dettagli di autenticazione immessi per Workspace ONE vengono trasmessi all'applicazione AirWatch Agent in modo che gli utenti non debbano reimmettere queste informazioni.

Viene avviata l'applicazione AirWatch Agent. Durante la registrazione del dispositivo con AirWatch Agent, gli utenti selezionano il tipo di proprietà e immettono il numero di asset del dispositivo, se configurato.

4 Quando **Consentire all'agente di effettuare e gestire chiamate telefoniche?** viene visualizzato, fare clic su **Consenti**.

AirWatch Agent convalida la registrazione, autentica l'utente e concede le autorizzazioni ad AirWatch sul dispositivo in uso.

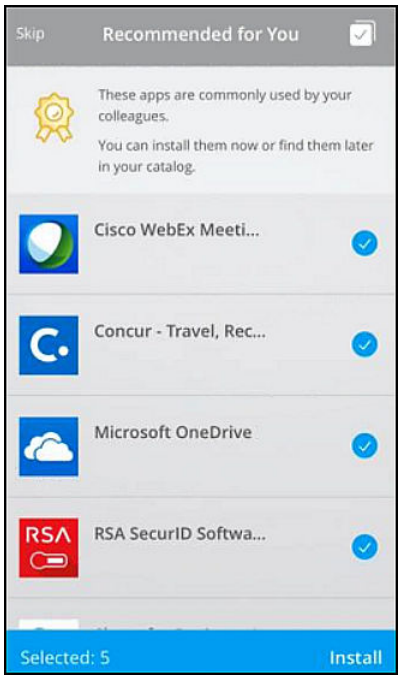
5 Quando verrà visualizzata la schermata**Attiva app dell'amministratore del dispositivo,** fare clic su **Attiva app dell'amministratore di questo dispositivo**.

Figura 5-10. Attivazione dell'app dell'amministratore del dispositivo

6 Agli utenti viene chiesto di concedere l'autorizzazione per accedere a varie funzionalità del dispositivo.

Ora il dispositivo è registrato in Workspace ONE UEM e Workspace ONE viene avviato. Viene visualizzata la schermata delle applicazioni consigliate.

Figura 5-11. Schermata delle applicazioni consigliate



7 Gli utenti possono selezionare le applicazioni che desiderano installare oppure saltare temporaneamente questo passaggio.

Ora il dispositivo è gestito da Workspace ONE UEM MDM. Se sono state selezionate applicazioni consigliate da installare, gli utenti iniziano a ricevere notifiche per tali applicazioni.

Applicazione di Workspace ONE per supportare l'integrazione del Device Enrollment Program di Apple

6

Il Device Enrollment Program (DEP) di Apple non supporta gli scenari in cui un cliente utilizza SAML per l'autenticazione utente. Tuttavia Workspace ONE ha implementato un modo univoco per il supporto di questo caso d'uso.

Tramite lo staging del dispositivo Workspace ONE UEM, gli amministratori possono assegnare il dispositivo a un utente di staging multidispositivo e consentire a Workspace ONE di riassegnare il dispositivo all'utente appropriato quando effettua l'accesso all'applicazione Workspace ONE.

L'applicazione Workspace ONE deve essere installata sul dispositivo durante la registrazione dell'utente di staging. Quando gli utenti accedono a Workspace ONE per la prima volta, Workspace ONE li autentica mediante il provider SAML configurato. Dopo che l'utente è stato autenticato, la proprietà del dispositivo passa dall'utente di staging multidispositivo all'utente della directory autenticato.

Prerequisito

L'utente della directory deve esistere in Workspace ONE UEM quando accede all'applicazione Workspace ONE. È possibile pre-caricare gli utenti in massa tramite CSV o applicare la seguente API per generare gli utenti secondo necessità.

Nota Il valore di Tipo di sicurezza deve essere uguale alla directory.

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

Flusso per il supporto dell'integrazione di DEP di Workspace ONE

Per implementare il supporto di Device Enrollment Program di Apple utilizzando Workspace ONE è necessario completare le seguenti attività.

- Installare l'applicazione Workspace ONE sui dispositivi iOS.
- Verificare l'esistenza di un utente di staging con la seguente configurazione di staging nella console di Workspace ONE UEM.
  a Passare a **Account > Utenti > Visualizzazione elenco** e selezionare l'account utente per il quale si desidera abilitare lo staging del dispositivo da modificare.

b Nella pagina **Aggiungi/modifica** utente, selezionare la scheda **Avanzate**. Scorrere verso il basso la sezione **Staging** e abilitare **Staging del dispositivo** e **Dispositivi multiutenti**.

Figura 6-1. Impostazione Dispositivi multiutenti in Workspace ONE UEM

- Assegnare al dispositivo l'utente di staging nel portale DEP di Apple e fornire il dispositivo all'utente finale.

  Per ulteriori informazioni sull'Apple Device Enrollment Program, vedere la Guida per la registrazione dei dispositivi Apple.

Funzionamento dell'integrazione

Quando l'utente accende per la prima volta il dispositivo, questo viene registrato e assegnato all'utente di staging multidispositivo. L'utente avvia l'applicazione Workspace ONE disponibile nella schermata principale e accede. Workspace ONE autentica l'utente mediante il provider SAML configurato.

Dopo che l'utente è stato autenticato, la proprietà del dispositivo passa dall'utente di staging multidispositivo all'utente della directory autenticato. Applicazioni, risorse e profili assegnati all'utente autenticato vengono inviati al dispositivo.

Nota Il gruppo di organizzazioni del dispositivo non viene modificato. Questa funzionalità non supporta la mappatura del gruppo di utenti (o la selezione manuale dell'utente in base al menu a discesa) che si trova nella sezione Impostazione registrazione della console di Workspace ONE UEM.

Distribuzione dell'applicazione mobile VMware Workspace ONE 7

Installando l'applicazione VMware Workspace ONE su dispositivi mobili, gli utenti possono accedere alle risorse che sono autorizzati a utilizzare.

Se le loro identità sono gestite con VMware Identity Manager, gli utenti possono accedere alle applicazioni per cui sono autorizzati utilizzando la funzionalità Single Sign-On. Essi inoltre possono accedere a un catalogo di app in cui possono aggiungere altre applicazioni.

L'interfaccia dell'applicazione Workspace ONE offre un'esperienza e opzioni simili a qualsiasi altro smartphone, tablet o computer desktop.

Se il dispositivo è registrato in Mobile Device Management (MDM), è possibile inviare in push l'applicazione Workspace ONE come applicazione gestita.

Questo capitolo include i seguenti argomenti:

Opzioni di gestione dei dispositivi in Workspace ONE UEM per le app pubbliche e interne per Workspace ONE

È possibile configurare la distribuzione delle applicazioni pubbliche e interne in base allo stato di gestione dei dispositivi. Qualsiasi dispositivo può accedere alle applicazioni configurate con accesso aperto. Alle applicazioni configurate con accesso gestito, invece, possono accedere solo i dispositivi a cui è concessa l'autorizzazione, tramite l'abilitazione con Servizi area di lavoro o Registrazione agente.

La tabella descrive le funzionalità per le configurazioni gestito e non gestito.

Tipo di accesso	Funzionalità	Descrizione	Usi consigliati
Accesso aperto (non gestito)	■ Catalogo di app self-service per risorse Web, Horizon e Citrix ■ Avvio di applicazioni Web/virtuali con Single Sign-On (SSO). ■ Protezione applicazioni con Touch ID / PIN. ■ Rilevamento jailbreak dispositivo. ■ Supporto per accesso condizionale di VMware Identity Manager, inclusi criteri di autenticazione e blocco dei dispositivi. ■ Accesso ad applicazioni native. ■ Distribuzione app interne e app SDK.	Gli utenti accedono a risorse sul proprio dispositivo senza concessione di autorizzazione amministrativa per accedere al proprio dispositivo. Le applicazioni con accesso aperto sono disponibili ai dispositivi indipendentemente dal loro stato di gestione. Gli amministratori non possono rimuovere sistematicamente le applicazioni native quando sono impostate sull'accesso aperto.	■ Fornire accesso alle applicazioni agli utenti finali immediatamente in fase di accesso, senza autorizzazioni di sicurezza elevate. ■ Consigliare l'uso di un'applicazione senza richiederne l'installazione. Gli utenti possono installare l'applicazione sul proprio dispositivo quando desiderano. ■ Applicazioni che non contengono dati aziendali sensibili e che non accedono alle risorse protette dell'azienda. ■ Distribuire applicazioni a personale ausiliario senza profilo MDM di Workspace ONE UEM.
Accesso gestito	■ Catalogo di app self-service per risorse Web, Horizon e Citrix ■ Avvio di applicazioni Web/virtuali con Single Sign-On (SSO). ■ Protezione applicazioni con Touch ID / PIN. ■ Rilevamento jailbreak dispositivo. ■ Supporto per accesso condizionale di VMware Identity Manager, inclusi criteri di autenticazione e blocco dei dispositivi. ■ Installazione gestita e diretta di app native. ■ Gestione di app interne e app SDK. ■ Supporto per la configurazione di app. ■ VPN per app ■ SSO One Touch per app native compatibili con SAML. ■ Profili dispositivo ■ Motore di conformità di Workspace ONE UEM	Gli utenti installano un profilo di gestione sul proprio dispositivo per concedere l'autorizzazione amministrativa per accedere al proprio dispositivo. Le applicazioni con accesso gestito sono disponibili per i dispositivi gestiti da Workspace ONE UEM. Se Workspace ONE UEM non gestisce il dispositivo, Workspace ONE richiede all'utente del dispositivo di eseguire la registrazione in Workspace ONE UEM. Se il dispositivo viene registrato, l'utente può continuare a utilizzare il dispositivo per accedere all'applicazione tramite Workspace ONE.	■ Rimuovere dati aziendali sensibili dai dispositivi quando gli utenti abbandonano l'organizzazione o smarriscono il proprio dispositivo. ■ Richiedere il tunneling dell'app per eseguire l'autenticazione e comunicare in modo sicuro con le risorse di back-end interne quando le applicazioni accedono all'intranet. ■ Abilitare Single Sign-On per le applicazioni. ■ Tracciare l'adozione degli utenti e lo stato di installazione delle applicazioni. ■ Distribuire l'applicazione automaticamente in fase di registrazione.

Per informazioni su dove configurare le opzioni di accesso gestito per le applicazioni interne o su come aggiungere applicazioni pubbliche per la distribuzione tramite Workspace ONE, vedere la guida Mobile Application Management di Workspace ONE UEM.

Piattaforme supportate per l'accesso aperto e gestito

Configurare il tipo di accesso per le applicazioni interne e pubbliche in base alla piattaforma.

	Accesso gestito	Accesso aperto
APPLICAZIONI INTERNE		
Android	X	X
iOS	X	X
Desktop Windows 10	X	-
Telefono Windows 10	X	-
APPLICAZIONI PUBBLICHE		
Android	X	X
iOS	X	X
Desktop Windows 10	-	X
Telefono Windows 10	-	X

Gestione dell'accesso alle applicazioni

Un singolo utente potrebbe essere autorizzato a una combinazione di accessi gestiti e aperti ad app native. L'approccio della gestione adattiva consente agli utenti finali di utilizzare applicazioni ad accesso aperto senza dover ricorrere necessariamente alla gestione. Quando gli utenti richiedono un'app nativa che richiede gestione, la gestione adattiva fornisce la sicurezza e il controllo aggiuntivi necessari per gestire quella app nativa.

Quando le applicazioni sono gestite, gli utenti devono abilitare i Servizi area di lavoro per installare e utilizzare le applicazioni gestite. Quando si carica un'applicazione nella console di Workspace ONE UEM, lo stato di accesso viene indicato come aperto o gestito in base alla configurazione dell'applicazione. Se ad esempio è selezionata l'opzione **Invia configurazione app**, un'applicazione è impostata per richiedere la gestione.

Le applicazioni che richiedono la gestione mostrano l'icona di una stella quando visualizzate nel catalogo nello stato non gestito. Per poter utilizzare l'applicazione, gli utenti devono scegliere di abilitare i Servizi area di lavoro mediante il processo di gestione adattiva. Se gli utenti tentano di scaricare un'applicazione su cui è presente l'icona della stella, ricevono un messaggio che richiede loro di abilitare i Servizi area di lavoro. Gli utenti possono fare clic su un link informativo sulla riservatezza per conoscere quale sarà l'impatto sulla riservatezza delle loro informazioni personali se scelgono di continuare con il processo di gestione adattiva. La notifica sulla privacy ricava automaticamente le impostazioni dall'ambiente Workspace ONE UEM in cui si sta per eseguire la registrazione. Dopo aver esaminato le informazioni

sull'impostazione della privacy, gli utenti possono procedere con l'abilitazione dei Servizi area di lavoro o tornare indietro e continuare a utilizzare l'applicazione Workspace ONE non gestita sul dispositivo. Quando gli utenti registrano i Servizi area di lavoro, l'icona della stella viene rimossa da tutte le applicazioni gestite.

Rimozione dell'accesso su dispositivi gestiti

Gli utenti possono disabilitare l'app Workspace ONE sul proprio dispositivo gestito tramite l'opzione Rimuovi account. Con la rimozione dell'account viene eseguita una rimozione dei dati aziendali dal dispositivo, che cancella l'accesso aziendale e riporta l'utente alla schermata di accesso. Gli amministratori possono eseguire la rimozione dei dati aziendali dalla console di Workspace ONE UEM per disabilitare i servizi di Workspace ONE.

L'esecuzione di un'azione Rimuovi account su dispositivi gestiti revoca l'accesso concesso tramite l'applicazione Workspace ONE e annulla la registrazione del dispositivo da Workspace ONE UEM. Le applicazioni che richiedevano la gestione vengono rimosse dal dispositivo e l'accesso alle applicazioni di produttività di Workspace ONE UEM, come Boxer, Browser e Content Locker, viene revocato.

Richiesta delle condizioni d'uso per accedere al catalogo di Workspace ONE

È possibile scrivere le condizioni d'uso di Workspace ONE della propria organizzazione e fare in modo che l'utente finale le accetti prima di poter utilizzare Workspace ONE.

Le condizioni d'uso vengono visualizzate dopo che l'utente accede a Workspace ONE. Gli utenti devono accettare le condizioni d'uso prima di poter passare al catalogo di Workspace ONE.

La funzionalità Condizioni d'uso include le opzioni di configurazione seguenti.

- Creare versioni delle condizioni d'uso esistenti.
- Modificare le condizioni d'uso.
- Creare più condizioni d'uso che possono essere visualizzate in base al tipo di dispositivo.
- Creare copie delle condizioni d'uso specifiche della lingua.

I criteri configurati per le condizioni d'uso vengono elencati nella scheda Gestione identità e accessi. È possibile modificare i criteri delle condizioni d'uso per correggere i criteri esistenti o creare nuove versioni dei criteri. La nuova versione delle condizioni d'uso che viene aggiunta sostituisce quella esistente. Se si modifica un criterio, non viene creata una nuova versione delle condizioni d'uso.

Nella pagina Condizioni d'uso è possibile visualizzare il numero di utenti che hanno accettato o rifiutato le condizioni d'uso. Fare clic sul numero dei consensi o su quello dei rifiuti per visualizzare un elenco degli utenti e del loro stato.

Configurazione e abilitazione delle condizioni d'uso

Nella pagina Condizioni d'uso, è possibile aggiungere i criteri delle condizioni d'uso e configurare i parametri di utilizzo. Dopo aver aggiunto le condizioni d'uso, abilitare l'opzione Condizioni d'uso. Quando gli utenti accedono a Workspace ONE, devono accettare le condizioni d'uso per accedere al proprio catalogo.

Prerequisiti

Testo dei criteri delle condizioni d'uso formattato in HTML da copiare e incollare nella casella di testo Condizioni d'uso. È possibile aggiungere le condizioni d'uso in inglese, tedesco, spagnolo, francese, italiano e olandese.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager, selezionare **Configurazione > Termini di utilizzo**.
2. Fare clic su **Aggiungi Condizioni d'uso**.
3. Immettere un nome descrittivo per le condizioni d'uso.
4. Selezionare **Qualsiasi** se i criteri delle condizioni d'uso si applicano a tutti gli utenti. Per utilizzare le condizioni d'uso in base al tipo di dispositivo, selezionare **Piattaforme dispositivi selezionati**, quindi selezionare i tipi di dispositivi in cui visualizzare questi criteri delle condizioni d'uso.
5. Per impostazione predefinita, la lingua delle condizioni d'uso che viene visualizzata per prima dipende dall'impostazione della preferenza della lingua del browser. Nella casella di testo, immettere il contenuto delle condizioni d'uso per la lingua predefinita.
6. Fare clic su **Salva**.

   Per aggiungere criteri delle condizioni d'uso in un'altra lingua, fare clic su **Aggiungi lingua** e selezionare un'altra lingua. La casella di testo del contenuto delle condizioni d'uso viene aggiornata ed è possibile aggiungere testo nella casella di testo.

   È possibile trascinare il nome della lingua per stabilire l'ordine in cui le condizioni d'uso vengono visualizzate.
7. Per iniziare a utilizzare le condizioni d'uso, fare clic su **Abilita Condizioni d'uso** nella pagina visualizzata.

Operazioni successive

Se si seleziona un tipo di dispositivo specifico per le condizioni d'uso, è possibile creare condizioni d'uso aggiuntive per gli altri tipi di dispositivi.

Visualizzazione dello stato dell'accettazione delle condizioni d'uso

I criteri delle condizioni d'uso elencati nella pagina Gestione identità e accessi > Condizioni d'uso indicano il numero di utenti che hanno accettato o rifiutato il criterio.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager, selezionare **Configurazione > Termini di utilizzo**.
2. Nella colonna Accettato/rifiutato, fare clic sul numero relativo ad Accettato a sinistra oppure sul numero relativo a Rifiutato a destra.

   In una pagina relativa allo stato viene visualizzata l'azione eseguita, ovvero l'accettazione o il rifiuto, insieme al nome utente, all'ID dispositivo, alla versione del criterio visualizzata, alla piattaforma utilizzata e alla data.
3. Fare clic su **Annulla** per chiudere la visualizzazione.

Ottenere e distribuire l'applicazione Workspace ONE

Gli utenti possono scaricare l'applicazione VMware Workspace ONE dall'App Store del dispositivo oppure gli amministratori possono configurare Workspace ONE UEM in modo che invii ai dispositivi l'applicazione Workspace ONE come applicazione pubblica.

Distribuire l'applicazione Workspace ONE dalla console di Workspace ONE UEM a gruppi e utenti specifici nell'organizzazione. Dopo l'accesso all'applicazione Workspace ONE sui loro dispositivi, gli utenti possono accedere alle applicazioni Web e SaaS per le quali dispongono di permessi.

I passaggi seguenti illustrano come effettuare il push dell'applicazione mobile Workspace ONE come applicazione gestita dalla console di Workspace ONE UEM. Per inviare l'applicazione è possibile eseguire anche l'introduzione guidata di Workspace ONE.

Nota Per informazioni dettagliate su come configurare applicazioni gestite in Workspace ONE UEM, consultare la guida di VMware Workspace ONE UEM Mobile Application Management (MAM) disponibile nel portale delle risorse all'indirizzo https://resources.air-watch.com.

Prerequisiti

Se si prevede di effettuare il push dell'applicazione mobile Workspace ONE dalla console di Workspace ONE UEM, preparare gruppi smart di utenti finali autorizzati per l'applicazione.

Procedura

1. Nella console di Workspace ONE UEM, passare a **App e libri > Applicazioni** > **Visualizzazione elenco > Pubblico**, quindi selezionare **Aggiungi applicazione**.
2. Selezionare la piattaforma, ovvero iOS, Android o Windows.

3 Selezionare **Cerca nell'App Store** e, nella casella di testo **Nome** , immettere `Workspace ONE` come parola chiave per individuare VMware Workspace ONE nell'App Store.

4 Scegliere **Avanti** e utilizzare **Seleziona** per caricare l'applicazione Workspace ONE dalla pagina dei risultati dell'App Store.

5 Configurare le opzioni di assegnazione e distribuzione per gli utenti di Workspace ONE nelle seguenti impostazioni della scheda.

Scheda	Descrizione
Informazioni	Immettere e visualizzare le informazioni relative a modelli di dispositivi supportati, valutazioni e categorie.
Assegnazione	Assegnare l'applicazione mobile Workspace ONE ai gruppi smart degli utenti finali che possono utilizzare l'applicazione sul proprio dispositivo.
Distribuzione	Configurare la disponibilità e le funzionalità avanzate di gestione della modalità aziendale (EMM, Enterprise Mobility Management), se opportuno. Per configurare automaticamente le applicazioni gestite, abilitare **Invia configurazione applicazione** e immettere le coppie chiave-valore App Configuration for Enterprise (ACE). Vedere Configurazione dell'applicazione Workspace ONE UEM per le coppie di valori delle chiavi delle aziende.
Condizioni per l'utilizzo	(Facoltativo) Abilitare le **Condizioni d'uso** per l'impiego dell'applicazione Workspace ONE.

6 Selezionare **Salva e pubblica** per rendere l'applicazione disponibile per gli utenti.

Eseguire questi passaggi per ogni piattaforma supportata.

Configurazione dell'applicazione Workspace ONE UEM per le coppie di valori delle chiavi delle aziende

Quando si distribuisce l'applicazione Workspace ONE come applicazione gestita in Workspace ONE UEM e si abilita Invia configurazioni applicazioni quando si inserisce l'app Workspace ONE dalla console di Workspace ONE UEM, è possibile preconfigurare le impostazioni di Workspace ONE applicate quando gli utenti installano e avviano l'app Workspace ONE.

Quando l'applicazione Workspace ONE viene caricata nella console di Workspace ONE UEM come applicazione mobile gestita, è possibile configurare l'URL del server di VMware Workspace ONE, il valore UID del dispositivo e il requisito per l'autenticazione del certificato nei dispositivi Android.

Tabella 7-1. Opzioni di configurazione dei dispositivi gestiti Workspace ONE nella console di Workspace ONE UEM

Piattaforma	Chiave di configurazione	Tipo di valore	Valore di configurazione	Spiegazione
Tutto	`AppServiceHost`	Stringa	**<URL server VMware Workspace ONE>**	Configura l'URL del server per VMware Workspace ONE sui dispositivi.
iOS	`deviceUDID`	Stringa	**{DeviceUid}** Inserire il valore UID del dispositivo. Non utilizzare la funzione Inserisci un valore di ricerca.	Tiene traccia dei dispositivi utilizzati per effettuare l'autenticazione nell'ambiente di VMware Identity Manager.

Tabella 7-1. Opzioni di configurazione dei dispositivi gestiti Workspace ONE nella console di Workspace ONE UEM (Continua)

Piattaforma	Chiave di configurazione	Tipo di valore	Valore di configurazione	Spiegazione
iOS	`SkipDiscoveryScreen`	Booleano	**`true`**	A partire dall'applicazione Workspace ONE versione 3.1, è possibile impostare la chiave di configurazione SkipDiscoveryScreen. Quando impostata su True, Workspace ONE tenta di passare oltre la schermata di indirizzo e-mail/URL server. Quando utilizzata con la chiave di configurazione `AppServiceHost`, gli utenti vengono portati immediatamente alla schermata di autenticazione. Se è utilizzato anche SSO mobile, gli amministratori possono fornire agli utenti finali un'esperienza continua e uniforme quando avviano Workspace ONE, iniziando a caricare immediatamente la propria app Workspace ONE.
Android e iOS	`RemoveAccountSignOut`	Intero	0 - L'opzione Rimuovi account viene visualizzata 1 - L'opzione Rimuovi account non viene visualizzata Se il valore non è impostato, l'opzione Rimuovi account viene visualizzata.	Se il valore è impostato su 1, l'opzione Rimuovi account non viene visualizzata nella pagina delle impostazioni di Workspace ONE per gli utenti. Gli utenti non possono rimuovere l'account di Workspace ONE dal proprio dispositivo. Se questo valore è impostato su 0 o non è impostato alcun valore, l'opzione Rimuovi

Tabella 7-1. Opzioni di configurazione dei dispositivi gestiti Workspace ONE nella console di Workspace ONE UEM (Continua)

Piattaforma	Chiave di configurazione	Tipo di valore	Valore di configurazione	Spiegazione
				account viene visualizzata. Se gli utenti fanno clic su Rimuovi account, Workspace ONE UEM esegue la rimozione dei dati aziendali nel dispositivo e annulla la registrazione del dispositivo in Workspace ONE UEM.

Registrazione dei domini e-mail per l'individuazione automatica

È possibile registrare il dominio di posta elettronica nel servizio di individuazione automatica per agevolare l'accesso da parte degli utenti finali al loro portale di app tramite l'applicazione Workspace ONE. Gli utenti finali immettono l'indirizzo di posta elettronica anziché l'URL dell'organizzazione.

Quando il dominio di posta elettronica dell'organizzazione è registrato per l'individuazione automatica, gli utenti finali immettono solo l'indirizzo di posta elettronica nella pagina di accesso per accedere al loro portale delle app. Immetteranno, ad esempio, **`nomeutente@myco.com`**.

Quando l'individuazione automatica non viene usata, la prima volta in cui gli utenti finali aprono l'applicazione Workspace ONE devono fornire l'URL completo dell'organizzazione. Immetteranno, ad esempio, **`myco.vmwareidentity.com`**.

Configurazione di Auto Discovery in VMware Identity Manager

Per registrare un dominio, è necessario immettere il dominio e l'indirizzo e-mail nella pagina Auto Discovery della console di VMware Identity Manager.

Al proprio indirizzo e-mail nel dominio si riceverà un messaggio e-mail con un token di attivazione. Per attivare la registrazione del dominio, immettere il token nella pagina Auto Discovery e verificare che il dominio registrato sia il proprio dominio.

Nota Per configurare Auto Discovery per le distribuzioni locali di VMware Identity Manager, è necessario accedere alla console di VMware Identity Manager come amministratore locale. Immettere l'ID e la password di Workspace ONE UEM creati nel sito Web di Workspace ONE UEM all'indirizzo https://secure.air-watch.com/register.

Procedura

1 Nella scheda Gestione identità e accessi della console di VMware Identity Manager, fare clic su **Configurazione > Auto Discovery**.

2 (Solo distribuzioni locali). Configurare l'URL di Auto Discovery di Workspace ONE UEM.

Opzione	Descrizione
URL di Auto Discovery	Immettere l'URL come https://discovery.awmdm.com.
ID AirWatch	Immettere l'indirizzo e-mail registrato in Workspace ONE UEM per accedere al sito Web corrispondente.
Password	Immettere la password associata all'account Workspace ONE UEM.

3 Nella casella di testo **Dominio e-mail** immettere il dominio e-mail delle organizzazioni da registrare.

4 Nella casella di testo **Indirizzo e-mail di conferma** immettere un indirizzo e-mail di tale dominio e-mail per ricevere il token di verifica.

5 Fare clic su **OK**.

Lo stato della registrazione del dominio e-mail viene contrassegnato con In sospeso. È possibile avere un solo dominio e-mail in sospeso alla volta.

6 Visualizzare l'e-mail e copiare il token di attivazione incluso nel messaggio.

7 Tornare alla pagina **Gestione identità e accessi > Auto Discovery** e incollare il token nella casella di testo Token di attivazione.

8 Fare clic su **Verifica** per registrare il dominio.

Il dominio e-mail viene registrato e aggiunto all'elenco di domini e-mail registrati nella pagina Auto Discovery.

Gli utenti finali possono ora immettere i propri indirizzi e-mail nell'applicazione Workspace ONE per accedere al portale della propria app.

Operazioni successive

Se si dispone di più domini e-mail, aggiungere un altro dominio e-mail da registrare.

Impostazione dell'autenticazione delle sessioni

Il servizio VMware Identity Manager include un criterio di accesso predefinito che controlla l'accesso degli utenti alle loro risorse VMware Identity Manager.

La durata della sessione di autenticazione configurata nelle regole dei criteri determina la quantità di tempo massima di cui gli utenti dispongono dopo l'ultimo evento di autenticazione per accedere alla pagina di avvio delle applicazioni o per avviare un'applicazione Web specifica. L'impostazione predefinita è otto ore. Dopo l'autenticazione, gli utenti hanno a disposizione otto ore per avviare un'applicazione Web, a meno che non diano avvio a un altro evento di autenticazione che estenderà il tempo a loro disposizione.

È possibile modificare il criterio predefinito in modo da cambiare la durata della sessione dalla console di gestione VMware Identity Manager, scheda Gestione identità e accessi, Gestisci > Criteri. Consultare la guida all'amministrazione di VMware Identity Manager, Gestione dei criterio di accesso.

Abilitazione del controllo di conformità per i dispositivi gestiti di Workspace ONE UEM

Quando gli utenti registrano i propri dispositivi, a scadenze regolari programmate vengono inviati dati campione che vengono utilizzati per valutare conformità. La valutazione di questi dati di esempio consente di verificare che il dispositivo soddisfi le regole di conformità impostate dall'amministratore nella console di Workspace ONE UEM (UEM). Se il dispositivo non rispetta la conformità, vengono intraprese le azioni corrispondenti configurate nella console di UEM.

Il servizio VMware Identity Manager include un'opzione dei criteri di accesso che può essere configurata per controllare lo stato di conformità del dispositivo nel server Workspace ONE UEM quando gli utenti accedono dal dispositivo. Grazie al controllo di conformità, è possibile impedire agli utenti di accedere a un'applicazione o di utilizzare Single Sign-On nel portale di Workspace ONE se il dispositivo non rispetta la conformità. La possibilità di accedere viene ripristinata quando il dispositivo rispetta nuovamente la conformità.

Se il dispositivo è compromesso, l'applicazione Workspace ONE si disconnette automaticamente e blocca l'accesso alle applicazioni. Se il dispositivo è stato registrato tramite la gestione adattiva, con un comando di rimozione dei dati aziendali emesso dalla console UEM è possibile annullare la registrazione del dispositivo e rimuovere le applicazioni gestite dal dispositivo. Le applicazioni non gestite non vengono rimosse.

Per ulteriori informazioni sui criteri di conformità di Workspace ONE UEM, consultare la guida VMware Workspace ONE UEM Mobile Device Management, nelle pagine della documentazione di VMware Workspace ONE UEM.

Strategie di distribuzione per l'impostazione di gruppi di organizzazioni di Workspace ONE UEM multipli

Workspace ONE UEM utilizza i gruppi di organizzazioni per identificare gli utenti e stabilire autorizzazioni. Quando Workspace ONE UEM è integrato con VMware Identity Manager, le chiavi delle REST API di amministrazione e utente di registrazione sono configurate al tipo di gruppo di organizzazioni di Workspace ONE UEM denominato Cliente.

Quando gli utenti si registrano in Workspace ONE da un dispositivo, all'interno di VMware Identity Manager viene attivato un evento registrazione dispositivo. Viene inviata una richiesta ad Workspace ONE UEM per richiamare tutte le applicazioni per le quali la combinazione utente/dispositivo è autorizzata. La richiesta viene inviata utilizzando le REST API per individuare l'utente all'interno di Workspace ONE UEM e inserire il dispositivo nel gruppo di organizzazioni appropriato.

Per gestire i gruppi di organizzazioni, in VMware Identity Manager è possibile configurare due opzioni.

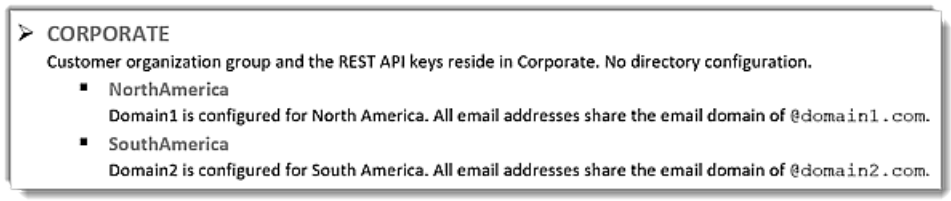
- Abilitare l'Auto Discovery di Workspace ONE UEM.
- Mappare gruppi di organizzazioni di Workspace ONE UEM a domini nel servizio di VMware Identity Manager.

Se non è configurata nessuna di queste opzioni, Workspace ONE tenta di individuare l'utente nel gruppo di organizzazione in cui viene creata la chiave delle REST API. Questo è il gruppo Cliente.

Uso dell'Auto Discovery di Workspace ONE UEM

Impostare l'Auto Discovery quando è configurata una singola directory per un gruppo figlio nel gruppo di organizzazioni Cliente, oppure quando sono configurate più directory sotto il gruppo Cliente con domini e-mail univoci.

Figura 7-1. Esempio 1



Nell'esempio 1, per l'Auto Discovery è registrato il dominio e-mail dell'organizzazione. Gli utenti inseriscono solo il proprio indirizzo e-mail nella pagina di registrazione di Workspace ONE.

In questo esempio, quando gli utenti del dominio NorthAmerica si registrano in Workspace ONE, inseriscono l'indirizzo e-mail completo nella forma user1@domain1.com. L'applicazione cerca il dominio e verifica che l'utente sia esistente o che sia possibile crearlo con una chiamata a directory nel gruppo di organizzazioni NorthAmerica. Il dispositivo può essere registrato.

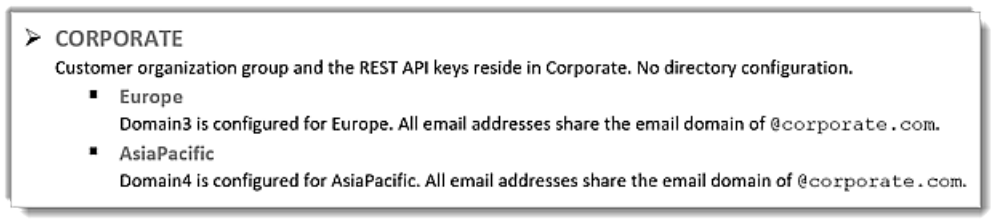
Uso della mappatura dei gruppi di organizzazioni di Workspace ONE UEM ai domini di VMware Identity Manager

Configurare il servizio di VMware Identity Manager per la mappatura dei gruppi di organizzazioni di Workspace ONE UEM quando sono configurate più directory con lo stesso dominio e-mai. Abilitare **Mappa domini a più gruppi di organizzazioni** nella pagina di configurazione di AirWatch nella console di VMware Identity Manager.

Quando l'opzione Mappa domini a più gruppi di organizzazioni è abilitata, i domini configurati in VMware Identity Manager possono essere mappati agli ID dei gruppi di organizzazioni di Workspace ONE UEM. È richiesta anche la chiave delle REST API di amministrazione.

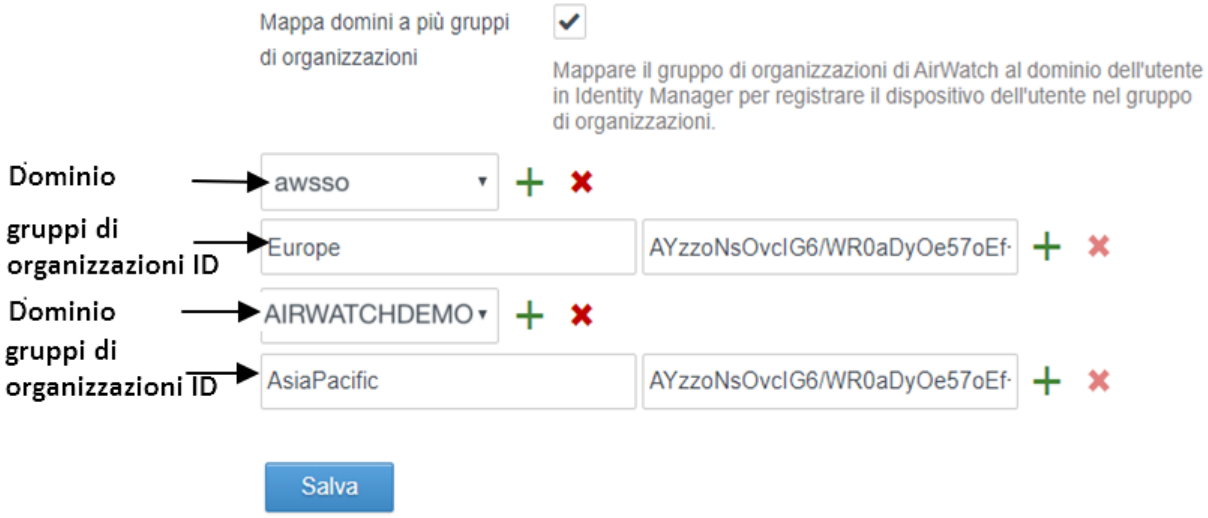
Nell'esempio 2, due domini sono mappati a gruppi di organizzazioni differenti. È richiesta la chiave delle REST API di amministrazione. La stessa chiave REST API di amministrazione è utilizzata per entrambi gli ID dei gruppi di organizzazioni.

Figura 7-2. Esempio 2



Nella pagina di configurazione di AirWatch nella console di VMware Identity Manager, configurare un ID gruppo di organizzazioni di Workspace ONE UEM specifico per ogni dominio.

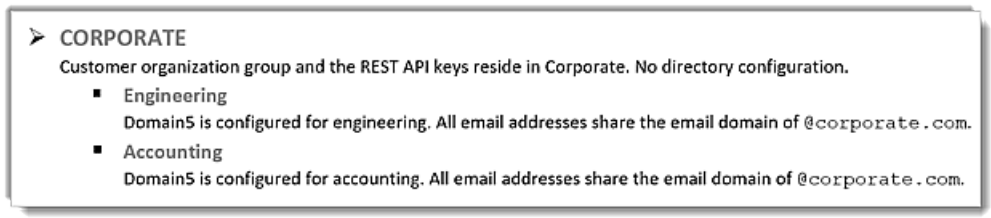
Figura 7-3. Esempio 2 Configurazione dei gruppi di organizzazioni



Con questa configurazione, quando gli utenti accedono a Workspace ONE dal proprio dispositivo, la richiesta di registrazione del dispositivo tenta di individuare utenti da Domain3 nel gruppo di organizzazioni Europe e utenti da Domain4 nel gruppo di organizzazioni AsiaPacific.

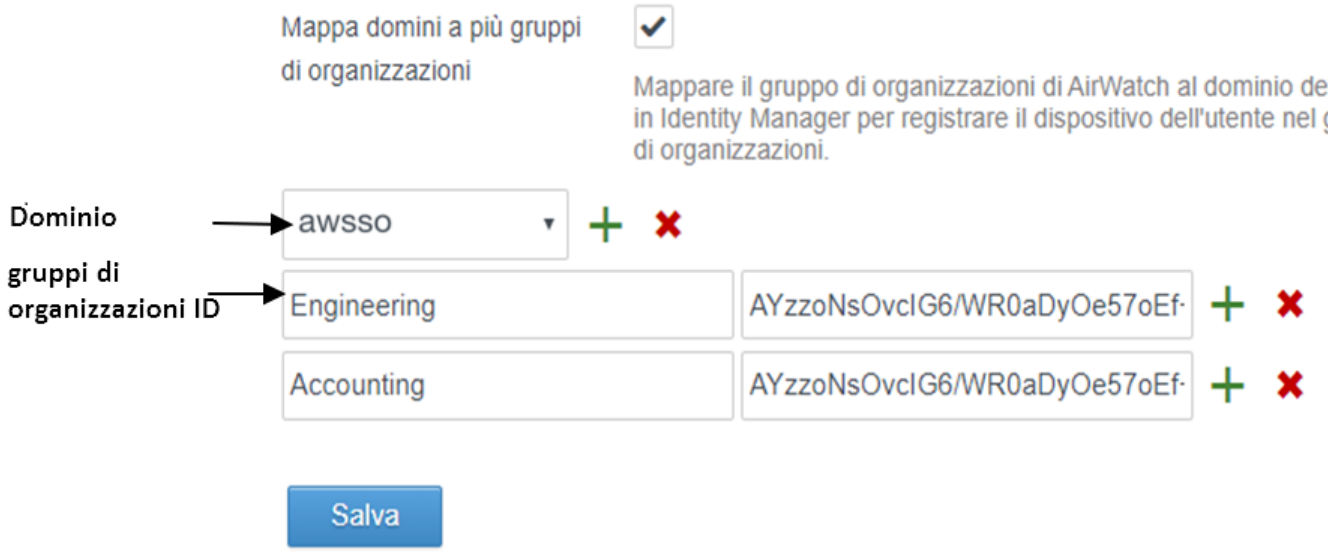
Nell'esempio 3, un dominio è mappato a più gruppi di organizzazioni di Workspace ONE UEM. Entrambe le directory condividono il dominio e-mail. Il dominio punta allo stesso gruppo di organizzazioni di Workspace ONE UEM.

Figura 7-4. Esempio 3



In questa configurazione, quando gli utenti si registrano in Workspace ONE, l'applicazione richiede agli utenti di selezionare in quale gruppo desiderano registrarsi. In questo esempio, gli utenti possono selezionare Engineering o Accounting.

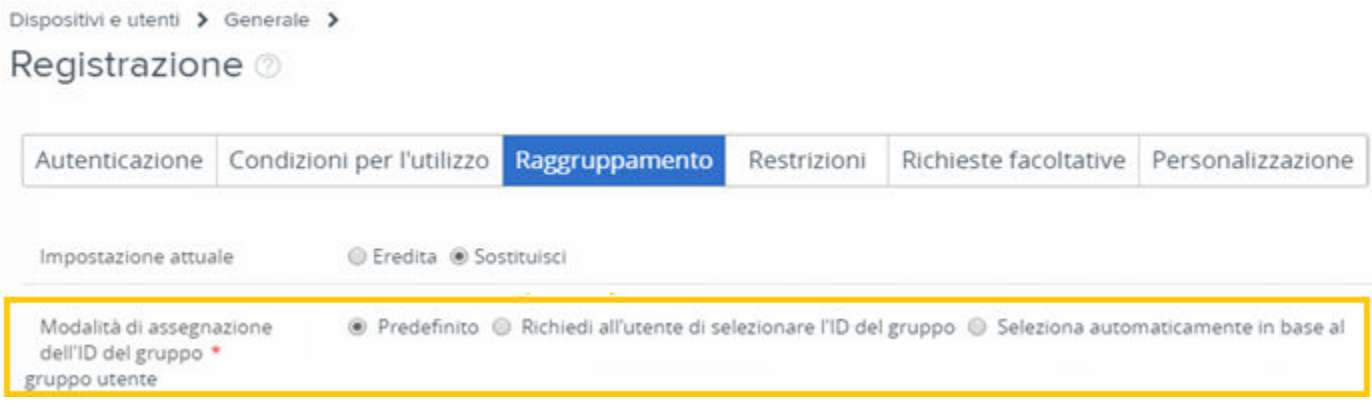
Figura 7-5. Gruppi di organizzazioni in cui le directory condividono lo stesso dominio



Inserimento dei dispositivi nel gruppo di organizzazioni corretto

Quando il record di un utente viene correttamente individuato, il dispositivo viene aggiunto al gruppo di organizzazioni appropriato. L'impostazione di registrazione di Workspace ONE UEM **Modalità di assegnazione ID di gruppo** determina in quale gruppo di organizzazioni inserire il dispositivo. Questa impostazione si trova nella pagina Impostazioni di sistema> Dispositivi e utenti > Generale> Registrazione> Raggruppamento della Workspace ONE UEM Console.

Figura 7-6. Registrazione dei gruppi di Workspace ONE UEM per i dispositivi



Nell'esempio 4, tutti gli utenti sono al livello del gruppo di organizzazioni Corporate.

Figura 7-7. Esempio 4

La collocazione del dispositivo dipende dalla configurazione selezionata per la modalità di assegnazione dell'ID del gruppo al gruppo di organizzazioni Corporate.

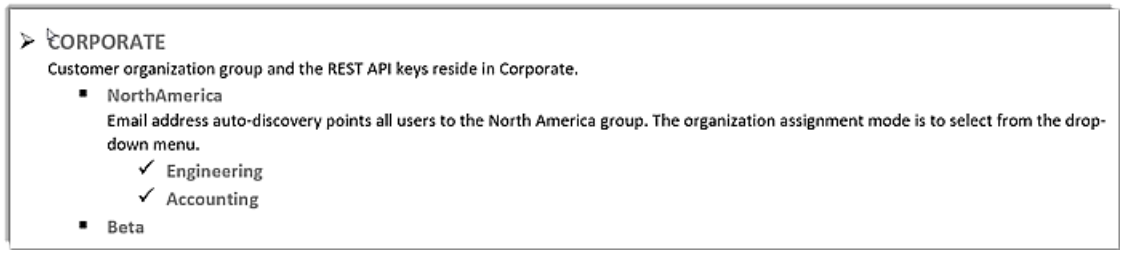
- Se è selezionata l'opzione Predefinita, il dispositivo viene inserito nello stesso gruppo in cui si trova l'utente. Nell'esempio 4, il dispositivo viene inserito nel gruppo Corporate.
- Se è selezionata l'opzione Richiedi all'utente di selezionare l'ID del gruppo, agli utenti viene richiesto di selezionare in quale gruppo registrare il proprio dispositivo. Nell'esempio 4, gli utenti vedono un menu a discesa all'interno dell'app Workspace ONE contenente le opzioni Engineering e Accounting.
- Se è selezionata l'opzione Seleziona automaticamente in base al gruppo utente, i dispositivi vengono inseriti in Engineering o in Accounting in base all'assegnazione al rispettivo gruppo di utenti e alla mappatura corrispondente nella console di Workspace ONE UEM.

Cos'è un gruppo nascosto

Nell'esempio 4, quando agli utenti viene richiesto di selezionare il gruppo di organizzazioni da cui registrare, essi possono anche specificare un valore di ID di gruppo non presente nell'elenco presentato dall'app Workspace ONE. Si tratta di un gruppo nascosto.

Nell'esempio 5, nella struttura del gruppo di organizzazioni Corporate, North America e Beta sono configurati come gruppi sotto Corporate.

Figura 7-8. Esempio 5



Nell'esempio 5, gli utenti inseriscono il proprio indirizzo e-mail in Workspace ONE. Dopo l'autenticazione, agli utenti viene mostrato un elenco che mostra Engineering e Accounting e da cui scegliere. Beta non è una delle opzioni visualizzate. Se gli utenti conoscono l'ID del gruppo di organizzazioni, possono specificare Beta manualmente nella casella di testo di selezione del gruppo e registrare correttamente il proprio dispositivo nel gruppo Beta.

Lavorare in Workspace ONE Portal

8

Quando l'applicazione Workspace ONE viene installata sui dispositivi, gli utenti possono connettersi a Workspace ONE per accedere in modo sicuro a un catalogo di applicazioni abilitate per loro dall'organizzazione. Se l'applicazione è configurata con SSO, gli utenti non devono immettere nuovamente le loro credenziali di accesso quando avviano l'app.

L'interfaccia utente di Workspace ONE funziona in modo simile su telefoni, tablet e desktop. La pagina Catalogo in Workspace ONE visualizza le risorse che sono state inviate in pushing a Workspace ONE. Gli utenti possono toccare o fare clic per cerare, aggiungere, applicare segnalibro e aggiornare le applicazioni. Facendo clic con il tasto destro del mouse su un'app, possono rimuoverla dalla pagina Segnalibri applicati e passare alla pagina Catalogo per aggiungere risorse autorizzate.

Questo capitolo include i seguenti argomenti:

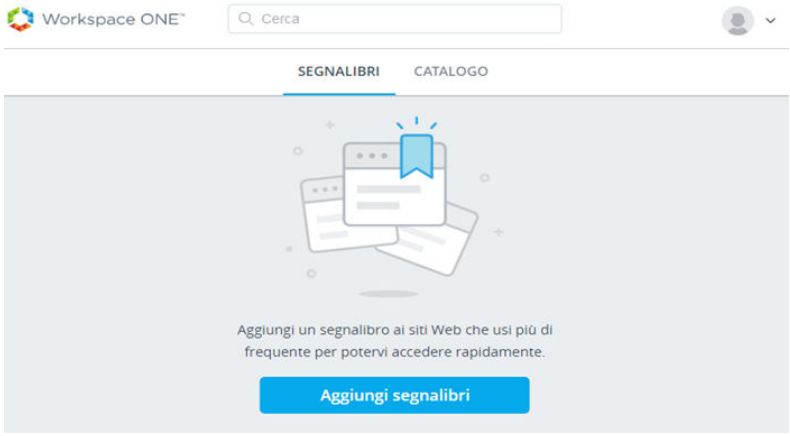
Utilizzo delle applicazioni in Workspace ONE

Il portale degli utenti di Workspace ONE è costituito da una scheda Catalogo e una scheda Segnalibri. Quando gli utenti accedono al proprio portale di Workspace ONE la prima volta, se la scheda Segnalibri è vuota viene visualizzata la scheda Catalogo.

Dopo il primo avvio, viene visualizzata automaticamente l'ultima scheda visitata. Se gli utenti preferiscono eseguire l'avvio dalla scheda Catalogo, possono utilizzare la visualizzazione Catalogo.

È possibile nascondere la scheda Catalogo o la scheda Segnalibri nel portale Workspace ONE per offrire un'esperienza utente specifica basata sulle proprie esigenze. È possibile modificare la configurazione del portale dalla pagina Catalogo > Impostazioni > Configurazione portale utente della console di VMware Identity Manager.

Figura 8-1. Visualizzazione iniziale della pagina Segnalibri



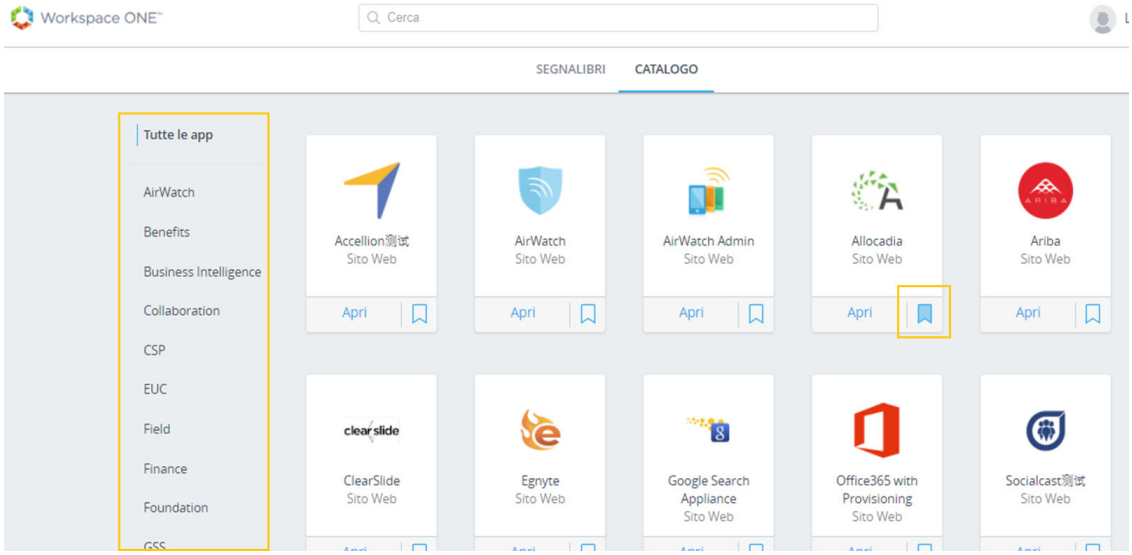
Dal catalogo, gli utenti possono installare applicazioni Web, mobile e virtuali per cui sono autorizzati. Le applicazioni Web e virtuali possono essere aperte direttamente dalla pagina del catalogo o dei segnalibri nell'app Workspace ONE.

Le applicazioni native come iOS e Android non possono essere contrassegnate con un segnalibro o avviate dalle pagine di Workspace ONE. Queste app vengono avviate dalla SpringBoard di iOS o Android.

Nella pagina del catalogo, è possibile organizzare le applicazioni in categorie logiche per consentire agli utenti di individuare più facilmente le risorse di cui hanno bisogno. Per impostazione predefinita, è presente una categoria denominata Consigliato. Quando si includono applicazioni nella categoria Consigliato, è possibile abilitare **Mostra app consigliate nella scheda Segnalibri** per pre-popolare la pagina Segnalibri con queste app.

Con questa configurazione, agli utenti viene offerto accesso immediato alle applicazioni consigliate al loro primo accesso al portale Workspace ONE.

Figura 8-2. Pagina Catalogo di Workspace ONE



Nota Le applicazioni mobile non sono disponibili quando si opera dai browser desktop.

Gli utenti possono avviare le applicazioni Web nei modi seguenti.

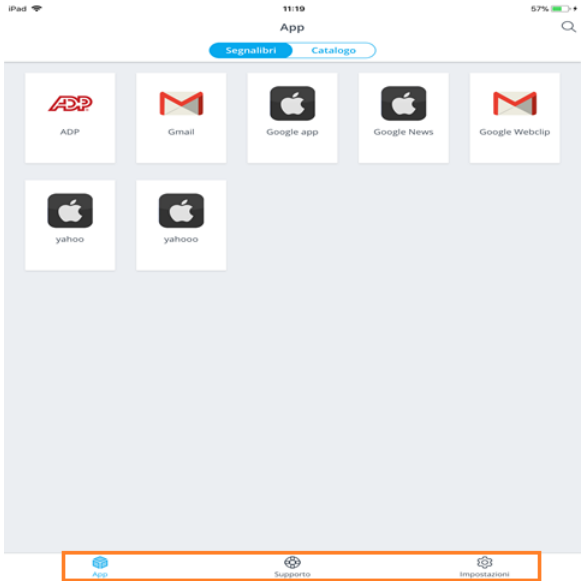
- Dalla scheda Segnalibri. L'utente fa clic sull'icona dell'applicazione per avviarla.
- Dalla scheda Catalogo. L'utente fa clic sulla casella con l'icona della freccia per aprire l'applicazione.
- Dalla ricerca Spotlight o dalla ricerca all'interno di Workspace ONE. Dalla ricerca Spotlight su dispositivi iOS, l'utente seleziona l'icona dell'applicazione dall'elenco. Dalla ricerca di Workspace ONE, l'utente fa clic sulla casella con l'icona della freccia per aprire l'applicazione.

Gli utenti possono accedere alle impostazioni di Workspace ONE dalla freccia del menu a discesa accanto al suo nome.

- Account. Informazioni sul profilo dell'utente, incluso nome, cognome e indirizzo e-mail.
- Dispositivi. Elenco dei dispositivi registrati nell'applicazione Workspace ONE e data e ora dell'ultimo accesso.
- Suggerimenti di un'applicazione. Suggerimenti sulla navigazione Workspace ONE dal dispositivo dell'utente.
- Informazioni su. Informazioni su copyright, brevetto e licenza di Workspace ONE.
- Preferenze. Impostazione di avvio predefinita quando si accede alle applicazioni remote di Horizon, visualizzando l'applicazione da Horizon Client o da un browser.

L'utente tocca l'icona dell'app di Workspace ONE sul proprio dispositivo per registrarsi nel rispettivo portale di app. Se l'utente ha creato segnalibri alle applicazioni, viene visualizzata la pagina Segnalibri. L'applicazione Workspace ONE sui dispositivi contiene i link a Supporto e Impostazioni.

Figura 8-3. Visualizzazione dei dispositivi del portale di Workspace ONE



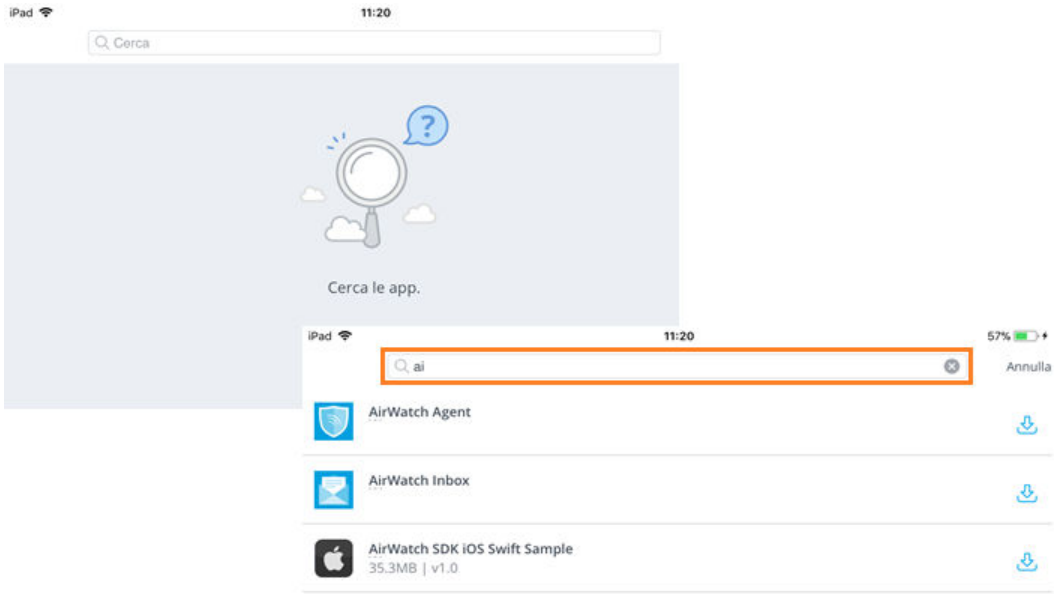
- La pagina Supporto contiene un link a Dispositivi e a Invia report. La pagina Dispositivi mostra la data e l'ora dell'ultimo accesso al dispositivo. Invia report consente all'utente di inviare informazioni diagnostiche o un altro feedback. Gli utenti possono attivare e disattivare questa funzionalità nelle impostazioni del dispositivo.
- La pagina Impostazioni mostra la versione dell'app Workspace ONE e l'informativa sulla privacy di VMware Workspace. Gli utenti possono rimuovere l'account dalla pagina Impostazioni per disconnettersi dall'applicazione Workspace ONE.

Utilizzo della ricerca in Workspace ONE

Gli utenti possono effettuare ricerche in Workspace ONE per trovare applicazioni per nome o per categoria.

Alle digitazioni degli utenti nella casella di testo di ricerca, vengono visualizzate le applicazioni corrispondenti alla stringa immessa.

Figura 8-4. Ricerche che mostrano risultati



Gli utenti possono avviare un'app Web o scaricare app native direttamente dai risultati di ricerca.

Su dispositivi iOS, gli utenti possono utilizzare Spotlight per cercare applicazioni presenti nel portale di Workspace ONE. Dalla schermata principale del dispositivo iOS, toccando e trascinando nella schermata è possibile rivelare il campo di ricerca di Spotlight. Digitando il nome di un'app contenuta nel portale di Workspace ONE, si apre Workspace ONE e viene avviata l'applicazione.

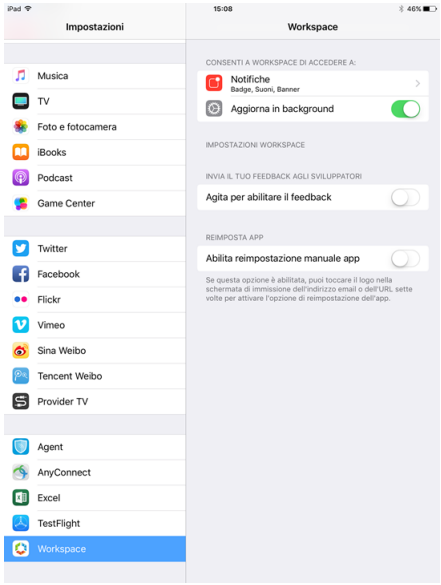
Aiutare gli utenti a segnalare problemi dai dispositivi iOS

Per i dispositivi iOS, è possibile utilizzare la funzione Rage Shake per inviare registri agli sviluppatori dell'app iOS.

Gli utenti possono agitare il proprio dispositivo e questo registrerà lo stato corrente, inviando per impostazione predefinita un messaggio e-mail agli sviluppatori dell'applicazione Workspace ONE. L'utente può specificare manualmente un altro indirizzo e-mail a cui inviare le informazioni.

Essi possono attivare la funzione Abilita feedback su Shake dalla pagina Impostazioni > Workspace del proprio dispositivo. È possibile utilizzare Rage Shake da qualsiasi schermata nel portale di Workspace ONE per inviare una segnalazione.

Figura 8-5. Funzione Abilita feedback in Shake



Quando un dispositivo iOS riceve un messaggio di errore simile a `questo dispositivo è registrato per un altro utente o ambiente`, è possibile utilizzare l'opzione di reimpostazione manuale dell'app per cancellare tutti i dati dell'app archiviati localmente sul dispositivo.

Impostazione di passcode per l'applicazione Workspace ONE

Nei dispositivi degli utenti deve essere abilitata la funzionalità che consente di evitare l'impostazione di un passcode. Se non è abilitata, al primo avvio dell'applicazione Workspace ONE agli utenti viene chiesto di creare un passcode. Il passcode deve essere immesso ogni volta che gli utenti accedono a Workspace ONE dal proprio dispositivo.

Se non si utilizza la funzionalità relativa ai passcode, agli utenti viene chiesto di impostare un passcode prima di poter accedere all'applicazione Workspace ONE. Il livello in cui il passcode viene impostato dipende dalla piattaforma. Per i dispositivi Android, il passcode viene impostato a livello dell'app. Per i dispositivi desktop di Windows e i dispositivi iOS che utilizzano Workspace ONE 3.2 o versioni precedenti, il codice d'accesso viene impostato a livello di dispositivo.

Nota I dispositivi iOS e Android supportano inoltre la funzionalità Touch ID, in grado di riconoscere le impronte digitali.

Workspace ONE è in grado di rilevare possibili problemi di sicurezza sui dispositivi. Se gli utenti disabilitano il codice d'accesso nel dispositivo, al successivo accesso all'applicazione Workspace ONE , viene richiesto di impostare un codice d'accesso prima di poter accedere a Workspace ONE. Se è abilitato un codice d'accesso a livello di app, gli utenti finali non possono disabilitare il loro codice d'accesso a livello di app.

Passcode a livello di applicazione sui dispositivi iOS

È possibile creare passcode più complessi dei passcode a quattro cifre dei dispositivi, che rappresentano il requisito minimo. Il passcode a livello di app può essere condiviso con altre app di produttività, ad esempio VMware Boxer.

È possibile designare il requisito del passcode locale per un'applicazione nella console di Workspace ONE UEM. Passare a Gruppi e impostazioni > Tutte le impostazioni > App > Impostazioni e criteri > Criteri di sicurezza > Tipo di autenticazione.

Quando è configurata l'autenticazione tramite passcode, agli utenti viene chiesto di impostare un passcode a livello di app se non esistono altre app di produttività, oppure di immettere il passcode condiviso con le altre app di produttività.

Se non è configurata l'autenticazione tramite passcode, nei dispositivi iOS è necessario un passcode del dispositivo.

Aggiunta di applicazioni native

Le applicazioni native sono programmi (definiti anche "app") sviluppati per uno specifico dispositivo mobile. Gli utenti possono visualizzare le applicazioni native autorizzate da Workspace ONE UEM nella pagina Catalogo Workspace ONE. Se ad esempio un utente visualizza il catalogo da un dispositivo iOS, vengono elencate solo le applicazioni iOS autorizzate per quell'utente.

Dalla pagina Catalogo gli utenti possono scegliere Installa per installare l'app sul proprio dispositivo. Alla selezione di Installa, compare una finestra pop-up che illustra all'utente l'operazione che seguirà. Le informazioni visualizzate dipendono dal tipo di app e dalla piattaforma. Per le applicazioni che includono l'icona di un lucchetto, è necessario che il dispositivo venga gestito da Workspace ONE UEM. Se un utente finale prova a scaricare un'app con l'icona del lucchetto, viene visualizzato il messaggio `Installation of this app requires enablement of Workspace Services`.

Utilizzo di VMware Verify per l'autenticazione degli utenti

Quando il servizio VMware Verify è abilitato come secondo metodo di autenticazione per l'autenticazione a due fattori per l'accesso a Workspace ONE dal proprio dispositivo, gli utenti devono scaricare l'app VMware Verify dall'App Store del dispositivo.

La prima volta che gli utenti accedono all'applicazione Workspace ONE, viene richiesto di inserire il nome utente e la password. Dopo il completamento della verifica del nome utente e della password, agli utenti viene chiesto di immettere il numero di telefono del proprio dispositivo per la registrazione nel servizio di VMware Verify.

Quando si fa clic su **Registrazione**, il numero di telefono del dispositivo viene registrato nel servizio di VMware Verify. Se l'utente non ha scaricato l'applicazione VMware Verify, gli viene presentata la richiesta di scaricarla.

Dopo l'installazione dell'applicazione, agli utenti viene chiesto di immettere lo stesso numero di telefono che hanno immesso in precedenza e di selezionare un metodo di notifica per ricevere un codice di registrazione monouso. Il codice di registrazione viene immesso nella pagina del PIN di registrazione.

Dopo la registrazione del numero di telefono del dispositivo, gli utenti possono usare il passcode monouso a tempo visualizzato nell'applicazione VMware Verify per accedere a Workspace ONE. Il passcode è un numero univoco, generato nel dispositivo, che viene costantemente cambiato.

Gli utenti possono registrare più dispositivi. Il passcode di VMware Verify viene automaticamente sincronizzato con ciascuno dei dispositivi registrati.

Invio di avvisi agli utenti di Workspace ONE

Gli amministratori possono notificare agli utenti di Workspace ONE gli imminenti periodi di inattività del sistema e lo stato della conformità inviando avvisi o richiedendo l'esecuzione di determinate azioni. Le notifiche vengono inviate tramite la console di Workspace ONE UEM.

Gli utenti possono gestire le modalità con cui riceveranno le notifiche dai loro dispositivi.

Utilizzo di Workspace ONE per dispositivi Android

I seguenti tipi di applicazioni possono essere abilitate tramite l'applicazione Workspace ONE per Android.

- applicazioni Web
- Applicazioni remote abilitate nel servizio VMware Identity Manager. Ad esempio applicazioni virtuali Horizon, Citrix XenApp e ThinApp.
- Applicazioni native, sia gestite che non gestite. Le applicazioni native sono app Android sviluppate per la piattaforma Android. Sono disponibili due tipologie.
  - Applicazioni pubbliche distribuite da Google Play Store.
  - Applicazioni interne distribuite privatamente tramite Workspace ONE UEM e non disponibili in Google Play Store.

  Applicazioni Web aperte in un browser. Gli utenti possono accedere ad applicazioni virtuali tramite VMware Horizon Client o Citrix Receiver.

Registrazione dell'applicazione Workspace ONE dai dispositivi Android

Gli utenti che accedono a Workspace ONE con un URL di server e credenziali validi possono accedere al catalogo unificato di Workspace ONE. Nel catalogo unificato, gli utenti possono vedere tutte le applicazioni a essi assegnate.

Gli utenti devono registrare l'app Workspace ONE per accedere alle applicazioni. Quando Workspace ONE ha stato registrato, gli utenti possono utilizzare le applicazioni Web e virtuali abilitate tramite VMware Identity Manager, app di produttività Workspace ONE UEM e app SDK senza gestione.

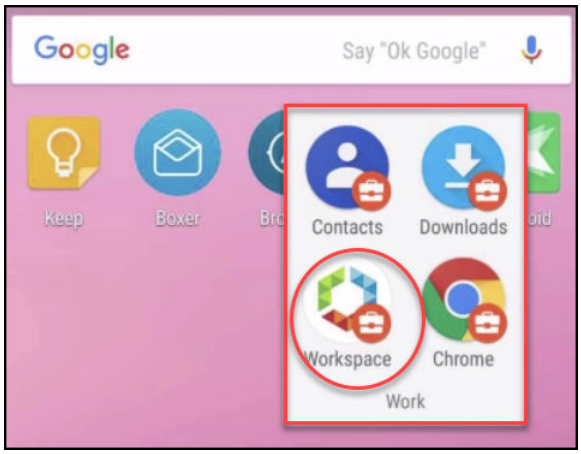
Nota Le app SDK sono inserite nel container e gestite tramite l'SDK di Workspace ONE UEM e non richiedono la gestione del dispositivo.

Gli utenti possono avviare la gestione adattiva, che abilita Android for Work sul dispositivo e consente la distribuzione di profili, criteri e app migliorate per il dispositivo.

Gestione di Android for Work con Workspace ONE

Abilitando Android for Work su dispositivi consente di separare i dati personali dai dati di lavoro al livello del sistema operativo. Android for Work crea una chiara separazione tra le app di lavoro e le app personali. Android for Work crea le applicazioni di lavoro con un attributo di lavoro Android distinto.

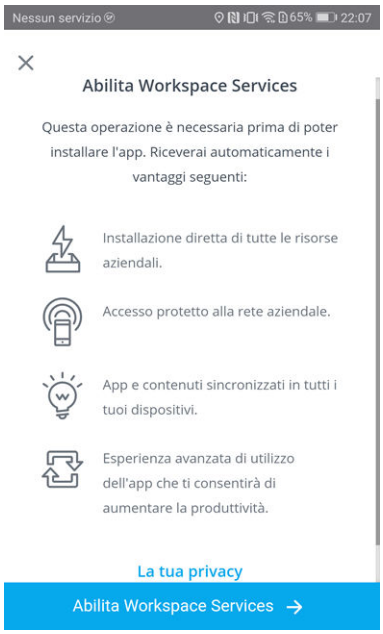
Figura 8-6. Contenuto di Android for Work



Gli amministratori determinano quali applicazioni nel catalogo richiedono la gestione di un dispositivo prima che sia possibile accedere all'app. Le applicazioni nel catalogo che richiedono la gestione mostrano il simbolo distintivo di una stella accanto al pulsante di download.

Quando gli utenti tentano di scaricare una di queste applicazioni, ricevono un messaggio che indica che l'applicazione richiede la gestione del dispositivo. Viene visualizzata una schermata in cui sono descritte le funzionalità e i vantaggi della gestione del dispositivo.

Figura 8-7. Pagina di introduzione di Workspace Services



Quando gli utenti accettano di attivare la gestione di Android for Work, vengono guidati nel processo di impostazione della gestione. Una volta implementata la gestione del dispositivo, sul dispositivo viene creato il container di Android for Work.

Utilizzo del catalogo di Workspace ONE

9

Quando Workspace ONE UEM e VMware Identity Manager sono integrati, il catalogo delle app di Workspace ONE è il repository di tutte le risorse che è possibile autorizzare per gli utenti. Gli utenti possono accedere alle applicazioni dell'azienda gestite nel catalogo di Workspace ONE sulla base delle impostazioni stabilite per l'applicazione.

Dal catalogo è possibile accedere alle applicazioni per Cloud, Mobile e Windows. Le applicazioni native sviluppate internamente o le app disponibili pubblicamente negli App Store possono essere rese disponibili per gli utenti finali dal portale di Workspace ONE.

Nelle pagine Catalogo di Workspace ONE, è possibile eseguire le seguenti attività

- Aggiungere nuove risorse al catalogo
- Visualizzare le risorse per le quali correntemente è possibile autorizzare gli utenti
- Accedere a informazioni su ogni risorsa presente nel catalogo

Alcune applicazioni Web possono essere aggiunte al catalogo direttamente dalle pagine Catalogo. Altri tipi di risorse richiedono l'esecuzione di azioni all'esterno della console di amministrazione. Vedere la guida di configurazione delle risorse di VMware Identity Manager per informazioni sull'impostazione delle risorse.

Gestione delle risorse nel catalogo

Prima di poter concedere agli utenti il permesso relativo a una determinata risorsa, è necessario inserire tale risorsa nel catalogo. Il metodo utilizzato per inserire una risorsa nel catalogo dipende dal tipo di risorsa in questione.

I tipi di risorse definibili nel catalogo per il permesso e la distribuzione agli utenti sono applicazioni Web, applicazioni Windows acquisite come pacchetti VMware ThinApp, pool di desktop Horizon Client e applicazioni virtuali Horizon, oppure applicazioni basate su Citrix.

Per integrare e abilitare pool di desktop e applicazioni Horizon Client, risorse pubblicate Citrix o applicazioni in pacchetto ThinApp, utilizzare la funzione di raccolta app disponibile nel menu a discesa della scheda Catalogo.

Per informazioni, requisiti, installazione e configurazione di tali risorse, consultare *Configurazione delle risorse in VMware Identity Manager*.

Aggiunta di applicazioni Web al catalogo della propria organizzazione

È possibile aggiungere applicazioni Web al catalogo selezionandole dal catalogo di applicazioni cloud oppure creando nuove applicazioni.

Il catalogo di applicazioni cloud contiene le applicazioni Web aziendali di uso comune. Queste applicazioni sono configurate parzialmente ed è necessario fornire informazioni aggiuntive per completare il record dell'applicazione. Il completamento della configurazione rimanente necessaria potrebbe richiedere anche la collaborazione dei rappresentanti degli account dell'applicazione Web.

Molte delle applicazioni nel catalogo di applicazioni cloud utilizzano SAML 2.0 o 1.1 per scambiare dati di autenticazione e autorizzazione per abilitare l'autenticazione Single Sign-On da Workspace ONE all'applicazione Web.

Quando si crea un'applicazione, è necessario immettere tutte le informazioni di configurazione per l'applicazione. La configurazione varia in base al tipo di applicazione che si sta aggiungendo. Per le applicazioni senza protocollo di federazione, è necessario solo un URL di destinazione.

Le applicazioni di provider di identità di terze parti configurati come origini di applicazioni in VMware Identity Manager vengono aggiunte come nuove applicazioni.

Quando si aggiunge un'applicazione, si seleziona anche un criterio di accesso per controllare l'accesso degli utenti all'applicazione. È disponibile un criterio di accesso predefinito ed è anche possibile creare nuovi criteri dalla pagina Gestione identità e accessi> Gestisci> Criteri. Per informazioni sui criteri di accesso, vedere *Amministrazione di VMware Identity Manager*.

Raggruppamento di risorse in categorie

È possibile organizzare le risorse in categorie logiche per consentire agli utenti di individuare facilmente la risorsa di cui necessitano nel loro portale Workspace ONE.

Quando si creano categorie, tenere presente la struttura della propria organizzazione, la funzione lavorativa delle risorse e il tipo di risorse. È possibile assegnare più di una categoria a una risorsa. È ad esempio possibile creare una categoria Associato vendite e un'altra categoria denominata Risorse reparto vendite. Assegnare Associato vendite a tutte le risorse vendite nel catalogo. Assegnare anche Risorse reparto vendite a risorse di vendita specifiche condivise solo con gli associati del reparto vendite.

Dopo aver creato una categoria, è possibile applicarla a qualsiasi risorsa presente nel catalogo. È possibile applicare categorie multiple alla stessa risorsa.

Quando gli utenti accedono al proprio portale Workspace ONE, possono vedere le categorie abilitate per la loro visualizzazione.

Consultare la guida all'amministrazione di VMware Identity Manager, Gestione del catalogo.

Branding personalizzato per i servizi VMware Identity Manager

10

È possibile personalizzare i loghi, i caratteri e lo sfondo utilizzati nella console di VMware Identity Manager, le schermate di accesso di utente e amministratore, la visualizzazione Web del portale delle applicazioni Workspace ONE e la visualizzazione Web dell'applicazione Workspace ONE nei dispositivi mobili.

È possibile utilizzare lo strumento di personalizzazione per adattare l'aspetto dei colori, dei loghi e del design caratteristici della società.

Questo capitolo include i seguenti argomenti:

Personalizzazione del branding nel servizio VMware Identity Manager

È possibile aggiungere il nome della società, il nome del prodotto e una favicon alla barra degli indirizzi per la console di amministrazione e il portale utente. È inoltre possibile personalizzare la pagina di accesso per impostare colori di sfondo corrispondenti ai colori e al design del logo della società.

Procedura

1. Nella scheda Gestione identità e accessi della console di VMware Identity Manager, selezionare **Configurazione > Branding personalizzato**.
2. Definire le impostazioni seguenti nella forma appropriata.

Campo modulo	Descrizione
	Scheda Nomi di marchi e logo
Nome azienda	L'opzione Nome azienda si applica sia ai desktop che ai dispositivi mobili. È possibile aggiungere il nome della propria azienda come titolo mostrato nella scheda del browser. Immettere il nuovo nome azienda sostituendo quello corrente.
Nome prodotto	L'opzione Nome prodotto si applica sia ai desktop che ai dispositivi mobili. Il nome prodotto viene visualizzato dopo il nome dell'azienda nella scheda del browser.

Campo modulo	Descrizione
Favicon	Una favicon è un'icona associata a un URL, che viene visualizzata nella barra degli indirizzi del browser. Le dimensioni massime dell'immagine della favicon sono 16 x 16 pixel. I formati supportati sono JPEG, PNG, GIF e ICO. Fare clic su **Carica** per caricare una nuova immagine e sostituire la favicon corrente. Viene visualizzata la richiesta di conferma del cambiamento. Il cambio viene effettuato immediatamente.
	Scheda Schermata di accesso
Logo	Fare clic su **Carica** per caricare un nuovo logo e sostituire quello corrente nelle schermate di accesso. Facendo clic su **Conferma** il cambio viene effettuato immediatamente. Le dimensioni minime consigliate per l'immagine da caricare sono 350 x 100 pixel. Se si carica un'immagine di dimensioni superiori a 350 x 100 pixel, l'immagine viene ridimensionata per adattarla a 350 x 100 pixel. I formati supportati sono JPEG, PNG e GIF.
Colore di sfondo	Colore visualizzato per lo sfondo della schermata di accesso. Sostituire il codice di colore esadecimale di sei cifre con il codice corrispondente al nuovo colore dello sfondo.
Colore di sfondo della casella	È possibile personalizzare il colore della casella della schermata di accesso. Sostituire il codice di colore esadecimale di sei cifre esistente con quello nuovo.
Colore di sfondo del pulsante di accesso	È possibile personalizzare il colore del pulsante di accesso. Sostituire il codice di colore esadecimale di sei cifre esistente con quello nuovo.
Colore testo del pulsante di accesso	È possibile personalizzare il colore del testo mostrato sul pulsante di accesso. Sostituire il codice di colore esadecimale di sei cifre esistente con quello nuovo.

Quando si personalizza la schermata di accesso, è possibile vedere le modifiche nel riquadro di anteprima prima di salvarle e renderle effettive.

3 Fare clic su **Salva**.

Gli aggiornamenti del branding personalizzato nella console di VMware Identity Manager e nelle pagine di accesso vengono applicati entro cinque minuti dal momento in cui si fa clic su Salva.

Operazioni successive

Controllare l'aspetto delle modifiche del branding nelle varie interfacce.

Aggiornare l'aspetto del portale Workspace ONE dell'utente finale e delle visualizzazioni su dispositivi mobili e tablet. Vedere Personalizzazione del branding per il Portale utente

Personalizzazione del branding per il Portale utente

È possibile aggiungere un logo, modificare i colori dello sfondo e aggiungere immagini per personalizzare il portale Workspace ONE.

Procedura

1 Nella scheda Cataloghi della console di VMware Identity Manager, selezionare **Impostazioni > Branding portale utente**.

2 Definire le impostazioni nella forma appropriata.

Elemento del modulo	Descrizione
Logo	Aggiungere un logo dell'intestazione che sarà il banner presente nella parte superiore della console di VMware Identity Manager e nelle pagine Web del portale Workspace ONE. Le dimensioni massime dell'immagine sono 220 x 40 pixel. I formati supportati sono JPEG, PNG e GIF.
	Portale
Colore di sfondo intestazione	Immettere un codice di colore esadecimale di sei cifre al posto di quello esistente per modificare il colore di sfondo dell'intestazione. Quando si digita con un nuovo codice di colore, il colore dello sfondo nella schermata di anteprima del portale dell'applicazione cambia di conseguenza.
Colore testo intestazione	Immettere un codice di colore esadecimale di sei cifre al posto di quello esistente per modificare il colore del testo visualizzato nell'intestazione.
Colore di sfondo	Colore visualizzato per lo sfondo della schermata del portale Web. Sostituire il codice di colore esadecimale di sei cifre con il codice corrispondente al nuovo colore dello sfondo. Quando si digita con un nuovo codice di colore, il colore dello sfondo nella schermata di anteprima del portale dell'applicazione cambia di conseguenza. Selezionare **Evidenziazione sfondo** per dare risalto al colore dello sfondo. Se l'opzione Evidenziazione sfondo è abilitata, nei browser che supportano più immagini di sfondo la sovrapposizione sarà visibile nelle pagine di avvio e del catalogo. Selezionare **Motivo di sfondo** per impostare il motivo triangolare preimpostato nel colore dello sfondo.
Colore di sfondo icona	Immettere un codice di colore esadecimale di sei cifre per modificare la casella del colore di sfondo che circonda le icone delle applicazioni.
Opacità sfondo icona	Per impostare una trasparenza, spostare il dispositivo di scorrimento sulla barra.
Nome e colore dell'icona	È possibile selezionare il colore del testo per i nomi elencati sotto le icone nelle pagine del portale delle app. Sostituire il codice di colore esadecimale con il codice corrispondente al nuovo colore dei caratteri.
Effetto lettering	Selezionare il tipo di lettering da utilizzare per il testo nelle schermate del portale Workspace ONE.
Evidenziazione sfondo	Se abilitato, per i browser che supportano immagini di sfondo multiple, il background sovrapposto viene visualizzato nelle pagine di catalogo e segnalibro.
Motivo di sfondo	Se abilitato, per browser che supportano più immagini di sfondo, le sovrapposizioni di sfondo vengono visualizzate nelle pagine di catalogo e segnalibro.
Immagine (facoltativa)	Per aggiungere un'immagine allo sfondo della schermata del portale delle app invece di un colore, caricare un'immagine.

3 Fare clic su **Salva**.

Gli aggiornamenti del branding personalizzato vengono aggiornati ogni 24 ore per il portale utente. Per apportare prima le modifiche, in qualità di utente amministratore aprire una nuova scheda e immettere il seguente URL (sostituire myco.example.com con il nome di dominio desiderato). `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

Operazioni successive

Esaminare l'aspetto delle modifiche del branding nelle varie interfacce.

Accesso ad altri documenti

11

Quando si configura Workspace ONE, potrebbe essere necessario fare riferimento alla documentazione per VMware Identity Manager e per VMware Workspace ONE UEM.

Nei centri di documentazione seguenti è possibile reperire documentazione aggiuntiva

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