Android Mobile Single Sign-On to VMware Workspace ONE

SEP 2018

VMware Workspace ONE
VMware Identity Manager
VMware Identity Manager 3.3

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

Implementing Mobile Single Sign-On Authentication for Workspace ONE UEM Managed Android Devices

1

Mobile single sign-on (SSO) for Android is an implementation of the certificate authentication method for VMware Workspace ONE® UEM (Unified Endpoint Management) managed Android devices. Mobile single sign-on allows users to sign in to their device and securely access their VMware Workspace® ONE® apps without reentering a password.

The VMware Tunnel® mobile app is installed on the Android device to add certificates and device ID information into authentication flows. The Tunnel settings are configured to access the VMware Identity Manager service for authentication, and the VMware Identity Manager service retrieves the certificate from the device for authentication.

When implementing mobile SSO for Android with the VMware Identity Manager service on premises, you configure the cert proxy service on the VMware Identity Manager service. After the cert proxy service is configured, you can configure certificate authentication in the VMware Identity Manager built-in identity provider from the VMware Identity Manager console.

When implementing mobile SSO for Android with the VMware Identity Manager service in the cloud, you can configure certificate authentication in the VMware Identity Manager built-in identity provider from the identity manager console. The cert proxy service is managed for you.

This chapter includes the following topics:

Supported Android Device

Android 5.1 or later is supported.

Applications accessed from an Android device must support SAML or another supported federation standard for single sign-on.

Mobile Single Sign-On Configuration Options for Android Devices

Mobile single sign-on authentication for Android devices can be configured to bypass the Tunnel server when VPN access is not required. For single sign-on, only the Tunnel mobile app is required.

Mobile Single Sign-On Without VPN Access

Mobile single sign-on authentication for Android devices can be configured to bypass the Tunnel server when VPN access is not required. Implementing Mobile SSO for Android authentication without using a VPN uses the same configuration pages as used for configuring the VMware Tunnel. Because you are not installing the Tunnel server, you do not enter the VMware Tunnel server host name and port. Instead you create a fictitious profile using the VMware Tunnel profile form. This fictitious profile prevents traffic from being directed to the Tunnel server. The Tunnel mobile app is used only for single sign-on.

In the Workspace ONE UEM console, you configure the following settings.

- Per App Tunnel component in the VMware Tunnel. This configuration allows Android devices access to managed public apps through the VMware Tunnel mobile app client.
- Per App Tunnel Profile. This profile is used to enable the per app tunneling capabilities for Android.
- In the Network Traffic Rules page, because the Tunnel server is not configured, you select Bypass so that no traffic is directed towards a Tunnel server.
- Create device traffic rules with a list of all the applications that are configured for per app VPN, the proxy server details, and the VMware Identity Manager URL.

Mobile Single Sign-On with VPN Access

When the application configured for single sign-on also is used to access intranet resources behind the firewall, configure VPN access and set up the Tunnel server. When single sign-on is configured with VPN, the Tunnel client can optionally route application traffic and login requests through the Tunnel server. Instead of the default configuration used for the Tunnel client in the console in the single sign-on mode, the configuration points to the Tunnel server.

Implementing Mobile SSO for Android authentication for managed Android devices requires configuring the VMware Tunnel in the Workspace ONE UEM console and installing the VMware Tunnel server before you configure Mobile SSO for Android in the VMware Identity Manager console. The VMware Tunnel service provides per app VPN access to Workspace ONE UEM managed apps. VMware Tunnel also provides the ability to proxy traffic from a mobile application to the VMware Identity Manager service for single sign-on.

In the Workspace ONE UEM console, you configure the following settings.

- Per App Tunnel component in the VMware Tunnel. This configuration allows Android devices access to internal and managed public applications through the VMware Tunnel mobile app client.

After the Tunnel settings are configured in the Workspace ONE UEM console, you download the VMware Tunnel installer and proceed with the installation of the server.

- Android VPN profile. This profile is used to enable the per app tunneling capabilities for Android.
- Enable VPN for each app that uses the application tunnel functionality from the Workspace ONE UEM console.
- Create device traffic rules with a list of all the applications that are configured for per app VPN, the proxy server details, and the VMware Identity Manager URL.

For detailed information about installing and configuring the VMware Tunnel, see the VMware Tunnel Guide on the VMware Workspace ONE UEM documentation page.

Configure VMware Tunnel Settings from Workspace ONE UEM Console

You enable the Per App Tunnel component in the VMware Tunnel settings to set up per app tunneling functionality for Android devices. Per app tunneling allows your internal and managed public apps to access your corporate resources on an app-by-app basis.

Note If you are configuring single sign-on for Android devices only and are not using VPN Access, in the Details page enter fictitious values for the host name and port, because for the single sign-on configuration this information is not used.

Procedure

1. In the Workspace ONE UEM console, navigate to **System > Enterprise Integration > VMware Tunnel > Configuration**.

   If this is the first time you configure VMware Tunnel, select Configure and follow the configuration wizard. Otherwise, select **Override** and select the **Enable VMware Tunnel** check box. Then click **Configure**

2. In the Configuration Type page, enable **Per-App Tunnel (Linux Only)**.

   Choose between **Basic** and **Cascade** mode. See the VMware Tunnel Guide for assistance with choosing the appropriate method.

   Click **Next**.

3. In the Details page, for the Per-App Tunneling Configuration, enter the VMware Tunnel server FQDN public host name and port if using VPN Access.

   Click **Next**.

4 In the SSL page, configure the Per-App Tunneling SSL Certificate. To use a public SSL, select the **Use Public SSL Certificate** check box. Click **Next**.

A Workspace ONE UEM (AirWatch) certificate can be generated automatically. If you prefer to use your public SSL certificate, check the text box and upload the certificate.

Note SAN certificates are not supported. Make sure that your certificate is issued for the corresponding server host name or is a valid wildcard certificate for the corresponding domain.

5 Click **Next**.

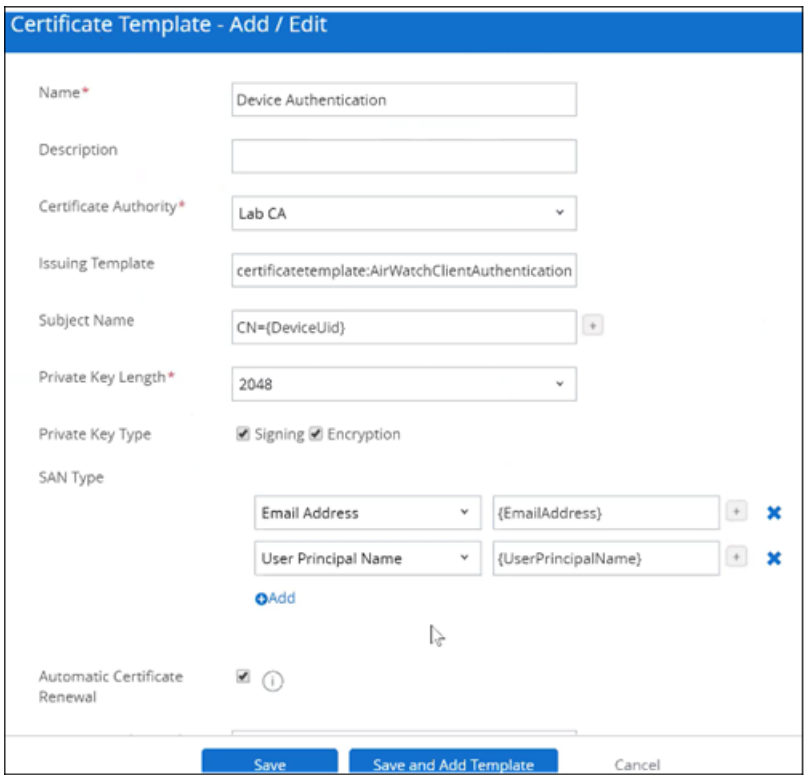
The Tunnel Device Root Certificate is automatically generated when you click Next.

6 In the Authentication page, select the certificate authentication type to use. Click **Next**.

Option	Description
Default	Select **Default** to use the Workspace ONE UEM issued certificates.
Enterprise CA	A drop-down menu listing the certificate authority and certificate template that you configured is displayed. You can also upload the root certificate of your CA.

If you select Enterprise CA, make sure that the CA template contains the subject name **CN={DeviceUid}:{EnrollmentUser}**. Make sure to include the colon (**:**). You can download the CA certificates from the VMware Tunnel configuration page.

Another option for specifying the device ID is to put a DNS SAN in the certificate with the value UDID={DeviceUid}.



7 Click **Next**.

8 (Optional) In the Miscellaneous page, enable the access logs for the Per-App Tunnel components. Click **Next**.

9 Review the summary of your configuration and click **Save**.

You are directed to the system settings configuration page.

10 Select the Configuration >General tab and click **Download Unified Access Gateway**.

What to do next

Configure the VMware Tunnel Settings for Workspace ONE UEM. For instructions, see the latest Unified Access Gateway documentation.

Configure Per App Tunnel Profile for Android

After you configured and installed the VMware Tunnel Per App Tunnel component, you can configure the Android VPN profile and add a version to the profile.

Procedure

1 In the Workspace ONE UEM console, navigate to **Devices > Profiles > Add Profile** and select **Android**.

2 Configure the General settings for Android if they are not already set up.

3 In the left column, select **VPN** and click **Configure**.

4 Complete the VPN Connection information.

Option	Description
Connection Type	Select **VMware Tunnel**.
Connection Name	Enter a name for this connect. For example, **`AndroidSSO Configuration`**.
Server	The VMware Tunnel server URL is automatically entered.
Per-App VPN Rules	Select the **Per-App VPN Rules** check box.

5 Click **Add Version**.

6 Click **Save & Publish**.

What to do next

Enable per-app VPN for the Android apps that can be accessed using Mobile SSO for Android. See Enable Per-App VPN for Android Apps.

Assign the device profile to a smart group. Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or are provisioned.

Enable Per-App VPN for Android Apps

The Per-App VPN Profile setting is enabled for Android apps that are accessed with VMware Identity Manager Mobile SSO for Android.

Prerequisites

- VMware Tunnel configured with the Per-App Tunnel component installed.
- Android VPN profile created.

Procedure

1. In the Workspace ONE UEM console, navigate to **Apps & Books > Applications > Native**.
2. Select the tab for the type of application, **Internal**, **Public**, or **Purchased**.
3. Select **Add Application** and add an app.
4. Click **Save & Assign**.
5. In the Assignment page, select **Add/Edit Assignment** and in the Advanced section. In the Advanced section, enable App tunneling and from the **Per-App VPN Profile** drop-down menu, select the Android VPN profile you created.
6. Click **Save & Publish**.

   Enable Per-App VPN for every Android app that is accessed with Mobile SSO for Android. While Per-App VPN is required, tunneling of app data is not required. The Tunnel app is configured on the device as a proxy for device traffic rules. For more information about adding or editing apps, see the VMware Workspace ONE UEM Mobile Application Management Guide on the VMware Workspace ONE UEM documentation page.

What to do next

Create the Network Traffic Rules. See Configure Network Traffic Rules in Workspace ONE UEM.

Configure Network Traffic Rules in Workspace ONE UEM

Configure the network traffic rules so that the VMware Tunnel client routes traffic to the web proxy for Android devices.

You list the Android apps that are configured with the per app VPN option to the traffic rules, and configure the proxy server address and the destination host name.

Configure the device traffic rules to control how devices handle traffic from specified applications. Device traffic rules force the VMware Tunnel app to send traffic through the tunnel, block all traffic to specified domains, bypass the internal network straight to the Internet, or send traffic to a web proxy site

For detailed information about creating network traffic rules, see the VMware Tunnel Guide.

Prerequisites

- VMware Tunnel is configured with the per-app tunnel component activated.

- Android VPN profile created.
- Per-App VPN enabled for each Android App that is added to the Network Traffic rules.

Procedure

1 In the Workspace ONE UEM console, navigate to **System > Enterprise Integration** > **VMware Tunnel > Network Traffic Rules**.

2 In the **Device Traffic Rules** tab, configure the device traffic rules settings as described in the VMware Tunnel Guide. Specific to the Mobile SSO for Android configuration, configure the following settings.

a Default Action. This rule is automatically configured and applies to all applications except Safari. The default action is always applied last.

Option	Description
Tunnel	Set the Action to **Tunnel** if VPN access is required for Mobile SSO for Android. All apps, except Safari, on the device configured for Per App VPN send network traffic through the tunnel.
Bypass	Set the Action to **Bypass** if VPN access is not required for Mobile SSO with Android. All apps, except Safari, on the device configured for Per App VPN bypass the tunnel and connect to the Internet directly. **Important** With this implementation, no traffic is sent to the Tunnel server when the Tunnel client is used only for single sign-on.

After the default rule is updated and the action is set to **Bypass**, a network traffic rule is added and configured for Android single sign-on.

b Select **Add** to crate additional rules as required.

c Select the up and down arrows to rearrange the ranking of your network traffic rules. The default rule is the last rule in the ranking.

d In the Application column, add the Android apps that are configured with the per app VPN profile.

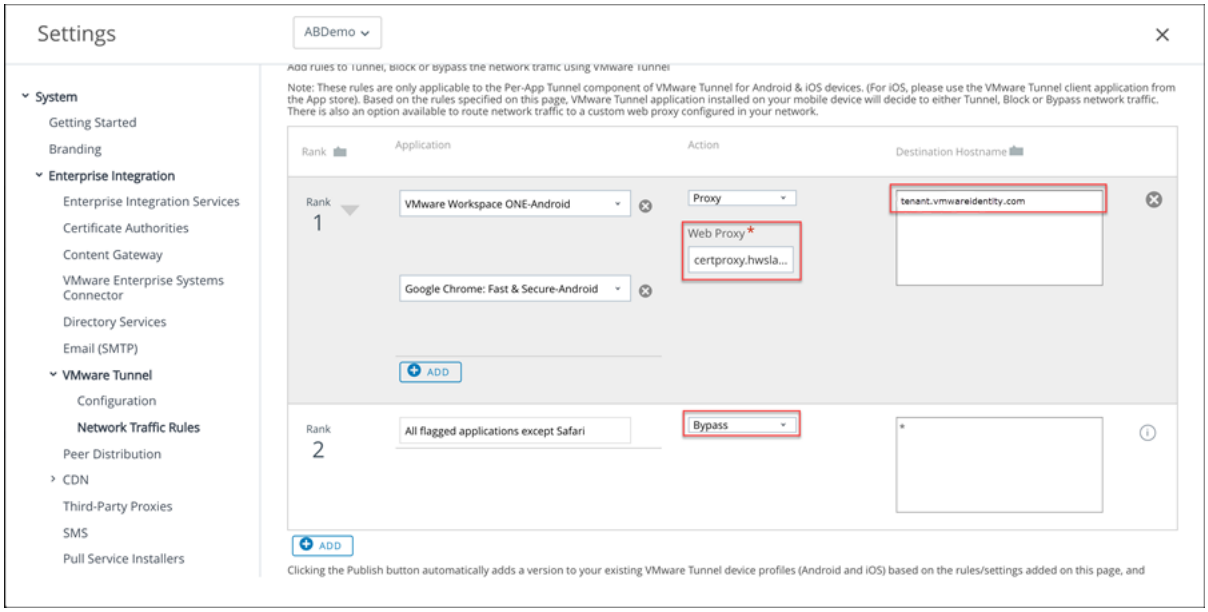
e For tenants hosted in the cloud, in the Action column, select Proxy and specify the web proxy information. For example, enter as `certproxy.vmwareidentity.<top-leveldomain>:5262`.

In the Destination Hostname column, enter your destination VMware Identity Manager host name. Enter as `<tenant>.vmwareidentity.<top-leveldomain>`. For example, `myco.vmwareidentity.com`. The VMware Tunnel client routes the traffic to the HTTPS proxy from the VMware Identity Manager host name.

f For on premises, in the Action column, select Proxy and specify the web proxy information. Enter the VMware Identity Manager host name and port. For example, `login.example.com:5262`.

Note For on-premises deployments, if you are providing external access to the VMware Identity Manager host, the firewall port 5262 (configurable) must be opened between devices on the Internet and the VMware Identity Manager host allowing Layer 4 TCP SSL passthrough on the load balancer/reverse proxy.

3 Click **Save**.



What to do next

Publish these rules. After the rules are published, the device receives an updated VPN profile and the VMware Tunnel application is configured to enable SSO.

Go to the VMware Identity Manager console and configure Mobile SSO for Android in the Built-in Identity Provider page.

Configuring Certificate Authentication for Android Mobile SSO

2

You configure certificate authentication to allow clients to authenticate with certificates on their Android devices for single sign-on to Workspace ONE.

An X.509 certificate uses the public key infrastructure (PKI) standard to verify that a public key contained within the certificate belongs to the user.

To enable signing in using certificate authentication, root certificates and intermediate certificate must be uploaded to the VMware Identity Manager service.

This chapter includes the following topics:

Certificate Authority required for Authentication with Android Devices

To enable logging in using certificate authentication, root certificates and intermediate certificates must be uploaded to the VMware Identity Manager service.

The intermediate (user) certificates are copied to the local certificate store on the Android device. The certificates in the local certificate store are available to all the browsers running on this Android device, with some exceptions, and therefore, are available to a VMware Identity Manager instance in the browser.

If a user cannot authenticate, the root CA and intermediate CA might not be set up correctly, or the service has not been restarted after the root and intermediate CAs were uploaded to the server. In these cases, the browser cannot show the installed certificates, the user cannot select the correct certificate, and certificate authentication fails.

Using Certificate Revocation Checking

You can configure certificate revocation checking to prevent users who have their user certificates revoked from authenticating. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

Certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure both CRL and OCSP in the same certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the Use CRL in case of OCSP failure check box is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL. Revocation checking does not fall back to OCSP if CRL fails.

Logging in with CRL Checking

When you enable certificate revocation, the VMware Identity Manager connector server reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked, authentication through the certificate fails.

Logging in with OCSP Certificate Checking

The Online Certificate Status Protocol (OCSP) is an alternative to certificate revocation lists (CRL) that is used to perform a certificate revocation check.

When you configure certificate-based authentication, when Enable Cert Revocation and Enable OCSP Revocation are both enabled, VMware Identity Manager validates the entire certificate chain, including the primary, intermediate and root certificates. The revocation check fails if the check of any certificate in the chain fails or the call to the OCSP URL fails.

The OCSP URL can either be configured manually in the text box or extracted from the Authority Information Access (AIA) extension of the certificate that is being validated.

The OCSP option that you select when you configure certificate authentication determines how VMware Identity Manager uses the OCSP URL.

- **Configuration Only**. Perform certificate revocation check using the OCSP URL provided in the text box to validate the entire certificate chain. Ignore the information in the certificate's AIA extension. The OCSP URL text box must also be configured with the OCSP server address for revocation checking.
- **Certificate Only (required)**. Perform certificate revocation check using the OCSP URL that exists in the AIA extension of each certificate in the chain. The setting in the OCSP URL text box is ignored. Every certificate in the chain must have an OCSP URL defined, other wise the certificate revocation check fails.
- **Certificate Only (Optional)**. Only perform certificate revocation check using the OCSP URL that exists in the AIA extension of the certificate. Do not check revocation if the OCSP URL does not exist in the certificate AIA extension. The setting in the OCSP URL text box is ignored. This configuration is useful when revocation check is desired, but some intermediate or root certificates do not contain the OCSP URL in the AIA extension.

- **Certificate with fallback to configuration**. Perform certificate revocation check using the OCSP URL extracted from the AIA extension of each certificate in the chain, when the OCSP URL is available. If the OCSP URL is not in the AIA extension, check revocation using the OCSP URL configured in the OCSP URL text box. The OCSP URL text box must be configured with the OCSP server address.

Configure Mobile SSO for Android Authentication in the Built-in Identity Provider

To provide single sign-on from Workspace ONE UEM-managed Android devices, you configure Mobile SSO for Android authentication in the VMware Identity Manager built-in identity provider.

Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.

Procedure

1. In the VMware Identity Manager console, Identity & Access Management tab, select **Manage > Authentication Methods**.
2. To enable and configure CertProxyAuthAdapter, click the **Mobile SSO (for Android devices)** pencil icon.

Option	Description
Enable Certificate Adapter	Select this check box to enable Mobile SSO for Android.
Root and Intermediate CA Certificate	Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded. The file format can be either PEM or DER.
Uploaded CA Certificates	The contents of the uploaded certificate file is displayed here.
User Identifier Search Order	Select the search order to locate the user identifier within the certificate. ■ **upn**. The UserPrincipalName value of the Subject Alternative Name ■ **email**. The email address from the Subject Alternative Name. ■ **subject**. The UID value from the Subject.
Validate UPN Format	Enable this check box to validate the format of the UserPrincipalName field.
Certificate Policies Accepted	Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID number (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs.
Enable Cert Revocation	Select the check box to enable certificate revocation checking. This prevents users who have revoked user certificates from authenticating.

Option	Description
Use CRL from Certificates	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate a certificate's status of revoked or not revoked.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL.
Enable OCSP Revocation	Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP failure	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
OSCP URL Source	Select the source to use for revocation checking. ■ **Configuration Only**. Perform certificate revocation check using the OCSP URL provided in the text box to validate the entire certificate chain. ■ **Certificate Only (required)**. Perform certificate revocation check using the OCSP URL that exists in the AIA extension of each certificate in the chain. Every certificate in the chain must have an OCSP URL defined, other wise the certificate revocation check fails. ■ **Certificate Only (Optional)**. Only perform certificate revocation check using the OCSP URL that exists in the AIA extension of the certificate. Do not check revocation if the OCSP URL does not exist in the certificate AIA extension. ■ **Certificate with fallback to configuration**. Perform certificate revocation check using the OCSP URL extracted from the AIA extension of each certificate in the chain, when the OCSP URL is available. If the OCSP URL is not in the AIA extension, check revocation using the OCSP URL configured in the OCSP URL text box. The OCSP URL text box must be configured with the OCSP server address.
OCSP Responder's Signing Certificate	Enter the path to the OCSP certificate for the responder. Enter as `/path/to/file.cer`
Uploaded OCSP Signing Certificates	The uploaded certificate files are listed in this section.
Enable Cancel Link	When authentication is taking too long, if this link is enabled, users can click Cancel to stop the authentication attempt and cancel the sign-in.
Cancel Message	Create a custom message that displays when the authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials`.

3 Click **Save**.

4 Select **Manage > Identity Providers**and click **Add Identity Provider**.

5 Select **Create Built-in IDP** or select an existing built-in identity provider.

Option	Description
Identity Provider Name	Enter the name for this built-in identity provider instance.
Users	The configured directories are listed. Select the User directory to authenticate.

Option	Description
Network	The existing network ranges configured in the service are listed. The network range that you use in the policy rule for Mobile SSO for Android must consist of only the IP addresses used to receive requests coming from the VMware Tunnel proxy server.
Authentication Methods	Select **Mobile SSO (for Android)**.
KDC Certificate Export	N/A

6 Click **Add** on the built-in identity provider page.

What to do next

Configure the default access policy rule for Mobile SSO for Android.

Adding Access Policy Rule

You must edit the default policy rules to add the Android Mobile SSO authentication method you configured.

See Managing Access Policies in the VMware Identity Manager Administration guide to learn more about setting up policy rules.

Procedure

1 In the VMware Identity Manager console Identity & Access Management tab, select **Manage > Policies**.

2 Click **Edit Default Policy** and then click **Next**.

3 Add a new policy rule, click **Add Policy Rule**.

Option	Description
If a user's network rang is	Select the network range for this policy rule.
and user accessing content from	Select **Android**.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If you do not select a group, the access policy applies to all users.
Then perform this action	Select **Authenticate using....**
then the user may authenticate using	Select **Mobile SSO (for Android)**.
If the preceding methods fails or is not applicable, then	Configure additional fallback authentication methods.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

4 (Optional) In Advanced Properties, create a custom access denied error message that displays when user authentication fails. You can use up to 4000 characters, which are about 650 words. If you want to send users to another page, in the **Custom Error Link URL** text box, enter the URL link address. In the **Custom Error Link text** text box, enter the text to describe the custom error link. This text is the link. If you leave this text box blank, the word `Continue` displays as the link.

5 Click **Save**.

6 Drag and drop this rule before the Web Browser rule in the list of default access policy rules.

7 Click **Next** to review the rules and then click **Save**.

Configuring the Cert Proxy Service on VMware Identity Manager Machines

3

For VMware Identity Manager on-premises deployments, the Cert Proxy service must be set up on the VMware Identity Manager machines to configure mobile single sign-on for Android devices.

The VMware Identity Manager cert proxy service is installed by default when you install VMware Identity Manager. You must enable and configure the VMware Identity Manager cert proxy service on the virtual appliances after VMware Identity Manager service is installed. The cert proxy service is enabled on Windows machines by default.

This chapter includes the following topics:

SSL Passthrough or Reencryption in the Cert Proxy Service

For Android certificate authentication, the cert proxy service runs on the VMware Identity Manager node as an independent service to receive connections on port 5262 and proxy the connections to the VMware identity Manager service on port 443 for authentication.

The HTTPS 443 traffic for VMware Identity Manager can be either set to Layer 7 SSL offloading on the load balancer/reverse proxy or allowed to SSL passthrough as Layer 4 TCP to the backend server. When 443 traffic is configured with SSL passthrough, the publicly trusted certificate is shared between the VMware Identity Manager service on port 443 and the CertProxy service on port 5262. No additional configuration is needed.

If the HTTPS traffic is SSL offloaded on the load balancer/reverse proxy, the VMware Identity Manager service uses a self-signed certificate for trust which is generated during the application installation process. Because 5262 must be set to SSL Layer 4 TCP with SSL passthrough that requires a publicly trusted SSL certificate, this leads to a certificate mismatch between the two services running on the host. To circumvent this problem, the CertProxy service requires a secondary port 5263 configured on the

server. Port 5263 shares the same self-signed certificate as the one running on the VMware Identity Manager service. Configuring the additional port 5263 allows the communication to be secured and trusted throughout the Mobile SSO process for Androids while also allowing HTTPS traffic decryption on the load balancer.

Deciding Between SSL Re-Encryption and SSL Offloading for HTTP 443 Traffic

The following is a decision matrix to help you set up the cert proxy service with the VMware Identity Manager service.

In this matrix, SAN certificates are defined as a certificate containing the VMware Identity Manager VIP FQDN and each node machine FQDN. The FQDN is in the format of a non-routable domain/sub-domain. Based on your VMware design use the matrix to determine if port 5263 is configured.

Table 3-1. Cert Proxy Configuration Decision Matrix

Public Namespace	DMZ Namespace	Certificate Type	Load Balancer Requirement	Cert Proxy Port 5263 Required
Shared Namespace (.com / .com)				
example.com	example.com	Wildcard, SAN	SSL Re-encryption required	No
example.com	example.com	Single Host CN	SSL Re-encryption required	Yes
example.com	example.com	Wildcard, SAN	SSL Passthrough required	No
Disjointed Namespace (.com / .dmz)				
example.com	example.dmz	Wildcard, Single Host CN	SSL Re-encryption required	Yes
example.com	example.dmz	SAN	SSL Re-encryption required	No
example.com	example.dmz	SAN	SSL Passthrough required	No

Figure 3-1. VMware Identity Manager Proxy Port Configuration in DMZ with Only Port 5262 Configured

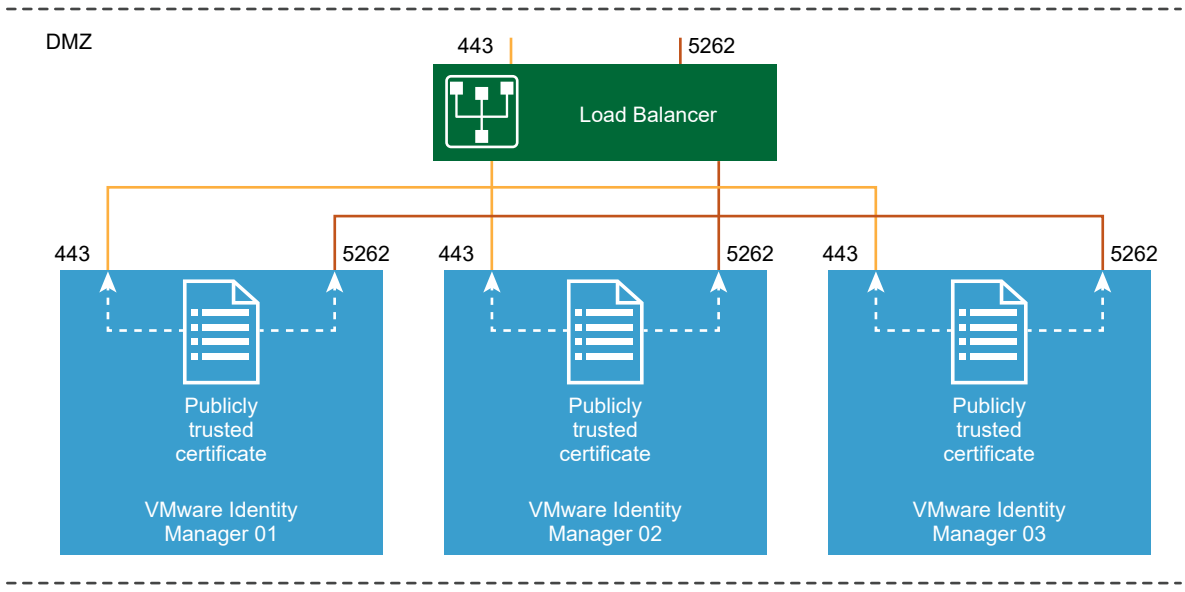
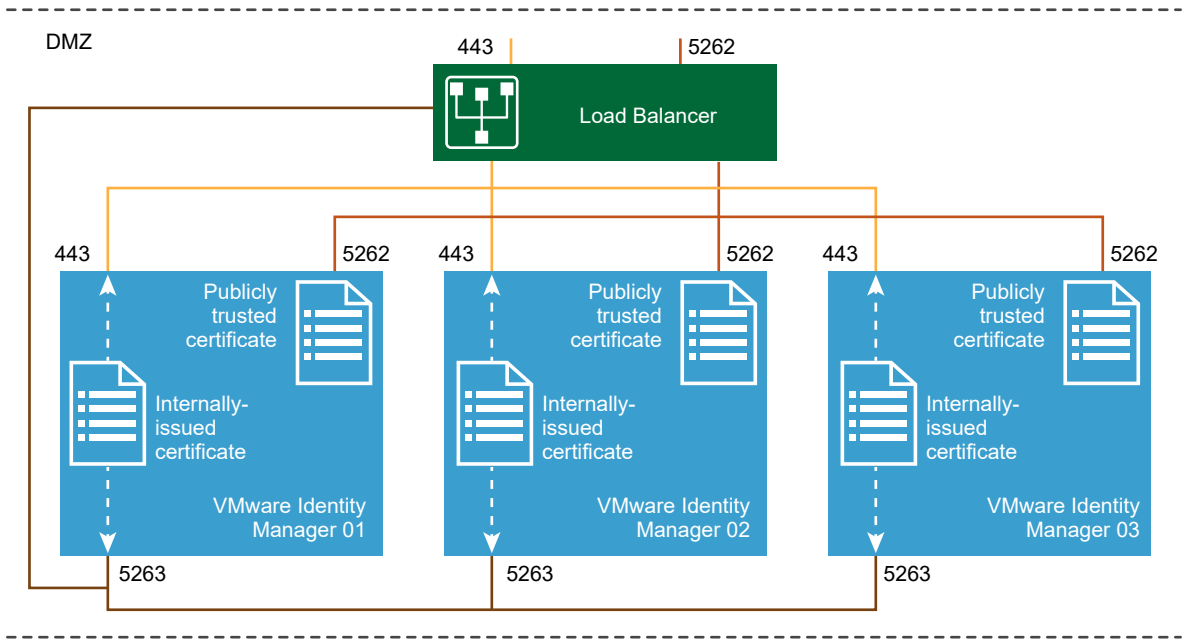


Figure 3-2. VMware Identity Manager Proxy Port Configuration in DMZ with Port 5262 and Port 5263 Configured



Load Balancer Requirements to Use the Cert Proxy Service

When the VMware Identity Manager nodes are configured in the DMZ behind a load balancer, all nodes must be configured to communicate with each other. The firewall rules are configured to allow the nodes to talk to each other on port 5262.

For the cert proxy service to work to direct requests correctly, the load balancer should be configured as follows.

- SSL re-encryption enabled.
- Publicly trusted certificate installed on the load balancer.
- X-Forwarded-For header enabled.
- RemotePort header enabled.
- Port 443 configured with a self-signed certificate on each node.
- Port 5262 configured for the cert proxy service, with SSL pass-through configured for certificate authentication. The SSL handshake is between the device and the service.
- Port 5263 configured as another instance of the cert proxy service to receive internal admin requests from the service.

How Certificates Work with the Cert Proxy Service

Two levels of certificates are used for certificate authentication, the certificate on the device and the certificate for VMware Identity Manager service on port 443.

A publicly trusted certificate is set up on the load balancer.

If performing SSL re-encryption, the self-signed certificate is required on each node.

When SSL passthrough is configured, an internally-issued certificate that includes the Subject Alternative Names (SAN) for all the hosts in the cluster is required on each node. The SAN with the host names allows all the nodes in the cluster to make requests to each other.

Set Up Cert Proxy for VMware Identity Manager

The cert proxy settings must be configured on the VMware Identity Manager service to manage the Android Mobile SSO requests.

Prerequisites

Cert Proxy set up is required only for on-premises deployments with Android devices.

- Load balancer correctly configured.
- Certificates upload to the VMware Identity Manager service.
- VMware Identity Manager for Linux, the cert proxy service running.

Procedure

1. Log in to the VMware Identity Manager console and select the **Appliance Settings** tab.
2. Click **Mobile SSO**.

3 Configure the Cert Proxy settings for Android Mobile SSO requests to the VMware Identity Manager service.

Option	Description
Destination Forced	When **Destination Forced** is selected, a single hostname or IP address must be provided in the Destination text box. All Android SSO requests are sent to that destination. This destination is either the load balancer or the localhost, depending on the VMware Identity Manager configuration.
Destination	If Destination Forced is enabled, enter the host name or IP address to use. If Destination Forced is not selected, enter the white-list of approved destinations that can receive Android SSO requests. The addresses in the list can be separated by a semicolon either in CIDR format, subnet format delimited by a space, or a single IP.
Allow RemotePort Header	Enable the use of the RemotePort header from the load balancer. The source port number of the request from the proxy to the identity manager service is added to the header. RemotePort header is required in the connection to tell the receiving node where to call to get the certificate.
Accept RemotePort From	Enter a white-list of approved addresses that can include the RemotePort header. The addresses in the list can be separated by a semicolon either in CIDR format, subnet format delimited by a space, or a single IP.

4 Verify that the hash value for the **Certificate Proxy Key** and the **Certificate Proxy Key (Identity Manager)** are the same. Check the config files cert-proxy.properties and runtime-config.properties.

These two text boxes are pre-populated with the hash value of the certificate keys of the cert proxy service and the VMware Identity Manager service.

The hashes must match. If the hashes do not match, the issue must be addressed in configuration files by copying the value of one service to the other.

5 Configure the cert proxy configuration for Android SSO through the VMware Identity Manager service.

Option	Description
Port	Usually two ports are configured for cert proxy. Port 5262 receives the external request from the Android device. Port 5263 receives the internal admin request from the VMware Identity Manager service.
Admin Port	If the port number configured in the Port text box is the port that receives the internal request from the VMWare Identity Manager service for the certificate, enable **Admin Port**. The port is usually 5263. If this port is not used to receive the internal request, do not enable this radio button.
SSL Certificate Type	Android SSO cert proxy is a separate service on the identity manager machine. Select **Passthrough** to reuse the pass-through certificate provisioned for VMware Identity Manager in the Appliance Settings > Install SSL Certificates page. If a different certificate is required, select **Custom** and upload the certificate in the **SSL Certificate Chain** text box.

6 To configure another port, click **Add Port** and configure the settings as described in step 5.

7 To save the port configuration, click **Save**.

8 When you make changes on this page that affect certificates, click **Restart Cert Proxy service** at the top of the page.

   Clicking Restart Cert Proxy service might require a restart of the VMware Identity Manager service.

What to do next

Set up the cert proxy service on each node. If cert proxy service is set up on the first machine, when you clone the identity manager service on the appliance or copy the files on a Windows machine, most of the proxy settings are configured. To verify that the cert proxy settings are set correctly, you can check the runtime-config.properties file

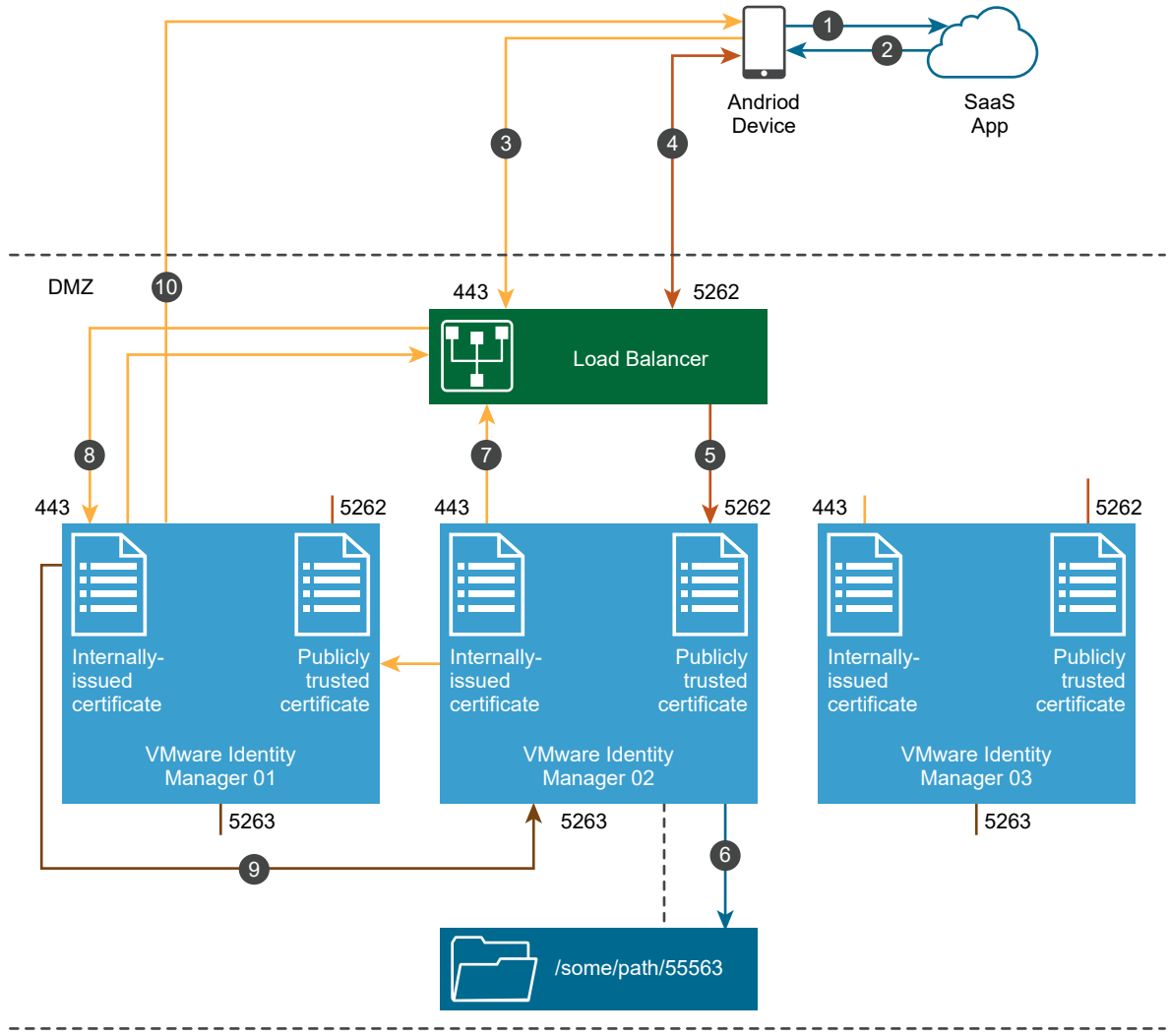
Authentication Approval Flow Through Cert Proxy for Android Single Sign-On

4

When the Workspace ONE UEM console and the VMware Identity Manager console are configured for Android mobile SSO authentication, you configured the network traffic rules so that the VMware Tunnel mobile app routes traffic to 5262. When users use their Android devices to launch an SAML app that requires single-sign on, the tunnel app intercepts the request and based on the device traffic rules, established a proxy tunnel to the Cert Proxy port 5262.

The following diagram shows the authentication approval flow when the cert proxy services is configured with both Port 5262 and port 5263.

Figure 4-1. Authentication Approval Flow for Android Mobile Single Sign-On with Port 5262 and Port 5263 Configured



The authentication flow with both port 5262 and port 5263 configured for cert proxy.

1 User starts a SAML app from an Android mobile device.

2 The SAML app requests authentication.

3 Identity Manager authentication on Port 443 is required to sign in to the app.

4 The network traffic rules are configured so that the VMware Tunnel app routes traffic to 5262. The Tunnel app intercepts the request and based on the device traffic rules, established a proxy tunnel to the Cert Proxy port 5262.

5 The load balancer is configured with SSL passthrough on port 5262 and the load balancer passes through the request to the cert proxy port 5262 on one of the nodes in the cluster.

6 The cert proxy service receives the request, extracts the user certificate, and stores it as a local file using the request's source port number, for example port 55563, as a reference key.

7 The cert proxy service forwards the request to VMware Identity Manager for authentication on port 443 on the load balancer. The sending node, Node 2 in this example, IP address is included in the X-Forwarded-For header and the original request source port number information (port 55563) in the RemotePort header.

8 The load balancer sends a request to port 443 on one of the nodes based on load balancer rules, Node 1 in this example. This request includes the X-Forwarded-For and the RemotePort headers.

9 The horizon service port 443 on Node 1 talks to the cert proxy service on Node 2 port 5263, which directs the service to /some/path/55563 to retrieve the user certificate and perform authentication.

10 The certificate is retrieved and the user is authenticated.