IMPLEMENTING SINGLE SIGN-ON (SSO) TO KERBEROS CONstrained DELEGATION AND HEADER-BASED APPS

VMware Identity Manager

February 2017 V1
Table of Contents

Overview ....................................................................................................................................................... 5
Benefits of BIG-IP APM and Identity Manager ............................................................................................. 5
Integration Overview .................................................................................................................................... 5
  Authentication Flow into KCD and Header-Based Apps ........................................................................... 7
Step-by-Step Integration Instructions........................................................................................................... 7
  Downloading SAML Metadata from Identity Manager ............................................................................. 8
  Uploading the Identity Manager Metadata into BIG-IP APM ............................................................... 9
  Downloading SAML Metadata from APM ................................................................................................. 13
  Uploading the APM Metadata into Identity Manager ............................................................................... 15
  Configuring Your App in Identity Manager ............................................................................................ 18
  Setting up Kerberos Constrained Delegation (KCD) in BIG-IP APM ..................................................... 20
  Setting up Domain Authentication ......................................................................................................... 21
  Creating the APM Access Profile ............................................................................................................ 22
  Creating Your Access Policy in APM ....................................................................................................... 24
  Creating Your VIP for Your Kerberos Web Application Servers .......................................................... 33
    Creating Your Pool .............................................................................................................................. 33
    Creating a Persistence Profile ............................................................................................................. 34
    Importing Client SSL Certificates ..................................................................................................... 35
    Creating a Client SSL Profile .............................................................................................................. 38
    Creating Your Virtual Server ............................................................................................................. 40
  Setting up Integration for Multiple Apps ............................................................................................... 42
    Testing and Troubleshooting ............................................................................................................. 42
    Setting up a Kerberos Service Account ............................................................................................... 42
Overview

This guide is designed to help you set up Single Sign on (SSO) to legacy web applications that use Kerberos Constrained Delegation (KCD) or header-based authentication.

Of course, there aren’t many IT organizations that only want to SSO into legacy web applications—you also want to provide SSO access to cloud apps, mobile apps, and other on-premises web apps. VMware Identity Manager™ and F5 BIG-IP Access Policy Manager (APM) work together to make SSO into all of these different app types simple for your end users. VMware and F5 also keep IT happy with enterprise secure features that ensure only your intended users get access to corporate resources.

Benefits of BIG-IP APM and Identity Manager

For end users, the benefits of the BIG-IP APM and Workspace ONE integration center around easy access to the apps and resources that they need to for work, including the following.

- SSO to a wide variety of cloud apps, mobile apps, on-premises web apps, and legacy apps using SAML, OAuth 2.0, OpenID Connect, WS-FED, and other protocols.
- Easy sign on using mobile SSO or installed certificates to minimize user interaction.
- Access to all their applications in one place, the Workspace ONE portal.

For IT admins, the benefits of this integration include all the above with the addition of these security features.

- BIG-IP APM’s ability to act as an authenticated reverse proxy, securely publishing on-premises apps outside your network.
- BIG-IP APM’s access control policies that ensure only authorized users get access to apps within your corporate network.
- Identity Manager’s conditional access policies, allowing IT admins fine-grained control of which users and devices should have access to apps. Conditional access policies can include device compliance checks, network range checks, authentication strength checks, and location checks.
- Identity Manager’s step-up authentication features, allowing IT to require multi-factor authentication for certain apps, users, devices, or contexts.

Integration Overview

In this guide, we’ll cover the integration necessary to SSO to apps using KCD and header-based authentication. For authenticating into apps using different authentication methods, see the VMware Identity Manager documentation or the F5 BIG-IP APM documentation.
To provide SSO to KCD and header-based apps, Identity Manager acts as an identity provider (IDP). BIG-IP APM acts as a service provider (SP). Users authenticate into the identity manager. Identity Manager then passes to APM the user’s authentication status and requests to open an app, as in the diagram below.
Authentication Flow into KCD and Header-Based Apps
An end user launches the authentication flow by trying to access an app from the Workspace ONE portal. The flow follows these steps.

1. User is granted access to Application List per Workspace One Permissions and Policy
2. End user is authenticated by Workspace ONE according to conditional access policies
3. Workspace ONE passes a SAML assertion to BIG-IP APM
4. BIG-IP APM transforms the SAML assertion into KCD or header-based format
5. The end user is logged in to the KDC or header-based Web Application

Step-by-Step Integration Instructions
To integrate the Identity Manager and APM, follow the steps below. Each step is explained in detail with screenshots in the following sections.

1. Downloading SAML metadata from Identity Manager
2. Uploading the Identity Manager metadata into BIG-IP APM
3. Downloading SAML Metadata from APM
4. Uploading the APM Metadata into Identity Manager
5. Configuring your app in Identity Manager
6. Setting up Kerberos Constrained Delegation (KCD) in APM
7. Creating the APM Access Profile
8. Creating your Access Policy in APM
9. Creating your pool in APM
Implementing Single Sign-on to Kerberos Constrained Delegation and Header-Based Apps

Downloading SAML Metadata from Identity Manager

In these steps, you’ll download an XML metadata file from the Identity Manager admin console that tells BIG-IP APM how to connect.

1. Open your Identity Manager tenant. You’ll need an admin account to access SAML metadata.
2. From the Identity Manager admin console, click the Catalog drop-down arrow > Settings.

3. Click SAML Metadata on the left side menu.
4. Right-click the Identity Provider (IdP) metadata link. Save the metadata xml file to your computer.
5. Save the downloaded file to a location you can access later. Make sure not to change the file format or extension from “.xml”.

Uploading the Identity Manager Metadata into BIG-IP APM
In these steps, you’ll upload the metadata you downloaded from the Identity Manager admin console.

1. Open your BIG-IP APM admin console.
2. Click Access Policy > SAML > BIG-IP as SP.
3. Click External IdP Connectors in the upper tabs.
4. Click Create drop-down menu. Select From Metadata.

5. Click Browse and select the file you saved earlier. Enter a friendly name for Identity Manager in the Identity Provider Name field. Then click OK.
6. You should see an IdP connector with the name you chose in a list of all your IdP connectors.

7. Create a DNS record for SAML SP Service for the upcoming virtual server. Make sure you use a wildcard certificate or that the name on your certificate exactly matches the DNS name for your server. If you have not created your certificate, create it before proceeding to the following steps. Copy the DNS name you create for the SAML SP service.
8. In the Big-IP Management Web Console, select the Local SP Services Tab and click Create.

9. Enter a name for your SP service. This SP service will be used to connect your app to APM and APM to Identity Manager. Under Entity ID use an https with the FQDN of the DNS name selected for the SP. For example, https://bigip-sp-for-idm.bd.f5.com.
10. Click **Security Settings**. The Message Signing Private Key and Message Signing Certificate fields will be prefilled from the Identity Manager metadata you imported into APM. Click **OK** to create your SP Service.

**Downloading SAML Metadata from APM**

1. Click the checkbox next to your newly created SP service. Then click **Bind/Unbind IdP Connectors**.
2. Click **Add New Row**. Select **SAML IDP Connector** from the drop-down menu. Click **Update**. Then click **OK** to close the dialog box.

3. Ensure the box is checked next to the Local SP then click **Export Metadata**.

4. Leave the Sign Metadata option set to **No**. Click **Download** which will save the metadata to the default downloads folder.
Uploading the APM Metadata into Identity Manager

1. Find the metadata file you saved in Downloading SAML Metadata from APM. Open the metadata file in a text editor. Note: It’s important to open the file in a text editor that will not change the XML format or insert characters, such as Notepad++. 

2. Select all and copy the metadata.
3. Open the Identity Manager admin console. Click the Catalog tab. Select + Add Application and then click ...create a new one.

4. In the Application Details page, enter an end-user-friendly name in the Name field. Select the SAML 2.0 POST profile from the Authentication Profile drop-down menu. You can also add a description or application icon to display to end users in the Workspace ONE portal. Click Next.
5. At the bottom of the Application Configuration page, in the Configure Via section, select the Meta-data XML radio button. Paste the APM metadata you copied from the text editor program into the Meta-data XML field. Then click Save.
Configuring Your App in Identity Manager
Before end users can use your app, you need to apply entitlement policies to it. In this example, we’ll entitle a group of users to use the app.

1. In the Identity Manager admin console, click **Add Group Entitlement**.

2. Click **or browse**... to see a list of all groups in Identity Manager.
Check the box next to the groups you want to entitle to the application. If you want users to request the application in the Workspace ONE catalog, leave the drop-down box set to User-Activated. If you want the application to be automatically added to the catalog for the groups you selected, set the drop down to Automatic. Click Save.

3. Click Done to finish the entitlement steps.
Setting up Kerberos Constrained Delegation (KCD) in BIG-IP APM

If you are integrating a KCD app, you should now set up KCD in APM.

1. Open the F5 BIG-IP admin console.
2. Click **Access Policy > SSO Configurations > Kerberos > plus icon (+)**.

3. In the **New SSO Configuration** menu, click **Kerberos**.
   - Enter a unique name for your KDC SSO Configuration
   - Set the Username Source field to `session.sso.token.last.username`
   - Set the User Realm Source field to `session.ad.last.actualdomain`
   - Set the Kerberos Realm field to your active directory domain (in CAPS).
   - Set the Account Name field to your Kerberos service account and enter your account password.

   If a Kerberos Service Account hasn’t been created it’s recommended to create one via the following documentation.

   - Set the Account Password and Confirm Account Password fields with the Password associated to the Kerberos service account.
   - Leave all other non-required fields with the default settings. (Required fields have a blue line). Click **Finished**.
Setting up Domain Authentication

1. In the BIG-IP admin console, click **Access Policy > AAA Servers > Active Directory > plus Icon ( + )**.

2. Enter a friendly name in the **Name** field.
   a. Set the Domain Name field to your Active Directory Domain Name (FQDN).
   b. Set the Server Connection radio button to **Use Pool** to increase resiliency.
   c. Set the Domain Controller Pool Name to a friendly name for your pool (no spaces allowed).
   d. Set the IP Address field to the IP Address of your domain controller.
   e. Set the Hostname field to the short name for your domain controller.
   f. Click **Add**, to add the domain controller to your pool.
   g. Repeat steps d, e, and f for each domain controller you want to add to the pool.
   h. Set the server pool monitor drop-down to **gateway_icmp**.
   i. Set the Admin Name field to your domain admin user.
   j. Set the Admin Password field to your domain admin’s password.
   k. Set the Group Cache Lifetime field to **30 days**.
Implementing Single Sign-on to Kerberos Constrained Delegation and Header-Based Apps

1. Set the Password Security Object Cache Lifetime to **30 days**.
   m. Click **Finished**.

Creating the APM Access Profile

1. Click **Main > Access Policy > Access Profiles > Access Profiles List > Plus icon ( + ).**
2. Name your new access profile. In the Profile Type drop-down, select All. In the Profile Scope drop-down, select Profile.

3. Scroll down to the bottom of the configuration.
   a. Set the SSO Configuration drop-down, select the Kerberos SSO profile created in Setting up Kerberos Constrained Delegation (KDC) in BIG-IP APM.
   b. In Languages chooser, click English to highlight it and click << button to move it to Accepted Languages.
   c. Click Finished.
Creating Your Access Policy in APM

1. Click **Access Policy > Access Profiles > Access Profiles List**. In the row for the access policy profile you created, click **Edit** in the Access Policy column to open the Visual Policy Editor.

![Visual Policy Editor](image1.png)

2. In the Visual Policy Editor click the plus icon (+) to the right of “fallback” to add a new item. (The following screen does not look like the directions above)

![Visual Policy Editor](image2.png)

3. In the popup, select the **Authentication** tab.
4. Scroll down and select the **SAML Auth** radio button. Click **Add Item**.

5. In the dropdown menu for AAA Server, select the SP service you created in [Downloading SAML Metadata from APM](#). Click **Save**.
6. In the Visual Policy Editor, select **Plus (+)** under **Successful** to add a new item in the tree.

7. Click the Assignment tab. Select the **Variable Assign** radio button and click **Add Item**.
8. Click **Add New Entry**.

9. Click the **change** link next to empty.
10. In the popup window
   a. Ensure the default **Custom Variable** is selected from the first drop-down menu.
   b. Ensure the default **Unsecure** is selected from the second drop-down menu.
   c. Enter `session.ad.last.actualdomain` as the variable value.
   d. Select **Text** in the third drop-down menu.
   e. Enter your Active Directory Domain Name (FQDN) in the Text field.
   f. Click **Finished**.

11. In the Variable Assign window, click **Add New Entry** again. Click the **change** link next to empty.

12. In the popup window
   a. Ensure the default **Custom Variable** is selected from the first drop-down menu.
   b. Ensure the default **Unsecure** is selected from the second drop-down menu.
   c. Enter `session.logon.last.username` as the variable value.
   d. Ensure the default **Custom Expression** is selected in the third drop-down menu.
e. Enter expr \{"[lindex [split [mcget {session.saml.last.identity}] "@"] 0]\}.

*NOTE: If the dialog box does not close after clicking Finished, make sure your expression includes straight double quote characters (" ) rather than curly double quote characters (” ”).

f. Click Finished.

13. Ensure that both Assignment fields are populated accordingly then click **Save**.

*Data in tab has been changed, please don't forget to save*
14. Click the plus icon (+) in the fallback line after Variable Assign box.

15. Click the Assignment Tab. Choose the SSO Credential Mapping radio button. Click Add Item.
16. In the SSO Token Username field, select **Username from Logon Page** from the drop-down menu. *Note: Leave the default values that appear in both fields and click Save.*

![Image of SSO Credential Mapping](image)

17. In the SAML Auth Successful > Variable Assign > SSO Credential Mapping row, click the Deny link in the ending box.
   a. In the Select Ending dialog box that displays, select **Allow**.
   b. Click **Save**.

![Image of Access Policy](image)
18. Your Access Policy flow should now match the following image. Click the **Apply Access Policy** link to ensure your changes are committed.

19. Close the Visual Policy Editor Tab in the browser.
Implementing Single Sign-on to Kerberos Constrained Delegation and Header-Based Apps

Creating Your VIP for Your Kerberos Web Application Servers

Creating Your Pool

Note: The steps below require a working Kerberos Constrained Delegation enabled app. If you want to use a test app, create it before beginning the following steps.

1. In the BIG-IP admin console, click Local Traffic > Pools > Pool List > ( + ) Plus. This will start the creation of a pool that relates to your Kerberos Web App server.
   a. Enter a unique friendly name for your app in the Name Field.
   b. In the Health Monitors box, select http or https depending on the current web application servers port and service and click the << button to make it active.
   c. In the Load Balancing Method box, select Least Connections (member).
   d. Click the New FQDN Node radio button.
   e. Optionally, you can enter a Friendly Name for the FQDN Node in the Node Name field.
   f. In the FQDN field, enter the FQDN of your Kerberos app.
   g. In the Service Port field, enter the service port for your app.
   h. Click Add.
   i. Repeat steps c – g for each additional server if you have multiple servers for your web app.
   j. Click Finished.
Creating a Persistence Profile

Create a Persistence Profile for your app in APM, follow the instructions below.

1. Click **Local Traffic > Profiles > Persistence > Plus icon (+)**.

2. In the New Persistence Profile screen, enter a friendly name in the Name field.
   a. In the Persistence Type field, select **Source Address Affinity**.
   b. Click **Finished**.
Importing Client SSL Certificates

Import the DNS or Wildcard Certificate as referenced in [Uploading the Identity Manager metadata into BIG-IP APM](#) into the BIG-IP.

1. Click **System > File Management > SSL Certificate List > Import ...**

2. When importing Certificates/Keys the Certificate **MUST** contain an exportable private key. In this use case we will import a PKCS 12 type certificate (PFX/P12).
   a. In the Import Type select **PKCS 12 (IIS)**. This will add additional items to the menu.
   b. In the Certificate Name field, give your certificate a unique friendly name.
   c. In the Certificate Source field, click **Choose File** to find your pfx/p12 file. Click Open.
3. In the Password field, enter the key password. click **Import**.

4. Next, import your Root CA and Intermediary CA certificate files. Click **System > File Management > SSL Certificate List > Import**...
5. When Importing Root/Intermediary CA Certificates, you can import each certificate individually or at once as a chain.
   a. Select **Certificate** for the Import Type field to expand the menu.
   b. In the Certificate Name field, enter a unique friendly name.
   c. In the Certificate Source field, click **Choose File** to find your certificate file.
   d. Find the location of your certificate file and click **Open**.

6. Click **Import**.
Creating a Client SSL Profile

Create a Client SSL profile for your app, follow the instructions below:

Note: To complete this step you must have already imported either a DNS Name Certificate or Wildcard Certificate as per previous section Importing Client SSL Certificates.

1. Click Local Traffic >Profiles > SSL > Client > Plus icon (+).

2. In the New Client SSL Profile enter the following.
   a. In the Name field, enter a unique friendly name.
   b. Ensure the default parent profile clientssl is selected.
   c. Change the configuration mode from Basic to Advanced in the drop-down menu.
   d. Click the check box next to Certificate Key Chain label.
   e. Click the Add in the Certificate Key Chain field.
3. In the Add SSL Certificate to Key Chain dialog box complete the following.
   a. In the Certificate field drop down menu, select the certificate imported in as described in the previous section.
   b. In the Key field drop down menu, select the key imported in the previous section.
   c. In the Chain field drop down menu, select the Root/Intermediary certificates imported in the previous section.
   d. In the Passphrase field, enter the encrypted password used on the Key.
   e. Leave OCSP to None.
   f. Click Add.

4. Scroll to the bottom of the Client SSL Profile and click Finished.
Creating Your Virtual Server

1. Click **Local Traffic > Virtual Servers > Virtual Servers List > Plus icon ( + ).**

2. In the New Virtual Server Profile, complete the following.
   a. In the Name field, provide a unique friendly name.
   b. In the Destination Address/Mask field, enter the IP address of your app. (IP address should equal the DNS IP Created in **Uploading the Identity Manager metadata into BIG-IP APM**.
   c. In the Service Port field, enter your app’s Service Port. – This will change the dropdown menu automatically.
   d. In the HTTP-Profile drop-down, choose the HTTP profile.
3. Continuing creating the New Virtual Server profile.
   a. In the SSL Profile (Client) box, select the client SSL profile you created in Creating a Client SSL Profile.
   b. In the Source Address Translation drop-down menu, select Auto Map.
   c. In the Access Profile drop-down menu, select the Access Profile you created in Creating the APM Access Profile.

4. Continuing creating the New Virtual Server profile.
   a. In the Default Pool drop-down menu, select the pool you created in Creating your pool.
   b. In the Default Persistence Profile drop-down menu, select the Persistence Profile you created in Creating a Persistence Profile.
   c. Click Finished.
Setting up Integration for Multiple Apps

If you have multiple KCD or header-based apps that you’d like to provide access to, you need to follow the steps beginning with **Uploading the APM Metadata into Identity Manager** for each new application. You do not, however, need to reload metadata into SAML.

For each of your KCD apps, follow these steps as described in this guide.

1. **Uploading the APM Metadata into Identity Manager**
2. **Configuring your app in Identity Manager**
3. **Setting up Kerberos Constrained Delegation (KCD) in APM**
4. **Creating the APM Access Profile**
5. **Creating your Access Policy in APM**
6. **Creating your pool in APM**

Testing and Troubleshooting

To test your app, log in to the Workspace ONE end user portal. You should see the app in the Workspace ONE portal. After clicking on the app, you should be SSO’d into the app.

1. What if I get an error while uploading metadata into Identity Manager?
   a. Make sure you copy and paste the metadata from a text editor that doesn’t add any characters or formatting to the XML.
2. What if I don’t see the app in the Workspace ONE portal?
   a. Check to make sure your test user is entitled to the app. See **Configuring your app in Identity Manager**.
3. What if I click on the app but I’m not logged in?
   a. Check your APM KCD settings. See **Setting up Kerberos Constrained Delegation (KCD) in APM**.
4. What if I get errors in the F5 APM logs /var/log/apm that indicate a problem with Kerberos authentication?
   a. Check your Kerberos SSO Service account is setup correctly
   b. Ensure your username/password is set correctly
   c. In some occasions it might be needed to manually configure the F5’s /etc/krb5.conf file to handle multiple KDC domain controllers.

Setting up a Kerberos Service Account

If you haven’t already configured Kerberos Constrained Delegation between APM and your app, you will need to create a Kerberos Service Account. Follow the steps below to create your account.

Use this documentation as listed above to create a service account for Kerberos Authentication. 