MobileIron Access Cookbook

Access with G Suite and Microsoft ADFS

September 27, 2017

Contents

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite is federated with an identity provider such as Microsoft ADFS for authentication. The user gets authentication from ADFS and obtains a SAML token for accessing applications in a cloud environment, such as G Suite.

This guide serves as step-by-step configuration manual for users using ADFS as an authentication provider with G Suite in a cloud environment.

Prerequisites

Verify that you have the following components in your environment:

- ADFS version 3.0
- **G Suite (SP) Metadata Files**
  Entity ID: google.com/a/<domain_name>
  Assertion Consumer Service URL: https://www.google.com/a/<domain_name>/acs
- **ADFS (IDP) Metadata Files**
  You must download the ADFS metadata files for ADFS (IdP)
  - Download ADFS metadata file from https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

Configuring G Suite and Microsoft ADFS with MobileIron Access

You must perform the following tasks to accomplish the configuration between G Suite and ADFS:

- Configure Access to Create a Federated Pair
- Configure the G Suite environment
- Configure the ADFS environment
- Configure G Suite to point to Access IdP Sentry
- Configure ADFS to point to Access SP Sentry
- Register Sentry to Access

Configure Access to Create a Federated Pair

You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider. It creates a federated pair.

Procedure

1. In Access, click **Profiles** > **Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. Use the default values for the other fields. Click **Save**.
3. Click **Profiles** > **Federated Pair** > **Add New Pair.**
4. Select **G Suite** option under the **Choose Service Provider**.
5. Enter the following details:
   - Name for the Federated Pair
   - Description
   - Select SP Proxy Signing Certificate
   - Select **Add Metadata**
     - **Entity ID**: google.com/a/<domain_name>
     - **Assertion Consumer Service URL**: https://www.google.com/a/<domain_name>/acs
   - (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user’s authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs.
6. Click **Next.**
7. Select **Microsoft ADFS** as the Identity Provider.
8. Upload the metadata file that you downloaded in the Prerequisites section.
9. Click **Done**.
10. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.

11. Click **Publish** to publish the profile.

Configure the G Suite environment

You must configure G Suite to use ADFS natively.

Prerequisites

Verify that you have downloaded the ADFS IdP certificate. This is required to upload to Google service provider.

Procedure

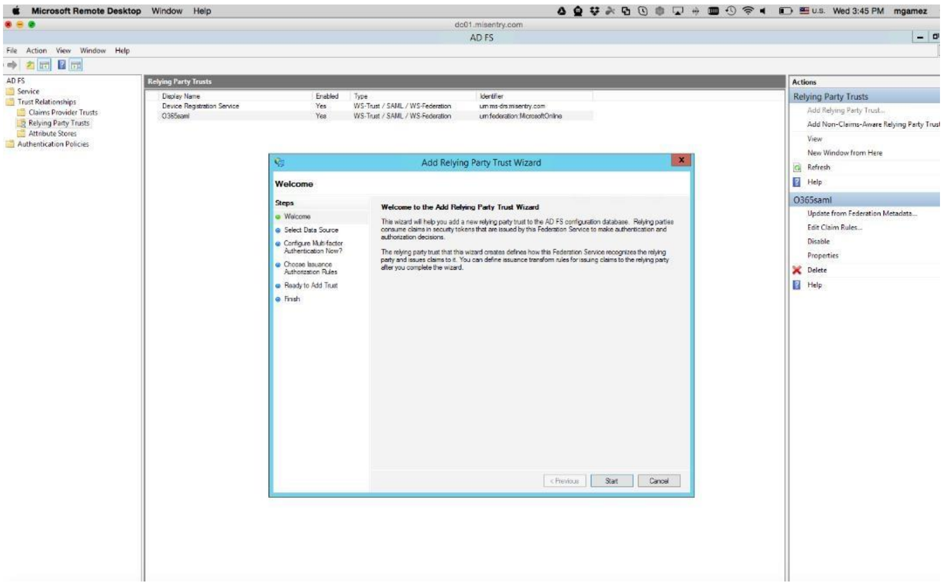
1. Login to the G Suite admin portal with admin credentials.
2. On the **Security** tab, **Setup SSO with third party identity provider**.
   - Enter the **Sign-in page URL**: https://<adfs_domain_name>/adfs/ls
   - Enter the **Sign-out page URL**: https://<adfs_domain_name>/adfs/ls
   - (Optional) Enter the **Change password URL**.
   - Upload ADFS IDP certificate file.
3. Click **Done**.

Configure the ADFS environment

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

Procedure

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Click **Start** > **Administrative tools** > **ADFS Management** > Expand **Trust Relationships.**
3. Click **Relying Party Trust.** In the right-hand pane, under the **Actions** section click **Add Relying Party Trust** and follow the prompts. Click **Start**.



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:misentry.com
O365saml	Yes	WS-Trust / SAML / WS-Federation	urn:federation:MicrosoftOnline

Add Relying Party Trust Wizard

Welcome

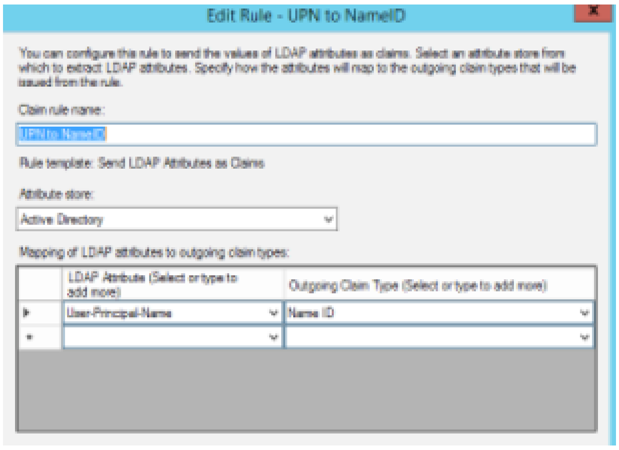
Steps
- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

4. **Select Data Source > Enter data about the relying party manually**. Click **Next**.
5. Enter the **Display name** and click **Next**.
6. Select **ADFS profile** and click **Next**.
7. Click **Browse** to configure the certificate and click **Next**.
8. Select the **Enable support for SAML 2.0 Web SSO protocol** option.
9. Enter the following URL in the **Replying party SAML 2.0 SSO service URL** and click **Next**.
   https://www.google.com/a/<domain_name>/acs
10. Enter the **Relying party trust identifier –** google.com/a/<domain_name> and Click **Add**.
11. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.
12. Select **Permit all users to access this relying party** and click **Next**.
13. At the end, select **Open Edit Claim rules dialog for relying party trust**.
14. In the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims** and click **Next.**
15. Configure **Claim rules** as follows:



Edit Rule - UPN to NameID

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
UPN to NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

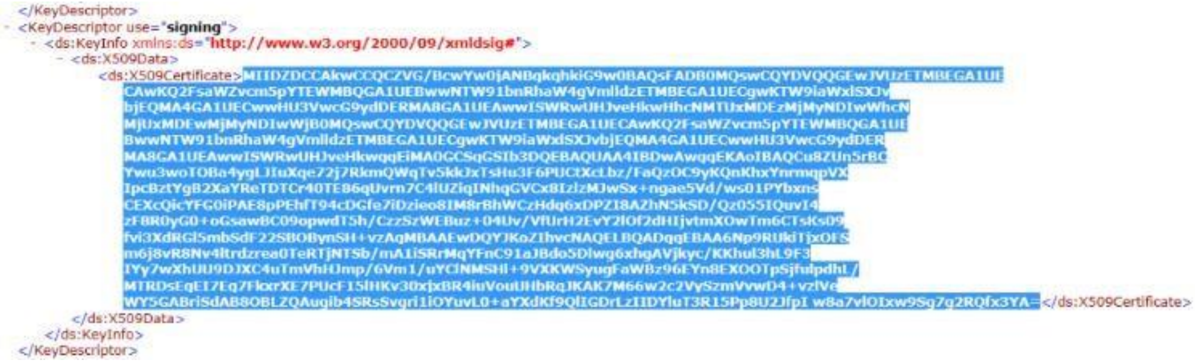
16. Add Rule and create a new rule name UPN to NameID.
17. Click **Apply** and OK.

Extracting the idp-proxy-signing-certificate

G Suite does not let you upload a metadata file. The information must be extracted from the IDP Proxy metadata file. Extract the Entity ID from the IDP Proxy metadata file.

Procedure

1. Open the SP Proxy metadata file that you downloaded when configuring Access for the federated pair.
2. Extract the certificate from the IDP Proxy metadata file and save it in the *.cer* file.



```
</KeyDescriptor>
- <KeyDescriptor use="signing">
  - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:X509Data>
        <ds:X509Certificate>MIIDZDCCAkwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzETMBEGA1UE
          CAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJv
          bjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTUxMDEzMjMyNDIwWhcN
          MjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
          BwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER
          MA8GA1UEAwwISWRwUHJveHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCu8ZUn5rBC
          Ywu3woTOBa4yglJIuXqe72j7RkmQWqTv5kkJxTsHu3F6PUCtXcLbz/FaQzOC9yKQnKhxYnrmqpVX
          IpcBztYgB2XaYReTDTCr40TE86qUvrn7C4lUZiqINhqGVCx8IzlzMJwSx+ngae5Vd/ws01PYbxns
          CEXcQicYFG0iPAE8pPEhfT94cDGfe7iDzieo8IM8rBhWCzHdq6xDPZI8AZhN5kSD/Qz055IQuvI4
          zFBR0yG0+oGsawBC09opwdT5h/CzzSzWEBuz+04Uv/VfUrH2EvY2lOf2dHIjvtmXOwTm6CTsKs09
          fvi3XdRGl5mbSdF22SBOBynSH+vzAqMBAAEwDQYJKoZIhvcNAQELBQADggEBAA6Np9RUkiTjxOFS
          m6j8vR8Nv4ltrdzrea0TeRTjNTSb/mA1iSRrMqYFnC91aJBdo5Dlwg6xhgAVjkyc/KKhul3hL9F3
          IYy7wXhUU9DJXC4uTmVhHJmp/6Vm1/uYClNMSHl+9VXKWSyugFaWBz96EYn8EXOOTpSjfulpdhL/
          MTRDsEqEI7Eq7FlcxrXE7PUcF15lHKv30xfxBR4iuVouUHbRqJKAK7M66w2c2VySzmVvwD4+vzlVe
          WY5GABriSdAB8OBLZQAugib4SRsSvgri1iOYuvL0+aYXdKf9QlIGDrLzIIDYluT3R15Pp8U2JfpI w8a7vlOIxw9Sg7q2RQfx3YA=</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </KeyDescriptor>
```

Configure G Suite to point to Access IdP Sentry

1. Open G Suite-IdP-Proxy-Metadata.xml file.
2. Copy the Entity ID URL.
3. Open the **G Suite** admin portal > **Security**.
4. Enter the Sign-In page URL.

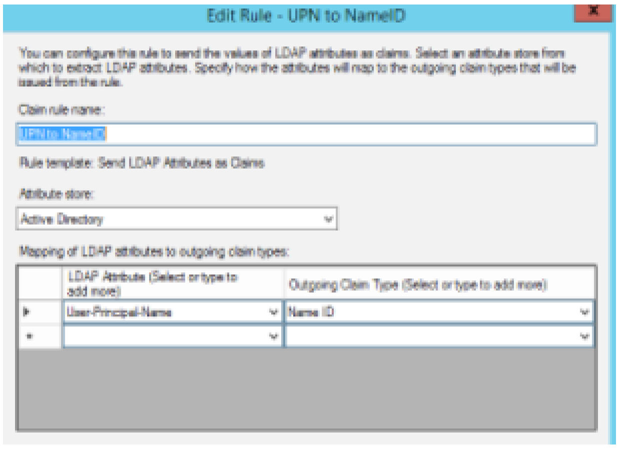
Note: The Sign-Out page URL can point to ADFS and not Sentry.

5. (Optional) Enter the Change Password URL.
6. Upload the IdP-proxy signing certificate that you saved.

Configure ADFS to point to Access SP Sentry

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Click **Start** > **Administrative tools** > **ADFS Management** > Expand **Trust Relationships.**
3. Click **Relying Party Trust.** In the right-hand pane, under the **Actions** section click **Add Relying Party Trust** and follow the prompts. Click **Start**.
4. Select **Import data about the relying party from a file** and click **Next**.
5. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.
6. Select **Permit all users to access this relying party** and click **Next**.
7. At the end, select **Open Edit Claim rules dialog for relying party trust**.

8. In the **Claim Rule Template** drop-down, select **Send LDAP Attributes as Claims** and click **Next.**
9. Configure **Claim rules** as follows:



Edit Rule - UPN to NameID

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

UPN to NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

10. Click **Apply** > **OK**.

Register Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Click **OK**.
6. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   (config)# accs config-fetch update

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Task Result

Single-sign-on service is now configured using SAML with G Suite as the service provider and Microsoft ADFS as the identity provider. This configuration lets you fetch the latest configuration from Access.

You must verify SSO access to G Suite using a browser.

- Open a browser and go to docs.google.com or drive.google.com. Log in with a user that exists in both the Active Directory and Google Domain. The browser must be redirected to the ADFS login page.
- Enter the user credentials. The browser must be redirected to G Suite.