



MobileIron Access Cookbook

Access with GoogleApps and Microsoft ADFS

June 20, 2017



Contents

Overview	3
Prerequisites.....	3
Configuring GoogleApps and Microsoft ADFS with MobileIron Access	4
Configure Access to Create a Federated Pair	4
Configure the GoogleApps environment	5
Configure the ADFS environment	5
Extracting the idp-proxy-signing-certificate.....	6
Configure GoogleApps to point to Access IdP Sentry	7
Configure ADFS to point to Access SP Sentry	7
Register Sentry to Access	8



Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as GoogleApps 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 GoogleApps.

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

Prerequisites

Verify that you have the following components in your environment:

- ADFS version 3.0
- **GoogleApps (SP) Metadata Files**
Entity ID: google.com/a/<domain_name>
Access 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 GoogleApps and Microsoft ADFS with MobileIron Access

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

- [Configure Access to Create a Federated Pair](#)
- [Configure the GoogleApps environment](#)
- [Configure the ADFS environment](#)
- [Configure GoogleApps 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>](https://www.google.com/a/<domain_name>)
 - **Access 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/curent/accs>.
6. Click **Next**.
7. Select **Microsoft ADFS** as the Identity Provider.
8. Upload the **IdP Proxy certificate** and the **IdP metadata** file that you downloaded.
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 GoogleApps environment](#)

You must configure GoogleApps to use ADFS natively.

Prerequisites

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

Procedure

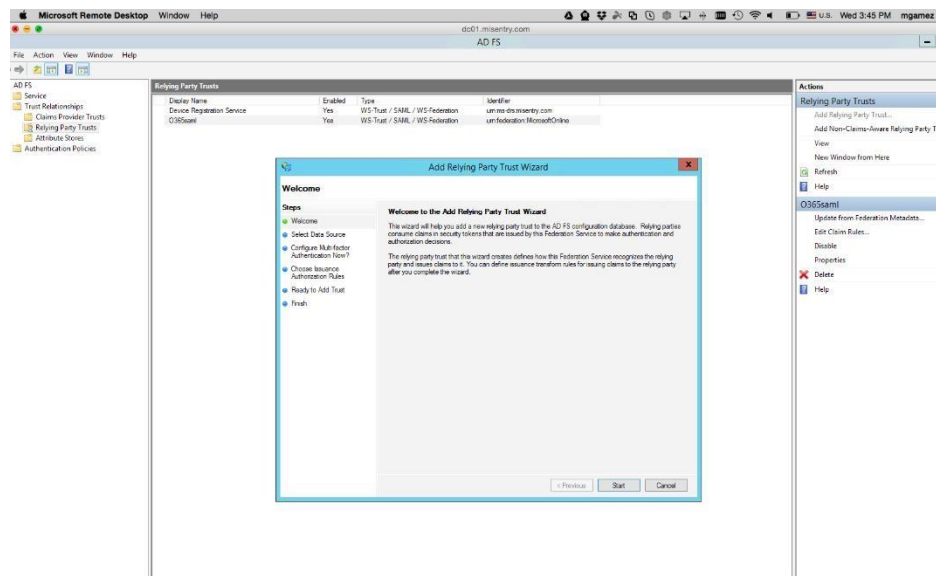
1. Login to the GoogleApps admin portal with admin credentials.
2. On the **Security** tab, **Setup SSO with third party identity provider**.
 - Enter the **Sign-in page URL**: https://<adfs_domain_name>/adfs/ls
 - Enter the **Sign-out page URL**: https://<adfs_domain_name>/adfs/ls
 - (Optional) Enter 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.

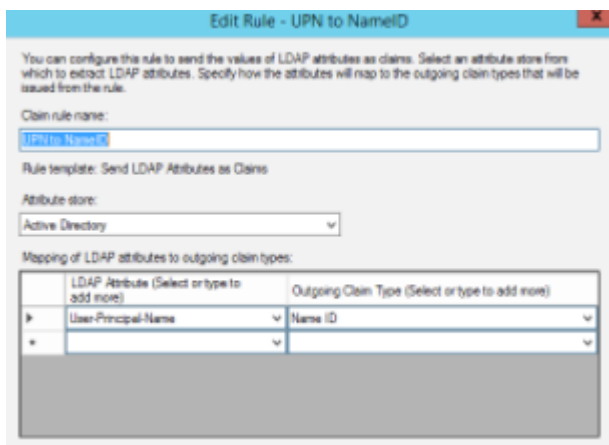
Procedure

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**.





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:



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

Extracting the idp-proxy-signing-certificate

GoogleApps 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. Login to GoogleApps portal with admin credentials.
2. Open the SP Proxy metadata file that you downloaded when configuring Access for the federated pair.
3. 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>MTIDZDCCAkWCCQCZVG/BcwYw0jANBqkghkiG9w0BAQSFADB0MQswCQYDVQOGEwJWUzETMBEGA1UE
      CAwKQ2FsaWZyb3VweWMBQGA1UEBwwNTW91bnRhaW4gVmllZzETMBEGA1UECgwKTW9laWxscQV
      bjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTEzMDZlMjMyNDIwWHcN
      MjUxMDEwMTM5NDIwWjB0MQswCQYDVQOGEwJWUzETMBEGA1UECgwKQ2FsaWZyb3VweWMBEGA1UE
      BwwNTW91bnRhaW4gVmllZzETMBEGA1UECgwKTW9laWxscQVbjEQMA4GA1UECwwHU3VwcG9ydDER
      MA8GA1UEAwwISWRwUHJveHkwHhcNMTEzMDZlMjMyNDIwWHcNMTUxMDIwMDE0MTA0C3QCS1b3DQEB
      AQAUA4IBDWAwqqEKAA0IBAQCu8ZUu5rBC
      Yww3wo1OBA4yglJiuXqeZj7RkmQWqTvsKkzTsh3F6PUICXclbz/FaQzOC9yKqnKbxYnmqpVX
      IpcBzTgB2XaYReTDTCr40TE86qUvm7C4IUziqINhqCVCxBLz:MDwSx+ngae5Vd/ws01PYbxs:
      CEXcQkYFG0IPAESpPEHtT94cDGlE7iDzie08IM8rBhWczHdq6xDPZ18AZhNSKSD/Qz0551QuvI4
      zf8R0yGD+oGawBC09opwdTSh/CzzSzWELBuz+04Uv/VUlrH2EvY2I0f2dHlJvtmX0wIm6CTskS09
      Fvi3XRGl5mbSdf22SB0hynSH+vzAgMBAALwDQYJKoZIhvcNAQELBQADggEBAAG6Np9RUhdiTxOI5
      m6j8vR8Nv4ltrzrea0tErtjNT5b/mALISRrMqYFnC91aJBdeSDlwq6xdgAVjkyC/KKhuL3ht9F3
      IY7zwxhUUDJXC4uTmVhiDmp/6VmI/uyCNMSHI+9VXXWSyugFaWBz96IYn8EXOOIpsjhapdhl/
      MTRDStqE1ZEq7FkcrXE7PIUCF1SHKv3DxpBR4luVoutlHbRqIKAK7M66w2c2YySzmVvwD4+yzIVc
      WY5GABrISdAB8OBLZQAuqib4SRsSvqr110YuvL0+aYxdkf9QIGDrLz11DYU13R15fp8U2Jfp1_wBa7vI0bW9SgZg2R0fX3YA=</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</KeyDescriptor>

```

[Configure GoogleApps to point to Access IdP Sentry](#)

1. Open GoogleApps-IdP-Proxy-Metadata.xml file.
2. Copy the Entity ID URL.
3. Open the **GoogleApps** 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:



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 GoogleApps 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 GoogleApps using a browser.

- Open a browser and go to docs.google.com or drive.google.com. Login with a user that exists in both the Active Directory and Google Domain. The browser must be redirected to ADFS log in page.
- Enter the user credentials. The browser must be redirected to GoogleApps and have access.



Copyright © 2016 - 2017 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.