Overview

System Requirements

Installation & Setup

Overview

1. Activating SSO Connect from the Admin Console
   - Show Node Structure
   - Create SSO Node
   - Add SSO Connection
   - Enterprise Domain
   - New User Provisioning

2. Install Keeper SSO Connect v11
   - Pre-Installation
   - Installation
   - SSO Connect SSL Key and Certificate
   - Status: Stopped
   - IdP Metadata
   - Identity Provider Attribute Mappings
   - Restarting the Keeper SSO Connect Service

3. Identity Provider Setup
   - Microsoft AD FS
     - Obtain Federation Metadata XML
     - Import Federation Metadata
     - Export Keeper SSO Connect Metadata
     - Finish AD FS Configuration
     - Create Relying Trust Party
     - Import Keeper Metadata
     - Create Claim Issuance Policy Rules
     - ADFS Troubleshooting
   - Azure
     - Create Enterprise Application
     - Configure the Application
     - Generate SAML Signing Certificate
     - Obtain Metadata XML
     - Import the Azure Metadata
     - User Provisioning
   - Okta
   - G Suite
This guide provides setup instructions for Keeper SSO Connect.

**Overview**

Keeper SSO Connect is a SAML 2.0 application which leverages Keeper’s zero-knowledge security architecture to securely and seamlessly authenticate users into their Keeper Vault and dynamically provision users to the platform. Keeper SSO Connect works with popular SSO IdP platforms such as G Suite, Microsoft AD FS / Azure, F5 BIG-IP APM, Okta, Centrify, OneLogin, Ping Identity and CAS to provide businesses the utmost in authentication flexibility.

Keeper SSO Connect is a software application that is installed on the enterprise’s on-premise, private or cloud servers. Users encryption keys are generated dynamically by Keeper SSO Connect, encrypted and stored locally on the installed server, providing the customer with full control over the encryption keys that are used to encrypt and decrypt their digital vaults.

The Keeper SSO Connect service application can be installed on a private on-premise or cloud-based server. Windows, Mac OS and Linux operating systems are supported.

On Microsoft Windows environments, the Keeper SSO Connect application runs as a standard Windows service. This ensures the service won’t exit when anyone logs off the PC and will automatically start up upon reboot. It can also be configured for High Availability (HA). In order to ensure the service is always active, Keeper SSO connect can be installed on multiple servers that sit behind a load balancer.

**System Requirements**

The Keeper SSO Connect is a lightweight service that can be installed on a private on-premise or cloud-based server. It is not resources intensive.

Supported platforms: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Red Hat Linux RHEL 6.8 or above, Centos 7 or above, Mac OS X Server. JRE 1.8 is required.

**Installation & Setup**

**Overview**

The basic steps for setting up Keeper SSO Connect are listed in the steps below. Detailed instructions are annotated further in this document.
1. Enable SSO Connect from the Keeper Admin Console
2. Install Keeper SSO Connect on your server (supports Windows, Mac, Unix/Linux)
3. Configure Keeper as a SAML 2.0 service provider on your existing Identity Provider

1. **Activating SSO Connect from the Admin Console**

Visit the Keeper Admin Console at [https://keepersecurity.com/console](https://keepersecurity.com/console) and login as the Keeper administrator.

**Show Node Structure**

SSO integration is applied to specific nodes (e.g. organizational units) within your Admin Console outside of the root node. To display the node structure, click on "Advanced Configuration" then "Show Node Structure".
Advanced Configuration

Email Invitations

Show Node Structure

Add Company Logo
* Appears on Web Vault and Desktop App header

Edit

Edit
Create SSO Node

Click on the "+" button to create a new node which will host the Keeper SSO Connect integration for AD FS. The node can be anywhere in your organizational structure. In the below example, the node is called "SSO - AD FS" and added beneath the root node.
Click "Create" then select the node.

Each SSO Connection can be associated with a node. Therefore, your organization is able to create multiple SSO connections assigned to different nodes.

**Add SSO Connection**

Click on the "Bridge/SSO" tab of the node.
Next, click on the "+ SSO Connection" link to create a new connection.

**SSO Connection**

Manage SSO Connect for Acme Corp

SSO Connect URL
190.123.123.445/880/sso-connect

Node
Acme Corp

Enterprise Domain
e.g. mycompanysso

New User Provisioning
- Dynamically provision users upon successful login to SSO
- Invite manually or use Keeper Bridge

[Save]
There are 2 parameters to configure. The "Enterprise Domain" and the "New User Provisioning" option.

**Enterprise Domain**

Every SSO Connection must be uniquely identified through the use of a supplied "Enterprise Domain" alias. This alias should be named something that is easy for your users to remember because they may need to type the name into their mobile and apps (iOS, Android, Mac, Windows) upon first logging into a new device.

**New User Provisioning**

Users can be dynamically provisioned to your Keeper Business account upon first successful authentication on SSO. For the best user experience, we recommend selecting this option. You can also manually invite users through the Admin Console "Users" tab, or invite users via the Keeper Bridge.

** The SSO Connect URL will update after the Keeper SSO Connect service is registered on the application.

After configuring the Enterprise Domain and New User Provisioning click save.

At this point, you can now configure the Keeper SSO Connect application.

2. **Install Keeper SSO Connect v11**

**Pre-Installation**

1. Download the Keeper SSO Connect application from the admin console and stage the executable on the server.
2. Install Java 8 if not currently installed.
   
   **NOTE:** Java 9 is not compatible.

3. Reboot the server

**Installation**

1. Extract the Keeper SSO Connect app.

2. Run KeeperSSOConnect-11.0.0 as administrator.
Ready to Install
Setup is now ready to begin installing Keeper SSO Connect on your computer.

DO NOT Uninstall the old SSO Connect.
Click Install to continue with the installation.
3. Upon successful completion of the new installation the app will launch a web browser. (We recommend using Google Chrome to perform the initial setup). If the configuration web page doesn’t launch you can launch it with the new SSO Connect Icon on the desktop.

If you receive an error connecting to the Keeper SSO Connect service, you need to reboot the server. Also, you need to ensure that your web browser is able to connect to keepersecurity.com over port 443. Keeper SSO Connect does not support the use of proxy servers or firewalls that perform SSL packet inspection.

4. Log into the SSO Connect Web UI with a Keeper Administrator account.
NOTE: This account should not be configured for Single Sign-On.
Enter Two Factor Authentication code if prompted

Select the SSO Connection (Enterprise Domain)

Once you successfully authenticate Keeper SSO Connect to your admin Console you will see the status tab:
Click on the Configuration link to begin the setup.
Enter the Hostname or IP Address. This address is what the Keeper client applications navigate to in order to initiate the SSO authentication process. If installing Keeper SSO Connect in an HA configuration, this is the address that points to the load balancer. This address can be either an IP or a hostname.

Configure the Private IP Address. This is the physical IP address of the NIC on the server. If a hostname is not used and if there is only one address associated with the server this entry will be the same as the Hostname or IP Address field.

In the example above, the IP address is 52.3.108.1 is the virtual or external address that gets routed to the local address 10.10.10.124. The Keeper SSO Connect service binds to the Private IP address.

Note: The IP/Hostname must be accessible by users who will be accessing Keeper. You may need to update your firewall to allow access over this IP and port.

SSO Connect SSL Key and Certificate

In order for the Keeper SSO Connect service to start an SSL Certificate is required. A self signed certificate can be generated. However, before deploying to production, it is recommended that a proper SSL Certificate from your certificate authority be generated and uploaded to this section. Self-signed certificates will generate security errors for your users.
Select your specific IDP. If your IDP is not in the pull down select “Default”.

Status: Stopped
Reasons your status is listed as Stopped:

1. Your SSL Certificate is missing or incorrect.
a. The hostname in the SSL certificate doesn't match the hostname in SSO Connect. **A wildcard SSL cert can be used or one created for the specific hostname. (i.e. if your hostname is Keeper.DOMAIN.com your cert should be set up for *.DOMAIN.com.

b. By default the “Use Certificate to Decrypt and Sign SAML Response/Request” should be selected.

** See Appendix A on creating a self-signed SSL cert if you need to create a self signed SSL certificate for testing or troubleshooting your SSL certificate.

IdP Metadata

1. Select your IdP Provider. If your provider is not listed select “Default”

2. The next step is to upload the IdP metadata file. This file can be downloaded from your IdP.
Identity Provider Attribute Mappings

Attribute Mappings do not require any changes. Just click Save.

Identity Provider Attribute Mappings

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Email or Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Last</td>
<td>Email</td>
</tr>
</tbody>
</table>

Restarting the Keeper SSO Connect Service

The Keeper SSO Connect runs as a service. Closing out the web interface does not stop the service. The service can be stopped and started from the Service MMC in windows..
3. Identity Provider Setup

Keeper SSO Connect can be integrated with any SAML 2.0 compliant IdP. Listed below are several of the more popular IdP’s along with specific setup instructions.

1. Microsoft ADFS
2. Azure
3. Okta
4. G Suite
5. OneLogin
6. Ping Identity
7. Centrify
8. F5
9. JumpCloud
**Microsoft AD FS**

**Obtain Federation Metadata XML**

Inside the AD FS Management application, locate the Federation Metadata xml file via URL Path "/FederationMetadata/2007-06/FederationMetadata.xml" as seen below:
Import Federation Metadata

Import the FederationMetadata.xml file into Keeper SSO Connect's configuration screen by dragging and dropping the file:

Click "Save" to save the configuration.
Export Keeper SSO Connect Metadata

Click the “Export Metadata” link on Keeper SSO Connect and copy the sso_connect.xml file to your IdP.
Finish AD FS Configuration

Create Relying Trust Party

Create Keeper SSO Connect as a Relying Trust Party:
Import Keeper Metadata

Import the Keeper Metadata that was exported previously from Keeper SSO Connect by completing the Relying Party Trust Wizard as seen in the steps below:

A.

B.
Select Data Source

Steps
- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

- Import data about the relying party published online or on a local network
  Use this option to import the necessary data and certificates from a relying party organization's federation metadata online or on a local network.
  Federation metadata address (host name or URL):
  Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file
  Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard validates the source of the file.
  Federation metadata file location:
  \Temp\KeeperSsoMetadata.xml
- Enter data about the relying party manually
  Use this option to manually input the necessary data about this relying party organization.

Choose Access Control Policy

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit everyone</td>
<td>Grant access to everyone</td>
</tr>
<tr>
<td>Permit everyone and require MFA</td>
<td>Grant access to everyone and require MFA</td>
</tr>
<tr>
<td>Permit everyone and require MFA for specific group</td>
<td>Grant access to everyone and require MFA for specific group</td>
</tr>
<tr>
<td>Permit everyone and require MFA from extranet access</td>
<td>Grant access to everyone and require MFA from extranet access</td>
</tr>
<tr>
<td>Permit everyone and require MFA from unauthenticated devices</td>
<td>Grant access to everyone and require MFA from unauthenticated devices</td>
</tr>
<tr>
<td>Permit everyone and require MFA, allow automatic device registration</td>
<td>Grant access to everyone and require MFA, allow automatic device registration</td>
</tr>
<tr>
<td>Permit everyone for intranet access</td>
<td>Grant access to intranet access</td>
</tr>
<tr>
<td>Permit everyone for extranet access</td>
<td>Grant access to extranet access</td>
</tr>
<tr>
<td>Permit everyone for unauthenticated devices</td>
<td>Grant access to unauthenticated devices</td>
</tr>
<tr>
<td>Permit everyone for unauthenticated devices, allow automatic device registration</td>
<td>Grant access to unauthenticated devices, allow automatic device registration</td>
</tr>
<tr>
<td>Permit everyone for devices in a specific group</td>
<td>Grant access to devices in a specific group</td>
</tr>
</tbody>
</table>

Policy
- Permit everyone
E. Add Relying Party Trust Wizard

Ready to Add Trust

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring | Identifiers | Encryption | Signature | Accepted Claims | Organization | Endpoints | Notes
--- | --- | --- | --- | --- | --- | --- | ---

Specify the endpoints to use for SAML and WS-Federation/Passive protocols.

<table>
<thead>
<tr>
<th>URL</th>
<th>Index</th>
<th>Binding</th>
<th>Default</th>
<th>Re</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Assertion Consumer Endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://acw10e.keeperqa.local:8443/sso-connect/saml/sso">https://acw10e.keeperqa.local:8443/sso-connect/saml/sso</a></td>
<td>0</td>
<td>POST</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SAML Logout Endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://acw10e.keeperqa.local:8443/sso-connect/saml/slo">https://acw10e.keeperqa.local:8443/sso-connect/saml/slo</a></td>
<td>Redirect</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

F. Add Relying Party Trust Wizard

Finish

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust was successfully added.

- Configure claims issuance policy for this application
G. Create Claim Issuance Policy Rules

To map attributes between AD FS and Keeper, you need to create a Claim Issuance Policy with "Send LDAP Attributes as Claims" and map the LDAP attributes to Keeper Connect attributes.

A.

B.
C.

Important: Ensure that 3 attributes ("First", "Last" and "Email") are configured with the exact spelling as seen above.

D.
E.

F. For Logout support we need to add two more Claim Issuance Policy rules:

G. Send Claims using a Custom Rule
The diagram shows the setup of AD FS (Active Directory Federation Services) for Keeper SSO Connect. It includes selecting rule templates for claim rules, such as sending claims using a custom rule. The context suggests managing trust relationships and relying party trusts within the federation services framework.
H. Create Opaque Persistent ID

To copy the syntax to add in the claims rule click on the link to the plain text file and paste the contents into the custom rule:

https://keepersecurity.com/sso_connect/Create_Opaque_Persistent_ID
I. Transform an Incoming Claim

![Image of AD FS software interface showing the process of adding a transform claim rule]

- **Select Rule Template**
  - **Steps**
    - Choose Rule Type
    - Configure Claim Rule
  - **Claim rule template:**
    - **Transform an Incoming Claim**
  - **Claim rule template description:**
    
    Using the Transform an Incoming Claim rule template, you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.
J. Create Persistent Name Identifier

Incoming claim type:  http://mycompany/internal/sessionid
Outgoing claim type:  Name ID
Outgoing name ID format:  Transient Identifier
ADFS Troubleshooting

If after setting up Keeper SSO Connect customer gets "SSO is not configured (undefined)" a possible root cause is missing or incorrect CRL configuration.

A simple fix/workaround is to disable all Certificate Revocation Check.

Possible Root Causes

Time skew

Ensure that Keeper Connect and the IdP have the same identical system time (within <1s).

Set ntp sync

PS C:\Windows\system32> w32tm /config /syncfromflags:manual /manualpeerlist:0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org,3.pool.ntp.org,0x8 /reliable:yes /update
Certificate Validation Failure

1. Verify the settings. Run a PowerShell as Administrator and look at ADFSRelyingPartyTrust:
   PS C:\Windows\system32> Get-ADFSRelyingPartyTrust

   You should see something like this:

   AllowedAuthenticationClassReferences : {}
   EncryptionCertificateRevocationCheck : None
   PublishedThroughProxy : False
   SigningCertificateRevocationCheck : None
   WSFedEndpoint :

2. Run the following two commands:
   PS C:\Windows\system32> Set-ADFSRelyingPartyTrust -TargetIdentifier https://DOMAIN:8443/sso-connect -EncryptionCertificateRevocationCheck None
   PS C:\Windows\system32> Set-ADFSRelyingPartyTrust -TargetIdentifier https://DOMAIN:8443/sso-connect -SigningCertificateRevocationCheck None

   Your Keeper SSO Connect setup is now complete!
Create Enterprise Application

From the Azure Cloud portal (https://portal.azure.com), click on “Enterprise Applications” on the left menu section. (If Enterprise Applications is not shown, admin can added to Favorites list).

(If the Enterprise Applications is not shown in the menu, admin can added to Favorites list under All services).

Next, Click +New application icon.

Type “keeper” in the search, select the application.
The app will open in the right window pane. Scroll down and select Add.
Configure the Application

Next, select the "Configure single sign-on" screen.

Configure single sign-on (required)

Configure your instance of Keeper Password Manager & Digital Vault to use Azure AD as its identity provider.

Select "SAML-based Sign-on": 
Under the "Domain and URLs" section, type in the "Sign on URL", "Identifier", and "Reply URL". These are the specific URL's to the SSO Connect server.

Show advanced URL settings

Identifier (Entity ID)  
https://51.143.157.142:8443/sso-connect/ 

Patterns: https://*.recovery.keeperapp.com:8443/sso-connect

Keeper Password Manager & Digital Vault Domain and URLs
Input the URLs and other details about your Keeper Password Manager & Digital Vault tenant into Azure AD.

* Sign on URL  
https://51.143.157.142:8443/sso-connect/saml/login

* Identifier  
https://51.143.157.142:8443/sso-connect/

* Reply URL  
https://51.143.157.142:8443/sso-connect/saml/sso
Example:
Sign on URL = https://keeper.domain.com:8443/sso-connect/saml/login
Identifier = https://keeper.domain.com:8443/sso-connect
Reply URL = https://keeper.domain.com:8443/sso-connect/saml/sso

Under the "User Attributes" section, select the “View and edit all other user attributes” to add needed attributes.

First, delete the 4 predefined SAML Tokens Attributes: givenname, surname, emailaddress, and name.

Next, click on the add button to add the following required attributes: First, Last and Email.

NOTE: It is important that the spelling and capitalization of the attribute is exactly as it appears (First, Last, Email) because these fields are case sensitive.

**Ensure the Namespace is left blank**
Note: If the UPN is not the same as the user's actual email address, select user.mail as the value for the Email attribute.

Generate SAML Signing Certificate

Select "Create new certificate".

Enter the expiration date and Save
After creating the certificate select Make new certificate active.

Obtain Metadata XML

To complete the integration between Microsoft Azure and Keeper SSO Connect, you must retrieve the Metadata XML file and import this file into the Keeper SSO Connect screen.

Click on the "Metadata XML" link:

This will download a file “Keeper Password Manager & Digital Vault.xml to your computer. This file will need to be transferred to the server running Keeper SSO Connect for the next step.
Import the Azure Metadata

Import the file saved in the previous step into Keeper SSO Connect’s configuration screen by dragging and dropping the file into the "SAML Metadata" section.

![Identity Provider](image)

**NOTE:** Don't forget to select Azure as the IDP Type.

User Provisioning

If only specific users or groups will be assigned to Keeper Password Manager the following setting will need to be changed. On the Keeper Password Manager & Digital Vault app, select “Properties”.
Next, change the “User assignment required” to yes and then save. This will ensure only the user and groups assigned to the application will be able to use it.
Lastly, on the "Users and groups" section select the users and/or groups that are to be provisioned to the Keeper application.

Your Keeper SSO Connect setup is now complete!
**Okta**

Login to the Admin section of the Okta portal.

Click on Admin

Click the "Applications" tab and select “Applications”.
Next, click the “Add Application” button.

In the application search field, type “Keeper Password”, and then select the “Add” button for the Keeper Password Manager and Digital Vault Application.

On the General Settings page, Enter the Entity ID from your Keeper SSO Connect server: (i.e. https://DOMAIN:8443/sso-connect where “DOMAIN is the server name or IP address of your Keeper SSO Connect application ). Then click the “Done” button.
Add users or groups on the “Assignments” page. (This step can be skipped and returned to after setup is complete.)
Next, click the “Sign On” tab.

Click the Edit button.

Next, check the “Enable Single Logout” setting and choose a certificate to upload.
* this can be the .pem file created in Appendix A

After clicking upload the name of the pem file along with the CN is displayed.
After the file is successfully uploaded, click save at the bottom of the Sign On page.

The setting will be saved.
Scroll down to the SAML 2.0 configuration section, download the "Identity Provider metadata" file. Rename the file to metadata.xml. This will be used in Step 8.

The Okta “View Setup Instructions link” provides additional setup instructions many of which are also found within this document.

Upload metadata.xml file into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen:

Click "Save" and your setup is complete.
G Suite

To access G Suite Admin Console, login to https://gsuite.google.com.

Then click on Sign in

A. Click on the "Apps" section

B. Click on "SAML apps"
C. Click on the + button

Then select custom app:

D. On the Google IdP Information screen, download the IDP metadata and save it to your computer for later.
E. Click "NEXT".
F. On the "Basic information" screen, type in the Application Name, Description and upload the Keeper logo file `keeper256x256.png`. Then click "NEXT".
G. On the Service Provider Details screen, you need to enter the "ACS URL" and "Entity ID". These values come from the Keeper SSO Connect configuration screen. Copy and Paste the information from SSO Connect to the Service Provider screen on G Suite:

Input the ACS URL and Entity ID from Keeper SSO Connect to G Suite screen:

Example:
Entity ID = https://keeper.domain.com:8443/sso-connect
ACS URL = https://keeper.domain.com:8443/sso-connect/saml/sso
H. Click "NEXT" then proceed to the Attribute Mapping screen. You need to click on "ADD NEW MAPPING" and create 3 fields: **First**, **Last** and **Email**. Map those fields **exactly** as it appears below. The spelling needs to be exact:

I. Click on "FINISH" and your G Suite setup is complete. You will be informed that you still need to import the IDP data on Keeper SSO Connect.
To enable Keeper SSO Connect, for your users, click the "more" button and enable:

- ON for everyone
- OFF
- ON for some organizations

Import G Suite Metadata

On the Keeper SSO Connect application configuration screen, drag-and-drop the metadata file saved in the previous step D above into the "SAML Metadata" section of Keeper SSO Connect:
Click on "Save" and verify that all of the parameters match your G Suite SAML connection screens.

Your Keeper SSO Connect setup is now complete!
**OneLogin**

Login to the OneLogin portal.

![OneLogin Login](image)

From the onelogin menu select “Apps” then “Add Apps”.

![OneLogin Apps Menu](image)

In the Search field, do a search for “Keeper” and select it from the search result.
On the “Add Keeper Password Manager” Click save

The next step is to download the SAML Metadata from OneLogin. Click the down arrow on the “MORE ACTIONS” button and select “SAML Metadata”.

The “onelogin_metadata_#####.xml” file will download to the browser. Copy this file to the Keeper SSO Connect server to be used in Step 8.

Next, select the Configuration tab.

On the OneLogin Configuration tab, fill in Domain Address and port of the Keeper SSO Connect server in the Application Details “Domain” field.
Click Save in the upper right hand corner to finish the setup.

Upload the Identity Provider SAML Metadata file into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen:

Click "Save" and your setup is complete.
Ping Identity
Login to the Ping Identity portal.

From the Ping Identity menu select “Applications”.

Then click “Add Application” and select “New SAML Application"
On the Application Details page, add the following data:

Application Name:  **Keeper Password Manager**  
Application Detail:  **Password Manager and Digital Vault**  
Category:  **Compliance** (or other)

Graphic:  Upload the Keeper Graphic  
[http://s3.amazonaws.com/keeper-email-images/common/keeper256x256.png](http://s3.amazonaws.com/keeper-email-images/common/keeper256x256.png)

Then click “Continue to Next Step”.
The next step is to download the SAML Metadata from Ping Identity. Click the Download link next to “SAML Metadata”.

SAML Metadata  Download

The “saml2-metadata-idp.xml” file will download to the browser. Copy this file to the Keeper SSO Connect server and upload it into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen: Click "Save".
The remaining step on the Keeper SSO Connect Server is to download the KeeperSsoMetadata.xml file and upload it to the Ping Application configuration.

Click “Export Metadata” on the Keeper SSO Connect.

Back on the Ping Identity application configuration, click the “Select File” button and choose the file “KeeperSsoMetadata.xml”.

Step 3 is the map the attributes. Click the “Add new attribute” button.

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Identity Bridge Attribute or Literal Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new attribute</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In attribute 1, type “First” in the Application Attribute column, select “First Name” in the Identity Bridge Attribute or Literal Value column, and check the Required button. Click the “Add new attribute” button.

In attribute 2, type “Last” in the Application Attribute column, select “Last Name” in the Identity Bridge Attribute or Literal Value column, and check the Required button. Click the “Add new attribute” button.

In attribute 3, type “Email” in the Application Attribute column, select “Email” in the Identity Bridge Attribute or Literal Value column, and check the Required button.

** Application Attributes, First, Last, Email must begin with a capital letter.
Click the “Save & Publish” button.

Review the setup and and then click the “Finish” button.

The Keeper Application should be added and enabled.

Setup is complete.
Centrify
Login to the Centrify Admin portal via the cloud login.

Switch to the Admin Portal from the pull down menu.

Close the Quick Start Wizard if it pops up. Select “Apps” from the menu then “Add Web Apps”.
On the Add Web Apps window, select the Custom tab and then scroll down and choose “Add” for SAML.

Select “Yes” to “Do you want to add this application?”. 
Close the Add Web Apps Window.

The next step is to upload Keeper’s SSO Metadata to Centrify.

In Keeper SSO connect, export the Keeper SSO Connect metadata using the "Export Metadata" link and save this file for the next step.
In the SAML Application Settings section in Centrify, select “Upload SP Metadata”.

Select “Upload SP Metadata from a file” and browse for the KeeperSSOMetadata.xml file. Select Ok.
Download the Identity Provider SAML Metadata. This will be uploaded to Keeper SSO Connect in section 8.

On the Description section enter “Keeper SSO Connect” in the Application Name field and select “Security” in the Category field.
Download the Keeper logo.

Click “Select Logo” and upload the Keeper logo (keeper60x60.png).

On the User Access section select the roles that can access the Keeper App:
Under the Account Mapping section, select Use the following...and input “mail”.

On the Advanced section, append the script to include the following lines of code:

```javascript
setAttribute("Email", LoginUser.Get("mail"));
setAttribute("First", LoginUser.FirstName);
setAttribute("Last", LoginUser.LastName);
```
**Note**
The above script reads the display name from the User Account section. The FirstName attribute is parsed from the first string of DisplayName and the LastName attribute is parsed from the second string of DisplayName.

Click "Save" to finish the setup.
Upload the Identity Provider SAML Metadata file into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen:

Click "Save" and your setup is complete.

F5
On the F5 BIG-IP APM, configure a new SAML IdP service for your Keeper platform:

Go to Access Policy -> SAML -> BIG-IP as IdP -> Local IdP Services
Navigate to: **Access Policy > SAML : BIG-IP as IdP - Local IdP Services.** Select your applicable IdP connection point and "Export Metadata".
Upload this file to the server where Keeper SSO Connect is installed. We'll need it in the next step.

Import the Metadata file extracted from F5 BIG-IP APM into SSO Connect.
Click "Save" to save the configuration and verify all settings look correct.

Export the Keeper SSO Connect Metadata file for configuration of F5 BIG-IP APM from the Export Metadata link.

Your Keeper SSO Connect setup is now complete!
JumpCloud

JumpCloud also provides instructions for setting up Single Sign On (SSO) with Keeper Security.

As listed in the JumpCloud SSO Prerequisites a public certificate and a private key pair are required. Instructions can be found here.

Log into the JumpCloud Administrator console.

Click the "Applications" tab on the side menu.
Next, click the “+” icon in the upper left corner.

Search for ‘Keeper’ in the Application list search bar. Click Configure on the Keeper Application.
Next, on Keeper Application connector page, enter the **IDP ENTITY ID**:

```
IDP ENTITY ID: i

https://wallyswidgets.com
```

The IDP ENTITY ID is a unique, case-sensitive identifier used by JumpCloud for this Service Provider (SP). This value should match the value specified in the “Entity ID” field of the Keeper SSO Connect. Your domain name, SSO Connect server name or IP address are possible examples.

Next, Upload the **IdP Private Key** (private.pem file) and **IDP Certificate** (cert.pem file).

```
IDP PRIVATE KEY: i

Upload IdP Private Key
```

```
IDP CERTIFICATE: i

Upload IdP Certificate
```

In the **SP Entity ID** field, enter the value found in the **Entity ID** field of the Service Provider Section from Keeper SSO Connect.

```
SP ENTITY ID: i

https://34.194.140.247:8443/sso-connect
```
In the **ACS URL** field, enter the value found in the **ACS URL** field of the Service Provider Section from Keeper SSO Connect.

ACS URL: ![Info icon](https://34.194.140.247:8443/sso-connect/saml/sso)

In the field terminating the **IdP URL**, either leave the default value or enter a plaintext string unique to this connector. (i.e. keepersecurity)

IDP URL:
https://sso.jumpcloud.com/saml2/ keepersecurity

In the **Display Label** field, enter a label that will appear under the Service Provider logo within the JumpCloud User console. (i.e. Keeper Security)

DISPLAY LABEL:
Keeper Security

To complete the configuration, click the “activate” button.

To complete the configuration, click the “activate” button.

Last step is to export the metadata from this connector to import it into the Keeper SSO Connect in Step 8.

Upload this file into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen:
Click "Save" and your setup is complete.
AWS SSO

Log into AWS and click on AWS Single Sign-On.

On the SSO Dashboard, click Configure SSO access to your cloud applications.

On the Applications menu, click on “Add a new application”.
Next select “Keeper Security” and click “Add”. **

**Keeper is working with AWS to develop an Application Connector.

Fill in the Display name and Description (optional) in the application details section.
In the AWS SSO metadata section, click the download button to export the AWS SSO SAML metadata file. This file gets imported in the SSO Connect IdP Metadata section on the configuration screen.

Copy this file to the Keeper SSO Connect server and upload it into the Keeper SSO Connect interface by dragging and dropping the file into the Configuration screen: Click "Save".

The remaining step on the Keeper SSO Connect Server is to download the Keeper sso_connect.xml metadata file and upload it to the AWS application.

Click "Export Metadata" on the Keeper SSO Connect.
Import the sso_connect.xml file to the Application metadata section on the application configuration screen.

![Screenshot of Keeper SSO Connect interface showing the Export Metadata button.](image)

**Import the sso_connect.xml file to the Application metadata section on the application configuration screen.**

**Application metadata**

AWS SSO requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

- **Application SAML metadata file**: sso_connect.xml
- **Application start URL**: 

If you don’t have a metadata file, you can manually type your metadata values.

* Required fields

![Screenshot showing the Save changes button highlighted.](image)

**After saving changes the “Configuration for Keeper Password Manager has been saved” success message will be displayed.**
Note: The Keeper SSL certificate cannot be larger than 2048K or the below error will be received.

Either, generate a smaller SSL certificate, re-export and import the metadata file or manually set the ACS URL and Audience URL in the AWS SSO application configuration.

Next, Ensure the Keeper application attributes that are to be mapped to AWS SSO are correct (These should be set by default. Click on the Attribute mappings tab.

The AWS string value to ${user:subject} and format is blank or unspecified. The Keeper Attributes are set as follows:

<table>
<thead>
<tr>
<th>Keeper Attribute</th>
<th>AWS SSO String value</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>${user:email}</td>
<td>unspecified</td>
</tr>
<tr>
<td>First</td>
<td>${user:givenName}</td>
<td>unspecified</td>
</tr>
<tr>
<td>Last</td>
<td>${user:familyName}</td>
<td>unspecified</td>
</tr>
</tbody>
</table>
Note: If your AWS email is mapped to the AD UPN (which may not be the actual email address of your users) it can be re-mapped to the email address associated in the users AD profile.
To make this change navigate to the “Connect Directory” on the AWS SSO page.

Click on the “Edit attribute mappings” button.

Attribute mappings

User attributes are used for generating SAML assertions for attributes in your connected directory. You can modify the

Change the AWS SSO “email” attribute from \${dir:windowsUpn} to \${dir:email}.

Edit attribute mappings

Specify which of the user attributes in AWS SSO map to corresponding user attributes in your connected directory. Learn more

<table>
<thead>
<tr>
<th>User attribute in AWS SSO</th>
<th>Maps to this attribute in your connected directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD_GUID</td>
<td>${dir:guid}</td>
</tr>
<tr>
<td>email</td>
<td>${dir:email}</td>
</tr>
<tr>
<td>familyName</td>
<td>${dir:lastname}</td>
</tr>
<tr>
<td>givenName</td>
<td>${dir:firstname}</td>
</tr>
<tr>
<td>middleName</td>
<td>${dir:initials}</td>
</tr>
<tr>
<td>name</td>
<td>${dir:displayName}</td>
</tr>
<tr>
<td>preferredUsername</td>
<td>${dir:displayName}</td>
</tr>
<tr>
<td>subject</td>
<td>${dir:windowsUpn}</td>
</tr>
</tbody>
</table>
Click on the the “Assigned users” tab and then the “Assign users” button to select users or groups to assign the application.

On the Assign Users window:

1. Select either Groups or Users
2. Type the name of a group or user
3. Click on the “Search connect directory” to initiate the search.

The results of the directory search will display under the search window.
Select the users/groups that are desired to have access to the application and then click the “Assign users” button.

Your setup is complete.
Firewall Configuration

On the server running Keeper SSO Connect, ensure you allow connections from Keeper SSO Connect via Inbound rules on the Windows Firewall, eg. port 8443 used by default, otherwise the request will be blocked.
Logging and Monitoring

Depending on the windows server operating system, SSO Connect Logs are located in either:

C:\Windows\System32\logs\ssoconnect.log

Or

C:\Windows\SysWOW64\logs\ssoconnect.log
Logging into your Keeper Vault (End-User Flow)

Keeper Vault Login Flow (SP-Initiated Connection)
Users can access Keeper directly from the Web Vault, Mobile App or Desktop App.

For example, from the Web App, visit https://keepersecurity.com/vault

Click on "Enterprise SSO Login"
Then enter the **Enterprise Domain** as provided by the Keeper Administrator (entered into the Keeper Admin Console in section 4 of this document) and click "Connect".
To complete the user’s profile, they must select a security question and answer.
Mobile app users can use the same flow by selecting "Enterprise SSO Login" during signup.
After account signup, the user is immediately logged into their Keeper Vault. Users will be presented with a quick start guide and helpful setup instructions.
Under the "Account" screen, you will see that the account is activated on the Keeper Business license.

https://keepersecurity.com/vault/#
Email Confirmation

When users are dynamically provisioned via Keeper SSO Connect, they will receive an email confirmation that contains helpful information including download links, Web Vault link and the "Enterprise Domain" info which is necessary to access Keeper from a new device.

Hello,

You have been successfully provisioned to your organization's Keeper account. You can now access Keeper from your web browser, mobile or desktop device.

When logging in for the first time on a new device, select the "Enterprise SSO Login" link and enter the Enterprise Domain name:

lurey_sso_gsuite

To download Keeper, visit our download page:
https://keepersecurity.com/download.html

Or, access Keeper's Web App at:
https://keepersecurity.com/vault

If you have any questions, please visit our support page.

Keeper Team
High Availability Configuration

1. Once the first instance has been installed and configured further SSO Connect instances can be installed. They will automatically pick up the primary configuration.
2. Any load balancing or failover must occur via a frontend load balancer (hardware or software, such as nginx or haproxy).
3. Make sure the individual instances of SSO Connect servers have a local hosts record that points to their own network IP address for the HA server FQDN.

Advanced Monitoring

The Keeper SSO Connect application provides a network-level HTTP request that you can integrate into existing monitoring systems. For example, based on the above example the URL for testing the application status can be found by following this URL:

https://34.195.7.51:8443/ping

If the service is active, you will get a JSON response below:

{"configuration":"Running","sync_revision":1035,"sync":"Thu Dec 21 18:16:26 UTC 2017","version":"01.0.0.102","sso":"Running","status":"Ready"}

FAQ’s

Why don’t you just bind the SSO service to all interfaces rather than require me to provide an IP?

The reason is that some customers have multi-homed servers and they do not want to bind to all interfaces for a number of reasons.

If internal IP is required, why does SSO connect let me leave it blank?

Reason being the internal IP is not required. You can leave it blank if the hostname resolves via DNS to the same external IP or even internal IP for Intranet. We have customers who use SSO strictly internal and the FQDN resolves to the internal IP. So that field can be left blank. It depends on your setup.
Why can’t my non-SSO users change their master password?

When SSO Connect is enabled on a node, all the users in the node and sub-nodes are under an enforcement to prevent the changing of their master password. This is done to prevent SSO users from bypassing authentication through the IdP.

If a user is not is not transition to SSO login, but desires to change their master password, they will need to be relocated to a node that doesn’t have the SSO enforcement.

I have invited a user, why can’t they create their vault via SSO Connect?

When logging in for the first time the onboarding process needs to occur on either the Web or the Desktop application. The Browser Extension’s do not facilitate the onboarding process of a new user, but will allow existing users to authenticate.

I am receiving the following error when a new user tries to connect for the first time:

```
{"result_code":"does_not_exist","message":"This user does not exist"}
```

There are two possible reasons for this error. The invited user is not in an SSO Enabled node within the Admin Console or the email address in the IdP doesn’t match the email address of the invited user. Try moving the user into the SSO Enabled node. If after verifying the user is in the correct node, try changing the SSO provisioning method from invited users to dynamic users. If the account gets created, it is most likely an email address mis-match.

I’m getting an error on Linux about writing to /tmp. How do I resolve?

On a linux system /tmp must have exec privileges. If /tmp does not have exec privileges, execution of "java -jar SSOConnect.jar" may show an exception similar to: java.lang.UnsatisfiedLinkError: /tmp/sqlite...

To resolve this, ensure you have exec permission on /tmp.

Can users login via SSO and natively?

Enterprises can have some users configured to natively login and other users on SSO, but once a user has been transitioned to SSO, they will only be able to access their vault via SSO.

I can SSO into Keeper using Chrome, Firefox, and the Desktop application, but I can’t connect with IE. Why?

IE has difficulty handling cross-domain redirects due to their multiple security zones. Add ".keepersecurity.com to Trusted Sites Zone in IE.
Support

If you have any questions or require assistance in configuring Keeper SSO Connect, please contact the Keeper Business Support team at: business.support@keepersecurity.com

Thank You!
Appendix A: Creating a Self-Signed Certificate (windows)

1. Download a copy of OpenSSL Binary (the version may have incremented since the publish of this document) such as:
   http://slproweb.com/download/Win32OpenSSL.Light-1.0.2m.exe
2. Run as admin and take the default settings
3. Open command prompt
4. mkdir c:\<hostname>
5. cd \<hostname>
6. set RANDFILE=c:\<hostname>.rnd
7. set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg
8. c:\OpenSSL-Win32\bin\openssl.exe
9. genrsa -out <hostname>.key 2048
10. req -new -x509 -days 3652 -key <hostname>.key -out <hostname>.pem
11. Enter in the following data. Be sure the common name matches the Hostname or IP. Just hit “enter” for Email.
   Country Name (2 letter code) []: US
   State or Province Name (full name) []: California
   Locality Name (e.g., city) []: Stanford
   Organization Name (e.g., company) []: Stanford University
   Organizational Unit Name (e.g., section) []: University IT
   Common Name (e.g., web.stanford.edu) []: example.stanford.edu [This needs to match the HOSTNAME/IP of the SSO Connect configuration]
   Email Address []:
12. pkcs12 -inkey <hostname>.key -in <hostname>.pem -export -out <hostname>.pfx