Keeper SSO Connect

© 2016 Keeper Security, Inc.
This guide provides setup instructions for Keeper SSO Connect on the AD FS identity platform.

**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 Microsoft AD FS to provide businesses the utmost in authentication flexibility.

Keeper SSO Connect is a software application that is installed on the enterprise customer’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.

**System Requirements**

Keeper SSO Connect’s service application requires installation on a private on-premises or cloud-based server with the below minimum requirements.

- Mac OS 10.7+
- Windows 7+
- Linux OS with Java 8

**Installation & Setup**

The steps for setting up Keeper SSO Connect are below:

1. Enable SSO Connect on a node from the Keeper Admin Console
2. Install Keeper SSO Connect on your server (supports Windows, Mac, Unix/Linux)
3. Configure Keeper as a "Relying Trust Party" on AD FS
Login to Keeper Admin Console

Visit the Keeper Admin Console at 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".
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.
Manage SSO Connect for SSO - AD FS

SSO Connect URL
Not Yet Defined

Node
SSO - AD FS

Enterprise Domain
lurey_sso_adfs

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

There are 2 parameters to configure here. 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.

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

Click on the "Download the Keeper SSO Connect" link on the "Bridge" tab in the Keeper Admin Console to download the application. You can select either Windows or Mac versions. SSO Connect should be installed on a Windows or Mac server that is always available to users. If SSO Connect is not running, users will be unable to login to their vault.

Download for Windows

Extract the zip file and launch the installer.
Login to Keeper SSO Connect

After installation of Keeper SSO Connect is complete, login to the application with your Keeper Administrator email address, master password and two-factor code (if enabled).
Proxy Configuration

Note: If you use a proxy server in your environment, click on the "gear" icon and select the proxy type and/or authentication.

The first time logging in, you will be prompted to select the SSO Connect enterprise domain name from the admin console. Select the AD FS connection and then click "Connect".
After connection is complete, you will be taken to the Keeper SSO Connect configuration page:

By default, the Host Name, Port and Server Base URL is automatically assigned. It will default to the local IP address of the computer, with port 8443.

If users will be accessing Keeper SSO Connect from outside of your internal network, the Host/Port must be publicly accessible, and the port number must pass through your firewall to the service.

Edit the "Host Name" and "Port" to the address that your users will be using to access the SSO service. In the example above, the IP address is 34.195.7.51 with port 8443. The "Server Base URL" will be automatically updated to reflect this host and port.

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.

SSL Certificate
By default, Keeper SSO Connect will use a self-signed certificate. Before deploying to production, it is recommended that you generate a proper SSL Certificate from your certificate authority and upload the file here. Self-signed certificates will generate security errors for your users.

IdP Metadata
The remaining step is to finalize the AD FS configuration and upload the AD FS SSO metadata file.
Configure AD FS

Obtain Federation Metadata XML

Inside the AD FS Management application, locate the Federation Metadata xml file via URL Path "/Federation/Metadata/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**

Export the Keeper SSO Connect metadata using the "Export Metadata" link and save this file for the next step on AD FS.
8. 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.
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.

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

URL
- SAML Assertion Consumer Endpoints
  - https://acw10e.keeperqa.local:8443/sso-connect/saml/sso
  - Index: 0
  - Binding: POST
  - Default: Yes

- SAML Logout Endpoints
  - https://acw10e.keeperqa.local:8443/sso-connect/saml/slo
  - Index: 0
  - Binding: Redirect
  - Default: No

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.
Important: Ensure that 3 attributes ("First", "Last" and "Email") are configured with the exact spelling as seen above.
F. For Logout support we need to add two more Claim Issuance Policy rules:
G. Send Claims using a Custom Rule
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
J. Create Persistent Name Identifier

Incoming claim type:  http://mycompany/internal/sessionid
Outgoing claim type:  Name ID
Outgoing name ID format:  Transient Identifier
**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.
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!

**Logging and Monitoring**

The Keeper SSO Connect "Incident Log" screen contains all activity, such as new Keeper account creation and errors. This screen is helpful in the initial deployment and testing, to ensure that all system functions are performing optimally.
Keeper SSO Connect runs as a service. Closing out the user interface does not stop the service. To fully stop the service, exit the application from the system tray:

Windows:

Mac OS:
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](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.

1. Create Your First Keeper Record
   Click to complete

2. Install the Browser Extension

3. Upload your First File or Photo
   Click to complete

4. Enable Two-Factor Authentication
   Click to complete
Under the "Account" screen, you will see that the account is activated on the Keeper Business license.
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.

Welcome to Keeper

Keeper Security <support@keepersecurity.com>

to me →

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

Follow us on Facebook and Twitter

© 2018 Keeper Security, Inc.
850 W. Jackson Suite 500, Chicago IL 60607 USA
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:

{"status":"success"}

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!