Configure SafeNet to accept EFT for SAML IDP access

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.3.3 and later

NOTE: This article provides guidelines for using a third-party tool with EFT. This article is not meant as formal support for that tool, but only as an example of setup options. Contact the third-party seller's support for detailed information about their product. Globalscape is not responsible for any configuration errors involving the third-party tool.

DISCUSSION

Below are some points regarding SafeNet's SAML Server:

- Safenet's IDP is available only in the cloud, there is no locally hosted option. Because of this in order to test against SafeNet we are required to obtain a trial Administrator account on SafeNet's Authentication Server.
- To get an administrator account contact Gemalto. Gemalto is the vendor for SafeNet.
- To create your account the Gemalto contact will send you a link to download a Mobile Pass token login account. You will need to download and install the Mobile pass invitation on a server or virtual machine.
- Download the mobile pass to obtain your Token and activate your account.
- Once activated, you will receive a secondary account activation email from Gelmato/SafeNet. Follow the email instructions.
- Once you have an active account, you will be able to log into the SafeNet Administration account and configure the IDP SAML backend. *Safenet uses Shibboleth as their IDP backend*.
- SafeNet SAML IDP Administrator login: https://cloud.safenet-inc.com/console/
- Your username is the email address; obtain your password from the MobilePass app you downloaded.

Configure SafeNet to accept EFT for SAML IDP access

- Log into the SAFENET Authentication Service
- Navigate to Virtual Servers > [click on the globalscape link] > comms > SAML
- Click **Saml Service Providers** link and then click **Add**.
- Enter your EFT Machine name for service provider and resource fields.
- When you click **Add**, Safenet will alert that it's unable to resolve the URL; click **Continue**. This is OK if you are testing from internal IPs; the EFT host address will not

be resolvable. This isn't an issue since EFT's SP just uses a POST commands to the SafeNet SAML server.

- Click **Continue** to accept the risk.
- EFT is now configured to be an acceptable SP for the SafeNet IDP.

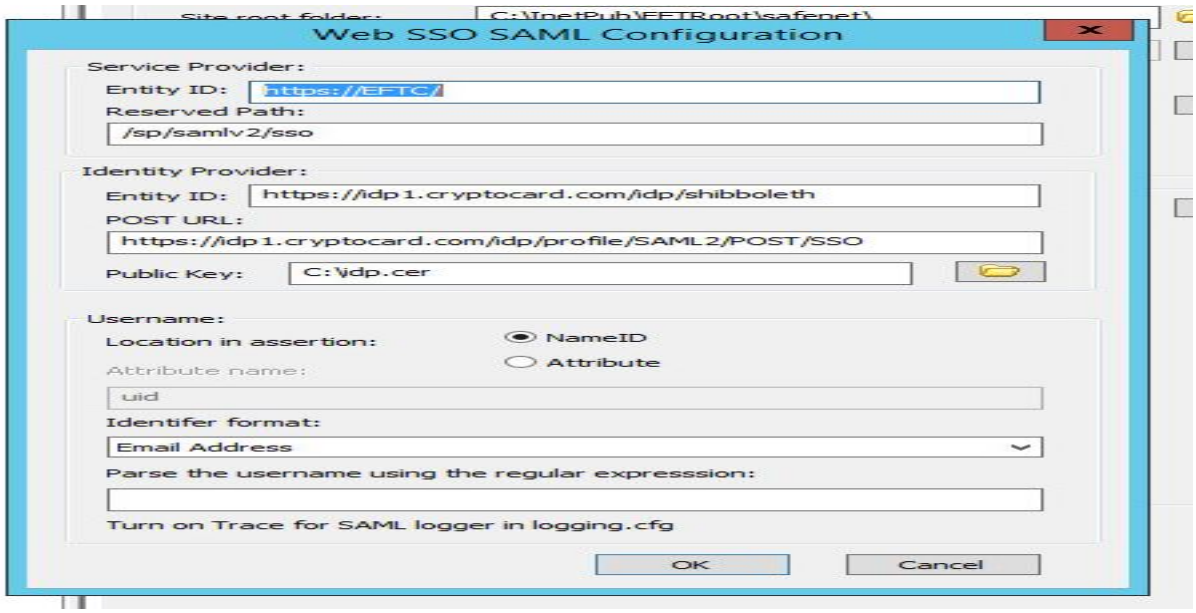
Create SAML Authenticated users

- On EFT, create a user named test with email address.
- Next, create a user on the SAML Server named.
- In the Shortcuts menu, click **Create User** and then create a user.
- Click the **Assignment** tab and search for the user you just created.
- Check user's link under the **User ID** column.
- Create a password for the user by clicking **Token's link > Password.**
- Next, add the SAML Server created previously as an active authenticator for user test. Select SAML login ID = UserID.
- Click on the SAML Services link and click **Add**.

Configure EFT to use SafeNet as the SSO IDP server

- Obtain the Safe's Entity ID and endpoint from the **Virtual Servers > Comms > SAML Service Providers** link.

Configure EFT as follows

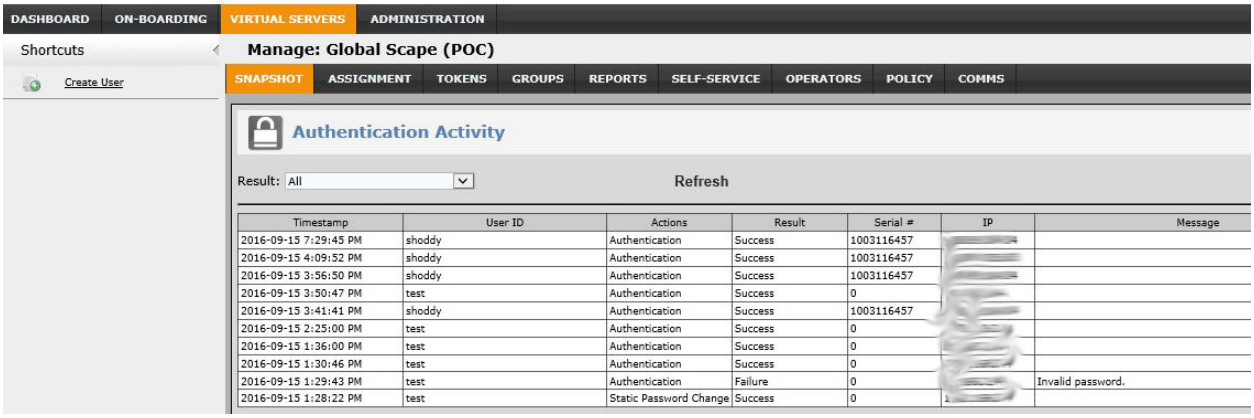


Log in via SSO

- Launch WTC and click **SSO Sign in**.
- You should be redirected to the SafeNet IDP login page, log in using the user and password you created earlier.
- Once authenticated you should be redirected to the user's WTC home directory.

Troubleshooting

SafeNet doesn't provide visibility to server-side logs. The only troubleshooting available is via the **Snapshot** tab. You can view your SSO login status via the **Snapshot > Authentication Activity** tab.



GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11323/Configure-SafeNet-to-accept-...