SevOne SAML Single Sign-On Setup Guide

30 November 2023
IBM SevOne NPM Version 6.7.0
Document Version 6.7.0.1

Table of Contents

SevOne Documentation

All documentation is available from the IBM SevOne Support customer portal.

1 About

Single Sign-On (SSO) is available with **dex**. This document provides details on how to configure **SAML** (Security Assertion Markup Language) using **Okta** and **Service Provided Initiated Azure Active Directory Single Sign-On** (sP-initiated Azure AD SSO) setups.

On a HSA, Single Sign-On must not be configured. Only configure Single Sign-On on the Cluster Leader. If a failover on a Cluster Leader happens, only then configure Single Sign-On on the HSA. When the Cluster Leader automatically fails over to the HSA, you are required to update Identity Provider configuration to now point to the HSA's IP Address / hostname.

In case of a failover, you need to modify your **Identity Provider** configuration (for example, Siteminder), to point to the new HSA instead of the failed Cluster Leader.

Single Sign-On logins do not create new users. Due to this, it requires the users to be added to NMS manually.

Risks of using IdP-Initiated Single Sign-On Flow

There are security implications of IdP (Identity Provider) initiated SAML before implementing it with SevOne NMS.
Currently, the version of **dex** SevOne uses, only supports **SP-initiated Single Sign-On**.
IdP-Initiated flows carry a security risk and are therefore NOT recommended. Make sure you understand the risks before enabling IdP-Initiated Single Sign-On.
In an IdP-initiated flow neither Auth0 (which receives the unsolicited response from the Identity Provider) nor the application (that receives the unsolicited response generated by Auth0) can verify that the user actually started the flow. Because of this, enabling this flow opens the possibility of an Login CSRF attack, where an attacker can trick a legitimate user into unknowingly logging into the application with the identity of the attacker. Please refer to Login CSRF section below for details.
SevOne recommends use of SP (Service Provider)-Initiated flows whenever possible. For details, please refer to https://auth0.com/docs/protocols/saml/idp-initiated-sso#risks-of-using-an-idp-initiated-sso-flow.

When a URL is used for Single Sign-On configuration, between the identity provider and NMS **dex** config, you must be consistent with using either the IP address or a DNS name. Please do not mix and match IP addresses and their corresponding DNS names.

The details in this document do not apply to single-peer clusters.

Terminology usage...

In this guide if there is,

- [any reference to *master*] OR
- [[if a CLI command contains *master*] AND/OR
- [its output contains *master*]],
  it means *leader*.

And, if there is any reference to *slave*, it means *follower*.

NOTICE

Starting SevOne NMS 6.7.0, MySQL has moved to **MariaDB 10.6.12**.

2 Configure SAML using Okta Setup

2.1 Prerequisite

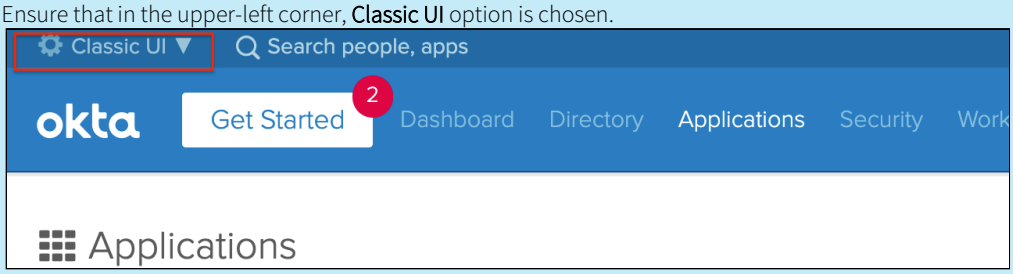
- IP Address of SevOne NMS Cluster Leader required.

> **IMPORTANT: Upgrade / Install SevOne NMS**
>
> To use Single Sign-On feature, you must be on SevOne NMS 5.7.2.15 or higher version.

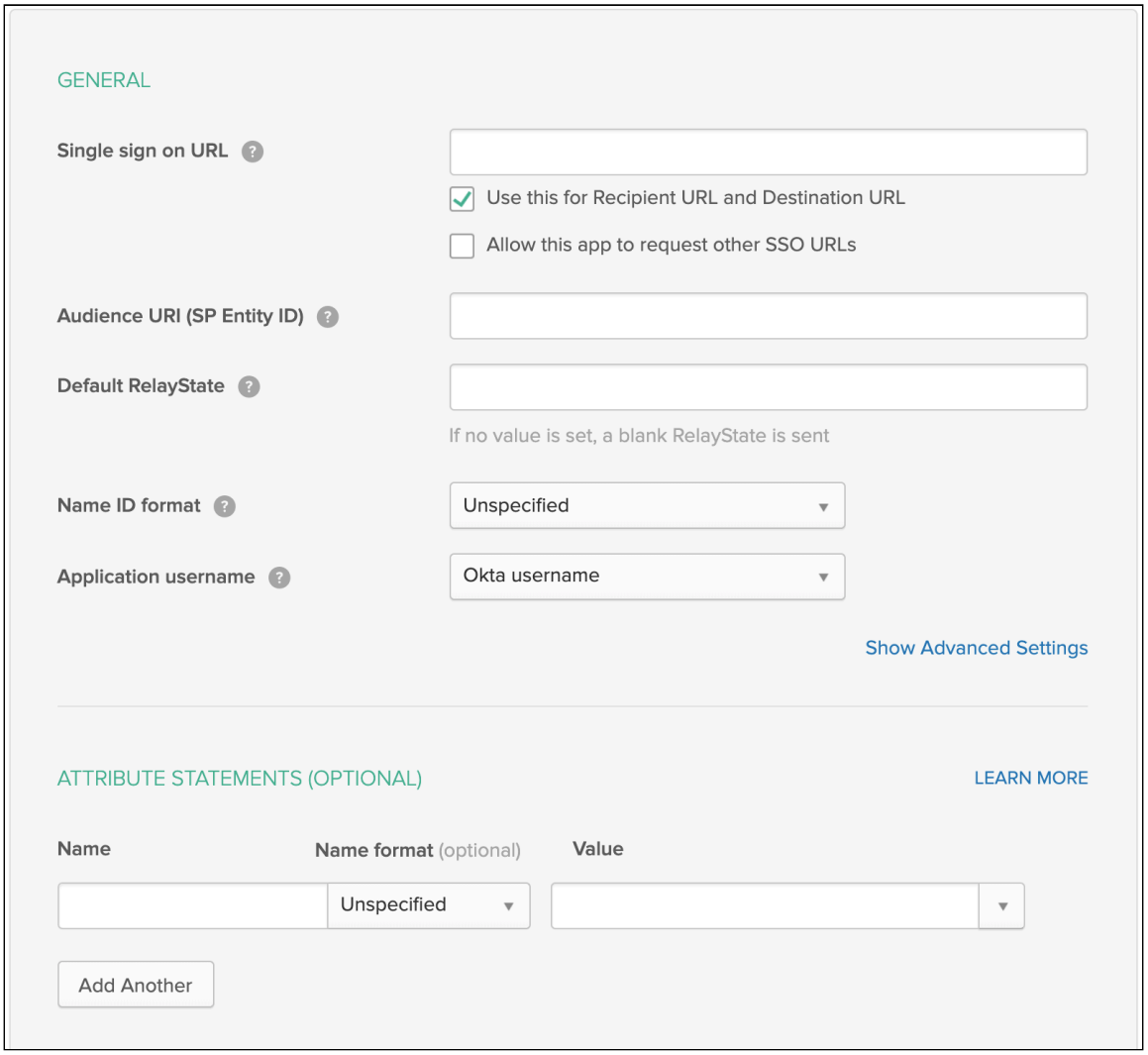
2.2 Login to Okta Account

> Two Factor Authentication (2FA) with Okta requires configuration of Multifactor Authentication (MFA) enrollment policies. Please refer to **https://help.okta.com/en/prod/Content/Topics/Security/healthinsight/required-factors.htm** for details.

1. Sign-in to your **Okta** account.
2. Click on **Admin** button in the upper-right corner.
3. Click on **Applications** drop-down and select **Applications**.
4. Click on **Add Application** button.
5. Click on **Create New App** button in the left-panel.

> Ensure that in the upper-left corner, **Classic UI** option is chosen.
>
> 
>

6. Choose **SAML 2.0** as a **Sign on method**.
7. Click on **Create** button to initiate **Create SAML Integration**.
8. Enter **App name**.
9. You may choose to add an **App logo**. This field is optional.
10. Click on **Next** button to Create / Configure SAML application.



2.3 Create / Configure SAML application

1. Create a new SAML application in your SAML provider site.
2. Add a **Single Sign-On URL**.

> **Example**
> https://<Cluster Leader IP address>/sso/callback

> If the SAML application requires Recipient and Destination URLs, use the above URL for both.

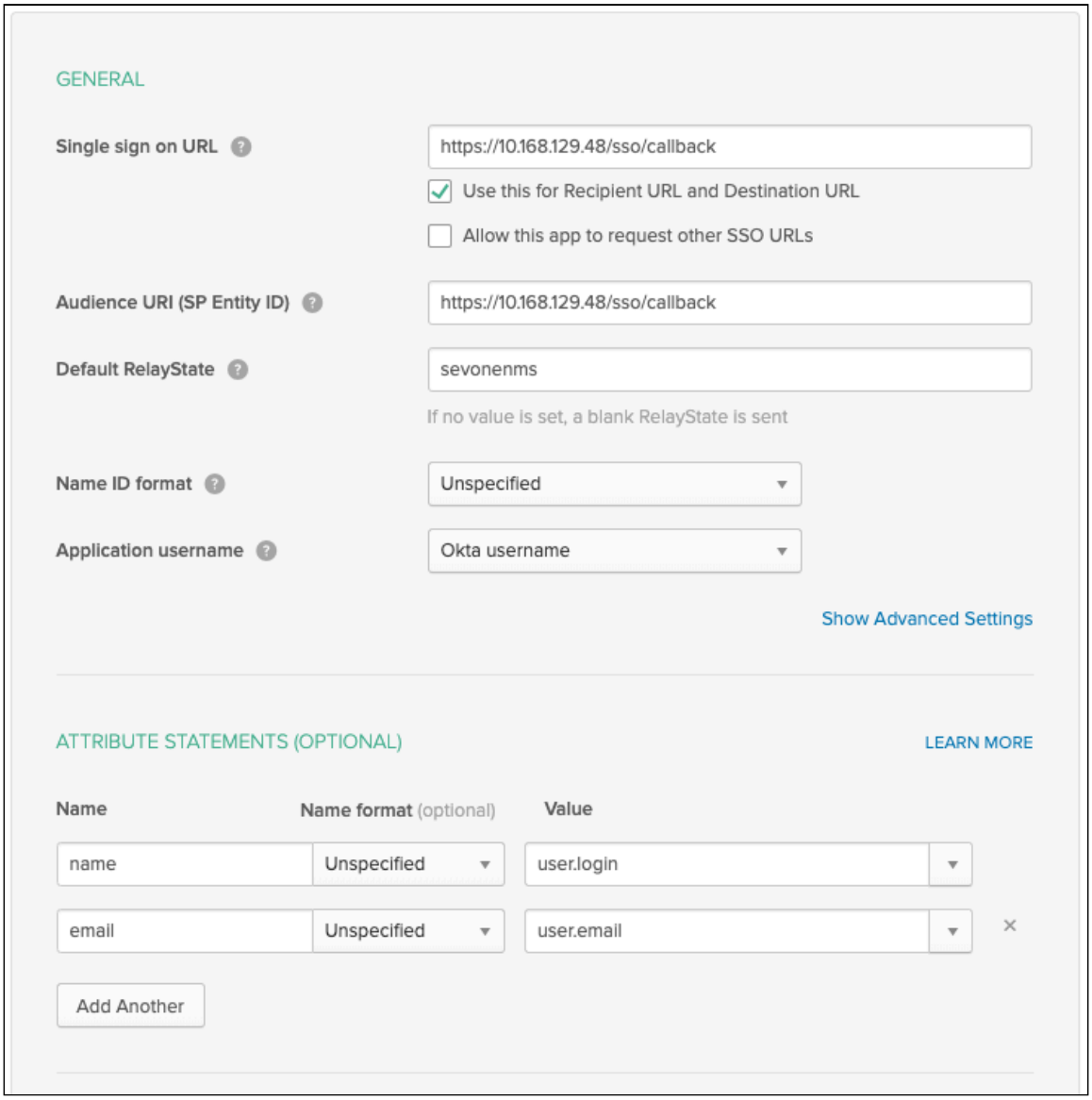
3. Add an **Audience URI** (also known as, **SP Entity ID**).

> **Example**
> https://<Cluster Leader IP address>/sso/callback

4. For **IdP** initiated login support, **Default RelayState** must be set to the NMS client ID, **sevonenms**.
5. Add an attribute statement for **name** that has the value that maps to the user login in SevOne NMS.
6. Your configuration must look as follows.

Example

In this example, 10.168.129.48 is the Cluster Leader IP address.



7. Provide permissions to the users to use the app.

2.4 Gather Information required for NMS configuration

You will need the following from the SAML provider in the NMS configuration.

1. The Identity Provider Single Sign-On URL.
2. The Identity Provider Issuer.
3. The x.509 certificate.

2.5 Configure Single Sign-On in NMS

Please make sure that once the appliance or Virtual Machine is configured with the Single Sign-On, its IP Address cannot be changed. Otherwise, Single Sign-On will fail.

1. Copy x.509 certificate, **/usr/share/pki/sso/saml.pem**, to SevOne NMS' cluster leader.

   If directory **/usr/share/pki/sso** does not exist, create it.

2. SSH into your Cluster Leader.

```
$ ssh root@<Cluster Leader IP address>
```

3. Run **/usr/local/scripts/dex_setup_template.sh** script to update the config template.

```
$ bash /usr/local/scripts/dex_setup_template.sh
```

   Running **dex_setup_template.sh** generates a new MySQL *dex password* as well as a new *OAuth secret*. If this script must be run again for any reason, please use the new password and secret for any editing to be done on the generated **/etc/dex/config.yaml** file. Failure to do so, results in the following authentication error for **all** active dex connectors.

   Error

```
Authentication Exception: Invalid client credentials.
```

4. Using the text editor of your choice, edit **/etc/dex/config.yaml** file.

```
$ vi /etc/dex/config.yaml
```

   a. Uncomment the SAML section (starting with line *- id: saml*) by removing the # from each line.

      The first 3 lines that start with ## should remain as comments.

   b. **id** - is an identifier unique to **dex**. If you do not have any other connections with **id** of SAML, you may leave it as is. This is for Internal Use Only, but must be unique if you are configuring multiple connectors.
   c. **name** - set to a reasonable value. This value will be displayed to users when presented with login options.
   d. **type** - leave as **saml**.
   e. Set **config.ssoURL** to the **Identity Provider Single Sign-On URL**.
   f. Set **config.ssoIssuer** to the **Identity Provider Issuer**.
   g. Set **config.ca** value to the file path where your **x.509** certificate is located. For example, **/usr/share/pki/sso/saml.pem**.
   h. Depending on your Identity Server Configuration, you may need to change the values of **config.usernameAttr** and **config.emailAttr** to match those of your server's attribute statements.
   i. If your Identity Server requires a **GET** authentication request, instead of the default **POST**, place the following line under the SAML connector config since it configures how **dex** must handle the SAML response.

```
authnRequestBindingType: "HTTP-Redirect"
```

5. If you used the **domain name** for <Cluster Leader IP address> in the previous section, replace all instances of the Cluster Leader IP address with the Domain Name.
6. If you have signed certificates set up on your SevOne NMS cluster, please update the following to validate these certificates. Under **sevone** > **connector** > **config**,
   a. Add **caCertFile** and set it with a path to your CA.
   b. Set **noVerify** to **false** to validate the certificates.
7. Please do not change any configuration in the **storage**, **web**, and **frontend** sections without first consulting with **SevOne Support**.
8. Your **dex** configuration file, **/etc/dex/config.yaml** must look like the following.

Example with detailed comments

```
# Note: Dex should only be running on the cluster master / leader
# the URL here can be the IP or the hostname of the cluster master / leader

# Cluster master / leader IP that will issue the valid auth tokens. This has to be reachable by DI, the NMS and the IdP
# If behind a proxy, this should be the proxy address to the cluster master / leader. The same proxy address for the issuer
# should be configured for the IdP, DI and the NMS. Everyone needs to agree on the issuer and it has to be the same
# in all of the login cases in order for SSO to work.
issuer: https://10.168.129.48/sso

# Backend storage for authenticated clients
storage:
  type: mysql
  config:
    host: 127.0.0.1:3307
    database: dex_db
    user: dex
    # This is the MySQL password used to allow access to the dex database
    password: jrFoHsG9xe2FjliSBgbNBgoblWCpkB54IgdvcogOK2BybtriJoYHG8b5NGoRrnhsFdTOmFaWUgd1eDROONDakKB4BqV70FWD8IASx6CktYgNizzkdYKd6aaIgyNqkwXc
    ssl:
      mode: "false"
logger:
  level: "debug"
  format: "text"


# The port where dex will run
web:
  http: 127.0.0.1:5556


# The login page for dex authentication
frontend:
  dir: /opt/dex/web
  theme: sevone
  issuer: SevOne


# The connector for doing local SevOne authentication
connectors:
```

```
40  - id: sevone
41    name: SevOne auth
42    type: sevone
43    config:
44      restUrl: "https://test-nms2.devops.sevone.com/api"
45      resetPassUrl: https://test-nms2.devops.sevone.com/doms/login/newPassword.html
46      caCertFile: "/etc/nginx/ssl/nginx.crt"
47      noVerify: true
48
49  # To get a SAML connector working, replace:
50  #   - The ssoURL and ssoIssuer with URLs from the SAML provider
51  #   - redirectURI/entityIssuer addresses need to point to the cluster master /
    leader hostname or IP
52  - id: okta
53    name: okta
54    type: saml
55    config:
56      # This is provided by the SAML provider (Okta, Siteminder etc). It has to be
    reachable by the user's browser.
57      ssoURL: "https://dev-835393.okta.com/app/sevonedev835393_testnms_1/
    exk13u9fndI6T6GmJ357/sso/saml"
58
59
60      # This is provided by the SAML provider (Okta, Siteminder etc). This has to be
    reachable by the user's browser.
61      ssoIssuer: "http://www.okta.com/exk13u9fndI6T6GmJ357"
62
63
64      # This URL handles the login authentication. It should be the NMS cluster
    master / leader.
65      # The user will be redirected here from the Identity Provider so this needs to
    be reachable.
66      redirectURI: "https://10.168.129.48/sso/callback"
67
68
69      # The certificate authority that was used to sign the SSL certificates for the
    connection
70      # This is provided by the SAML provider
71      ca: /usr/share/pki/okta/okta-cert.pem
72
73
74      # The name of the field that contains the username attribute
75      usernameAttr: name
76
77
78      # The name of the field that contains the email attribute
79      emailAttr: email
80
81  oauth2:
82    # skips asking the user to grant permission for login
83    skipApprovalScreen: true
84    # the OpenID Connect flow types to enable. DO NOT EDIT
85    responseTypes: ["code","token","id_token"]
86
87  # This defines which applications can authenticate using dex. Below is an example
    NMS configuration,
88  # but other applications (e.g. DI) can be configured here
89  staticClients:
90  # The client_id. Use this id as the 'Default Relay State' when configuring a SAML
    Service Provider.
91  - id: sevonenms
92    # The redirect URIs matter for SP initiated logins (client (NMS) initiated
    logins).
93    # It should contain all the peers in the cluster with both their hostnames and
    IPs that are
94    # allowed to do SP initiated login. Also with HTTP and HTTPS access.
95    # The user can be redirected to one of these after a successful login.
96    redirectURIs:
97    - 'http://test-nms2.devops.sevone.com/callback.php'
```

```
98      - 'https://test-nms2.devops.sevone.com/callback.php'
99      - 'http://10.168.129.48/callback.php'
100     - 'https://10.168.129.48/callback.php'
101     name: 'SevOne NMS'
102     # The client_secret for the NMS client. The NMS will need this to initiate login.
103     secret:
        EAvgtOGIsxjcFdl2aaKoEOmlOCY3G7LVNdiDnf3ZiIqSdcw5xKYlaodmaUIHqFg9bVHIzYmG50wV9oAhYm6
        WrBO7npuf713CUH9Tq5lgEjfHtTH8Zlpzkt1C9ilMBIDI
104     # samlInitiated is required to enable SAML's IdP initiated flow. If not using
        SAML, you may omit this section.
105     samlInitiated:
106       # This is where users will finally be redirected after a SAML IdP initiated
        login.
107       # It can be any peer in the cluster.
108       redirectURI: https://10.168.129.48/callback.php
109
110   # The client_id. For Data Insight we need a separate static client as we configure
        the redirectURIs differently.
111   # This id will be used in oidc configuration on Data Insight as 'clientId'
112   - id: sevonedi
113     # These redirect uris will be datainsight servers which are configured to use
        this nms dex instance for auth.
114     # All valid hostnames should be here.
115     redirectURIs:
116     - 'https://10.168.10.11/callback'
117     - 'https://datainsight.example.com/callback'
118     name: 'SevOne DI'
119     # The client_secret for the Data Insight client. This should be the same as the
        one configured for the sevonenms static client
120     # This will be used in the Data Insight oidc configuration as 'clientSecret'
121     secret:
        EAvgtOGIsxjcFdl2aaKoEOmlOCY3G7LVNdiDnf3ZiIqSdcw5xKYlaodmaUIHqFg9bVHIzYmG50wV9oAhYm6
        WrBO7npuf713CUH9Tq5lgEjfHtTH8Zlpzkt1C9ilMBIDI
122     # samlInitiated is required to enable SAML's IdP initiated flow. If not using
        SAML, you may omit this section.
123     samlInitiated:
124       # This is where users will finally be redirected after a SAML IdP initiated
        login.
125       # This should be the datainsight url they came from
126       redirectURI: https://10.168.10.11/callback
127
128   # Let dex keep a list of passwords which can be used to login to dex.
129   # We don't allow that so lets keep it disabled.
130   enablePasswordDB: false
```

9. Restart SSO service. Please refer to section Restart Single Sign-On Service.
10. Enable SSO. Please refer to section Enable Single Sign-On.

> **SevOne NMS** is using **SAML**. However, **SevOne Data Insight** is using **OpenID-Connect**. Please refer to *SevOne Data Insight Administration Guide* > section **Configuration** > subsection **OpenID Connect** for details.
> **dex** wraps SAML in OpenID-Connect tokens.

3 Configure SAML using Azure Active Directory Single Sign-On Setup

3.1 Prerequisite

- Azure Active Directory (AD) subscription. If you do not have a subscription, you may obtain a free account.
- Azure Active Directory (AD) Security Assertion Markup Language (SAML) Toolkit Single Sign-On (SSO) enabled subscription.

> Please refer to https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/saml-toolkit-tutorial for details.

- IP Address of SevOne NMS Cluster Leader required.

> IMPORTANT: Upgrade / Install SevOne NMS
>
> To use Single Sign-On feature, you must be on SevOne NMS 5.7.2.15 or higher version.

3.2 Create / Configure Azure Active Directory Single Sign-On application

> For now, create your own Azure active directory single sign-on application. In the future, this will change so that the user can use the existing gallery application supporting SAML SSO.

1. Login to the Azure portal.

   > Your account must be an Azure subscription administrator / owner.

2. Navigate to **Azure Active Directory** under **Azure Services**.
3. Click **Add** button to add an Enterprise application.
4. Click **Create your own application** button.

   > If the button is unavailable, your account may not have the correct permissions.

   a. Enter application name.
   b. Select **Integrate any other application application you don't find in the gallery**. i.e., Non-gallery.
5. From left navigation bar, under **Manage**, click **Users and groups**.

   > Here, you will determine which Azure users to provide access to Single Sign-On.

6. Click **Add user/group**, and select the Azure users and groups to have access to Single Sign-On.
7. Click **Assign** after users and groups have been added.
8. From left navigation bar, under **Manage**, click **Single sign-on**.
9. Select **SAML** as the single sign-on method.

   > You are now on **SAML-based sign-on** page.
   > To go back, click **Single sign-on** under **Manage** in the left navigation bar.

10. Click in section **Basic SAML Configuration** to edit.
    a. Change **Identifier (Entity ID)** to **https://*<Cluster Leader IP address>*/sso/callback** where *<Cluster Leader IP address>* is the IP address of your SevOne NMS cluster leader.
    b. Change **Reply URL (Assertion Consumer Service URL)** to **https://*<Cluster Leader IP address>*/sso/callback** where *<Cluster Leader IP address>* is the IP address of your SevOne NMS cluster leader.

    > This field is used for IDP-initiated SSO, so it will not be used, but is required for application setup.

11. Click **Save** followed by ✕ to close.

    > If you get a pop-up asking if you want to test the app, decline it for now.

12. Click in section **User Attributes & Claims** to edit.
13. Claim name for value **user.mail** must be **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name**.
14. Click **Add new claim**.
    a. Enter name as **displayname**.
    b. Enter namespace as **http://schemas.microsoft.com/identity/claims**.
    c. Enter source attribute as **user.displayname**.
15. In section **SAML Signing Certificate**,
    a. for **Certificate (Base64)** > click **Download**.

    > ⚠ The raw certificate will not work.

16. In section **Set up <your application name>**, you will need the login URL for the next steps.

3.3 Configure Single Sign-On in NMS

> ⓘ Please make sure that once the appliance or Virtual Machine is configured with the Single Sign-On, its IP Address cannot be changed. Otherwise, Single Sign-On will fail.

1. Copy x.509 certificate, **/usr/share/pki/sso/saml.pem**, to SevOne NMS' cluster leader.

   > ⚠ If directory **/usr/share/pki/sso** does not exist, create it.

2. SSH into your Cluster Leader.

```
$ ssh root@<Cluster Leader IP address>
```

3. Run **/usr/local/scripts/dex_setup_template.sh** script to update the config template.

```
$ bash /usr/local/scripts/dex_setup_template.sh
```

> ⓘ Running **dex_setup_template.sh** generates a new MySQL *dex password* as well as a new *OAuth secret*. If this script must be run again for any reason, please use the new password and secret for any editing to be done on the generated **/etc/dex/config.yaml** file. Failure to do so, results in the following authentication error for **all** active dex connectors.
>
> **Error**
>
> ```
> Authentication Exception: Invalid client credentials.
> ```

4. Using a text editor of your choice, edit **/etc/dex/config.yaml** file.

```
$ vi /etc/dex/config.yaml
```

   a. Uncomment the SAML section (starting with line *- id: saml*) by removing the # from each line.

> The first 3 lines that start with ## should remain as comments.

b. **id** - is an identifier unique to **dex**. If you do not have any other connections with **id** of SAML, you may leave it as is.
c. **name** - is the text that will be shown on the user interface of Single Sign-On page. You may have a string with spaces if you wrap it in quotation marks.
d. **type** - leave as **saml**.
e. **ssoURL** - on Azure, under the 4th section of **Single Sign-On** page, Set up <your application name>, copy the Login URL and paste it here, wrapping in quotation marks. For example, "SSO Login URL".
f. **ssoIssuer** - change the name of this field to **entityIssuer** and set the field to **"https://<Cluster Leader IP address>/sso/callback"**; it must be wrapped in quotes.
g. **redirectURI** - leave as-is.
h. **ca** - set field as **/usr/share/pki/sso/saml.pem**.
i. **usernameAttr** - set to **"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"**; it must be wrapped in quotes. This maps to the name attribute in the 2nd section of the SAML-based **Single Sign-On** page, under **Attributes & Claims**.
j. **emailAttr** - set to **"http://schemas.microsoft.com/identity/claims/displayname"**; it must be wrapped in quotes. This maps to the **EmailAddress** attribute in Azure.

Example

```
- id: saml
  name: saml
  type: saml
  config:
    ssoURL: "SSO Login URL"
    entityIssuer: "https://<Cluster Leader IP address>/sso/callback"
    redirectURI: "https://<Cluster Leader IP address>/sso/callback"
    ca: /usr/share/pki/sso/saml.pem
    usernameAttr: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
    emailAttr: "http://schemas.microsoft.com/identity/claims/displayname"
```

5. Restart SSO service. Please refer to section Restart Single Sign-On Service.
6. Enable SSO. Please refer to section Enable Single Sign-On.

4 Restart Single Sign-On Service

Restart Single Sign-On service, **dex**, on the Cluster Leader for the configuration changes to take effect.

```
$ ssh root@<Cluster Leader IP address>
$ supervisorctl restart dex
```

5 Enable Single Sign-On

1. Log into the SevOne GUI as an **administrator**.

   > ⚠ If you are already logged in, refresh the user interface.

2. From the navigation bar, click on the **Administration** menu and select **Cluster Manager**.
3. Click on **Cluster Settings** tab.
4. Choose **Login** subtab.
5. Field **Enable Peer Certificate Verification** must be unchecked if you are using an unsigned SSL certificate.
6. Select the **Enable Single Sign-On** check box to enable Single Sign-On.
7. Click **Save** to save the Login settings.

   > ⓘ If you have followed the instructions to configure **dex** but have encountered the following error, it may be related to one of the following issues.
   >
   > | **Error** |
   > | --- |
   > | *Login did not save successfully. The following errors were reported: Single Sign-On - Invalid configuration. Please configure Dex before enabling Single Sign-On.* |
   >
   > - You may need to regenerate the SSL certificate for your appliance. Please refer to **Generate a Self-Signed Certificate or a Certificate Signing Request** guide for details on generating the SSL certificate.
   >
   > ⚠ Please make sure the Common Name when generating your certificate request matches the **OpenID-Connect Issuer URL** field on this page. It should be the appliance IP address.
   >
   > - Configured DNS server in NMS should be able to resolve the **OpenID-Connect Issuer URL**.

6 Redirect on Logout

If you only have IdP initiated login enabled, NMS has the ability to redirect externally on logout or session timeout.

Execute the following command to add the destination URL to the Cluster Leader's database.

```
$ mysqlconfig -h $cluster_master_ip -e "INSERT INTO net.settings(setting, value) \
VALUES('logout_url', '$destination_url') ON DUPLICATE KEY UPDATE value = VALUES(value)"
```

7 HSA Configuration

If the Cluster Leader fails over to its HSA, Single Sign-On will stop working. Please make sure that **dex** is not running on an HSA prior to a failover - it should be kept in ***stopped*** state. If you have **dex** running on an HSA prior to a failover, ability to login will be impaired on the entire NMS cluster.

Once the Cluster Leader fails over to the HSA, the authentication will fallback to local SevOne authentication. At this point, **dex** can be configured for Single Sign-On. And, **dex** can now be started and Single Sign-On can be enabled from the User Interface.

When the Cluster Leader fails over to the HSA, the Identity Provider configuration must be updated to point to the HSA's IP Address / hostname.

Execute the following steps to enable Single Sign-On on the HSA.

1. Fail over the Cluster Leader to the HSA.
2. Make sure the HSA has a valid **dex** config. This includes a valid **dex secret** and **dex MySQL password**. To ensure the conditions are met, run the following setup script each time a failover/takeover happens.

```
$ bash /usr/local/scripts/dex_setup_template.sh
```

> This will regenerate a bare-minimum working **dex** configuration with a valid **dex secret** and **dex MySQL password**. Update the existing **/etc/dex/config.yaml** file with the newly generated **dex secret** and **dex MySQL password**.

3. Port all configuration options from the Cluster Leader's **/etc/dex/config.yaml** file on to the HSA.

> Even if the setup script is used to generate a valid **dex** configuration, you are still required to port the configuration from the Cluster Leader.

4. Restart **dex** on the HSA.
5. Enable Single Sign-On from the graphical user interface. Execute the steps below.
   a. From the navigation bar, click the **Administration** menu and select **Cluster Manager**.
   b. Click on **Cluster Settings** tab.
   c. Click on **Login** subtab.
   d. Unselect the **Enable Single Sign-On** check box.
   e. Click **Save** to save the settings.
   f. Select the **Enable Single Sign-On** check box.
   g. Click **Save** to save the settings.

> The same steps must be taken when a failback is performed from the HSA to the Cluster Leader.

> **SevOne NMS** is using **SAML**. However, **SevOne Data Insight** is using **OpenID-Connect**.
> **dex** wraps SAML in OpenID-Connect tokens.

8 Upgrade Process

If you are upgrading from SevOne NMS 5.7.2.15, had Single Sign-On enabled, and **dex** configuration has changed, you will need to re-enable Single Sign-On. Please follow the steps below.

1. SSH into the Cluster Leader IP address.

```
$ ssh root@<Cluster Leader IP address>
```

2. Rerun the setup script.

```
$ bash /usr/local/scripts/dex_setup_template.sh
```

3. A new config will be written to **/etc/dex/config.yaml**. And, it will save the old config to **/etc/dex/config.yaml.backup**.
4. Copy and paste the custom config from **connectors** section in **/etc/dex/config.yaml.backup** to the **connectors** section in **/etc/dex/config.yaml**.

> IMPORTANT
>
> - **yaml** files are sensitive about indentations. Please be sure your indentation is correct.
> - If you had any other custom config outside of **connectors** section in the old config file, you will need to transfer that config over to the new config file as well.

5. Restart Single Sign-On service, **dex**, on the Cluster Leader for the configuration changes to take effect.

```
$ supervisorctl restart dex
```

> For **IdP** initiated login support, **Default RelayState** must be set to the NMS client ID, **sevonenms**. Please refer to Default RelayState for more details.

9 Login CSRF

Details in this section have been gathered from https://support.detectify.com/support/solutions/articles/48001048951-login-csrf. For examples and additional details, you may click on this link.

Login CSRF is a type of attack where the attacker can force the user to log in to the attacker's account on a website and thus reveal information about what the user is doing while logged in. The risk varies depending on the application and hard to detect / evaluate it. If a public registration for the application exists, the risk of an attack increases drastically as it is very easy for the attacker to create an account and thus, know the credentials for it.

Login CSRF is like any other CSRF. The only difference is that it occurs on the login form. For additional information, you may search for CSRF in general from your web browser.

To prevent Login CSRF, you must implement a token system in your code to ensure that a random token (i.e., CSRFToken) is generated which is set as a cookie and as a hidden value in the form. When the form is submitted, the code must check if the token in the form is the same as the token in the cookie and if the token matches, you will be able to log in.

The token works as a protection because the attacker does not know the value of the cookie CSRFToken and therefore, cannot send that value in the form.

10 Troubleshooting

10.1 Is DEX Running?

To identify the status of **dex** on the Cluster Leader, you must execute the following command.

> dex must be running on **Cluster Leader** and **/etc/dex/config.yaml** file must be present.

1. SSH to Cluster Leader.

```
$ ssh <Cluster Leader IP address>
```

2. The following provides the options available to check the **dex** status.

SevOne-dexctl status 'help'

```
$ SevOne-dexctl status --help

USAGE:
    SevOne CLI script to check (and fix) dex status
    /usr/local/scripts/SevOne-dexctl status [OPTIONS]

    OPTIONS:
        --autofix -a | If the status is wrong, try to fix it
        --help -h    | Print usage and exit
```

3. Execute this command to check the **dex** status.

```
$ SevOne-dexctl status
```

SevOne-dexctl status will return one of the following messages.

Example: SevOne-dexctl status > returns SUCCESS

> dex is expected to be RUNNING and it is RUNNING
>
> --- Expecting status RUNNING
> --- Supervisor status:
> --- dex RUNNING pid 16845, uptime 2 days, 14:29:11
> ✓✓✓ Status matches, all good

This indicates that you are on the Cluster Leader, /etc/dex/config.yaml file is present, and dex is RUNNING.

Example: SevOne-dexctl status > returns FAILURE

dex is expected to be RUNNING but it is STOPPED

```
--- Expecting status RUNNING
--- Supervisor status:
--- dex                    STOPPED   Oct 02 09:45 PM
!!! Status does not match, please check /var/log/dex.log for details
```

In this scenario, make sure that, you are on the Cluster Leader and /etc/dex/config.yaml file is present prior to **restarting** dex or add **--autofix** / **-a** option to **SevOne-dexctl status** command. This can be done in the following ways.

```
$ supervisorctl restart dex

OR

$ SevOne-dexctl status --autofix
```

If you are **not on Cluster Leader** but **dex** is RUNNING, **SevOne-dexctl status** will inform you that,

- dex should not be running
- dex is running
- you should stop dex

SevOne-dexctl status script does not consider if Single Sign-On is enabled.

Single Sign-On can be enabled from the SevOne NMS Graphical User Interface. Enter the URL of your Cluster Leader, from the navigation bar, click on **Administration** menu, select **Cluster Manager**, select tab **Cluster Settings**, subtab **Login**. You will see field **Enable Single Sign-On** under **Single Sign-On** section.

11 FAQs

1. What is **Default RelayState**?
   In SAML spec, the RelayState is an optional parameter. We use the Default RelayState to signify specific login journey inside **dex** and it is important to be matched by both the **IdP** configuration and the **dex config.yaml** file. Currently it is set to NMS Client ID, **sevonenms**.
   For additional details, please refer to *https://stackoverflow.com/a/34351756*

2. What is **NMS Client ID**? Why is it set to **sevonenms**?
   NMS Client ID is set to **sevonenms** but, it can be changed.
   The NMS Client ID is passed in the **Default RelayState** field from the **IdP** in order to trigger the authentication against the correct client setup in dex. This is needed as dex can support multiple different clients and we use it to distinguish an NMS specific authentication journey.

3. What is the difference between **Identity Provider Single Sign-On URL** & **Identity Provider Issuer**?
   These are provided from the **IdP** configuration and must be part of a valid IdP configuration. The customer must configure **dex** accordingly.

4. What is **x.509 Certificate**?
   This is the **IdP** provided certificate. Each IdP must have a certificate that needs to be copied on SevOne NMS box and **dex** must be configured to use it for validation purposes.

5. What does **ssoURL** & **ssoIssuer** mean in **/etc/dex/config.yaml** file?
   The **ssoURL** and the **ssoIssuer** must be provided by the **IdP**. These are customer specific and must be configured by the customer. If the customer has a working IdP configuration then, they should be able to specify the ssoURL and ssoIssuer from the IdP configuration.

6. What does **redirectURI** & **entityIssuer** mean in **/etc/dex/config.yaml** file?
   The **redirectURI** and **entityIssuer** must point to the NMS Cluster Leader's IP address. **redirectURI** is a URL that handles the login authentication. The user will be redirected here from the **Identity Provider** so, the URL must be reachable.
   For example, https://10.168.128.11/sso/callback, where 10.168.128.11 is the <Cluster Leader IP address>.

7. How can I determine if I have **only IdP initiated login enabled**?
   IdP relates to a specific SAML workflow. Generally, this is what most customers will use and it depends on their requirements. Service Provider initiated login is also available through **dex** but it has to be configured accordingly.

8. Does SevOne support SHA-256 or higher certificate signing algorithm?
   Yes.

9. What are the certificate signing options?
   Applications can only sign SAML assertions.

10. What is the requirement for IdP?
    Base64-encoded and URLs.

11. Is Service Provider Metadata required?
    No.

12. Is SAML JIT support required?
    No.

13. Is User Provisioning support required?
    No.

12 References

- https://www.identityserver.com/articles/the-dangers-of-saml-idp-initiated-sso