Vertiv™ Liebert® SiteScan™ Web

Single Sign-On (SSO) Add-On Technical Note

AUGUST 2024

Technical Note Section Outline

1. Overview

The Single Sign-On add-on allows you to use an Identity Provider of your choice to access your BAS system. The Identity Provider's authentication functions concurrently with the traditional BAS sign-in. The SSO add-on can be configured to use SAML or OIDC. Refer to the following sections to properly configure and log in using SSO.

NOTE: The SSO add-on is only available for systems running firmware version 9.0 or later.

2. Requirements

To successfully configure the SSO add-on, you must complete the following requirements:

- Run firmware version 9.0 or later with the latest cumulative patch applied on your system.
- Download the sso.addon file.
- Download the SSO license.
- Backup your system regularly to ensure the add-on's data is also backed up.
- Ensure there is adequate disk space available to store the add-on's data.
- After installing the add-on, configure the SSO add-on in SiteBuilder (see section 3).
- Configure the add-on to use SAML or OIDC (see section 4 or 5, depending on your selection).
- Map the Identity Provider email.

NOTE: If you need additional assistance, please contact your Vertiv Technical Support representative.

3. Configuring the SSO Add-on in SiteBuilder

Before using the SSO add-on, you must configure the system in SiteBuilder using the following procedure.

To configure the SSO add-on in SiteBuilder:

1. Download and install the add-on.
2. In SiteBuilder, navigate to the *Configure – Preferences* page.
3. On the Web Server tab, open Authentication Provider and click *ssoauthclient*.
4. Click *Apply*, and then click *OK*.

5. Log into the BAS system locally as an Administrator to continue setting up the SSO add-on. The add-on can now be configured to use SAML or OIDC.

4. Configuring the SSO Add-on for SAML

To configure the SSO add-on to use SAML, you must first verify the required Identity Provider Configurations for SAML, and then set up the SSOAuthclient Addon (Service Provider). Both tasks are described in the following sub-sections.

Verify the Required Identity Provider Configurations for SAML

The Identity Provider must have the following configurations for successful login through SAML via the SSO add-on:

- Single sign-on URL and Single Logout URL of the service provider.
    - For example: `http or https://<your BAS domain>/~index`
    - **NOTE: If your SAML Identity Provider only supports HTTPS Single Sign-On and Single Logout URLs, you must configure the BAS to use HTTPS.**
- Audience URI (SP Entity ID)/SP Issuer is a unique identifier that should also be passed to the SSO add-on configuration.
- SAML Authentication Response and Assertion from the Identity Provider must be signed with an SHA256 Signature Algorithm.
    - Encryption and Signature Certificate: A X509 public certificate and its private key must be generated and maintained by the administrator to encrypt the SAML assertion and sign logout requests. The public certificate must be uploaded to the Identity Provider's Encryption Certificate and Signature Certificate fields. The public certificate and private key are required for the add-on's Service Provider Public Certificate and Service Provider Private Key fields.
    - OpenSSL is one method to create the X509 Service Provider Public Certificate and Private key. The OpenSSL example below generates the X509 certificate and private key. The certificate and key expire in 365 days.
        - For example: `openssl req -x509 -nodes -days 365 -new -out<your-public-certificate-name>.crt`
        - **NOTE: The expiration days and name of the public certificate can be modified.**
- Assertion must be encrypted, and the public X.509 certificate (generated by the Administrator) must be uploaded to the Identity Provider's Encryption certificate field.
- If a Logout Request signature is required by the Identity Provider, the same public X.509 certificate used for encryption (generated by the administrator) must be uploaded to the Identity Provider's Signature Certificate field.
- The Identity Provider should not Verify Request Signatures because the Authentication Request generated by the SSO add-on is not signed.
- The ACS URL/ Single sign-on URL configured on the SAML Identity Provider is used for redirecting the Authentication response/assertion back to the Service Provider instead of the ACS URL on the Authentication Request.
- SAML Assertion NameId should return the email address of the user, which is mapped in the BAS. (Identity Providers may do this by default, but it can be changed by the Identity Provider administrators).

Set Up SSOAuthclient Addon (Service Provider)

To configure the SSO add-on to use SAML:

1. Log into the BAS as an Administrator.
2. From the System Options tree, click *System Settings*.
3. Navigate to *Add-ons – Details – Main Page*.
4. Click *SAML*.
5. Enter the required information as described in Table 1.1 SAML Service Provider Configurations.
6. Click *Apply*. You are now ready to map the Identity Provider email to an Operator in the BAS (see section 6).

Table 1.1 SAML Service Provider Configurations

IN THIS FIELD...	ENTER THIS INFORMATION...
Identity Provider Issuer	Identity Provider Entity ID/ Issuer (provided by the Identity Provider)
Identity Provider Single Sign-On URL	Provided by the Identity Provider Also referred to as "SP-Initiated Redirect Endpoint"
Identity Provider Single Logout URL	Provided by the Identity Provider
Identity Provider X.509 Certificate	Copy and paste the contents of your identity provider's X.509 certificate. (provided by the Configure the Identity Provider to sign the SAML response and assertion with SHA256 sig
Service Provider Entity ID/ Issuer.	Audience URI (SP Entity ID) Also referred to as "Audience URI" or "Audience Restriction"
Service Provider Assertion Consumer Service (ACS) URL	`http or https://<your BAS domain>/~index` Also referred to as "Redirect or login" URL
Service Provider Single Logout URL	`http or https://<your BAS domain>/~index` Also referred to as "Redirect or logout" URL
Service Provider X.509 Public Certificate	Copy and paste the contents of the X509 public certificate that was generated for the En Certificate. **NOTE Authentication requests are not signed by this service provider.**
Service Provider Private Key field	The contents of the private key that was generated. **NOTE Authentication requests are not signed by this service provider.**

5. Configuring the SSO Add-on for OIDC

Verify required Identity Provider Configurations for OIDC. The ID token must include the “email” claim, which is usually part of the standard OIDC claims.

To configure the SSO add-on to use OIDC:

1. Log in to the BAS as an Administrator
2. From the System Options tree, click *System Settings*.
3. Navigate to *Add-ons – Details – Main Page*.
4. Click *OIDC*.
5. Enter the required information as described in Table 1.2 OIDC Service Provider Configurations.
6. Click *Apply*. You are now ready to map the Identity Provider email to an Operator in the BAS (see section 6).

Table 1.2 OIDC Service Provider Configurations

IN THIS FIELD...	ENTER THIS INFORMATION...
Token URL	Token endpoint from Identification Provider
Authorize URL	Authorization endpoint from Identification Provider
Logout URL	Logout endpoint from Identification Provider
Public Keys URL	JWKS / Public keys endpoint from Identification Provider
Client ID	Client ID from Identification Provider
Client Secret (Optional)	Client Secret from Identification Provider
Redirect on Login	`http or https://<your BAS domain>/~index`
Redirect on Logout	`http or https://<your BAS domain>/~index`

6. Mapping the Identity Provider Email to an Operator

To map the Identity Provider email to an Operator:

1. From the System Options tree, click *Operators*.
2. Click *Add* to add a new Operator.
3. Create a new Operator using your Identity Provider email address in the Login Name field.
4. Open Sign-On Mode and click *Single Sign-On*.

   NOTE: No password is required for this Operator. Password requirements are handled by Identity Provider.
5. Click *Accept*. You are now ready to log into the BAS using the Identity Provider.

7. Logging into the BAS using SSO

After completing all configurations for SSO and mapping for the Identity Provider email, you can now log into the BAS with SSO.

NOTE: If desired, local login is available using Login Name and Password. The SSO add-on does not interfere with local login or existing operator configurations.

To log into the BAS using SSO:

1. From the Login page of the BAS, click *Log in with Single Sign On*.

   NOTE: When using SSO, do NOT enter a local Login Name or Password and do NOT click *Log in*.

2. Log in using the Identity Provider login process.
3. When prompted to log in using the SSO Operator name, verify that the name is correct.
4. Click *Yes*.