Single Sign On (SSO) Add-on User's Guide

v1.0 for 9.0 systems and later

Catalog No. 11-808-1066-01

Rev. 6/12/2024

⚠ Important changes are listed in Document Revision History at the end of this document.

All rights reserved. All trademarks are the property of their respective owners.

The content of this guide is furnished for informational use only and is subject to change without notice. Carrier assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Contents

What is the Single Sign On (SSO) add-on?

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 *in addition to* the traditional BAS sign-in.

The SSO addon can be configured to use *SAML* or *OIDC*.

Requirements

- You are running a v9.0 or later (or Cloud) system with the latest cumulative patch applied
- You have downloaded sso.addon file
- You have purchased and downloaded the SSO license
- Your system is backed up regularly to ensure the add-on's data is also backed up
- You have adequate disk space available to store the add-on's data
- After installing the add-on, you must *Configure the SSO add-on in SiteBuilder* (page 1)
- You have configured the add-on to use *SAML* (page 2)or *OIDC* (page 4).
- You have *Mapped your Identity Provider email* (page 4)

See "Installing an Add-on User Guide" for the following:

- Installing an add-on
- Applying a license
- Running an add-on
- Upgrading an add-on

Configuring the SSO add-on in SiteBuilder

Before you can use the SSO add-on, you must configure your system in SiteBuilder.

1 Download and install the add-on.

2 In SiteBuilder, go to **Configure** > **Preferences**.

3 On the **Web Server** tab, open **Authentication Provider** and select **ssoauthclient**.

4 Click **Apply**, and then click **OK**.

5 Log in to your BAS system locally as Administrator to continue setting up the SSO add-on. You can now configure the add-on to use *SAML* (page 2)or *OIDC* (page 4).

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company

Configuring the SSO add-on for SAML

Follow the steps below to configure the SSO add-on for use with SAML.

1. *Verify required Identity Provider Configurations for SAML* (page 2).
2. *Set up SSOAuthclient Addon (Service Provider)* (page 3)

Verify required Identity Provider Configurations for SAML

The identity provider needs to have the following configurations for the user successfully login through SAML via the SSO addon.

- **Single sign-on URL and Single Logout URL of service provider**: 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 BAS must be configured to use HTTPS.
- **Audience URI** (SP Entity ID)/SP Issuer: This unique identifier should also be passed to the SSO Addon configuration.
- **SAML Authentication Response and Assertion** from the Identity Provider must be signed with a 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**.
  - One method you can use to create the X509 Service Provider Public Certificate and Private key is OpenSSL. The OpenSSL example below generates the X509 certificate and private key. The certificate and key expire in 365 days.

    NOTE The expiration days and name of the public certificate can be modified.

    ```
    openssl req -x509 -nodes -days 365 -new -out
    <your-public-certificate-name>.crt
    ```
- **Assertion**: The 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.
- **Logout request**: If the Identity Provider requires the Logout request to be signed, 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 since the Authentication Request generated by the SSO addon is not signed.
- **ACS URL/ Single sign-on URL**: The ACS URL/ Single sign-on URL configured on the SAML Identity Provider is used for redirecting the Authentication response/assertion back to Service Provider instead of the ACS URL on the Authentication Request.
- **SAML Assertion NameId**: The SAML Assertion NameId should return the email address of the user which is mapped in your BAS. (Identity Providers may do this by default, but it can be changed by the Identity Provider administrators).

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company

Set up SSOAuthclient Addon (Service Provider)

1. Log in to your BAS as Administrator.
2. On the **System Options** tree, select **System Settings**.
3. Go to the **Add-ons** tab. Under **Details**, click **Main Page**.
4. Select **SAML**.
5. Enter the required information described below.

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 Identity Provider) Configure the Identity Provider to sign the SAML response and assertion with SHA256 signature algorithm.
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 **Encryption and Signature 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.

6. Click **Apply**.
7. You must now *Map your Identity Provider e-mail to an Operator* (page 4) in your BAS.

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company

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.

Follow the steps below to configure the SSO add-on for use with OIDC.

1. Log in to your BAS as Administrator.
2. On the **System Options** tree, select **System Settings**.
3. Go to the **Add-ons** tab. Under **Details**, click **Main Page**.
4. Select **OIDC**.
5. Enter the required information described below.

In this field...	Enter this information...
Token URL	Token endpoint from your Identification Provider
Authorize URL	Authorization endpoint from your Identification Provider
Logout URL	Logout endpoint from your Identification Provider
Public Keys URL	JWKS / Public keys enpdoint from your Identification Provider
Client ID	Client ID from your Identification Provider
Client Secret (Optional)	Client Secret from your Identification Provider
Redirect on Login	`http` or `https://<your BAS domain>/~index`
Redirect on Logout	`http` or `https://<your BAS domain>/~index`

6. Click **Apply**.
7. You must now *Map your Identity Provider e-mail to an Operator* (page 4) in your BAS.

Mapping Identity Provider e-mail to an Operator

1. On the **System Options** tree, select **Operators**.
2. Click **Add** to add a new Operator.
3. Create a new Operator as described in your *BAS User Manual*, using your Identity Provided e-mail address in **Login Name**.
4. Open **Sign On Mode** and select **Single Sign On**.

   NOTE No password is required for this Operator. Password requirements are handled by your Identity Provider.
5. Click **Accept**.
6. You are now ready to *log in to your BAS* (page 5) using your Identity Provider.

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company

Logging in to your BAS using SSO

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

NOTE Do not enter in your local **Login Name** or **Password**. Do not click **Log in**.

2 Log in using your Identity Provider login process.

3 When prompted to log in using the SSO Operator name, verify the name is correct and then click **Yes**.

NOTE If desired, you can still log in locally using **Login Name** and **Password**. The SSO add-on does not interfere with local log on or existing Operator configurations.

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
		No updates yet	

* For internal use only

All trademarks used herein are the property of their respective owners.

© 2024 Carrier. All rights reserved.
A Carrier Company