Implementing single sign-in

This topic only applies to the On-Demand version of RapidResponse.

Print

If your company already has a single sign-in environment that uses an identity provider with SAML2 authentication, you can integrate RapidResponse into this environment. User accounts must be the same in RapidResponse and your identity provider.

To integrate RapidResponse with your identity provider, each program's federation metadata can be provided for the other. This metadata is an XML file that describes how the application and identity provider can interact with each other. Your identity provider's metadata must be provided to Kinaxis Customer Support, and the RapidResponse metadata must be provided or imported to your identity provider.

Using the information specified in the metadata, the identity provider can process authentication requests coming from RapidResponse, and RapidResponse can process responses coming from the identity provider. A trust relationship is established between the identity provider and RapidResponse using the metadata, so the user can sign in to RapidResponse using the identity provider's information.

To improve security, the requests and responses between RapidResponse and the identity provider can be encrypted using HTTPS. You can also encrypt SAML assertions using public key encryption with x.509 certificates. These certificates can be configured by Kinaxis Customer Support.

When users sign in using the identity provider, their sign-in experience is provided by that system. Accessing RapidResponse launches the identity provider's authentication, which allows the user to sign in to RapidResponse.

Implementing an SSI environment using SAML2 authentication includes the following steps:

1. Create RapidResponse user accounts that are mapped to the user accounts defined in the identity provider. For more information, see User accounts for SAML2 authentication (step 1).
2. Obtain the metadata from the identity provider. For more information, see Obtaining the identity provider metadata (step 2).

3. Obtain the metadata from RapidResponse for use in the identity provider. For more information, see Obtaining RapidResponse metadata (step 3).
4. Provide users with the link to sign in to RapidResponse. For more information, see Providing the link to sign in to RapidResponse (step 4).

User accounts for SAML2 authentication (step 1)

When SAML2 authentication is used, the identity provider returns a NameID to RapidResponse, which must map to a RapidResponse user ID. Even though a password is required when creating a user account, SAML2 authentication does not require a user's RapidResponse password to sign in. Because the password is not used to sign in, you can choose to not tell users what their RapidResponse passwords are.

Because users do not know their passwords, the passwords should be set to never expire and the users should not be allowed to change their passwords. If a password expires, the user will be unable to change it or sign in, and might be locked out of RapidResponse. If the password can be changed, the user is prompted to change the password the first time they sign in to RapidResponse.

If your company is installing RapidResponse for the first time, you should ensure that for each user you create, the RapidResponse user ID is available as a NameID from your identity provider.

If your company is upgrading RapidResponse, your existing user accounts might not be appropriate for your identity provider. In this case, you can copy each user and give the copy a user ID that matches the NameID available from your identity provider. For more information about copying users, see To duplicate a user account from the Administration pane.

If you delete a user account from the identity provider, you should also delete the user in RapidResponse. Deleted users will be unable to use SSI, but can still sign in to RapidResponse using their user ID and password if the password is known.

Obtaining the identity provider metadata (step 2)

Depending on your identity provider, the metadata might be available from a publicly accessible URL, or you might need to export it to a file. For information about how to obtain the metadata, consult your identity provider's documentation.

After you have obtained the metadata URL or file, you must provide it to Kinaxis Customer Support. If the metadata is available as a URL, you must ensure that URL is accessible outside your company's firewall. For more information, contact your network administrator.

Obtaining RapidResponse metadata (step 3)

The metadata required to integrate RapidResponse with the identity provider can be found in the following location:

`https://rapidresponse.kinaxis.com/CompanyID/saml2.metadata`

or

`https://region.kinaxis.net/CompanyId/saml2.metadata`

Where `CompanyID` is your company's identifier as provided by Kinaxis and `region` is the region code of your RapidResponse URL.

Depending on your identity provider, you can either include this URL directly in your identity provider, or you can save the metadata as an XML file and then import it. For information about including this information in your identity provider, consult your identity provider's documentation.

Providing the link to sign in to RapidResponse (step 4)

After SSI has been set up and the metadata for each program integrated, you can provide users with a link that allows them to automatically sign in to RapidResponse with their authenticated identities. Users who click the link are allowed to sign in if they are authenticated by the identity provider.

Users can sign in using the following links:

Client	URLs

Java client	`https://rapidresponse.kinaxis.com/CompanyID/saml2`
	or
	`https://region.kinaxis.net/CompanyId/saml2`

Web client	`https://rapidresponse.kinaxis.com/Web/CompanyID/saml2`
	or
	`https://region.kinaxis.net/web/CompanyId/saml2`

Mobile client	`https://rapidresponse.kinaxis.com/Mobile/CompanyID/saml2`
	or
	`https://region.kinaxis.net/mobile/CompanyId/saml2`

Where `CompanyID` is your company's identifier as provided by Kinaxis and `region` is the region code of your RapidResponse URL.

Allowing users to use prompted sign in

Users who receive their RapidResponse messages in their email can click resource links, which opens the resource in RapidResponse. If the user does not have RapidResponse open when they click the link, it is launched and they are signed in. By default the user is signed in automatically, but you can choose to require users to enter their credentials. This allows you to ensure only valid users can access RapidResponse by clicking these links.

If you allow users to provide credentials, each user must know their RapidResponse password. However, they will only need to enter their password when they launch RapidResponse from a resource link or if they sign out.

To request users be allowed to provide their credentials, contact Kinaxis Customer Support.

This topic is part of the the *RapidResponse Administration Help*.

SEND FEEDBACK