Configuring / Preparing to retrieve SOAP web services input / Using a SOAP web service to authenticate with an application

Using a SOAP web service to authenticate with an application

SOAP web service input device and notification objects can use a SOAP web service to authenticate with an application. RICOH ProcessDirector supports both API key and session authentication. Input device objects authenticate when they poll for input. Notification objects authenticate when they send status to the application.

For API key authentication, you put an authorization code in a **Static credential** property or define an HTTP user ID and password. The authorization code or the HTTP user ID and password is sent to the web service that exchanges data. The web service then authenticates with the application and returns a response.

For session authentication, you put authentication credentials (user ID and password) and other values in a set of authentication request properties. The input device or notification first calls a SOAP web service to authenticate with the application. After a successful authentication, the web service returns a token to the input device or notification. The token is transmitted in the call to the web service that exchanges data.

- If the application allows one session per user, set up your objects to call the web services with different user IDs and passwords.
- Session authentication occurs with every web service call and logging out is not required. Make sure that the length of the session for each set of credentials is shorter than the time between calls to the web service. For example, the session for an input device expires after 10 minutes. When you configure the input device, specify a polling interval greater than 10 minutes.

To get an API key or authentication credentials for an application, contact the company that hosts the application. For format and syntax requirements, refer to the documentation of the application.

To use a SOAP web service to authenticate:

1. Click the **Authentication** tab on the SOAP web service input device or notification.
2. Follow the instructions for the type of authentication that the application requires:
   - For API key authentication, specify the authentication code as the value of the **Static credential** property.
     Leave all the other properties blank. You have completed this procedure.
   - For session authentication, leave the **Static credential** property blank. Go to the next step and specify the other properties.
3. Set the **Authentication request URL** property to the URL that RICOH ProcessDirector uses to authenticate with the application.
   If the application requires authentication credentials in the URL, specify them using the required format and syntax.
4. For the value of the **Authentication request payload** property, specify the body of the web services request that the input device or notification submits to the application for authentication.
   In these examples, the payload includes three elements: `<Credentials>`, `<Name>`, and `<Password>`. The value of the `<Password>` element is a symbol that uses the **Authentication request password** property.
   This example uses the **Authentication request password** property for input devices:
   `<Credentials> <Name>myname</Name> <Password>${WebService.AuthRequestPwd}</Password></Credentials>`
   This example uses the **Authentication request password** property for notifications:
   `<Credentials> <Name>myname</Name> <Password>${WSNotification.WebService.AuthRequestPwd}</Password> </Credentials>`
   The symbol is resolved when the authentication request is sent.
5. Set the **Authentication SOAP request** property to the SOAP request that RICOH ProcessDirector created when you imported the WSDL file.

   For example, you want to use the **AuthenticateUser** SOAP request. You prepended **PrintShop** to the names of the SOAP requests when you imported them. Select **PrintShop-AuthenticateUser**.
6. Set the **Authentication response attribute** property to the XPath expression that identifies the credential for the session in the response from the web service.
7. Set the **Authentication request password** property to the password for your account with the application.
   The password is encrypted when it is stored in RICOH ProcessDirector.

For both API key and session authentication, RICOH ProcessDirector stores the static credential or token returned from the application in a property.

- For input devices, the property is **WebService.Credential**.
- For notifications, the property is **WSNotification.WebService.Credential**.

When you specify values on the **Request** tab for a SOAP web service input device or notification, you specify the **WebService.Credential** or **WSNotification.WebService.Credential** property as a symbol.

RICOH ProcessDirector substitutes the value of the static credential or token for the symbol when it transmits the request to the web service.

Now that you have specified the values required to authenticate with the application, complete the steps for defining and configuring the input device or notification. Return to one of these topics:

- Preparing to retrieve SOAP web services input.
- Preparing to send status to a SOAP web service.

Parent topic: Preparing to retrieve SOAP web services input