Genesys Intelligent Automation Help

Two-factor Authentication

4/2/2026

Contents

Two-factor Authentication

The two-factor authentication MicroApp adds an extra layer of security to a self-service application.

Use case: After customers provide an account number as a form of identification, they're asked to enter a code that was delivered to them via email or SMS, or one they accessed via an external authentication application, such as Google Authenticator.

Intelligent Automation supports two types of two-factor authentication:

- Internal authentication - Intelligent Automation generates a code internally and delivers the code to the user's verified email address or phone number (SMS).
- External authentication - Customers use their own systems to authenticate a user.

Internal authentication

With internal authentication, Intelligent Automation generates a code internally and delivers the code to the user's verified email address or phone number (SMS).

The process is as follows:

1. If the user has more than one verified contact method, Intelligent Automation prompts the user to select an authentication method. For example, Press 1 to receive the code via email. Press 2 to receive the code via SMS. If the user has only one verified contact method, Intelligent Automation skips to Step 3 in this process.
2. The user enters a response.
3. Intelligent Automation generates the code and delivers it to the user's preferred contact method (SMS, for example).
4. Intelligent Automation prompts the user to enter the code.
5. When the user enters the code, Intelligent Automation checks the code and its timestamp.
6. If the code and timestamp are valid, Intelligent Automation grants access. If the code or timestamp is invalid, Intelligent Automation generates and send another code and prompts the user to enter the new code. It does this until the **Maximum Attempts at Sending an Authentication Code** value is reached.

Configuring contact methods

Email

Configure the following server settings to enable Email communication:

- Email.SMTP.Host – The hostname of the customers SMTP server.
- Email.SMTP.Port – The port number on which the SMTP host is running.

SMS

Configure the following server settings to enable SMS communication:

- SMS.Method – The type of request required by the customers SMS Gateway e.g. POST
- SMS.URL – The URL for the customer's SMS gateway
- SMS.RequestHeaders – any headers which need to be sent in the format "HeaderName1:HeaderValue1","HeaderName2:HeaderValue2" etc. Can be blank
- SMS.RequestBody – anything which needs to be included in the request body. This is specific to each customer's own setup and can be blank.
- SMS.Timeout – Time in milliseconds to wait before declaring an error in contacting the SMS gateway
- SMS.PlusSymbolBeforeRecipientNumber – true or false. Determines whether we need to add a "+" symbol to the recipient number before attempting to send

External authentication

With external authentication, Intelligent Automation hands the code generation and verification process over to an external authentication application, such as Google Authenticator. In this case, Intelligent Automation skips the **send code** web service.

The process is as follows:

1. If the user has more than one verified contact method, Intelligent Automation prompts the user to select an authentication method. For example, Press 1 to receive the code via email. Press 2 to receive the code via Google Authenticator. If the user has only one verified contact method (in this example Google Authenticator), Intelligent Automation skips to Step 3 in this process.
2. The user enters a response.
3. The user retrieves the code from the external application and enters it into the Intelligent Automation application
4. Intelligent Automation checks with the external application that the code is valid.
5. The external application returns a the validation result (for example **success**).
6. If the result is successful (i.e. the code is valid), Intelligent Automation grants access. If the result is unsuccessful (i.e. the code is invalid), Intelligent Automation prompts the user to enter another code, until the **Maximum Attempts at Sending an Authentication Code** value is reached.

Web service details

For both internal and external authentication, web service calls are made to either verify a contact method or to send and verify an authentication code. This section describes the available web

services. **Note**: You can write your own wrapper web service or use Intelligent Automation Integration Hub.

Check Verified Contact Methods Web Service

This web service applies to both internal and external authentication.

The web service should return XML in the following format:

```
<checkVerifiedContactMethods>
                    <status>success</status>
                    <methods>
                           <method name="email" value="youremail@genesys.com"/>
                           <method name="authenticator"/>
                           <method name="SMS"/>
                    </methods>
</checkVerifiedContactMethods>
```

- **Status** - The values **success** and **not found** indicate whether the information was found.
- **Methods** - Describes which valid contact methods are available to the customer. The options are **email**, **SMS** or **authenticator**. You can assign an optional value to either **email** or **SMS** and those variables will be configured with that value on the **Settings** page. Using the example above, if **Variable Name for Customer Email Address** is set to **CustomerEmail** on the Settings page, then Intelligent Automation sets a variable called **CustomerEmail** to **youremail@genesys.com**. If you don't assign a value, Intelligent Automation assumes the variable is already set.

Send Authentication Code Web Service

This web service applies to external authentication only.

Use the request parameter **TwoFactorAuthSelectedMethod**. This parameter will tell the web service which method the customer selected (Email, SMS, or Authenticator).
Expected XML response:

```
<sendAuthenticationCode>
                <status>success</status>
</sendAuthenticationCode>
```

Intelligent Automation only checks for a **success** or **incorrect code** status, but the <status> parameter can contain any valid path, such as **error** to indicate that an attempt to send an authentication code has failed.

Code Authentication Web Service

This web service applies to external authentication only.

Use the request parameter **authCode_nbest1**. This parameter contains the code that the customer entered. The web service checks this against the code sent out previously.
Expected XML response:

```
<codeAuthentication>
                <status>success</status>
</codeAuthentication>
```

Intelligent Automation only checks for a **success** or **incorrect code** status, but the <status> parameter can contain any valid path, such as **error** to indicate that an attempt to send an authentication code has failed.

Enabling Two-factor Authentication

Two-factor Authentication settings are enabled on the **Applications > Two Factor Authentication Settings** page in the Intelligent Automation user interface.

Setting	Description
Contact Methods and Behavior	
Variable Name for Customer Email Address	The user's verified email address.
Variable Name for Customer Phone Number	The user's verified phone number.
Behaviour if No Verified Contact Method Available	The name of a valid path in the callflow (for example, **agent**). This can be either a default path or a path coming from the Link block that calls the MicroApp.
Maximum Attempts at Sending an Authentication Code	The maximum number of times that Intelligent Automation generates and delivers a new code.
Behaviour After Exceeding Maximum Code Send Attempts	The name of a valid path in the callflow (for example, **agent**). This can be either a default path or a path coming from the Link block that calls the MicroApp.
Maximum Attempts at Verifying an Authentication Code	The maximum number of times that Intelligent Automation will process a verification request for a single authentication code.
Behaviour After Exceeding Maximum Code Verification Attempts	The name of a valid path in the callflow (for example, **agent**). This can be either a default path or a path coming from the Link block that calls the MicroApp.
Skip Options	If a user has passed authentication and the application returns to the module at any point, the application will not attempt to go through the verification process again.
Code Generation Options	
Select an option for the code generation	Options are Internal and External.
External Code Generation Options	
Prompt Wording	Enter the name of the external authenticator application (for example, Google Authenticator).
Web Service details	Provide the Web Service URL for test calls and production calls. For external authentication, the web services are as follows: • Check Verified Contact Methods Web Service • Send Authentication Code Web Service

Setting	Description
	• Code Authentication Web Service Refer to the Web service details section above for more information.
Web Service Timeout (milliseconds)	When this value is reached, the code is no longer valid. When setting this value, consider the time it takes for the user to retrieve the code and the time it takes to enter it.
Internal Code Generation Options	
Number of digits for the Generated Code	Intelligent Automation automatically updates the callflow according to the value specified here. Important For external authentication, Intelligent Automation isn't privy to this information, so you need to manually change the grammar settings for **Enter Code** in the same way you would for other MicroApps.
Web Service details	Provide the Web Service URL for test calls and production calls for the following web service: • Check Verified Contact Methods Web Service Refer to the Web service details section above for more information.
Internal Code Expiration Time (minutes)	When this value is reached, the code is no longer valid. When setting this value, consider the time it takes for the user to receive the code and the time it takes to enter it.
• Email Address 'From' • Email Subject • SMS Number 'From'	Sender information that appears in the email or text message to the use