



Agent Single Sign-On

Contents

What is Agent Single Sign-On (SSO)?	3
JWT SSO	3
Enable JWT SSO in your Comm100 Account	3
User Management after Enabling JWT SSO	5
Log into your Comm100 account with SSO	5
Technical Implementation Details	6
JWT Algorithm and Token Type	7
JWT Attributes	7
Comm100 JWT SSO endpoint	8
Remote Login URL Parameter (redirect_url)	8
Code examples for JWT SSO Implementation	8
SAML SSO	9
Enable SAML SSO in your Comm100 Account	9
User Management after Enabling SAML SSO	11
Log into your Comm100 Account with SSO	11
Technical Implementation Details	13
Required user attributes	13
Assigning an identity provider for Comm100	13
Configuring the SAML server for Comm100	14
Agent SSO FAQ	15

What is Agent Single Sign-On (SSO)?

Comm100 Agent SSO allows your agents to use a single set of login credentials to access Comm100 as they do for other business applications in your technology stack. You only need to log in once to move securely between Comm100 and other applications without the need to log into separate accounts or remember multiple usernames and passwords. Comm100 supports Agent SSO via JWT (JSON Web Token) or SAML (Security Assertion Markup Language) standards.

JWT SSO

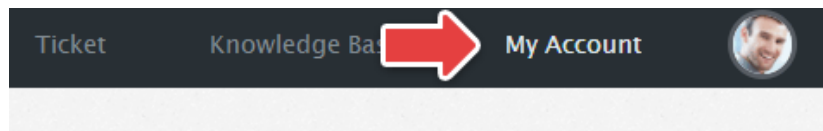
You will require the following information from your IT team:

- The remote login URL for your JWT service where Comm100 will redirect your agents for remote authentication.
- (Optional) The remote logout URL where comm100 can redirect users after they sign out of Comm100.

You may require some additional information from Comm100 to configure the JWT authentication system. Please refer to the Technical Implementation Details at the end of this section.

Enable JWT SSO in your Comm100 Account

1. Log into your Comm100 Control Panel and navigate to the My Account module.



2. Click Security on the left, and enable Agent Single Sign-On.



3. Switch to JWT SSO and fill in the required information.

As mentioned above, please collaborate with your tech team to get the JWT Remote Login URL and Remote Logout URL. The Shared Secret is randomly generated the moment you enable JWT SSO. This is a shared secret token between you and Comm100. Your tech team will need this token for JWT authentication.

You can also find the SSO login URL displayed on the setup page. Share this link with your agents as they will need it to log into Comm100 once you set up Agent SSO.

Agent Single Sign-On

Comm100 Agent SSO allows your agents to have a single login across Comm100 and other applications. You only need the need to log into separate accounts and remember multiple usernames and passwords. Comm100 supports Agent SSO.

Enable YES

Once Agent SSO is set up, your agents can log into the Comm100 account with SSO via the following link:
https://[redacted]/AdminManage/LoginSSO.aspx?:[redacted]

SAML SSO

JWT SSO

Agent use the SSO service via JWT to log into the Comm100 account. [Learn more](#)

Remote Login URL: *

This is the URL that Comm100 will redirect your agents to for remote authentication.

Remote Logout URL:

This is the URL that Comm100 will redirect your agents to after they log out.

Shared Secret: [Reset](#)

This is the shared secret token between you and Comm100.
Copy and paste it where your JWT server uses for authentication.


[Save Changes](#) [Discard](#)

4. Click Save Changes to complete the setup.

User Management after Enabling JWT SSO

After you enable Agent SSO, please note the following:

- Only the account administrator can use their Comm100 email and password to log into their Comm100 account once JWT authentication has been enabled. Other users can only sign in via the enabled SSO platform and they cannot update or reset their Comm100 password.
- Agents will only be able to sign in via SSO once the account administrator creates an agent account with an email address that matches their email in your SSO platform. If they try to login to Comm100 using their Comm100 credentials, they will see this message:



Error signing into the account

Please note that with Agent SSO enabled, non-admin agents can only login via SSO. To do so, please click the Sign in with custom SSO link below.


Log into your Comm100 account with SSO

After you enable agent SSO and connect Comm100 to your SSO platform, your non-admin agents will need to log into Comm100 via your SSO service.

1. **Go to your account User Sign-In page.**
2. **Click Sign in with Custom SSO.**

User Sign in

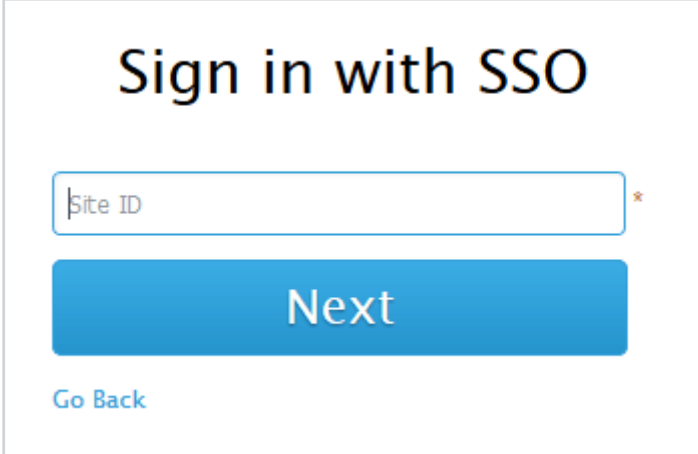
 *
 *
 Auto Login [Forgot your password?](#)

or
[Sign in with custom SSO](#) 

3. Provide your Comm100 Site ID and click Next.

Note: As mentioned in the previous section you can find the complete SSO login URL which includes the Comm100 Site ID in the JWT SSO configuration page of the Comm100 control panel. Example:

<https://hosted.comm100.com/adminmanage/LoginSSO.aspx?siteid=1000124>



The screenshot shows a web form titled "Sign in with SSO". It contains a text input field with the placeholder text "Site ID" and a red asterisk to its right. Below the input field is a large blue button with the text "Next". At the bottom left of the form is a link that says "Go Back".

4. Comm100 redirects you to the JWT configured login system.

5. If you've already signed in to your own login system, you will be authenticated and logged into your Comm100 account automatically. If you are not yet signed in to the JWT configured system, log into that system first and you will be authenticated for access Comm100.

Technical Implementation Details

This section provides implementation details for your IT team on the following elements:

- JWT Algorithm and Token Types
- JWT Attributes
- Comm100 JWT SSO endpoint
- Remote Login URL Parameter (redirect_url)
- Code examples for JWT SSO Implementation

JWT Algorithm and Token Type

Please specify HS256 as the JWT algorithm in the header of your JWT payload. HS256 indicates that this token is signed in using HMAC-SHA256.

```
{  
  "typ": "JWT",  
  "alg": "HS256"  
}
```

JWT Attributes

An email address is required for Comm100 to uniquely identify the user. Using the attributes listed in the table below, you can send additional user profile data which will be synced between your JWT login system and Comm100.

Attribute	Required	Description
email	Yes	Email of the user being signed in. It is used to identify the user record in Comm100.
name	No	The name of a user. The user in Comm100 will be created or updated accordingly.

Comm100 JWT SSO endpoint

After successfully authenticating the user, redirect the user along with the JWT payload to the Comm100 endpoint: https://<portal_domain>/adminwebservice/SSO/SSOJWTConsumer.aspx

If your live chat is on our hosted cloud platform, you can check the example URL below:

<https://hosted.comm100.com/adminwebservice/SSO/SSOJWTConsumer.aspx>

The payload should be base64-encoded and appended to the URL as a query string. The JWT payload must be sent to your Comm100 system using the https protocol. Here is an example:

https://<portal_domain>/adminwebservice/SSO/SSOJWTConsumer.aspx?jwt={payload}

Remote Login URL Parameter (redirect_url)

When Comm100 redirects a user to your remote login page, it also passes a URL parameter named 'redirect_url'. The parameter contains the page to which Comm100 will return the agent after authentication. Append the parameter (name and value) to the Comm100 JWT endpoint.

Code examples for JWT SSO Implementation

You can find [JWT SSO examples in our GitHub repository](#) to help you with your implementation.

SAML SSO

If you are using Microsoft Azure Active Directory (Azure AD) as your SAML identity provider, refer to this tutorial for a quick start with [SAML SSO Integration between Comm100 Live Chat and your Azure AD](#).

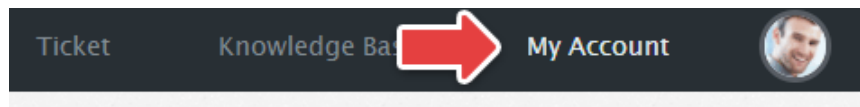
Please read the following sections to enable the SAML Agent SSO option in your Comm100.

- You will require the following information from your IT team:
- The SAML login URL to which Comm100 will redirect your agents for remote authentication
- (Optional)The remote logout URL where Comm100 can redirect users after they sign out of Comm100.
- The SAML certificate from your SAML server. X.509 certificates are supported and should be in PEM or DER format.

You may require some additional information from Comm100 to configure the SAML authentication system. Please refer to the Technical Implementation Details at the end of this section.

Enable SAML SSO in your Comm100 Account

1. **Log into your Comm100 Control Panel and navigate to the My Account module.**



2. **Click Security on the left, and enable Agent Single Sign-On.**



Dashboard

Agents

Security 1

Permissions

Password Policy

IP Restrictions

Audit Log

Agent Single Sign-On 2

Others

Agent Single Sign-On

Comm100 Agent SSO allows your agents to have a single login across Comm100 and other applications without the need to log in. Comm100 supports Agent SSO via [SAML \(Security Assertion Markup Language\)](#).

Agent Single Sign-On (SSO) disabled successfully.

If Enable Agent SSO YES 3

3. Switch to SAML SSO, and fill in the required information.

As mentioned above, please collaborate with your IT team to get the Remote Login URL, Remote Logout URL, and your SAML certificate issued by your SAML Identity Provider.

You can also find an SSO login URL displayed on the setup page. Share this link with your agents as they will need it to log into Comm100 once you set up Agent SSO.

Agent Single Sign-On

Comm100 Agent SSO allows your agents to have a single login across Comm100 and other applications. You only need to log in once and can move swiftly bet the need to log into separate accounts and remember multiple usernames and passwords. Comm100 supports Agent SSO via [SAML \(Security Assertion Markup\)](#)

If Enable YES

Once Agent SSO is set up, your agents can log into the Comm100 account with SSO via the following link:
https://[redacted].comm100.com/AdminManage/LoginSSO.aspx?siteId=[redacted]

SAML SSO
 Agents use the SSO service via SAML to log into the Comm100 account.

SAML SSO URL: *
 This is the URL that Comm100 will invoke to redirect the agents to your Identity Provider.
 Note that our Assertion Consumer Service URL is https://[redacted].comm100.com/AdminWebService/SSO/SSOSAMLConsumer.aspx

Remote Logout URL:
 This is the URL that Comm100 will redirect your agents to after they log out.

Certificate:
 You can obtain the certificate from your SAML Identify Provider.


JWT SSO

4. Click Save Changes to complete the setup.

User Management after Enabling SAML SSO

After you enable the agent SSO, please note that:

- Only your account administrators can use their original Comm100 username and password to log into their Comm100 account after Agent SSO with SAML or SAML authentication has been enabled. Non-admin agents can only sign in to Comm100 via the enabled SSO platform and they cannot update or reset the password they use in Comm100.
- Agents will only be able to sign in via SSO once the account administrator creates an agent account with an email address that matches their email in your SSO platform. If they try to login to Comm100 using their Comm100 credentials, they will see this message:



Error signing into the account

Please note that with Agent SSO enabled, non-admin agents can only login via SSO. To do so, please click the Sign in with custom SSO link below.


Log into your Comm100 Account with SSO

After you enable agent SSO and connect Comm100 to your SSO platform, your non-admin agents will need to log into Comm100 via your SSO service.

1. **Go to your account User Sign-In page.**
2. **Click Sign in with Custom SSO.**

User Sign in

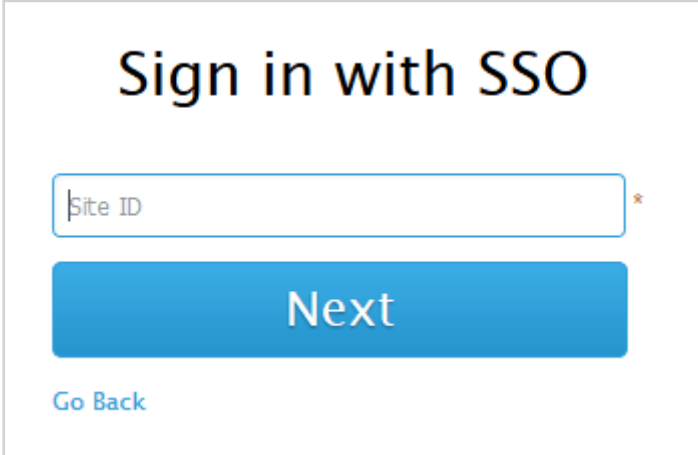
 *
 *
 Auto Login [Forgot your password?](#)

or
 

3. Provide your Comm100 Site ID and click Next.

Note: As mentioned in the previous section you can find the complete SSO login URL which includes the Comm100 Site ID in the SAML SSO configuration page of the Comm100 control panel.

Example: <https://hosted.comm100.com/adminmanage/LoginSSO.aspx?siteid=1000124>



The screenshot shows a web form titled "Sign in with SSO". It features a text input field labeled "Site ID" with a red asterisk to its right, indicating a required field. Below the input field is a large blue button with the text "Next". At the bottom left of the form, there is a link labeled "Go Back".

4. Comm100 redirects you to the SAML configured login system.
5. If you've already signed in to the SAML system, you will be authenticated and log into your Comm100 account automatically. If you have not signed in, log into your SAML system first to be authenticated and given access Comm100.

Technical Implementation Details

This section provides implementation details for your IT team on the following elements:

- Required user attributes
- Configuring the identity provider for Comm100
- Configuring the SAML server for Comm100

Required user attributes

Attribute	Description
email	Email of the user signing in. It is used to uniquely identify the user record in your Comm100 account.

Assigning an identity provider for Comm100

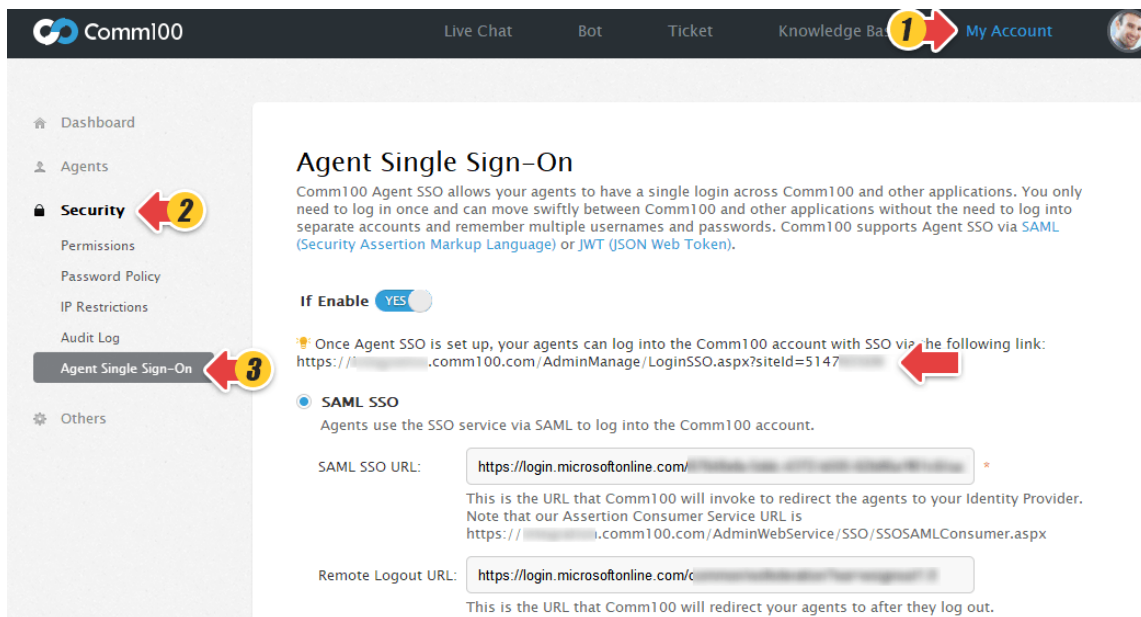
Attribute	Value
entityID	comm100

Configuring the SAML server for Comm100

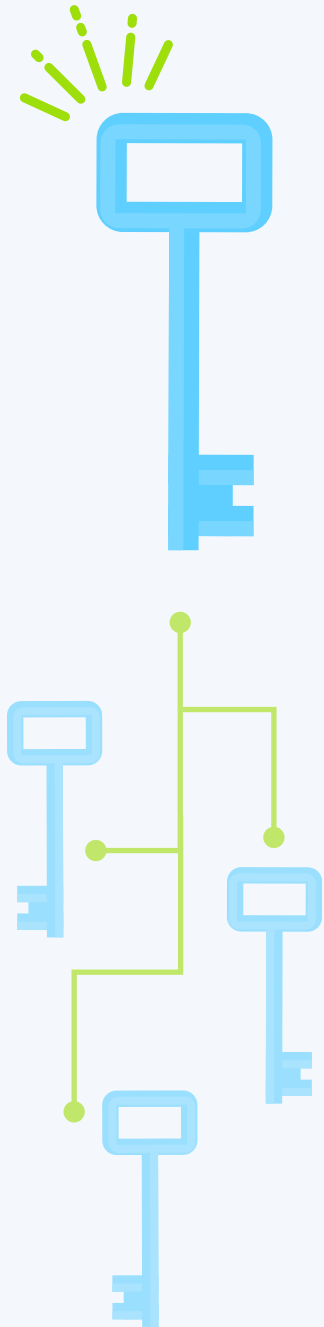
When configuring the integration with Comm100, you may need the following information:

- Assertion Consumer Service(ACS) URL

You can find the ACS URL when enabling the SAML SSO in your Comm100 account.



- Redirects to SAML Single Sign-on URL: Use HTTP POST



Agent SSO FAQ

Do you support AD/LDAP integration?

Yes, Comm100 supports AD/LDAP integration.

I received error message 'Error Signing into the account. This account does not exist in Comm100 or its status has been set inactive.'

Please make sure the SSO email and the agent email in Comm100 are the same.

When Agent SSO is configured is there an auto-login option for the agents without having to input any info manually?

Only the first login requires inputting the site ID. If an agent has already signed into the SSO System, when he/she visits the dedicated sign-in URL or clicks the "Sign in with Agent SSO" link for the second time, he/she will sign into Comm100 system automatically.

Error on Comm100 SSO Login page: Site ID is invalid.

Please check if you have enabled Agent SSO for this account with SiteId XX? If not, you might see this error.

We received errorcode=3, what does that mean?

Below is a screen shot of the different error codes the system uses. In this case, error code 3 refers to a 'Normal Error'. Our technical support team will help you find out the detailed reason for this.

```
loginSuccess = 0,  
operatorIPBlock = 1,  
adminIPBlock = 2,  
normalError = 3,  
operatorPasswordExpired = 4,  
operatorPasswordWillExpire = 5,  
operatorIPBlockAndShowVCode = 6,  
adminIPBlockAndShowVCode = 7,  
normalErrorAndShowVCode = 8,  
operatorPasswordExpiredAndShowVCode = 9,  
operatorPasswordWillExpireAndShowVCode = 10,  
  
multipleSites = 11,  
verificationCodeNotRightAndShowVCode = 12,  
verificationCodeNotRight = 13,  
sitePurged = 14,  
operatorExceed = 15,  
SSOEmailError = 16,
```

Can you please give us the JWT SSO examples?

Please find them at https://github.com/comm100/comm100_jwt_sso_examples

Does Comm100 SSO implementation support Identity Provider initiated SSO?

Currently, Comm100 does not support IdP initiated SSO.



Let's chat

Comm100 is a leading global provider of omnichannel customer experience solutions with a mission to make online service and support delivery more genuine, more personalized, and more productive through meaningful conversations.

[Learn More](#)