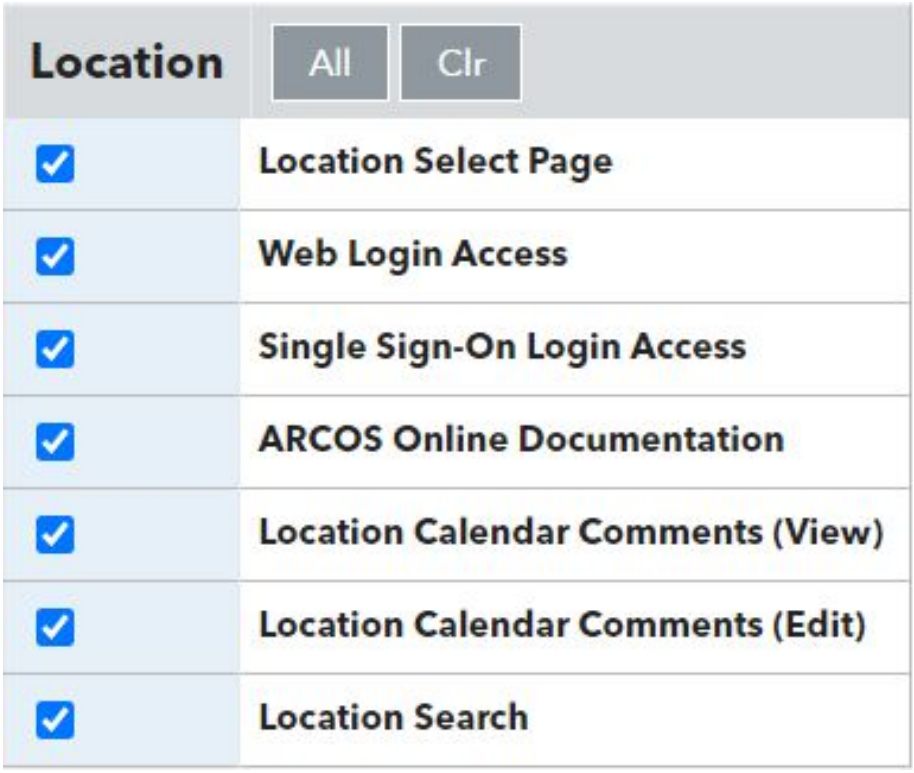
Quickstart Guide | Callout Single Sign-On

After **Callout Single Sign-On Config Admin** has been enabled in your system, there are steps that will need to be taken in order to give your employees the ability to login to ARCOS via Single Sign-On.

ARCOS Admin

To give users the ability to login to ARCOS via Single Sign-On, begin by logging into ARCOS and going to Sys Admin > Security and click the **modify** link for any security group you wish to give Single Sign-On login access to.

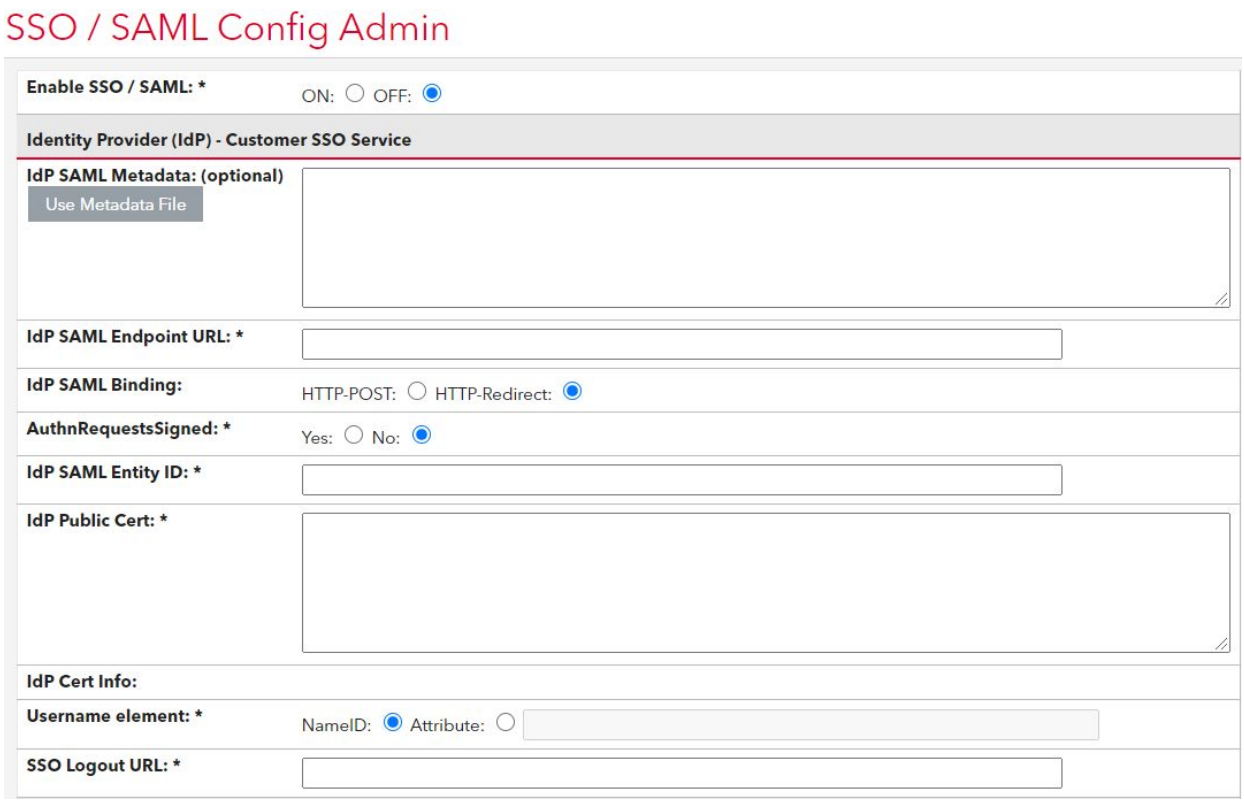


The security group will need the following items enabled to be able to login via SSO successfully:

- **Web Login Access** - this gives users base level ARCOS application login access.
- **Single Sign-On Login Access** - this gives users the ability to login via Single Sign-On

Clicking the checkbox next to these items and then clicking the **Save** button on this page will grant members of this security group the ability to perform these actions, **HOWEVER**, ARCOS will not prompt users to login via Single Sign-On until it has been enabled in **SSO / SAML Config Admin**.

At the ARCOS Admin level, under Sys Admin > SSO Config, you will see **SSO / SAML Config Admin**.

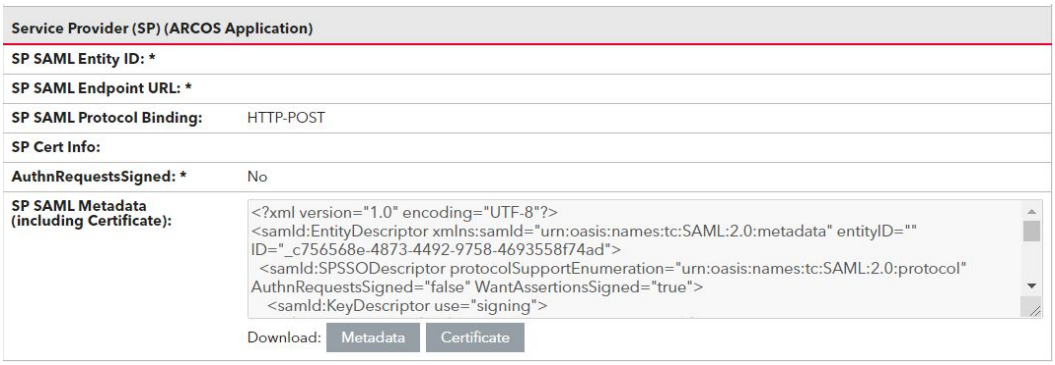


SSO can be configured without being enabled. The **Enable SSO / SAML** radio button group identifies whether ARCOS will attempt to have the user login via SSO. Users will only be able to login via SSO if this is set to **ON**.

The **Identity Provider (IdP) - Customer SSO Service** section is where you or your technical support will need to enter information in order to configure ARCOS to communicate with your IdP service.

- **Idp SAML Metadata: (optional)** - this is extraneous data which may or may not be included with SAML Authentication requests.
- **IdP SAML Endpoint URL** - the URL which SAML Authentication requests should be directed to.
- **IdP SAML Binding** - this identifies the type of HTTP binding the IdP allows. Typically, HTTP-POST is used and HTTP Redirect may not be allowed.
- **AuthnRequestsSigned** - this identifies whether ARCOS will sign Authentication Requests.
- **IdP SAML Entity ID** - this identifies the issuer element in Authentication Responses.
- **IdP Public Cert** - the public certificate used to validate Authentication Responses from the IdP.
- **Username element** - this, by default, is NameID, if Attribute is selected, then the name of the element containing the user's Web ID must be provided (this is cAsE sEnSiTiVe).
- **SSO Logout URL** - this is the URL users are directed to when they log out of ARCOS.

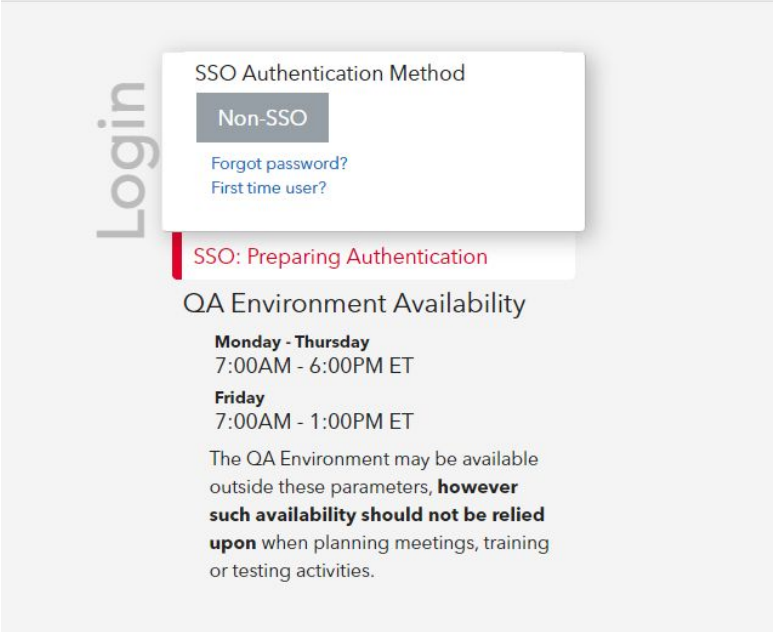
Below this, we have the **Service Provider (SP) (ARCOS Application)** section. This section is non-configurable and only to be referred to as needed.



Once the desired configuration has been made to this page, the changes can be implemented by clicking the **Submit** button. If SSO is enabled without users having the appropriate SSO login security permission enabled, they will still be able to login with their normal ARCOS Web ID and password.

ARCOS User

After Single Sign-On has been enabled for your ARCOS system, users will be prompted to login via SSO.



The user is not required to take any action when they see this screen if they are logging into ARCOS via SSO. ARCOS will load briefly and the user's authentication request will be submitted to the IdP. Once ARCOS receives and processes a response, they will be logged into ARCOS as normal or they will be prompted to login through their IdP.

Example:

If your company uses Microsoft for an IdP and they are not logged into the account when they attempt to login to ARCOS, they will be redirected to a Microsoft login page and expected to login with their company credentials. After this they would be redirected to ARCOS and logged into ARCOS.

If a user does not have SSO Login access but does have an ARCOS account with Web Login access, they may login with their ARCOS account credentials by clicking the **Non-SSO** button that appears. Users who are able to login via SSO will, as a result, be able to login with their Web ID and password. There is **NOT** currently a way to configure ARCOS to allow employees to **ONLY** login via SSO.