Windows desktop SSO configuration

Use Windows desktop single sign-on (SSO) to allow immediate and secure access to resources via Kerberos-based authentication.

To enable this feature on any SecureAuth IdP realm, the SecureAuth IdP appliance must be joined to the company domain. Window desktops must be on the same company domain, with the ability to process and use Kerberos tickets.

You can configure realms to use Windows desktop SSO in any of the following ways:

Windows SSO
: When the Begin Site is configured to use *Windows SSO* login workflow, you have the option to include multi-factor authentication (MFA) and adaptive authentication. This method is more secure because it includes the Device Recognition layer.

Windows SSO (skip workflow)
: When the Begin Site is configured to use *Windows SSO (skip workflow),* it bypasses the login workflow, skips MFA, and routes the user directly to the Post Authentication page once it validates the Kerberos ticket. This method bypasses the Device Recognition layer, however, it increases system performance.

Prerequisites

- SecureAuth IdP version 9.3
- SecureAuth IdP realm or integrated application with the following configured:
  - Overview tab
  - Data tab / Directory integration
  - Workflow tab
  - Multi-Factor Methods configuration
  - Post Authentication configuration
  - Logs tab
- Microsoft Active Directory in use and integrated with SecureAuth IdP

  > On the New Experience user interface in version 9.3, you can configure an Active Directory integration or SQL Server integration to be applied to applications made from App onboarding library templates. Configure the remaining components – for example, Workflow, Multi-Factor Methods, and Adaptive Authentication tabs – on the Classic Experience user interface.

- Set up custom identity SPN to leverage Integrated Windows Authentication (IWA)

Enable universal Windows desktop SSO in the environment

The most effective way to enable universal Windows desktop SSO is to push out a local intranet URL via Group Policy Object (GPO); however, end users can also configure their own devices and browsers to enable this feature.

To enable Windows desktop SSO

1. Add the SecureAuth IdP server Fully Qualified Domain Name (FQDN) to the **Local intranet** list of websites in Chrome, Internet Explorer, and Firefox browsers.

   ### Chrome

   #### Chrome

   a. In the Google Chrome browser, click the **menu** icon (3 vertical dots) on right of the address toolbar.
   b. Click **Settings**.
   c. Scroll to the bottom of the page and expand the **Advanced** section.
   d. In the System section, click **Open proxy settings**.
      The Internet Properties dialog opens.
   e. Select the **Security** tab.
   f. Click **Local intranet**.
   g. Click **Sites**.
   h. Click **Advanced**.
      The Local intranet dialog opens.
   i. Enter the FQDN of the SecureAuth IdP server (for example, https://secureauth.company.com/).

> Wildcards are an option in addition to FQDNs, however, it lessens the security stance.

j. Click **Add**.
k. Click **Close** and **OK** to the remaining dialogs.

Internet Explorer

Internet Explorer

a. In the Internet Explorer browser, click the **gear** icon on right side of the address toolbar.
b. Click **Internet options**.
The Internet Options dialog opens.
c. Select the **Security** tab.
d. Click **Local intranet**.
e. Click **Sites**.
f. Click **Advanced**.
The Local intranet dialog opens.
g. Enter the FQDN of the SecureAuth IdP server (example: https://secureauth.company.com/).

> Wildcards are an option in addition to FQDNs, however, it lessens the security stance.

h. Click **Add**.
i. Click **Close** and **OK** to the remaining dialogs.

Firefox

Firefox

a. On the Firefox address bar, type ***about:config*** and press **Enter**.
b. Accept the warranty risk message and continue.
c. On the configuration page, search for ***network.automatic*** .
d. Double-click ***network.automatic-ntlm-auth.trusted-uris*** .
The Enter string value dialog opens.
e. Enter the SecureAuth IdP domain name in the dialog (example: https://company_SecureAuth_FQDN.com).

> Wildcards are an option in addition to FQDNs, however, it lessens the security stance.

f. Click **OK** and close Firefox.

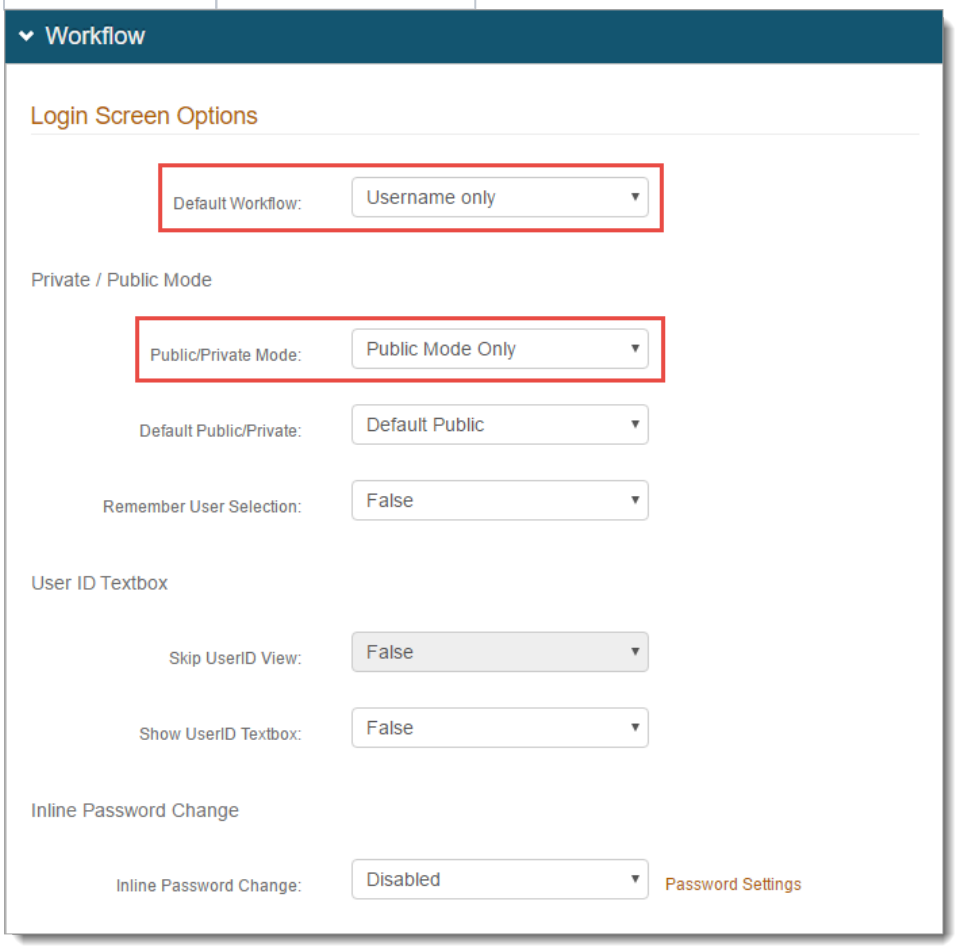
2. Grant the "Authenticated Users" group access to the signing certificate being used in the realm.
For instructions, see Grant Permission to Use Signing Certificate Private Key.
3. Install the Machine Key Tool per the instructions in the document.

a. Run the **Machine Key Tool** to assign "Authenticated Users" permissions to the RSA .NET Framework Configuration Key.
b. Select option **A** on the **Privileges** tab in the document.

SecureAuth IdP Web Admin - Classic Experience configuration

1. Go to the **Workflow** tab.
2. In the **Workflow** section, set the following:

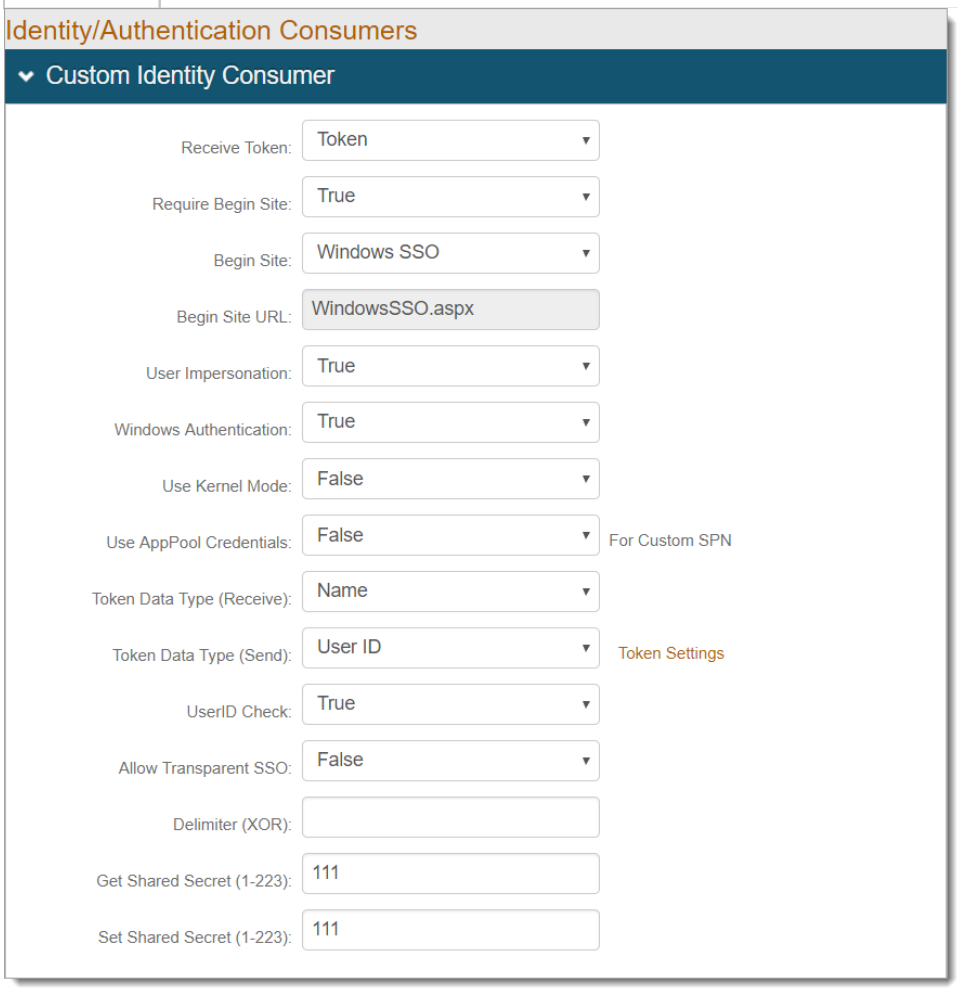
Default Workflow	Set to **Username only**.
Public/Private Mode	Set to **Public Mode Only**.



3. In the **Custom Identity Consumer** section, set the following:

Receive Token	Set to **Token**.
Require Begin Site	Set to **True**.
Begin Site	Use any of the following options: • To include MFA and adaptive authentication in login workflow, set to **Windows SSO**. This method adds the Device Recognition layer, and is more secure. • To skip the login workflow and go directly to the Post Authentication page, set to **Windows SSO (skip workflow)**. This method does not include MFA, adaptive authentication, and increases performance.
Begin Site URL	Depending on the Begin Site selection, this field is auto-populated with **WindowsSSO.aspx** or **WindowsSSO2.aspx**.
User Impersonation	Set to **True**.
Windows Authentication	Set to **True**.
Use Kernel Mode	To use custom Service Principal Names for Integrated Windows Authentication (Kerberos), set to **True**.

AppPool Credentials	To use custom Service Principal Names for Integrated Windows Authentication (Kerberos), set to **True**.



4. Click **Save**.