Add Single Sign-On domain

This article describes how to add a Single Sign-On domain in Nexus Hybrid Access Gateway.

Expand/Collapse All

Related information

- Single sign-on

Step-by-step instruction

1. Log in to the Hybrid Access Gateway administration interface with your admin user.

When using SSO, always add the SSO domain before you enable it on a resource.

1. In the Hybrid Access Gateway administration interface, go to **Manage Resource Access > SSO Domains**
   - Registered SSO domains are listed, click a registered SSO domain to edit or delete it.
2. Click **Add SSO Domain** to add a new SSO domain.
3. Enter a SSO domain **Display Name**.
4. Select **Domain Type**.
5. Available options are:

   a. Text (default, used for domains of the type NTLM, Basic, and Form-based.)
   b. Cookie
6. SSO Restrictions

   - Cache on session only
     When **Cache on session only** is checked, SSO credentials are cached (kept in memory) and only valid during the user session. When the option is not checked (default), the SSO credentials are stored persistently on the user account.

     > ⚠ When **Domain Type** is set to Cookie, this option is not available.

   - User Inactivity
     Check **Enable inactivity check** and specify a period of time (set in number of days, weeks, or months) during which users are allowed to be inactive, that is, not access the domain. When the period has passed, credentials must be re-entered for access to the domain to be granted. This option is not available when **Cache on session only** has been selected.
   - Absolute Time Limit
     Check **Enable time limit check** and specify a period of time (set in number of days, weeks, or months) during which users’ SSO credentials are valid. When the period has passed, credentials must be re-entered for access to the domain to be granted. This setting is independent of user inactivity. This option is not available when **Cache on session only** has been selected.