Recast

SSO with NTLM overview

Last Modified on 04.16.26

Application Workspace supports Windows New Technology LAN Manager (NTLM) based authentication in combination with an LDAP Active Directory identity source to achieve SSO.

Configuration requirements

- Only supported with a Microsoft Active Directory based identity source.
- The name of the identity source needs to match the Active Directory NetBIOS domain name, not the FQDN of the domain.
- In the identity source's **Authentication** tab, you must select the *NTLM* protocol option
- The Application Workspace Server performing the NTLM authentication needs to be a member server in the Active Directory forest containing the domain.

Client machine restrictions

- The FQDN of Application Workspace needs to be added to the "Intranet Zone" within Internet Explorer to perform NTLM authentication for IE and the Application Workspace Launcher.
- The FQDN of Application Workspace needs to be defined as an A-record within the DNS for both IE and the Application Workspace Launcher.
- For other supported browsers (Internet Explorer, Firefox, Google Chrome, Opera, Microsoft Edge, Safari), consult the relevant product documentation on how to activate NTLM authentication.

NTLM based authentication will only be triggered when SSO is explicitly activated for Application Workspace. See Overview for available options.

For more information about NTLM, see Microsoft documentation.