- Configure Kerberos on Workspace on page 56

  To configure Workspace to provide Kerberos authentication, you must join to the domain and enable Kerberos authentication on Workspace.

- Configure Internet Explorer to Access the Web Interface on page 57

  You must configure the Internet Explorer browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using Internet Explorer.

- Configure Firefox to Access the Web Interface on page 58

  You must configure the Firefox browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using Firefox.

- Configure the Chrome Browser to Access the Web Interface on page 58

  You must configure the Chrome browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using the Chrome browser.

Configure Kerberos on Workspace

To configure Workspace to provide Kerberos authentication, you must join to the domain and enable Kerberos authentication on Workspace.

Procedure

1 Go to Connector Services Admin and select **Join Domain**.

2 On the Join Domain page, enter the information for the Active Directory domain.

   a In the **AD Domain** text box, enter the fully qualified domain name of the Active Directory. The domain name you enter must be the same Windows domain where the Workspace appliance resides.

   b In the **AD Username** text box, enter the user name of an account in the Active Directory that has permissions to join systems to that Active Directory domain.

   c In the **AD Password** text box, enter the password associated with the AD Username. This password is not stored by Workspace.

   d Click **Join Domain**.

   The Join Domain page is refreshed and displays a message that you are currently joined to the domain.

3 On the Connector Services Admin page, select **Auth Adapters** and click **Edit** in the KerberosldpAdapter row.

   a The Name field shows KerberosldpAdapter as the name. You can change this.

   b In the **Directory UID Attribute** text box, enter the account attribute that contains the user name.

   c Check **Enable Windows Authentication** to extend authentication interactions between users' browsers and Workspace.

   d Check **Enable NTLM** to enable NT LAN Manager (NTLM) protocol-based authentication.

   e Check **Enable Redirect** if round-robin DNS and load balancers do not have Kerberos support. Authentication requests are redirected to Redirect Host Name. If this is checked, enter the redirect host name in **Redirect Host Name** text box.

   f Click **Save**.