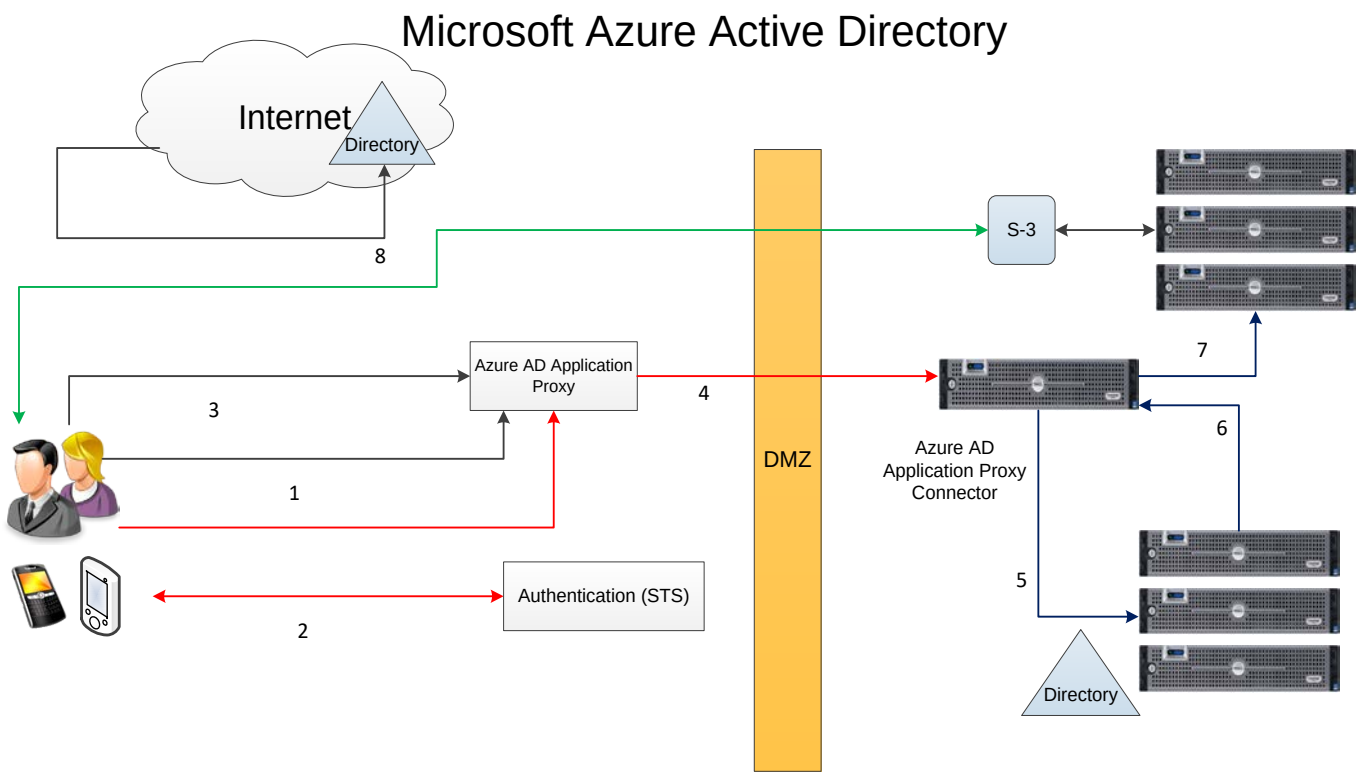
SAML Integration: Single Sign-On (SSO) for Cloud Apps



1. The user enters the URL to access the on-premises application through Application Proxy.

2. Application Proxy redirects the request to Azure AD authentication services to preauthenticate. At this point, Azure AD applies any applicable authentication and authorization policies, such as multifactor authentication. If the user is validated, Azure AD creates a token and sends it to the user.

3. The user passes the token to Application Proxy.

4. Application Proxy validates the token and retrieves the User Principal Name (UPN) from it, and then sends the request, the UPN, and the Service Principal Name (SPN) to the Connector through a dually authenticated secure channel.

5. The Connector performs Kerberos Constrained Delegation (KCD) negotiation with the on-prem AD, impersonating the user to get a Kerberos token to the application.

6. Active Directory sends the Kerberos token for the application to the Connector.

7. The Connector sends the original request to the application server, using the Kerberos token it received from AD.

8. The application sends the response to the Connector, which is then returned to the Application Proxy service and finally to the user.