Design Considerations for Integrated Features

Single Sign-On (SSO) Considerations

The Single Sign-on feature authenticates and authorizes users for all the contact center solution applications and services. Authentication is the process of validating the identity of a user: "you are who you say you are." Authorization is the process of confirming that an authenticated user is permitted to perform the action they are requesting: "you can do what you are asking to do." When you enable SSO in the contact center solution, users only sign in once to gain access to all of their Cisco browser-based applications and services.

To support SSO for the contact center solution, you must install and configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. For a current list of supported Identity Provider products and versions, see the Unified CCX Compatibility related information located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Authentication and authorization are managed for the contact center solution by the Cisco Identity Service (Cisco IdS). When an SSO-enabled user signs in, the Cisco IdS interacts first with your Identity Provider (IdP) to authenticate the user. The IdP stores user profiles and provides authentication services to support SSO sign-ins. When the user is authenticated, the Cisco IdS exchanges information with the Cisco service the user is attempting to access to confirm that the user is authorized for the role they are requesting. When the user is authenticated, the Cisco IdS issues an access token that allows the user to access the application. Once access is established during a particular session, the user can switch among contact center solution applications without presenting credentials again.

Note The user credentials are only presented to the IdP. The contact center solution applications and services only exchange tokens; they do not see the users' information.

To integrate your IdP with your contact center solution, you perform the following administrative tasks:

- Establish a trust relationship between the Cisco IdS and the Identity Provider.
- Set the SSO mode in your system to enable users for SSO.
- Register on the Single Sign-On web page to onboard the single sign-on components.

- Perform **Test SSO Setup** on the single sign-on web page to test the status of registration of each component. You will be redirected to the Identity Provider for authentication. If the **Test SSO Setup** is successful then the **Enable** option is enabled.

SSO Message Flow

An SSO user's access token is issued by Cisco IdS to validate the users accessing the corresponding applications. When the user is found valid each application performs the authorization locally. Cisco IdS supports authorization Code Grant Flow as defined in OAuth 2.0 and in turn uses SAML v2.0 to authenticate users before issuing auth code.

When a user browses to a web page for an SSO-enabled service, the authentication request is redirected to the Cisco Identity Service. Cisco Identity Service generates a SAML authentication request and directs it to the Identity Provider. The IdP presents a sign-in page to the user at the browser to collect the user's credentials. After the IdP authenticates the user, the IdP issues a SAML assertion to the Cisco IdS. The assertion contains trusted statements about the user, for example, username and privileges.

The assertions must have attributes. The Cisco IdS extracts **uid** and **user principal** and generates and delivers authorization code to the SSO enabled application. The application on receiving the authorization code will request IDs For Access and Refresh Tokens.

Access Tokens are used by applications to validate user information and Refresh Token are used to request new Access Tokens. These token have a validity period associated with each one of them.

Note A new Access token and Refresh token pair can be obtained only before the Auth code expires.

Access Tokens can be refreshed only when both the current access token and the refresh token are valid and not expired.

If the refresh tokens expire you can not refresh an access token. Thus you need to be authenticated again and the auth code need to ne requested again.

Together SAML and OAuth make it possible for a user to authenticate while only exposing user credentials to the authentication provider. The username and password are only presented to the IdP. The contact center solution applications and services do not see the user information. Only the SAML assertion and the OAuth token are exchanged.

Single Sign-On High Availability Considerations

Every core component in the contact center solution has the Cisco Identity Service client that supports an high availability mode. Any SSO enabled application can connect to either to the local Cisco Identity Service instance or to the remote.

By default it will connect to the local instance of Cisco Identity Service. The Local Cisco Identity Service is the default and the preferred Cisco Identity Service that runs locally.

Cisco Identity Service client supports failover if the remote Cisco Identity Service is configured when the local Cisco Identity Service fails. When the local Cisco Identity Service is available again the Cisco Identity Service client fails back to the local Cisco Identity Service.

The below table provides the details of Cisco Identity Service client failover and failback in different states of the local and remote Cisco Identity Service:

Table 1: Failover and Failback Scenarios of Cisco Identity Service Client Based on the State of Cisco Identity Service

Local Cisco Identity Service	Remote Cisco Identity Service	Cisco Identity Service Client Connects to
IN_SERVICE	Not Applicable	Local Cisco Identity Service
PARTIAL_SERVICE	IN_SERVICE	Remote Cisco Identity Service
PARTIAL_SERVICE	PARTIAL_SERVICE	Local Cisco Identity Service
OUT_OF_SERVICE	PARTIAL_SERVICE	Remote Cisco Identity Service
OUT_OF_SERVICE	OUT_OF_SERVICE	None
OUT_OF_SERVICE	Not Configured	None

Single Sign-On Design Impacts

This section details few of the design impacts of the Single Sign-On (SSO) feature. The implementation requires you to use only HTTPS protocol to access all the web applications. The HTTP access to web applications is not supported when the SSO is enabled.

Authentication Modes in Unified CCX

You can choose from two different authentication modes when deciding about implementing SSO:

- **SSO** - Enable **all** agents, supervisors, and administrators (administrators of the Cisco Unified CCX Administration or Cisco Unified CCX Serviceability application) in the deployment for SSO.
- **Non-SSO** - Use existing Unified CM-based or local authentication.

Applications in SSO Mode

- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse
- Cisco Finesse-hosted gadgets
- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability.

Note The Cisco Finesse IP Phone Agent is not supported in SSO enabled mode.

Single Sign-On can independently function on Unified CM and Unified CCX. It is not inter dependant on each other.

Applications not SSO Enabled

The following applications are not Single Sign-On enabled:

- Cisco Finesse Administration
- Cisco Identity Service Administration
- Disaster Recovery System
- Cisco Unified OS Administration
- Cisco Unified Serviceability
- Standalone Cisco Unified Intelligence Center
- Cisco Unified CCX Editor
- Real Time Monitoring Tool
- Cisco Customer Collaboration Platform
- Cisco Workforce Optimization
- Cisco Finesse Desktop Chat
- Any Third Party Application.

Qualified Identity Providers

If you use any Identity Provider (IdP) outside of the listed IdPs in the table below, Cisco IdS supports the IdP as long as the IdP is SAML 2.0 compliant and meets the following requirements described in the subsequent SAML Request and Response sections:

- SAML Request Attributes
- Expectations from SAML Response

IdP Metadata Schema

When you configure IdS and exchange Metadata between Cisco Identity Service (IdS) and the Identity Provider (IdP), ensure that the IdP Metadata file should confirm to the SAML metadata schema at:

https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd

SAML Request Attributes

SAML request supports the following SAML 2.0 bindings:

- **HTTP-POST** binding
- NameIDFormat in SAML request must be **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**
- SAML request must be signed using **SHA-256**.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       ID="s25f4fb66688cf429e430034f4cceac00b6124570d" Version="2.0"
       IssueInstant="2018-10-29T10:01:39Z"
Destination="https://win-adfs30-151.uccxteam.com/adfs/ls/"
       ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
```

```
       AssertionConsumerServiceURL="https://ccxssodemo1.cisco.com:8553/ids/saml/response">
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ccxssodemo1.cisco.com</saml:Issuer>
    <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
           Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
          SPNameQualifier="ccxssodemo1.cisco.com" AllowCreate="true"></samlp:NameIDPolicy>
</samlp:AuthnRequest>
```

Expectations from SAML Response

The following are the expectations from SAML Response:

- The entire SAML response (message and assertion) is signed or only the message is signed but not the SAML assertion alone is signed.
- SAML Assertion must not be encrypted.
- SAML response must be signed using **SHA-128**.
- SAML response must be signed using **SHA-256**.
- NameIDFormat in SAML response must be **urn:oasis:names:tc:SAML:2.0:named-format:transient**.
- **uid** and **user_principal** attributes should be present in SAML assertion in the AttributeStatement section.

  The "uid" attribute value must be the user Id using which users log in to Cisco contact centre applications that are SSO enabled and the "user_principal" attribute value must be in uid@domain format.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
Destination="https://ids-ssp-node.cisco.com:8553/ids/saml/response"
    ID="_6a309495-d3c2-4a28-b8e3-289f8f5355bd"
InResponseTo="s21c84ba20862f573f5daec121c305ba6aac877843"
    IssueInstant="2017-08-10T13:20:26.556Z" Version="2.0">
    <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://ADFSServer.cisco.com/adfs/services/trust

    </Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
 />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#_6a309495-d3c2-4a28-b8e3-289f8f5355bd">
            ..........
            </ds:Reference>
        </ds:SignedInfo>
        ..........
        ..........
     </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_df3bdbcf-a225-4e97-b00a-a199bdda3d2c"
        IssueInstant="2017-08-10T13:20:26.556Z" Version="2.0">
        <Issuer>http://ADFSServer.cisco.com/adfs/services/trust</Issuer>
        ..............

        ..............
            <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="http://ADFSSserver.cisco.com/adfs/services/trust"
```

```
                    SPNameQualifier="ids-ssp-node.cisco.com">CISCO\Admin121</NameID>
                <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <SubjectConfirmationData
                        InResponseTo="s21c84ba20862f573f5daec121c305ba6aac877843"
                        NotOnOrAfter="2017-08-10T13:25:26.556Z"
                        Recipient="https://ids-ssp-node.cisco.com:8553/ids/saml/response" />
                </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2017-08-10T13:20:26.556Z"
                NotOnOrAfter="2017-08-10T14:20:26.556Z">
                <AudienceRestriction>
                    <Audience>ids-ssp-node.cisco.com</Audience>
                </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
                <Attribute Name="user_principal">
                    <AttributeValue>Admin121@cisco.com</AttributeValue>
                </Attribute>
                <Attribute Name="uid">
                    <AttributeValue>Admin121</AttributeValue>
                </Attribute>
            </AttributeStatement>
            <AuthnStatement AuthnInstant="2017-08-10T13:18:12.086Z"
                SessionIndex="_df3bdbcf-a225-4e97-b00a-a199bdda3d2c">
                <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef>

                </AuthnContext>
            </AuthnStatement>
        </Assertion>
</samlp:Response>
```