WebEx Connect - Single Sign On

Technical Overview

October 2009

Cisco Systems Inc.
3979 Freedom Circle, Santa Clara, CA 95054

Corp: +1-408-435-7000 **Sales:** +1.877.50.WEBEX

www.webex.com

Introduction

One of the goals of the Cisco - WebEx Connect™ platform is to provide comprehensive management of user identities for an organization. This will facilitate ease of use and policy controls based on the user's role and group affiliations inside the organization. This paper provides an overview of standards based mechanisms to achieve single sign on (SSO) from an organization's intranet to Connect.

Using Connect SSO functionality, users have the ability to sign into their corporate network and launch Connect without entering a separate Connect username and password. After users are authenticated with Connect, they will also be automatically authenticated to their WebEx Meeting site to schedule and host web conferences.

For more information about SSO to the WebEx Meeting site (not necessarily involving Connect) see the "WebEx Federated SSO Authentication" technical note:

http://developer.webex.com/c/document_library/get_file?folderId=22041&name=DLFE-902.pdf

Corporate User SSO to WebEx Connect

With SSO, users can authenticate to their corporate network and launch WebEx Connect and host WebEx Meetings without entering separate user credentials.

Requirements

Identity and Access Management System

Customers need an Identity Management System (IDMS) that conforms to the SAML 2.0, or WS-Federation 1.0 standard. Customers can develop their own SAML-compliant IDMS using programming libraries such as OpenSAML (http://www.opensaml.org/) or they can purchase a commercial third party IDMS. The IDMS should be able to generate SAML or WS-Federation Assertions digitally signed with the private key of an X.509 certificate.

Commercial SAML compliant IDMS systems include:

- Computer Associates SiteMinder
- Sun Microsystems OpenSSO Enterprise
- Ping Identity Ping Federate
- Oracle Access Manager

Microsoft Active Directory Federation Services supports WS-Federation 1.0

X.509 Certificate

Customers need to acquire an X.509 public key digital certificate from a Certificate Authority or provision their own certificates. Certificate Authorities are trusted institutions including government agencies and companies such as Verisign and Thawte.

To configure SSO from a customer intranet to Connect, organizations should upload a valid X.509 Base 64 encoded certificate to the Connect server using the Org Admin tool. Each SAML or WS-Federation assertion posted to the Connect server for SSO must be digitally signed with the matching private key.

Connect SSO Process Flow

WebEx Connect supports Service Provider (SP) initiated SSO using the Redirect/Browser POST binding for SAML 2.0. The WebEx Connect client opens a browser window to the customer's Identity Management System (IDMS) which serves as the user's Identity Provider (IdP). This section describes each step in the SSO process.

1. User launches Connect Client
2. Connect Client opens a browser window to the customer's IDMS.
3. IDMS will challenge the user to enter their credentials if they haven't already logged into the corporate network.
4. IDMS will validate the user's credentials against the corporate directory, usually an LDAP server.
5. IDMS sends a signed SAML or WS-Fed assertion with a unique user identifier such as a corporate username.
    - If customer is using Auto Account creations and this is the first time the user is accessing Connect the assertion will include profile info (first name, last name, email address, etc.).
6. Connect Authentication Service (CAS) validates the user specified in the SAML or WS-Fed assertion with the Connect database.
    - If this is the first time the user has used Connect then AS provisions the new user in the Connect database.
7. CAS returns a validated user token to the Connect Client. The user can now use IM and access their Spaces.

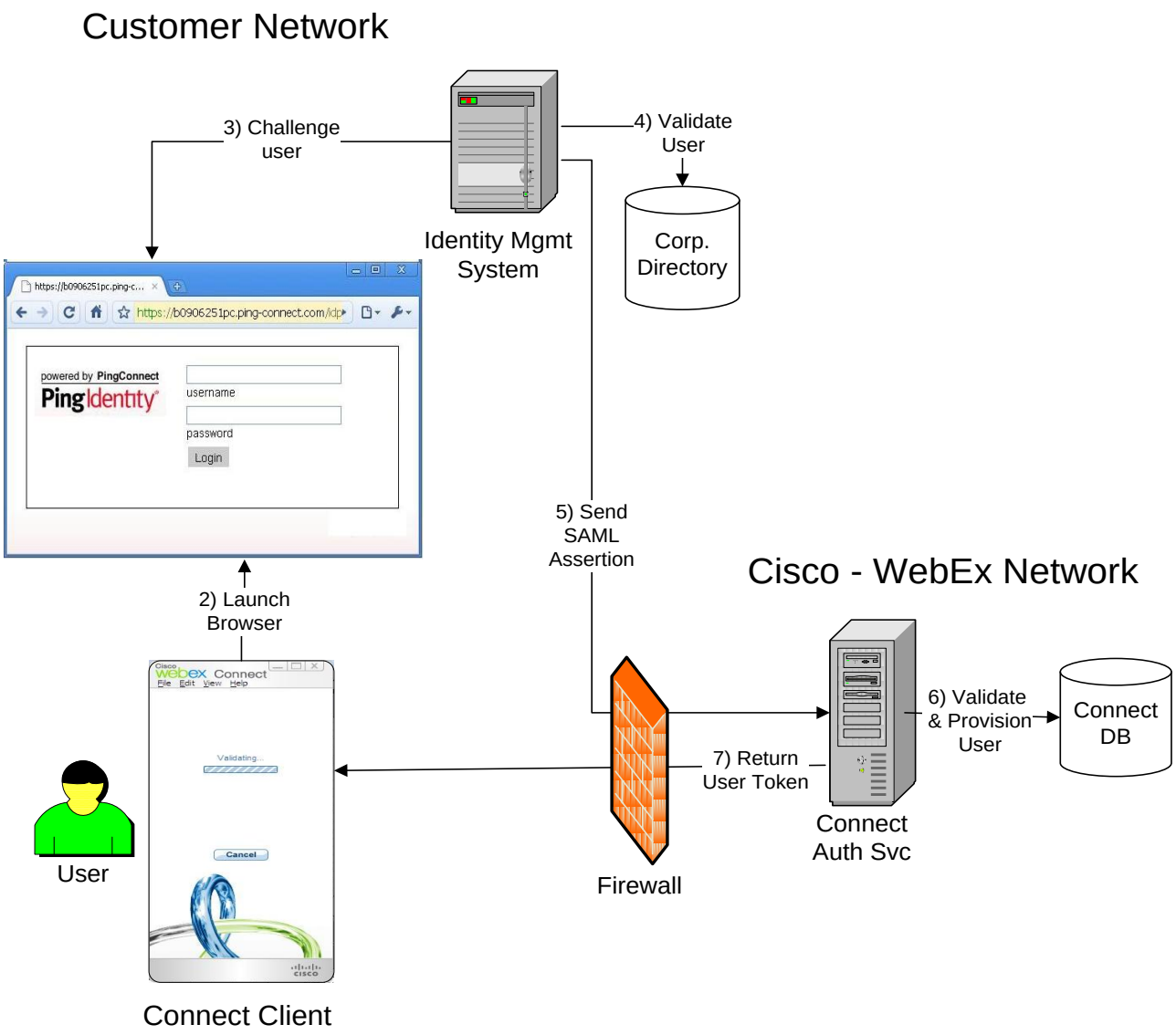

Figure 1: SSO Process flow

Example SAML 2.0 Response

Here is an example of a SAML 2.0 response containing a signed assertion. The assertion requires either an attribute "uid" containing the Connect username or an "email" attribute containing the user's email address. This assertion includes user profile attributes for Auto Account creation.

```
<Response xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://acme.webex.com/dispatcher/SAML2AuthService?siteurl=acme"
ID="_06bff71973342ad24ba31790591bb010e963"
InResponseTo="s250ce91cf92b24a7694686158ddea33b6c1ce7fa9" IssueInstant="2008-09-
05T19:08:05Z" Version="2.0">
   <ns1:Issuer xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion"
   Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">acme</ns1:Issuer>
   <Status>
   <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </Status>
   <ns2:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="_e72cfdeffbf9288cfa75e2423a932abb35d5" IssueInstant="2008-09-05T19:08:05Z"
   Version="2.0">
   <ns2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   acme</ns2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:Reference URI="#_e72cfdeffbf9288cfa75e2423a932abb35d5"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:DigestValue
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">p5AbejgL5K4nGDp3HXHfp3VPhmE=</ds:D
      igestValue>
      </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      TtMcc6pnIxbDcLulI8/hJS9A74dR2w05dO676PK7KT48d8sGFoXXTgpWgy++7+AZTpQCjHPcv88c
      dAh4PtripoBlpZ++xErKQ/ee/rxsP2mOr7LrNE4QoqUbiOCd68kHz9QjxOApTIr6d4YXNfeHD62O
      </ds:SignatureValue>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Certificate xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      MIIErjCCA5agAwIBAgIQZMQJL9PYyWwQloty2TFcIzANBgkqhkiG9w0BAQUFADBrMQswCQYDVQQG
      EwJVUzEtMCsGA1UEChMkVHJ1c3RlZCBTZWN1cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MS0wKwYD
      VQQDEyRUcnVzdGVkIFNlY3VyZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDgwNTE2MDAwMDAw
      WhcNMTAwNTE2MjM1OTU5WjCB/TELMAkGA1UEBhMCVVMxFDASBgNVBAgTC0NPTk5FQ1RJQ1VUMRIw
      EAYDVQQHEwlGQUlSRklFTEQxITAfBasdawerweasdmVyYWwgRWxlY3RyaWMgQ29tcGFueTEwMC4G
      A1UECxMnR0UgQ29ycG9yYXRlIENJUyhjb3JwdDUwOCBwb2xpY3lzZXJ2ZXIpMS0wKwYDVQQLEyRQ
      cm92aWRlZCBieSBHZW5lcmFsIEVsZWN0cmljIENvbXBhbnkxFzAVBgNVBAsTDkVudGVycHJpc2Ug
      U1NMMScwJQYDVQQDEx5mZWRlcmF0aW9uLnN0YWdlLmdlY29tcGFueS5jb20wgZ8wDQYJKoZIhvcN
      AQEBBQADgY0AMIGJAoGBALxifpE26Rq2/uu6aykFJs3FqVg8/jh+F52JFRFdqmE6X2BHwIvTyrAe
      Xxa3qCBrFuUkmuopAMB9Fa0EF/JRSTvCyrPbls2ad3f34fvfAsCspdorx4d/Bc57UiqBXD/MSRWD
      S4lIYu9z2HXP1vTmu8zn4pkGCKatwvzmyX8kHjQbAgMBAAGjggE9MIIBOTAfBgNVHSMEGDAWgBQx
      </ds:X509Certificate>
      </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
```

```
   <ns2:Subject>
     <NameID Format=”urn:oasis:names:tc:SAML:1.1:nameid-
     format:emailAddress”>johnd@acme.com</NameID>
     <ns2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <ns2:SubjectConfirmationData
        InResponseTo="s250ce91cf92b24a7694686158ddea33b6c1ce7fa9" NotOnOrAfter="2008-
        09-05T19:09:35Z"
        Recipient="https://swapi.webexconnect.com/cas/SAML2AuthService.do?org=acme.com
        "/>
     </ns2:SubjectConfirmation>
   </ns2:Subject>
   <ns2:Conditions NotBefore="2008-09-05T19:07:35Z" NotOnOrAfter="2008-09-
05T19:09:35Z">
       <ns2:AudienceRestriction>
                    <ns2:Audience>http://www.webex.com</ns2:Audience>
      </ns2:AudienceRestriction>
      <ns2:AudienceRestriction>
             <ns2:Audience>http://www.webex.com</ns2:Audience>
      </ns2:AudienceRestriction>
   </ns2:Conditions>
   <ns2:AuthnStatement AuthnInstant="2008-09-05T19:08:05Z"
SessionIndex="VOZ+dlWSTR33dFexpmtMlIFti7M=KDtVbw==" SessionNotOnOrAfter="2008-09-
05T19:09:35Z">
      <ns2:AuthnContext>
      <ns2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
      edTransport</ns2:AuthnContextClassRef>
            </ns2:AuthnContext>
   </ns2:AuthnStatement>
         <ns2:AttributeStatement>
            <ns2:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
            format:unspecified">
              <ns2:AttributeValue>johnd@acme.com</ns2:AttributeValue>
              </ns2:Attribute>
              <ns2:Attribute Name="firstname"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
              <ns2:AttributeValue>John</ns2:AttributeValue>
              </ns2:Attribute>
              <ns2:Attribute Name="lastname"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
              <ns2:AttributeValue>Doe</ns2:AttributeValue>
              </ns2:Attribute>
              <ns2:Attribute Name="email"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
              <ns2:AttributeValue>johnd@acme.com</ns2:AttributeValue>
              </ns2:Attribute>
              <ns2:Attribute Name="optionalParams"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
              <ns2:AttributeValue>displayName=John Doe</ns2:AttributeValue>
              <ns2:AttributeValue>jobTitle=Product Manager</ns2:AttributeValue>
              <ns2:AttributeValue>companyName=Acme Widgets</ns2:AttributeValue>
              <ns2:AttributeValue>BusinessPhone=408.323.2345</ns2:AttributeValue>
              <ns2:AttributeValue>streetLine1=4610 Patrick Henry
Dr.</ns2:AttributeValue>
              <ns2:AttributeValue>city=Santa Clara</ns2:AttributeValue>
              <ns2:AttributeValue>state=CA</ns2:AttributeValue>
             <ns2:AttributeValue>zipCode=95054</ns2:AttributeValue>

              </ns2:Attribute>
         </ns2:AttributeStatement>
    </ns2:Assertion>
</Response>
```

Connect Authentication to WebEx Meeting Services

After users authenticate with Connect, they will automatically authenticated with their WebEx meeting site to schedule and host online meetings.

C5 Release

When a Connect user wants to host a WebEx meeting for the first time they are prompted to enter their WebEx site name, username and password. The WebEx meeting credentials are cached locally in the Window's registry so the user does not have to re-enter them to host later WebEx meetings. However if the user tries to host a WebEx meeting on another computer, they will have to re-enter their WebEx sitename, username and password.

Having Connect prompt the user for their WebEx username and password will not work if an organization has enabled SSO between their intranet and their WebEx meeting site. If SSO is enabled, users usually will not know their WebEx site password which is usually set to random strings.

C6 Release

In the C6 release, after the user is authenticated to Connect, the system will match their Connect account to their WebEx meeting site account and automatically authenticate them to host WebEx meetings.

By default the user's Connect account is linked to their WebEx site account by matching the user's Connect username to their email address on the WebEx site. If the organization's usernames do not match the WebEx email address, the customer admin can specify another Connect user profile field (company ID, etc) to match the WebEx site username or email address field.

When a user wants to start a WebEx meeting from Connect:

1. Connect client requests a WebEx Meeting session ticket from the Connect server
2. Connect server retrieves the WebEx meeting site for the user's org or group specified in the Org Admin tool.
3. Connect server authenticates to the WebEx Meeting servers.
4. Connect server identifies the user's WebEx site account by matching the Connect and WebEx user profile fields defined in the Connect Super Admin tool.
5. If a matching WebEx user account is found then the Connect server returns a WebEx Meeting session ticket.
    - Otherwise:
        a) If the WebEx site is set as an existing site in the Org Admin tool then Connect Server returns a user not found exception.
        b) If the WebEx site is set as a new site in Org Admin then the Connect Server will automatically provision a new WebEx meeting account and returns a session ticket.
6. Connect client makes WebEx XML and URL API calls to host meetings and authenticate using the WebEx Meeting session ticket.

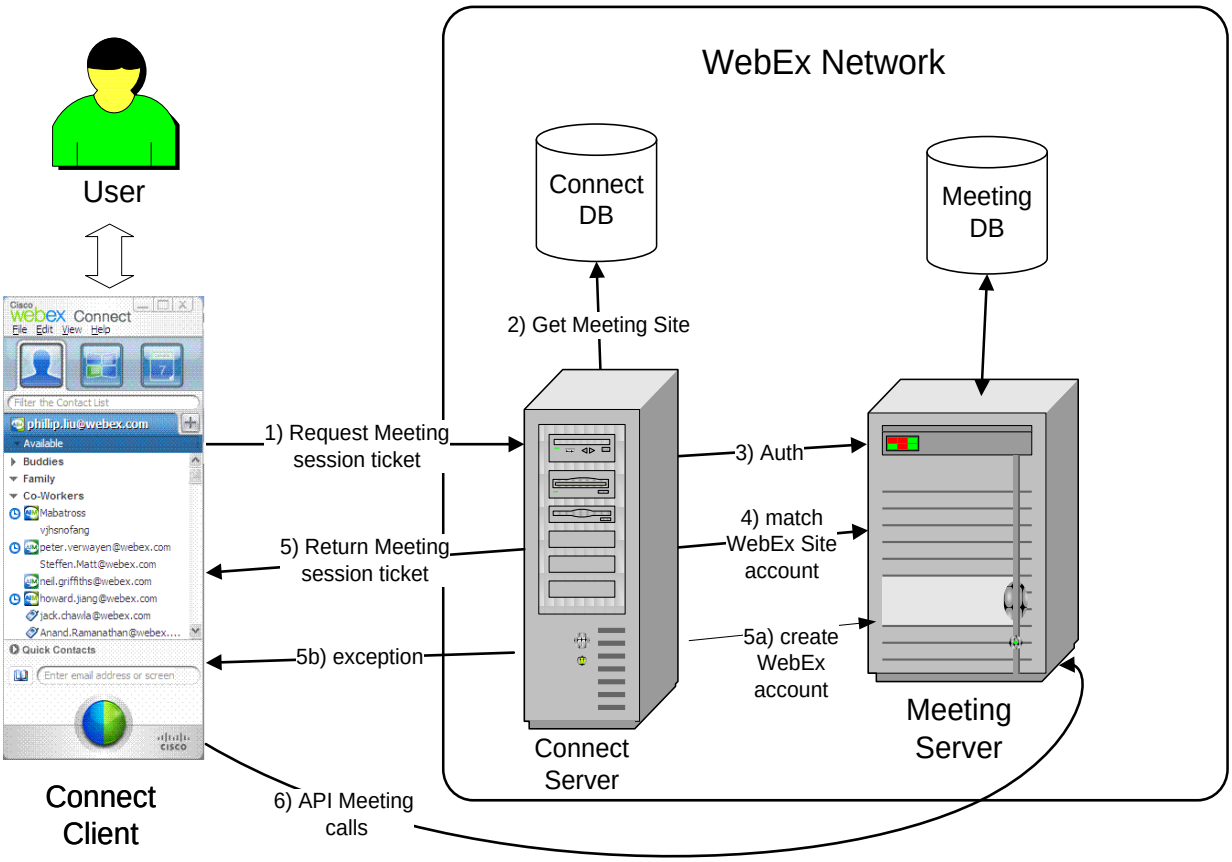

Figure 2: Connect authentication to WebEx Meeting Services

Reference

SAML v2.0 Technical Overview

J. Hughes, et al., Technical Overview of the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, February 2005. http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0.pdf

X.509 Certificates

Public key certificate, Wikipedia, May 2005. See http://en.wikipedia.org/wiki/Digital_certificate

X.509 Certificates and Certificate Revocation Lists, Sun Microsystems, May 2001. See http://java.sun.com/j2se/1.4.2/docs/guide/security/cert3.html