External Server Component Configuration for SIP Federation

This section provides information on the External Server Component Configuration for SIP Federation.

- Microsoft Component Configuration for SIP Federation, on page 1
- Requirements for SIP Federation with AOL, on page 4

Microsoft Component Configuration for SIP Federation

The following tables provide a brief checklist to configure federation on the Microsoft OCS and Access Edge servers. For detailed instructions on setting up and deploying the OCS server and the Access Edge server, refer to the Microsoft documentation.

Table 1: Configuration Tasks for Microsoft Components - OCS Server

Task	Procedure
Enable Global Federation Setting	1. In the global forest branch in the left pane, choose **Properties** > **Global Properties** > **Federation**. 2. Check the **Enable Federation and Public IM Connectivity** check box. 3. Enter the FQDN and the port number for the internal interface of the Access Edge server.
Configure the Access Edge server address	1. In the global forest branch in the left pane, choose **Properties** > **Global Properties** > **Edge Servers**. 2. In the **Access Edge and Web Conferencing Edge Servers** window, click **Add** . 3. Enter the FQDN for the internal interface of the Access Edge server.

Task	Procedure
Enable Each Front End Federation Setting	You need to enable the federation setting for each front-end server that is federating: 1. In the front-end server branch in the left pane, choose **Properties** > **Front End Properties** > **Federation**. 2. Check the **Enable Federation and Public IM Connectivity** check box.
Check your users are enabled for MOC and for Federation	- Choose the **Users** tab and check that your users are enabled for MOC. - If your user is not present in this list, you need to enable the user for MOC in Microsoft Active Directory. - You also need to enable the user for **Public IM Connectivity** in Microsoft Active Directory. Refer to the Microsoft Active Directory documentation at the following URL: http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx
Configure the security certificates	- You need to configure security certificates between the OCS server and the Access Edge server. - A CA server is required to perform this procedure. - Please refer to the Microsoft documentation for details on configuring security certificates between these servers.

Table 2: Configuration Tasks for Microsoft Components - Access Edge Server

Task	Procedure
Configure DNS	In the Microsoft enterprise deployment, you need to configure an external SRV record for all Access Edge Servers that points to _sipfederationtls._tcp.*domain*, over port 5061, where *domain* is the name of the SIP domain of your organization. This SRV should point to the external FQDN of the Access Edge server.

Task	Procedure
Configure IM and Presence Service as an IM Provider	**1.** On the external Access Edge server, choose **Start** > **Administrative Tools** > **Computer Management**. **2.** In the left pane, right-click **Microsoft Office Communications Server 2007**. **3.** Choose the **IM Provider** tab. **4.** Click **Add**. **5.** Check the **Allow the IM service provider** check box. **6.** Define the IM service provider name, for example, the IM and Presence Service node. **7.** Define the network address of the IM service provider, in this case the public FQDN of the IM and Presence Service node. **8.** Ensure that the IM service provider is not marked as “public”. **9.** Click the filtering option **Allow all communications from this provider** option. **10.** Click **OK**. In the IM and Presence Service enterprise deployment, you need to configure a DNS SRV record for each IM and Presence Service domain. The DNS SRV record should point to _sipfederationtls._tcp.*IM and Presence_domain* over port 5061, where *IM and Presence _domain* is the name of the IM and Presence Service domain. This DNS SRV should point to the public FQDN of the IM and Presence Service node.
Check the Access Method Settings	**1.** Iin the console tree, right-click on Microsoft Office Communications Server 2007. **2.** Choose **Properties** > **Access Methods**. **3.** Check the **Federation** check box. **4.** Check the**Allow discovery** check box if you are using DNS SRV.

Task	Procedure
Configure Access Edge to use TLSv1	1. To open the Local Security Policy, choose **Start** > **Administrative Tools** > **Local Security Policy**. **Note** If you are configuring this on a domain controller, the path is **Start** > **Administrative Tools** > **Domain Controller Security Policy**. 2. In the console tree, choose **Security Settings** > **Local Policies** > **Security Options**. 3. Double-click the FIPS security setting in the details pane. 4. Enable the FIPS security setting. 5. Click **OK**. **Note** There is a known issue with remote desktop to the Access Edge server with FIPS enabled on Windows XP. Refer to Unable to Remote Desktop to Access Edge for a resolution to this issue.
Configure the security certificates	• You need to configure security certificates between the OCS server and the Access Edge server. • A CA server is required to perform this procedure. • Please refer to the Microsoft documentation for details on configuring security certificates between these servers.

Requirements for SIP Federation with AOL

License Requirements for AOL Federation

You must order the AOL-FEDERATION SKU license from Cisco to allow you to turn on interdomain federation between the IM and Presence Service and AOL. When you submit this license request, Cisco requests from you the AOL customer routing and contact information described in the later sections of this topic. After Cisco receives your AOL customer routing and contact information, AOL federation between the IM and Presence Service and AOL is turned on.

Related Information -

AOL Routing Information Requirements

AOL Provisioning Information Requirements

Related Topics

AOL Routing Information Requirements, on page 5

AOL Provisioning Information Requirements, on page 5

AOL Routing Information Requirements

When you configure interdomain federation between the IM and Presence Service and AOL SIP Access Gateway, you must provide AOL with the following information.

Deployment Type	Provide (for each domain)	Notes
No load balancer	• The public FQDN of the federation routing IM and Presence Service node: <sip.domain.com> • The domain name of the IM and Presence Service node: @<domain.com>	• IM and Presence Service server certificate subject CN must match FQDN of the IM and Presence Service node • The CA that signs the IM and Presence Service server certificate must be trusted by the AOL server.
Load balancer	• The FQDN of the load balancer: <lb.domain.com> • The domain name of the load balancer: @<domain.com>	• IM and Presence Service server certificate subject CN must match FQDN of the load balancer. • The CA that signs the IM and Presence Service server certificate must be trusted by the AOL server.
	The secure SIP federation port of the IM and Presence Service node that is used for the domain	The AOL SIP Access Gateway connects (by way of SSL) to the IP address that is returned by an nslookup on this port. The default port is 5061.

We recommend that you work with your Cisco support representative to provide this information to AOL.

AOL Provisioning Information Requirements

We recommend that you work with your Cisco support representative to provide the following contact and provisioning information to AOL:

- The name of the enterprise, company or other.
- All local domain names hosted by IM and Presence Service, which are used for federation (for example, companyabc.com, sales-companyabc.com). From Release 10.5(1), you can find a full list of these names on the **Cisco Unified CM IM and Presence Administration** > **Presence Domains** window.
- The publically resolvable FQDN of the IM and Presence Service node that is being used for federation.
- The customer contact details: name, email address, phone number.
- Copy of certificate(s):

Note For further information on the required certificates, see AOL Routing Information Requirements.

- If the certificate is signed by a Certificate Authority, root certificate including the whole chain of certificates of the Certificate Authority must be provided.
- The base 64 encoding of the certificate(s) is required, for example:

```
BEGIN CERTIFICATE-----
MIIGKDCCBRCgAwIBAgIKH5c9LAAIAAGTvjANBgkqhkiG9w0BAQUFADCBizETMBEG
CgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCW1pY3Jvc29mdDEUMBIG.....
6HKfdML7AkWOV0Wiwc8HUb/0iFmfB24jWOnjj3NW15k0tDJXmbSMuAxjZ/2dZ4dA
4zd4FeZvoCzyVglPkoLvA0Z+AJyOkO7/tie4EF3n/kEedaPWimv2TpRrlAP5lBXn
tbM82NpEDaSqzg0d4Dswqe7W30CKGgUBYS1fO7xJHSRju719D+H7XivmjvU= -----END
CERTIFICATE-----
```

Note See, License Requirements for AOL Federation for further information on this process.