Integration Troubleshooting

IM and Presence Service Tracing

On the IM and Presence Service node, the SIP Proxy is responsible for SIP request routing, while the XCP SIP Federation Connection Manager is responsible for SIP Protocol Translation between Microsoft SIP and native XMPP. Therefore, these services are central to the SIP partitioned intradomain federation integration between IM and Presence Service and Skype for Business/Lync/OCS.

The XCP Router is a core service of IM and Presence Service. It determines whether the request recipient is a Microsoft server user or an IM and Presence Service user.

The locations of the log files are as follows:

- Logs for XCP SIP Federation Connection Manager: `/var/log/active/epas/trace/xcp/log/sip-cm-3_000*.log`
- Logs for SIP Proxy: `/var/log/active/epas/trace/esp/sdi/esp000*.log`
- Logs for XCP Router: `var/log/active/epas/trace/xcp/log/rtr-jsm-1_000*.log`

Example of SIP Proxy Logging

```
2:26:18.719 |PID(25333) sip_protocol.c(5964) Received 536 bytes TCP packet from
10.53.56.17:34282SUBSCRIBE sip:ysam@implync.net SIP/2.0^M
From:
<sip:fbear@implync.net>;tag=a4cdaec0-1138350a-13d8-45026-4d755b8a-2162aa7a-4d755b8a^M

To: <sip:ysam@implync.net>^M
Call-ID: a30386f0-1138350a-13d8-45026-4d755b8a-2c25871c-4d755b8a^M
CSeq: 1 SUBSCRIBE^M
Via: SIP/2.0/TCP 10.53.56.17:5080;branch=z9hG4bK-4d755b8a-926d95b4-3c330144^M
Expires: 7446^M
Accept: application/pidf+xml, application/cpim-pidf+xml^M
User-Agent: Cisco-Systems-Partitioned 8.0^M
Max-Forwards: 70^M
```

```
Event: presence^M
Contact: <sip:10.53.56.17:5080;transport=TCP>^M
Content-Length: 0^M
…
22:26:18.719 |ID(25333) sip_sm.c(4977) SIPGW Partitioned Fed UA Header found in
this request
22:26:18.719 |ID(25333) sip_sm.c(5010) This is a partitioned federation request,
 skip User Location DB lookup
22:26:18.719 |ID(25333) sip_sm.c(5200) This is an outbound Partitioned federation
 request.
 22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1435)
Routing: dipping for cuplcs.net
22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1473) Routing:
 Found domain route for cuplcs.net:10.53.56.18:5061;TLS pwf 1:1:5
22:26:18.719 |ID(25333) sip_dns.c(811) "A" Query for 10.53.56.18 successful, Got
 1 IP addresses
22:26:18.719 |ID(25333) sip_dns.c(139) A Record : 10.53.56.18
```

Example of SIP Federation Connection Manager Logging

The following is a extract from an outbound request log:

```
21:48:44.277 |SIPGWDir.cpp:463: [FROM XMPP] <presence from='fbear@implync.net'
to='ysam@implync.net' type='probe'/>...
...
21:48:44.743 |SIPGWController.cpp:622: Skipping DNS lookup: <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWController.cpp:704: Entering _handleOutContinue: <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWController.cpp:989: _findSession (JID): local(fbear@implync.net)
 remote(ysam@implync.net)
21:48:44.743 |SIPGWController.cpp:999: _findSession: Session not found
21:48:44.743 |SIPHostInfo.cpp:82: hostinfo(0x09a10ce8) refInc: 3
cuplcs.net:cuplcs.net
21:48:44.743 |SIPGWSession.cpp:58: Creating SIPGWSession sess=0x09a5a090
local=fbear@implync.net remote=ysam@implync.net
21:48:44.743 |SIPGWController.cpp:1017: _findSession: Made new session:
sess=0x09a5a090 local(fbear@implync.net) remote(ysam@implync.net)
21:48:44.743 |SIPGWSession.cpp:990: sess=0x09a5a090 Entering handleOut: <presence
 from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWSession.cpp:1090: _createOutgoingSubs local=fbear@implync.net,
 remote=ysam@implync.net
48:44.744 |SIPSubs.cpp:1037: from=<sip:fbear@implync.net> to=<sip:ysam@implync.net>
 local_contact=sip:10.53.56.17:5080;transport=TCP
remote_contact=sip:ysam@implync.net
```

Example of XCP Router Logging

```
12:29:24.762 |debug sdns_plugin-1.gwydlvm453 sdns_plugin handling:<presence
type='subscribed' to='ysam@implync.net' from='bbird@implync.net'><status>Already
 Subscribed</status></presence>
12:29:24.762 |debug ConnectionPool.cpp:166 connection pool checkout: ccm2/dbuser
 (success)
12:29:24.762 |debug IdsODBC.cpp:648 Performing SQL operation select userid, jsmid
 from enduser, enterprisenode where my_lower(xep106userid) = my_lower(?) and
primarynodeid=id
12:29:24.763 |debug ODBCConnection.cpp:315 (elapsed 0.002407) select userid, jsmid
 from enduser, enterprisenode where my_lower(xep106userid) = my_lower(?) and
primarynodeid=id
12:29:24.763 |debug CUPDatabaseAlgorithm.cpp:311 This is probably a Partitioned
```

```
OCS user ... redirecting to cm-3-sip-fed-s2s.gwydlvm453 component
12:29:24.763 |debug IdsODBC.cpp:229 (elapsed 0.000137) rollback
12:29:24.763 |debug ConnectionPool.cpp:207 connection pool checkin: ccm2/dbuser
(success)
12:29:24.763 |debug sdns_plugin-1.gwydlvm453 sdns_plugin redirecting to:
cm-3-sip-fed-s2s.gwydlvm453
```

You can enable debug tracing for the SIP Proxy, XCP SIP Federation Connection Manager and XCP Router on the Cisco Unified IM and Presence Service Serviceability user interface.

Configure Tracing on the IM and Presence Service

The following procedure describes how to configure tracing for the SIP Proxy, XCP SIP Federation Connection Manager and XCP Router services on the Cisco Unified IM and Presence Serviceability GUI. Repeat this procedure for each service that you want to configure for tracing.

Caution Debug level tracing can affect system performance. Enable debug level tracing only when required and reset to default log settings after the investigation is complete.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace** > **Configuration**.

Step 2 Choose the IM and Presence Service node, and click **Go**.

Step 3 Choose **IM and Presence Services** from the **Service Group** drop-down list, and click **Go**.

Step 4 From the Service drop-down list, choose one of the following options and click **Go**:

a) Cisco SIP Proxy
b) Cisco XCP SIP Federation Connection Manager
c) Cisco XCP Router

Step 5 Check the check box for **Trace On**.

Step 6 In the Trace Filter Settings area, choose the Debug Trace Level from the drop-down list. If you want to enable debug level tracing on the traces choose **Debug**.

Step 7 When you configure tracing for the SIP Proxy, there are a number of trace options under Trace Filter Settings. Check the check boxes for the following traces:

a) Enable SIP TCP Trace
b) Enable SIP TLS Trace
c) Enable Server Trace
d) Enable SIP Message and State Machine Trace
e) Enable Method/Event Routing Trace
f) Enable Routing Trace

Step 8 Click **Save**.

See the Cisco Unified IM and Presence Serviceability Online Help for more information about initiating debug tracing for each of these services.

Related Topics

Microsoft Server SIP Tracing, on page 4

Microsoft Server SIP Tracing

The Skype for Business/Lync/OCS SIP Proxy component is responsible for all SIP request routing. To debug any routing issues, you can enable debug tracing on the Microsoft server (Standard Edition or Enterprise Edition) using the method that is specific to your Microsoft server.

Enable SIP Tracing on Lync

The following procedure describes how to enable SIP tracing on Lync.

Procedure

Step 1 Choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Logging Tool**.

Step 2 In the Components area, check the **SIPStack** check box.

Step 3 Set Logging Level to All and click **Start Logging**.

Step 4 When you are ready to stop the trace click **Stop Logging**.

Step 5 Choose **Analyze Log Files** to view the logs.

Step 6 For a more structured analysis of the logs, download the Snooper tool and use it to view the log files.

Related Topics

IM and Presence Service Tracing, on page 1
Snooper Tool

Enable SIP Tracing on OCS

The following procedure describes how to enable SIP tracing on OCS.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Do one of the following depending on the edition:

a) If you are using Standard Edition, right-click on the OCS server name and choose **Logging Tool** > **New Debug Session**.

b) If you are using Enterprise Edition, right-click OCS pool name and choose **Logging Tool** > **New Debug Session**.

Step 3 In the Components area, check the **SIPStack** check box and in the Level area, click **All**.

Step 4 When you are ready to begin logging, click **Start Logging**.

Step 5 When you are ready to stop logging, click **Stop Logging**.

Step 6 Click **Analyze Log Files** to view the OCS SIP Proxy log analysis.

Related Topics

IM and Presence Service Tracing, on page 1
Snooper Tool

Common Integration Problems

This section describes some common integration problems.

Lync 2013 Client Repeatedly Logs out and Back in after IM and Presence Service User is Added to its Contact List

Troubleshooting Steps

1. Ensure that you have added all the required Access Control List (ACL) entries to IM and Presence Service and that the Cisco Sip Proxy service was restarted after adding any ACL entries.
2. If the problem persists, add an ACL entry of **All**, and then restart the Cisco SIP Proxy.

For more information about adding ACL entries, see topics related to configuring the incoming access control list.

Microsoft Server User Does Not Receive Pop-up when Added to IM and Presence Service Contact List

Troubleshooting Steps

1. If a valid availability state is shown for the contact, check whether the Microsoft Lync or Microsoft Office Communicator user previously accepted a subscription from the IM and Presence Service client user.

   Microsoft server subscription authorization is permanent, which means that if an IM and Presence Service client user removes and re-adds a Microsoft Lync or Microsoft Office Communicator user, no second pop-up appears.
2. If the “Waiting for Confirmation” state is shown for the contact, perform the remaining troubleshooting steps as required.
   - Ensure that the contact has a valid MOC SIP URI.
   - Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.
   - Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
   - Check that the partitioned federation routing mode applies to the chosen deployment.
   - Advanced Routing is supported only in single-cluster IM and Presence Service deployments.

- Ensure that the IM and Presence Service static routes are correctly configured to route requests to the Microsoft server. To do this, check the SIP Proxy logs on the IM and Presence Service user home node to see whether the SIP Proxy returns a SIP 408 Request Timeout error for the SIP NOTIFY request to the Microsoft server.

  Also check that an IM and Presence Service static route exists for the domain of the OCS/Lync user.
- If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
- If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 10.
- Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP NOTIFY.
- At the very least, there must be an IP address entry for each IM and Presence Service node.
- If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

Microsoft Server User Receives a Pop-up when Added to an IM and Presence Service Contact List but Has No Availability after Accepting

Troubleshooting Tip

Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Skype for Business/Lync/OCS servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.

IM and Presence Service User Does Not Receive a Pop-up when a Microsoft Lync or Microsoft Office Communicator User Adds the User to their Contact List

Troubleshooting Steps

1. If a valid availability state is shown, check whether IM and Presence Service is configured to automatically approve subscription requests from users within the local presence domain. If this feature is enabled, IM and Presence Service automatically approves the request without a pop-up to the IM and Presence Service user.
2. Otherwise, if "Status Unknown" or "Presence Unknown" is shown for the contact, perform the remaining troubleshooting steps as required.
3. Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.
4. Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
5. Check that the partitioned federation routing mode applies to the chosen deployment.

Advanced Routing is supported only in single-cluster IM and Presence Service deployments.

6. If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
7. If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 10.
8. Ensure that a static route that points to the routing IM and Presence Service node is configured on each Skype for Business/Lync/OCS Standard Edition server or Enterprise Edition pool. A static route should also be configured for each IM user domain that is configured on IM and Presence Service.
9. Ensure that each IM and Presence Service node is resolvable by Domain Name Service (DNS) from the Microsoft server deployment.
10. Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP NOTIFY message.
    a. At the very least, there must be an IP address entry for each IM and Presence Service node.
    b. If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.
11. Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Microsoft servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.
12. If this is a multicluster IM and Presence Service deployment, ensure that inter-cluster peering is correctly configured.
    a. Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Inter-Clustering** on the publisher node of the cluster that contains the designated routing IM and Presence Service node.
    b. Ensure that the list of inter-cluster peers includes a peer for the cluster on which the IM and Presence Service user is provisioned and that the number of Associated Users for that peer is greater than 0.
    c. Choose the inter-cluster peer to validate the Inter-cluster Peer Status.
    d. Ensure that there are no errors highlighted.

Microsoft Server User Does Not Receive IMs Sent by an IM and Presence Service User

Troubleshooting Steps

1. Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.
2. Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
3. Check that the partitioned federation routing mode applies to the chosen deployment.

   Advanced routing is supported only in single-cluster IM and Presence Service deployments.
4. Ensure that IM and Presence Service static routes are correctly configured to route requests to Skype for Business/Lync/OCS. To do this, check the SIP Proxy logs on the IM and Presence Service user home

node to see whether the SIP Proxy returns a SIP 408 Request Timeout error for the SIP INVITE request to the Microsoft server.

Also check that an IM and Presence Service static route exists for the domain of the OCS/Lync user.

5. If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
6. If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 10.
7. Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP INVITE request.
   a. At the very least, there must be an IP address entry for each IM and Presence Service node.
   b. If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

IM and Presence User Does Not Receive IMs Sent by a Microsoft Server User

Troubleshooting Steps

1. Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Server node.
2. Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
3. Check that the partitioned federation routing mode applies to the chosen deployment.

   Advanced routing is supported only in single-cluster IM and Presence Service deployments.
4. For Microsoft Lync, ensure that TLS encryption is configured.
5. If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
6. If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 10.
7. Ensure that a static route that points to the routing IM and Presence Service node is configured on each Skype for Business/Lync/OCS Standard Edition server or Enterprise Edition pool.

   Also check that an IM and Presence Service static route exists for the domain of the Microsoft server user.
8. Ensure that each IM and Presence Service node is resolvable by DNS from the MIcrosoft server deployment.
9. Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP INVITE.
   a. At the very least, there must be an IP address entry for each IM and Presence Service node.
   b. If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

10. Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Microsoft servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.
11. If this is a multicluster IM and Presence Service deployment, ensure that inter-cluster peering is correctly configured.
    a. Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Presence** > **Inter-Clustering** on the publisher node of the cluster that contains the designated routing IM and Presence Service node.
    b. Ensure that the list of inter-cluster peers includes a peer for the cluster on which the IM and Presence Service user is provisioned and that the number of Associated Users for that peer is greater than 0.
    c. Click the inter-cluster peer to validate the Inter-cluster Peer Status.
    d. Ensure that there are no errors highlighted.

Microsoft Server User Updates and IMs Take up to 40 Seconds to Appear

Troubleshooting Steps

The most common reason for such delays is missing DNS configuration within the deployment. IM and Presence Service performs a reverse DNS lookup of the Skype for Business/Lync/OCS IP address from which it received the inbound SIP requests. If the IP address does not resolve to a hostname, the reverse lookup times out after approximately 20 seconds. If this occurs, the following log is generated in the SIP Proxy logs: incoming ACL check took over 2 seconds – check DNS.

To solve this problem, ensure that a DNS Pointer (PTR) record exists for each Microsoft server IP address.

When Advanced Routing Is Enabled, No Availability Is Exchanged Between IM and Presence Service and Microsoft Server

Troubleshooting Steps

1. Verify that Cisco Unified Communications Manager is synchronizing user data from Active Directory for all Skype for Business/Lync/OCS users.

   Advanced Routing is dependent on the Microsoft server SIP URI being synchronized to Cisco Unified Communications Manager from Active Directory.
2. Verify that Advanced Routing is enabled only if this is a single-cluster IM and Presence Service deployment.

IM and Presence Service User Does Not Appear in the Microsoft Server Address Book

Troubleshooting Steps

1. Ensure that a full synchronization by the Skype for Business/Lync/OCS Address Book Service has taken place since the IM and Presence Service user was migrated from the Microsoft server. This synchronization happens nightly by default.

2. Request the Microsoft Lync or Microsoft Office Communicator user to sign out and sign in to trigger a download of the new address book. By default, it may take more than an hour to download the new address book from the Microsoft server.
3. If the IM and Presence Service user was previously a Microsoft Lync or Microsoft Office Communicator user, ensure that the IM and Presence Service user still has their old Microsoft server SIP URI populated in Active Directory (msRTCSIP-PrimaryUserAddress).
4. If the IM and Presence Service user was not previously a Microsoft Lync or Microsoft Office Communicator user or if their old Microsoft server SIP URI has been cleared from Active Directory, you must manually populate the Active Directory msRTCSIP-PrimaryUserAddress field to ensure that the IM and Presence Service user appears in the Microsoft server address book. You must enter **`sip:user's_uri`** in the msRTCSIP-PrimaryUserAddress field.

IM and Presence Service Unable to Route Interdomain Federation Requests through Microsoft Server Deployment

Troubleshooting Steps

1. Verify that the Skype for Business/Lync/OCS deployment is correctly configured for interdomain federation. To do this, ensure that Microsoft server users can federate.
2. Ensure that the Cisco SIP Proxy and the Cisco SIP Federation Connection Manager are running on each IM and Presence Service node.
3. Ensure that IM and Presence Service is configured for interdomain federation to the external domain and that Direct Federation is enabled.
4. Ensure that a static route is configured on IM and Presence Service for the external domain and that the static route points to the Microsoft server.
5. Ensure that the external domain is included in the IM and Presence Service Access Control List (ACL).

TLS Handshake Errors between the IM and Presence Service and Microsoft Servers

Troubleshooting Steps

1. Verify that Skype for Business/Lync/OCS has been configured to listen for mutual TLS connections on port 5061.
2. Verify that the IM and Presence Service Application Listeners have been configured such that the Presence Peer Authentication Port is set to 5061.
3. Verify that the IM and Presence Service certificate is signed by the same certificate authority as the Microsoft server.
4. Verify that none of the Microsoft server or IM and Presence Service certificates have expired.
5. Verify that the Microsoft server certificate is configured for both Server Authentication and Client Authentication.

- Such certificates have an OID value of "1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2"
- If the certificate is configured for Server Authentication only, it has an OID value of "1.3.6.1.5.5.7.3.1"

6. Verify that the IM and Presence Service TLS Peer Subjects list contains the Subject Common Name (CN) used in certificates provided by the Microsoft server during TLS handshaking.
7. Verify that the IM and Presence Service TLS Peer Authentication TLS Context is configured correctly and that all TLS Peer Subjects have been chosen.

Incorrect SIP URI Specified for Microsoft Lync or Microsoft Office Communicator Users when Added to Cisco Unified Personal Communicator Contact List

Troubleshooting Step

Verify that the Cisco Unified Personal Communicator registry configuration is correct, in particular the LDAP_AttributeName_uri and LDAP_UriSchemeName subkeys. For more information see the chapter for Configuring Active Directory for in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* .

Display Names not Shown for Microsoft Lync or Microsoft Office Communicator Contacts on Cisco Unified Personal Communicator

Troubleshooting Step

Verify that the Cisco Unified Personal Communicator registry configuration is correct, in particular the LDAP_AttributeName_uri and LDAP_UriSchemeName subkeys. For more information, see topics related to configuring Active Directory in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

User Migration Troubleshooting

This section describes user migration tracing and common user migration problems.

User Migration Tracing

This section describes tools used for user migration tracing.

Export Contact List Tool

The Export Contact List tool allows an administrator to export contact lists in bulk from Skype for Business/Lync/OCS for migrating users. With each run the tool generates a log file called ExportContactsLog<Timestamp>.txt. The log file contains details about any failures or errors that have occurred. The log file is saved to the same location as the tool itself.

Some common reasons why errors can occur include:

- Incorrect input filename specified
- Misspellings in input file
- Users specified are not associated with the Microsoft server/pool that the tool is being run against

The following is an example of a log file for the Export Contact List tool:

```
>>------------------- 18/05/2011 16:59:38 ------------------->>Version: 2.1
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Current line item is: sip:ExampleUser@dtstfedcup2.com
[DEBUG] Exit>> ExportContacts.ExportContactsUtilities.getAllSipUriFromStandardFile
[DEBUG] Enter>> ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[DEBUG] Total number of users found is: 1
[DEBUG] Processing user number: 1
[INFO]  Preparing to get contacts for User [sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Searching for userInstanceId [SELECT * FROM MSFT_SIPESUserSetting WHERE
PrimaryURI = 'sip:ExampleUser@dtstfedcup2.com']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com, InstanceId
 : {7D777FD5-A8F6-8243-B4D6-7F331008C58C}
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Searching for contacts [SELECT * FROM MSFT_SIPESUserContactData WHERE
UserInstanceID = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found contact:  SIPURI : [SIP:lyncContact@dtstfedcup2.com] with GroupId:
 [1]
[DEBUG] Found contact:  SIPURI : [SIP:ExampleUser@dtstfedcup2.com] with GroupId:
 [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getGroups
[DEBUG] Searching for groups [SELECT * FROM MSFT_SIPESUserContactGroupData WHERE
 UserInstanceID = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found group:  groupName : [General] with GroupId: [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getGroups
[INFO]  User Processed Successfully
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>> ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[INFO]  Summary:
[INFO]  1 users successfully processed
[INFO]  0 users not found
[INFO]  0 users could not be processed due to errors
<<------------------- 18/05/2011 16:59:41 -------------------<<
```

Related Topics

IM and Presence Service BAT Contact List Import, on page 15

Disable Account Tool

The Disable Account tool connects to Active Directory (AD) and updates the users' Skype for Business/Lync/OCS attributes to disable their Microsoft server account. With each run the tool generates a log file called DisableAccountLog<Timestamp>.txt. The log file contains details about any failures or errors that have occurred. The log file is saved to the same location as the tool itself.

Some common reasons why errors can occur with this tool include:

- Incorrect input filename specified
- Misspellings in input file
- User does not exist in the Microsoft server database
- The administrator who is running the tool does not have read/write permissions for the AD
- The administrator did not allow enough time for the changes applied to AD by this tool to propagate down to the Microsoft server database. The migration may fail if the administrator moves on to the next migration step without validating that the changes have taken effect in the Microsoft server database.

The following is an example of a log file for the Disable Account tool:

```
>>------------------- 18/05/2011 17:02:07 ------------------->>Version: 2.0
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.AccountDisable.DisableUsersInFile
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.GetSipUriFromLine
[INFO]  Preparing to Disable Communications Server Account for User
[sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> DisableAccount.LdapConnection.DisableAccount
[INFO]  Searching for user [sip:ExampleUser@dtstfedcup2.com]
[INFO]  Search results returned
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[INFO]  Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com, DisplayName
 : Example User, Enabled : True
[DEBUG] Committed changes to the AD
[INFO]  User Account Disabled
[DEBUG] Exit>> DisableAccount.LdapConnection.DisableAccount
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.DisableUsersInFile
[INFO]  Summary:
[INFO]  1 users successfully processed
[INFO]  0 users not found
[INFO]  0 users could not be processed due to errors
<<------------------- 18/05/2011 17:02:08 -------------------<<
```

For more information about using the Disable Account tool, see topics related to disabling Microsoft server accounts for migrating users.

Delete Account Tool

The Delete Account tool allows you to delete migrating users so that presence requests for these users are later routed to IM and Presence Service while ensuring the deleted users are not removed from the contact list of any users that remain on Skype for Business/Lync/OCS. After you run the Delete Account tool, the tool generates a log file called `DeleteAccountLog<Timestamp>.txt` to the same directory as the tool. The log file contains details about any failures or errors that have occurred.

Some common reasons why errors can occur with this tool include:

- Incorrect input filename specified
- Incorrect database instance name specified
- Misspellings in the input file
- User does not exist in the Microsoft server database

The following is an example of a log file for the Delete Account tool:

```
>>------------------- 02/12/2013 15:13:50 ------------------->>
Version: 10.x.x-xx
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Attempting to Open connection with String :
Server=lyncServer\rtclocal;Database=rtc;Trusted_Connection=yes;
[DEBUG] Connection Opened Ok
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Resource']
[DEBUG] Found id [1077578877]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the Resource Table, appears to be a valid Communications Server
Database
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Endpoint']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Container']
[DEBUG] Found id [1202103323]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'HomedResource']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'CertificateStore']
[DEBUG] Found id [1826105546]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the CertificateStore table, dealing with a version of Lync.
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'ForestDirectory']
[DEBUG] Found id [853578079]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the ForestDirectory table, Creating Lync2013 Connection
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.CheckConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.CheckConnection
```

```
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DisableUsersInFile
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[INFO]  Preparing to Delete Communications Server Data for User
[lyncUser@lyncDomain.net]
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[INFO]  Found user [lyncUser06@cork.com] with ResourceId [1010], proceeding to
delete data
[DEBUG] Enter>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Ran dbo.RtcpDeleteHomedResourceTransaction for resource [1010]
[DEBUG] Deleted CachedContainerMember for resource [1010]
[DEBUG] Deleted ContainerMemberUser for resource [1010]
[DEBUG] Deleted PromptedSubscriber for resource [1010]
[DEBUG] Deleted Delegate for resource [1010]
[DEBUG] Ran RtcpDeleteConferenceParticipantByEnterpriseId for resource [1010]
[DEBUG] Deleted UserPolicy for resource [1010]
[DEBUG] Deleted ResourcePhone for resource [1010]
[DEBUG] Deleted RtcItem for resource [1010]
[DEBUG] Deleted PUIDDirectory for resource [1010]
[DEBUG] Deleted ResourceDirectory for resource [1010]
[DEBUG] Committing transaction for resource [1010]
[INFO]  Completed Updates for resource [1010]
[DEBUG] Exit>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DisableUsersInFile


Summary:
 Users successfully processed:      1
 Users not found:                   0
 Users not processed due to errors: 0
<<------------------- 02/12/2013 15:13:50 -------------------<<
```

For more information about using the Delete Account tool, see topics related to deleting user data from the database for migrating users.

IM and Presence Service BAT Contact List Import

The IM and Presence Service Bulk Administration Tool (BAT) tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file.
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

To access this log file, complete the following procedure:

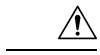
1. Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Bulk Administration** > **Job Scheduler**.
2. Click **Find**, and then choose the Job ID of the contact list import job.
3. Click the **Log File Name** link to open the log.

If you require further detail on any BAT job, see the Bulk Provisioning Service debug logs. You can access these logs at the following location: `/var/log/active/cm/trace/bps/log4j/bps000*.txt`

You can enable debug logging for the Bulk Provisioning Service on the **Cisco Unified IM and Presence Serviceability** user interface.

Configure Bulk Provisioning Service Logging on the IM and Presence Service

The following procedure describes how to configure Bulk Provisioning Service logging on IM and Presence Service.



Caution Debug level tracing can affect system performance. Enable debug level tracing only when required and reset to default log settings after the investigation is complete.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace** > **Configuration**.

Step 2 Choose the IM and Presence Service node and click **Go**.

Step 3 Choose **Database and Admin Services** from the Service Group drop-down list and click **Go**.

Step 4 Choose the **Bulk Provisioning Service** from the Service drop-down list and click **Go**.

Step 5 Choose **Trace On**.

Step 6 In the Trace Filter Settings, choose the Debug Trace Level. If you want to enable debug level on the traces, choose **Debug**.

Step 7 Click **Save**.

Related Topics

Export Contact List Tool, on page 11

IM and Presence Service Bulk Administration Tool Contact Rename

The IM and Presence Service Bulk Administration Tool (BAT) allows you to rename the contact ID (JID) in user contact lists from one format to another. For example, you can rename a user's contact ID from firstname.lastname@domain.com to userid@domain.com and the BAT updates each user's contact list with the new contact ID.

The Bulk Administration Tool writes the results of the contact rename job to a log file. The log file contains the following information:

- The number of contacts that have been successfully retrieved.
- The number of internal server errors that were encountered while trying to retrieve the contacts.

- The number of contact rename records that were ignored. The log file lists a reason for each record at the end of the log file.
- The number of contact rename records in the CSV file that were unprocessed due to an error that caused the bulk job to finish early. This error rarely occurs.
- The number of users that were notified of their contact changes.
- The number of users that could not be notified of their contact changes.

To access this log file, complete the following procedure:

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Bulk Administration** > **Job Scheduler**.
2. Click **Find** and choose the Job ID of the contact rename job.
3. Click the **Log File Name** link to open the log.

The following are common reasons why errors occur:

- The Cisco XCP Router service is stopped on a node in the cluster.
- The format of the uploaded CSV file is incorrect. You must ensure that the format of the file is correct and that the file header is present. For more information about the file format, see the related topic regarding the rename of contact IDs.
- Contact IDs have invalid characters or exceed the maximum allowed length.

If you require more detail about any bulk administration job, see the Bulk Provisioning Service debug logs. You can access these logs at the following location:
`/var/log/active/cm/trace/bps/log4j/bps000*.txt`.

You can enable debug logging for the Bulk Provisioning Service on the **Cisco Unified Serviceability** user interface. For more information, see topics related to debug logging and configuring BAT provisioning service logging.

Related Topics

Rename Contact IDs in IM and Presence Service Contact Lists
Configure Bulk Provisioning Service Logging on the IM and Presence Service, on page 16

Common User Migration Problems

This section describes some common user migration problems.

Application Failed to Initialize Properly - Error Occurs When Running Any of the User Migration Tools

Troubleshooting Steps

While attempting to run any of the user migration tools you may receive the following error: "Application failed to initialize properly". The reason for this error is that you are attempting to run the user migration tools without the .NET 2.0 Framework installed. Each of the user migration tools that Cisco provides requires that at least version 2.0 of the .NET Framework is installed on the server where you are running the tool.

The .NET 2.0 Framework comes installed as standard on Windows Server 2003 R2 or newer.

Export Contact List Tool does not Produce an Output File for Lync Users

Troubleshooting Steps

To export contact lists from a Lync server you must include the database instance parameter. If you omit the database instance parameter or enter an incorrect database parameter, an error is written to the Export Contact List log. Check the log to determine whether you omitted the database parameter or entered an incorrect parameter.

Follow these steps to find the database instance for each server/pool:

1. Open a powershell window on a front-end server in the pool.
2. Run the following cmdlet:

```
Get-CsManagementConnection
```

The database instance name is the value of the Data Source parameter in the command output.

Export Contact List Tool Log Shows getAndPrintContactsForUsers Error

Troubleshooting Steps

If you run the export tool for Lync users and see the following error in the log, “Error occurred in getAndPrintContactsForUsers”, then the Export Contact List tool cannot connect to the Lync database. Verify that the user account running the tool has the appropriate read permissions for the Lync database. Verify that dbo execution account privileges are granted to the RTC database. If this doesn't solve the issue, verify that there are no typographic errors in the database instance name.

Export Contact List Tool - Log Summary Shows Several Users as Not Found

Troubleshooting Steps

1. If you are using an IM and Presence Service exported file as the input, check that the correct domain is being used for the -d/ parameter and that there are no typographic errors in the file.
2. If you are using a SIP URI file as the input, check that the users are valid (exist in Active Directory [AD] and Skype for Business/Lync/OCS) and that they are entered correctly in the input file with the “sip:” prefix.
3. If you are not using an IM and Presence Service exported file or a SIP URI file as the input, or if you are using the OU input file, the user accounts are most likely disabled in AD. Re-enable the user accounts and run the tool again.

Export Contact List Tool - Tool Does Not Show the Progress Bar and Does Not Produce an Output File of Exported Contacts when Run in Normal Mode

Troubleshooting Steps

1. Check for the following error in the Export Contact List log: “Unable to connect to LDAP using IP/FQDN/Hostname: [some_ip_or_hostname].”

a. If the error exists, check that the address supplied for the Active Directory (AD) server is correct.
b. If the address supplied is valid, then ping the AD server to check that there is network connectivity between it and the Skype for Business/Lync/OCS server.
c. If there is connectivity, ensure that the user has the required privileges to access the AD server.

2. Check for the following error in the Export Contact List log: “Failed to open file….”
   a. If the error exists, the filename used for the -f/ parameter is misspelled or invalid.
   b. Check also that the input file does not contain spaces or special characters in its filename.
3. If you are running the Export Contact List Tool on OCS, ensure that you did not enter the database instance parameter. The database instance parameter is needed to export contacts from Lync only.

Disable Account Tool - Log Shows Unable to Connect to LDAP Using IP/FQDN/Hostname

Troubleshooting Steps

1. Check that the address supplied for the Active Directory (AD) server is correct.
2. If the address supplied is valid, ping the AD server to check that there is network connectivity between it and the Skype for Business/Lync/OCS server.
3. If there is connectivity, ensure that user has the required privileges to access the AD server.

Delete Account Tool - Unable to Find the Microsoft Server Database or Server Instance

Troubleshooting Steps

1. The Delete Account tool must be run against each database instance to ensure that the account is correctly deleted.
2. For OCS, follow these steps to find the database instance for each server/pool:
   a. On the OCS management console, choose the pool name under the Enterprise Pools (Enterprise Edition) or the server name under Standard Edition Servers (Standard Edition).
   b. In the right pane, choose the **Database** tab.
   c. The database instance name is the first item under **General Settings**.
3. For Lync, follow these steps to find the database instance for each server/pool:
   a. Open a powershell window on a front-end server in the pool.
   b. Run the following cmdlet:

      ```
      Get-CsManagementConnection
      ```

      The database instance name is the value of the Data Source parameter in the returned output.

Delete Account Tool - Log Shows Error While Connecting to the SQL Server

Troubleshooting Steps

1. Check the Delete Account tool logs to see the reason for this error. If the error is “The user is not associated with a trusted SQL Server connection”, the user running the tool does not have the required privileges to write to the Skype for Business/Lync/OCS database.
2. Rerun the tool with a user account that has the required privileges.

BAT Contact List Update - Uploaded Contact List File Not in Drop-Down List

Troubleshooting Steps

1. Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Bulk Administration** > **Upload/Download Files** and click **Find**.
2. Check that the file exists and that its function type is Import Users' Contacts – Custom File.
3. If a file exists with the incorrect function type, delete the file. If you deleted the file, or there is no file, upload the file again and ensure that its target is Contact Lists and its transaction type is Import Users' Contacts – Custom File.

BAT Contact List Update - No Log file Exists on Results Page after BAT Job

Troubleshooting Steps

If the log for the BAT import contacts job is missing from the job result page, the BAT job was run from a subscriber node. The log is accessible only from the publisher node. Log in to **Cisco Unified Communications Manager IM and Presence Administration** on the publisher node to view the log.

BAT Contact List Update - A User's Contacts Are Not Imported During BAT Job

Troubleshooting Steps

1. Check the job results log file for any specific errors.
2. Ensure that the user is licensed for IM and Presence.
3. Ensure that the user is assigned to a node within this cluster.
4. Ensure that the contact's domain is valid.

BAT Contact List Update - A User's Contacts Are Partially Imported During BAT Job

Troubleshooting Steps

1. Check the job results log file for any specific errors.
2. Ensure that the missing contacts are in a valid format in the CSV file.
3. Check that the user’s number of contacts does not exceed the Maximum Contact List Size on the system.

4. Check that the user's number of watchers does not exceed the Maximum Watchers on the system.

BAT Contact List Update - No Contacts are Imported During BAT Job

Troubleshooting Steps

1. Check the job results log file for any specific errors.
2. Ensure that the import file is in a valid format.
3. Ensure that all the users are licensed for IM and Presence Service.
4. Ensure that all the users are assigned on the local cluster.
5. Ensure that the Cisco Presence Engine service is running on all nodes within the cluster.

Migrating User Status Appears as Status Unknown or Presence Unknown to Microsoft Server Users during the Migration Process

Troubleshooting Steps

1. Ensure that contacts have been fully migrated to IM and Presence Service as described in this document.

   There is a period during the migration process when availability of migration contacts is not visible to Microsoft Lync or Microsoft Office Communicator users. Cisco recommends that user migration takes place during a scheduled maintenance window to reduce the occurrence of such issues.

2. Request Microsoft Lync or Microsoft Office Communicator users to sign out and sign in again.

   After the migrated contacts are imported into IM and Presence Service, Microsoft server users do not see availability for these contacts until they have signed out and back in to their clients.

3. If the problem persists, ensure that the migration steps were correctly followed, as defined in this document.
   - Verify that the updates that were applied by the Disable Account tool were synchronized to Skype for Business/Lync/OCS before you ran the Delete Account tool.
   - Ensure that you ran the Delete Account tool on all Standard Edition Microsoft servers or Enterprise Edition pools.
   - If these steps were not performed correctly, then repeat to resolve this issue as follows:
     - Run the Disable Account tool.
     - Verify that the AD updates made by the Disable Account tool have synchronized to the Microsoft server.
     - Run the Delete Account tool.

4. If migrated contacts are still appearing with a state of "Presence Unknown" there may be an issue with the integration between the IM and Presence Service and the Microsoft server. To help troubleshoot integration issues, see Common Integration Problems, on page 5.