From Zero to Hero

Sametime Unified Telephony Lite Client:
Configuring SIP trunks to third-party audio/video equipment
Contents

Edition Notice........................................................................................................................................... 4

1 Introduction............................................................................................................................................... 5
  1.1 What is Sametime Unified Telephony Lite Client?............................................................................ 5
  1.2 How Sametime Unified Telephony Lite Client uses SIP trunking...................................................... 5
  1.3 Terms used in this guide ................................................................................................................... 6
  1.4 Making calls with Sametime Unified Telephony Lite Client............................................................. 7
  1.5 Sametime Unified Telephony Lite Client limitations......................................................................... 10
  1.6 Example Sametime Unified Telephony Lite Client configuration.................................................... 11

2 Designing the dial plan............................................................................................................................. 12
  2.1 Customizing telephone numbers....................................................................................................... 12
  2.2 Mapping dial strings to SIP endpoints............................................................................................... 12
  2.3 Planning routing rules....................................................................................................................... 13
    2.3.1 Defining routing conditions......................................................................................................... 13
    2.3.2 Defining routing destinations...................................................................................................... 14

3 Enabling Sametime Unified Telephony Lite Client............................................................................. 16
  3.1 Activating the Sametime Unified Telephony Lite Client license....................................................... 16
  3.2 Enabling the Sametime Unified Telephony Lite Client feature....................................................... 18
  3.3 Modifying the Sametime policy to allow SIP trunking calls............................................................. 20

4 Verifying the ports used by the Sametime Media Manager components.............................................. 21
  4.1 Verifying the ports for a single Media Manager server.................................................................... 21
  4.2 Verifying the ports for a stand-alone SIP Proxy/Registrar or Conference Manager............................ 22
  4.3 Verifying the ports for a cluster of SIP Proxy/Registrars.................................................................... 23

5 Disabling SIP security............................................................................................................................. 24
  5.1 Changing the security role for the SIP Proxy/Registrar...................................................................... 24
  5.2 Disabling TLS on the SIP Proxy/Registrar......................................................................................... 25

6 Configuring a custom attribute for authentication.............................................................................. 27

7 Configuring the inbound and outbound routes for Sametime.............................................................. 28
  7.2 Configuring the inbound route to Sametime...................................................................................... 28
  7.3 Configuring the outbound route to Cisco UCM.............................................................................. 31

8 Configuring Cisco UCM as a SIP endpoint for Sametime calls............................................................ 34
  8.1 Launching the UCM Administration Web Page.................................................................................. 34
Note: Before using this information and the product it supports, read the information in "Notices."

This edition applies to version 8.5.2 of IBM Sametime Unified Telephony Lite Client (program number 5724–J23) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
1 Introduction

The IBM® Unified Communications and Collaboration (IBM UC²®) vision makes easy to find, reach, and collaborate with others through a unified user experience. This strategy is implemented by means of the IBM Sametime® Unified Telephony and Sametime Unified Telephony Lite Client software offerings that make it easy for you to access and manage telephone communications from inside the Sametime Connect or Lotus Notes® client.

This guide examines the rich set of features, architecture, and configuration options for Sametime Unified Telephony Lite Client by walking you through an example configuration of the SIP trunking feature with third-party audio/video equipment.

1.1 What is Sametime Unified Telephony Lite Client?

Sametime 8.5.2 introduces Sametime Unified Telephony Lite Client, which provides a new SIP trunking feature for the integration of the Sametime Connect client with third-party audio and video equipment used within your organization. Sametime Unified Telephony Lite Client is a separately licensed feature that builds on your Sametime Standard deployment to add SIP-based telephony to the feature set.

Sametime Unified Telephony Lite Client's SIP trunking feature provides the ability for a Sametime Connect client to make and receive point-to-point calls, using the Sametime Audio/Video Conferencing service provider, across the Internet to external SIP endpoints such as Cisco Unified Communications Manager. When the Sametime Connect user dials a phone number or SIP URI (a SIP-based address), Sametime Unified Telephony Lite Client establishes a SIP-based internet telephone call.

1.2 How Sametime Unified Telephony Lite Client uses SIP trunking

A SIP trunk is a direct IP network connection between the Sametime Media Manager's SIP Proxy/Registrar component and an external SIP endpoint. During deployment, the Sametime Administrator defines a unique static route that the SIP trunk uses for this connection.

Once the SIP trunk is configured, both inbound and outbound SIP-based calls are supported by the Sametime Media Manager's Conference Manager component, which facilitates the interaction of the Sametime Audio/Video Conferencing Service with the Sametime client's softphone components (used for telephony).
### 1.3 Terms used in this guide

This guide uses the following specialized terms when explaining how you can configure the Sametime Unified Telephony Lite Client feature in your Sametime deployment:

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>dial plan</td>
<td>The set of dial strings (phone numbers), routes (connections), and rules (conditions) that enable one user to place a telephone call to another user.</td>
</tr>
<tr>
<td>dial string</td>
<td>A numbering scheme that establishes the format (expected number and pattern of characters) for a telephone number. The dial string specifies how to interpret character sequences dialed by the user, and how to convert those sequences into a telephone number for an outbound call.</td>
</tr>
<tr>
<td>MCU</td>
<td>Multipoint Control Unit: a bridge that interconnects calls from multiple sources, enabling three or more endpoints to participate in a single call. Also known as a mixer.</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network: the traditional international telephone system based on copper wires carrying analog voice data. Telephone service carried by the PSTN is sometimes called plain old telephone service (POTS).</td>
</tr>
<tr>
<td>(S)RTP</td>
<td>(Secure) Real-time Transport Protocol: a standardized packet format used for delivering audio and video data over the Internet.</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol: a signaling protocol used for negotiating an audio/video session over the Internet.</td>
</tr>
<tr>
<td>SIP endpoint</td>
<td>A user agent that implements Session Initiation Protocol to send and receive audio/video data.</td>
</tr>
<tr>
<td>SIP trunk</td>
<td>A transmission channel between two points using Session Initiation Protocol. SIP trunking is an advanced form of VoIP that supports conference calls (multiple people can speak) and multicast sessions (one person speaks, many listen) in addition to traditional two-party phone calls.</td>
</tr>
<tr>
<td>SIP URI</td>
<td>An address used for calling someone with internet-based telephony using the SIP protocol; think of it as the person's internet-based telephone number. A SIP URI resembles an email address and is written in the following format: sip:user@host:port; for example: sip:<a href="mailto:tjwatson@example.com">tjwatson@example.com</a> or sip:<a href="mailto:16175551212@phonesystem.example.com">16175551212@phonesystem.example.com</a>. Just as a phone number identifies a particular telephone or mobile phone user, a SIP URI identifies a particular computer phone user or desktop video conferencing device in Sametime Unified Telephony Lite Client.</td>
</tr>
<tr>
<td>softphone</td>
<td>A component of the Sametime Connect client (stand-alone or embedded in Lotus Notes) that acts as an interface allowing you to dial numbers and carry out other phone functions using a screen (that of your computer or mobile device) and your mouse, keyboard, or keypad.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security: an encryption protocol that provides secure communications over the Internet. Early versions of TLS were called SSL (Secure Socket Layer).</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol: a generic term used to describe the routing of voice conversations over the Internet or through any other IP-based network. In its basic implementation, VoIP enables a two-party conversation but does not support phone conferences (multiple people can speak) or multicast sessions (one person speaks, many listen) as SIP trunking does.</td>
</tr>
</tbody>
</table>
1.4 Making calls with Sametime Unified Telephony Lite Client

To the user, the only difference between making calls with conventional Sametime audio/video capabilities and Sametime Unified Telephony Lite Client is the use of SIP URIs. Just like a phone number identifies a telephone or mobile phone user, a SIP URI identifies a computer phone or desktop video-conferencing device in Sametime Unified Telephony Lite Client.

As in previous releases of Sametime, users can initiate calls from several different areas of the user interface. When Sametime Unified Telephony Lite Client is configured, the user can enter either a phone number or a SIP URI:

- **Right-click options**
- **Quickfind**
- **Action Bar icons**
- **Phonebook**
- **Dialing keypad**
- **Call History**
If the user searches for a contact using QuickFind, Sametime searches the call history, the phone book, and the LDAP directory for the specified telephone number or SIP URI. For example, if the user types "sip:" in the QuickFind box, Sametime searches for SIP URLs (contacts beginning with "sip:"

![Image 1](image1.png)

When Sametime locates the telephone number or SIP URI, a call is initiated. When the call is connected, the Call Status dialog box appears to let the user know that the connection is complete. In this picture, user Sam Curman is placing a call with Sametime Unified Telephony Lite Client:

![Image 2](image2.png)

The callee (the person receiving the call) is notified next. If the call is made to the callee's telephone, the telephone rings. If the call is made to a computer softphone, the Call dialog box appears on the callee's computer, allowing that person to accept or decline the call:

![Image 3](image3.png)
Adding SIP URIs to the Sametime Phonebook

You can add SIP URIs to your Sametime Phonebooks just as you add telephone numbers. For example:

1. In the Connect client, open the Sametime Phonebook by clicking **Tools Sametime > Phonebook**.

2. Fill in the New Entry form, and then click the **Add** button to add this entry to the phonebook:

3. If you want this user to appear in your Contacts list, click the **Show in Contact List** that appears above the form.

4. When you have finished adding contacts, click the **Save** button to save your updates to the phonebook.
1.5 Sametime Unified Telephony Lite Client limitations

Sametime Unified Telephony Lite Client's SIP Trunking functionality has the following features and limitations:

- Sametime Unified Telephony Lite Client's SIP trunking feature is limited to point-to-point calls with the Sametime Audio/Video Conferencing service provider.
- Only Sametime Connect stand-alone and embedded clients (within Lotus Notes) are supported; browser-based clients cannot serve as an endpoint for SIP-based calls.
- Users cannot call into a Sametime meeting using Sametime Unified Telephony Lite Client.
- NAT traversal via Sametime 8.5.2 TURN server is not supported.
- Call-routing rules and preferences are not supported.
- Point-to-point calls are supported between one Sametime Connect Client user and one external SIP endpoint (including conference bridges).

The SIP Trunking functionality is implemented according to the following Internet Engineering Task Force (IETF) standards publications:

- [RFC 3264](https://tools.ietf.org/html/rfc3264) An Offer/Answer Model with the Session Description Protocol (SDP)
- [RFC 3551](https://tools.ietf.org/html/rfc3551) RTP Profile for Audio and Video Conferences with Minimal Control
- [RFC 2833](https://tools.ietf.org/html/rfc2833) RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
1.6 Example Sametime Unified Telephony Lite Client configuration

The example configuration used in this guide includes a Sametime Community Server and a Sametime Media Manager server in the Sametime 8.5.2 deployment, plus Cisco Unified Communications Manager 8.0.1.

In this configuration, the Sametime user is running Sametime Connect client, which hosts the Sametime Softphone. The Sametime Media Manager is installed on a single computer, which hosts the SIP Proxy/Registrar, Conference Manager, and Packet Switcher components. The SIP Proxy/Registrar functions as a SIP endpoint, routing calls to and from the Sametime client.

The Cisco UCM (Unified Communication Manager) is installed on its own computer and functions as the SIP endpoint for users with Cisco desk phones. Cisco UCM serves as a PBX, or trunk, to the desk phone users; the connection between Cisco UCM and the Sametime SIP Proxy/Registrar is called the SIP trunk.
2 Designing the dial plan

Before you begin configuring Sametime Unified Telephony Lite Client, you should figure out how calls from Sametime will connect to the third-party SIP endpoint by working out a dial plan. A dial plan is the set of dial strings (phone numbers), rules (conditions), and SIP endpoints (destinations) that enable one user to place a telephone call to another user. Planning the dial plan now means you won't have to stop and figure this out while stepping through the configuration screens later.

2.1 Customizing telephone numbers

The Sametime 8.5.2 Software Development Kit includes documentation and a sample application for a new Telephone Number Service extension that allows you to control the retrieval and formatting of telephone numbers used to make telephone calls from the Sametime client. This extension is useful when phone numbers retrieved from the corporate directory, or entered by users, might require modification to meet dialing plan requirements; for example during the telephony integration of a deployment that depends on LDAP entries other than the default telephoneNumber attribute. For more information, see Chapter 5 of the Sametime Telephony API Guide (ClientTelephony.pdf), available in the Sametime SDK at the IBM developerWorks site.

2.2 Mapping dial strings to SIP endpoints

For each type of phone or video device supported by your deployment, define the format of the dial string (what the user enters to make a call), the SIP endpoint that will route the call, and the device that will receive calls from that SIP endpoint.

Later, you will configure routes that map each device's dial string to its designated SIP endpoint, and rules that define how that mapping works. When a user dials a string to initiate a call, the routing rules are consulted and if a matching dial string format is found, the call is routed to the associated SIP endpoint, which in turn directs the call to the corresponding telephone or device.

Create a table like the one shown here, where you specify a dial string pattern, the name of the SIP endpoint that services calls matching that pattern, and the name of the end-user device that receives the call. This will help you define routes and routing rules.

<table>
<thead>
<tr>
<th>Dial String</th>
<th>SIP endpoint</th>
<th>Phone/Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>512250300X</td>
<td>Sametime SIP Proxy/Registrar</td>
<td>Sametime Softphone</td>
</tr>
<tr>
<td>14XXX</td>
<td>Cisco Unified Communications Manager</td>
<td>Cisco Desk Phone</td>
</tr>
<tr>
<td>14000</td>
<td>Cisco Unified Communications Manager</td>
<td>Cisco Unity Voice mail</td>
</tr>
<tr>
<td>9XXXXXXXXXXXXXX</td>
<td>Cisco Unified Communications Manager</td>
<td>PSTN (traditional telephone system)</td>
</tr>
<tr>
<td>@vcs.lotus.com</td>
<td>Tandberg Video Conferencing</td>
<td>Video Conferencing device</td>
</tr>
<tr>
<td>514XX</td>
<td>Avaya Session Manager</td>
<td>Avaya Communication Manager Desk Phone</td>
</tr>
</tbody>
</table>
The example configuration used in this guide includes only the Sametime softphone (used by Sametime clients) and the Cisco desk phone; however, Appendix B presents a more complex configuration that includes the additional devices shown in this table and demonstrates how to prioritize the routing rules.

2.3 Planning routing rules

Routing rules tell Sametime where to direct calls under certain conditions. The rule consists of one or more conditions, and a destination (SIP endpoint) where call requests that meet the conditions will be routed.

When you create routing rules for the example configuration in section 7, "Configuring the inbound and outbound routes for Sametime", the conditions and destination addresses are provided for you. When you deploy Sametime Unified Telephony Lite Client for yourself, you should take the time to plan the routing rules in advance to ensure an error-free configuration.

Note Some of the fields used to define routing rules must be formatted as regular expressions. Appendix A contains information on constructing regular expressions.

2.3.1 Defining routing conditions

A routing rule must include at least one condition; if it includes multiple conditions, the SIP call request must satisfy all of them to be matched to the associated route. As soon as a match is found, Sametime stops checking other conditions and routes the call; however, you can configure multiple routes with a different condition for each and then prioritize them.

The routing rule can include conditions in any or all of these SIP request fields:

<table>
<thead>
<tr>
<th>SIP request field</th>
<th>Description</th>
<th>Example condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>A predefined value indicating the type of request. Select the appropriate value from the field's list. If you do not select a method, then all methods are accepted by this condition.</td>
<td>INVITE, INFO, MESSAGE, or ANY</td>
</tr>
</tbody>
</table>
| Source Address          | The originating caller's IP address, which must match the pattern specified in the regular expression that you provide.                                                                                  | You could specify a single IP address: 9\.3\.186\.215  
Or use an expression to specify a range of IP addresses: 9\.3\.186\.215|9\.3\.186\.216                                         
Notice that the . is preceded with the escape character \ so it can be interpreted as a period and not the "any character" symbol. |
| Request URI             | The resource, usually the origin server, on which to apply the request. The URI must match the pattern specified in the regular expression that you provide.                                                  | For example:                                           |
|                         | .*example\.com.* matches these incoming initial requests: sip:example.com:5060;transport=tcp SIP/2.0  
sips:subdomain.example.com:5061 SIP/2.0                                                   |
| Contact Header          | The SIP URI of the originating caller. The URI must match the pattern.                                                                                                                                   | For example:                                           |
specified in the regular expression that you provide.

matches incoming initial requests with either of these contact header values:

```
<sip:20110@192.0.2.12:5060;transport=tcp>
<sips:user9920100@192.0.2.12:5061;transport=tcp>
```

2.3.2 Defining routing destinations

The routing destination is the SIP endpoint where the call will be directed. For incoming calls, the destination is the Sametime Media Manager's SIP Proxy and Registrar component. For outgoing calls, the destination is the third-party SIP endpoint.

You will specify a call's destination by constructing its address. There are two ways to construct the destination address: by pushing address information into one of the route's header fields, or by replacing the original request URI with the destination address.

**Push a Route header field**

Pushing a Route header field lets you define the destination address using the following fields in the outgoing call request's Route header:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>The scheme can be either <strong>SIP</strong> or <strong>SIPS</strong> (the secure version of SIP); the default is SIP. This field is required.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or fully qualified host name of the destination server (the SIP endpoint). For incoming calls, use the fully qualified domain name of the Sametime Media Manager's Conference Manager component. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the destination server (the SIP endpoint) is listening on for SIP-based communications. For incoming calls, use the port that the Sametime Media Manager's Conference Manager component is listening for SIP communications (typically port 5063 for unsecured communications and port 5062 for secure communications). This field is optional; if you do not provide a value, the server uses the correct port.</td>
</tr>
<tr>
<td>Transport</td>
<td>The network transport protocol to use for sending SIP messages: <strong>TCP</strong> or <strong>TLS over TCP</strong> (UDP is not supported). Use the same transport protocol throughout the entire route (from the Sametime client to the SIP Proxy/Registrar to the third-party SIP endpoint). For example, if the Media Manager is configured to use TLS for SIP communications, you must use TLS for all routes. This field is optional. If you do not provide a value, the server supplies a transport protocol.</td>
</tr>
</tbody>
</table>
**Replace a Request-URI**

Replacing the Request URI lets you substitute the destination address for the original Request URI in the outgoing call request. Supply values for the **Request-URI pattern** and **Output pattern** to create a destination address formed by a regular expression.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request-URI pattern</td>
<td>A regular expression defining the pattern of the original Request URI. Use this field to extract fields or parameters from a Request-URI of a SIP request. A variable stores the part of the Request-URI matched by the part of the regular expression inside the parentheses, indicated by a number. The variables are recalled with the dollar-sign, for example, $1, $2, and so on. These fields or parameters can be used to build the Output pattern. This field is optional.</td>
</tr>
<tr>
<td>Output pattern</td>
<td>A regular expression defining the pattern of the destination's URI (address). This field can contain either a SIP URI or a replacement expression with variables for example, $1, $2, and so on. Variables store the portion of a parenthesized pattern captured from the Request-URI pattern field. After processing any captured variables, the resulting field value must be a valid SIP or SIPS URI. <strong>Note</strong> If you do not provide a value in the Request-URI pattern field, this field must contain a valid SIP or SIPS URI.</td>
</tr>
</tbody>
</table>

The URI created using the output pattern is substituted into the original Request URI and then used for routing the call request.

**Examples:**

- Route all incoming SIP requests to this specific destination: sip:example.com;transport=tcp
  
  Request-URI pattern: empty
  
  Output pattern: sip:example.com;transport=tcp

- Route incoming SIP requests to a new host, keeping the original user name
  
  Request-URI pattern: sip:(.+}@.*
  
  Output pattern: sip:$1@example.com

  The variable $1 in the Output pattern refers to the first submatch in the Request-URI pattern, which is the first match enclosed in parentheses (in this example, the user name). In this example, the $1 will match the .+ portion of the Request-URI pattern.

- Route incoming SIP requests to "host," keeping the original user name if the user-name prefix in the Request-URI is "45."
  
  Request-URI pattern: sip:(45.+)@.*
  
  Output pattern: sip:$1@host
3 Enabling Sametime Unified Telephony Lite Client

Configuring Sametime Unified Telephony Lite Client requires you to activate a special product license, enable the Sametime Unified Telephony Lite Client feature, and set a new policy to allow SIP trunking calls.

You will perform all of the tasks in this section on the Sametime System Console.

3.1 Activating the Sametime Unified Telephony Lite Client license

Sametime Unified Telephony Lite Client is a separately licensed application that adds SIP trunking functionality to a Sametime Standard deployment. You must purchase the "IBM Sametime Unified Telephony Lite Client V8.5.2 Multiplatform Multilingual" product and then activate the license to enable configuration settings in the Sametime user interface.

1. On the computer hosting the Sametime System Console, open a browser and download the "IBM Sametime Unified Telephony Lite Client V8.5.2 Multiplatform Multilingual" image from the Passport Advantage web site to a temporary folder.

2. Open a command window, change to the folder containing the license enablement tool that you downloaded, and extract the files to the SametimeSystemConsole installation directory.

3. The license enablement files are stored in a subdirectory called SUTLiteClient; change to that directory.

4. Run the following command to activate the Sametime Unified Telephony Lite Client license:

   Linux: ./LiteClient.sh path_to_STSCServerCell
**Windows:** `LiteClient.bat path_to_STSCServerCell`

where `path_to_STSCServerCell` is the full path to the "STSCServerCell" (Sametime System Console cell) directory on that computer.

For example:

**Linux:** 
`./LiteClient.sh /opt/IBM/WebSphere/STSC/STSCServerCell`

**Windows:** `LiteClient.bat C:\IBM\WebSphere\STSC\STSCServerCell`

5. Accept the license agreement when prompted.
3.2 Enabling the Sametime Unified Telephony Lite Client feature

Enabling the Sametime Unified Telephony Lite Client feature allows the Sametime Media Manager to support the SIP trunking feature implemented in Sametime Unified Telephony Lite Client so that Sametime clients can make calls to third-party SIP endpoints, which in turn route calls to end-user devices such as telephones, softphones, and conference room video systems.

**Note** This setting is not available in the Sametime user interface until you activate the special product license in the previous task.

1. Log in to the Sametime System Console:
   a) From a browser, enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the Sametime system console server:
      
      \[http://serverhostname.domain:8700/ibm/console\]
      
      For example:
      
      \[http://sametime.example.com:8700/ibm/console\]
   b) Log in to the Integrated Solutions Console using the WebSphere® Application Server administrator ID and password that you created when you installed the Sametime System Console.
   c) On the navigation tree, click **Sametime System Console**.

2. Navigate to the Sametime Media Manager's administration pages:
   a) On the navigation tree, click **Sametime Servers > Sametime Media Manager**.

   ![Screen Shot](image)

   b) In the list of Deployment Identifiers, click one of the following:
      
      - If you installed all of the Media Manager components on a single computer, click the Media Manager server.
      - If you installed the Media Manager components on separate computers, click the Media Manager server and select the name of the Conference Manager deployment.

3. On the Configuration page, locate the "Sametime Unified Telephony Lite" section, click **Allow the use of Sametime Unified Telephony Lite clients**, and then click **OK**.
You do not need to restart the server at this point; you will restart it when you complete the remaining tasks in this section. Stay logged in to the Sametime System Console for the next task.
3.3 Modifying the Sametime policy to allow SIP trunking calls

Now that the Sametime Unified Telephony Lite Client feature has been enabled, set the policy that allows clients to use SIP trunking so they can take advantage of the new feature.

1. On the navigator, click Sametime System Console > Manage Policies.

2. On the Policies page, click the Media Manager tab.

3. On the Media Manager tab, select Sametime Media Manager Default Policy in the table, and then click the Edit button at the top of the table.

4. On the Media Manager default policies page, locate the "Sametime Unified Telephony Lite Client" section, select Allow calls that use SIP Trunk capability, and then click OK.
4 Verifying the ports used by the Sametime Media Manager components

Before you can set up static routes for SIP trunk calls, you must ensure that SIP traffic is directed to the correct ports. Connections from the third-party SIP trunk should be directed to the SIP Proxy/Registrar, which in turn routes communications to the Conference Manager so they can be directed to the Sametime client.

In the example (unsecured) configuration, the Conference Manager is listening on Port 5063 and the SIP Proxy/Registrar is listening on Port 5080. You will configure the SIP trunk connection (to the Cisco UCM in our example) to send inbound traffic to port 5080 so it can be handled by the SIP Proxy/Registrar, which will redirect the call to the Conference Manager (on port 5063) so routing to the Sametime client.

4.1 Verifying the ports for a single Media Manager server

If all of the Sametime Media Manager components are hosted in a single computer, follow these steps to verify the ports for both the SIP Proxy/Registrar component and the Conference Manager component.

1. On the Sametime System Console, log in to the Integrated Solutions Console as the WebSphere administrator (it may already be open from the last task).
2. In the navigation tree, click Servers > Server Types > WebSphere application servers.
3. In the list of WebSphere application servers, click STMediaServer.
4. On the Configuration page, locate the "Communications" section and click Ports.
5. In the Ports table, look for the port used by the Conference Manager, and write down the value:
   - If you are configuring TCP (unsecured) communications: SIP_DEFAULTHOST
   - If you are configuring TLS (secure) communications: SIP_DEFAULTHOST_SECURE

6. Next, check the port used by the SIP Proxy/Registrar, and write the value down:
   - If you are configuring TCP (unsecured) communications: SIP_ProxyRegHOST
   - If you are configuring TLS (secure) communications: SIP_ProxyRegHOST_SECURE

7. Skip to section 5, "Disabling SIP security".
4.2 Verifying the ports for a stand-alone SIP Proxy/Registrar or Conference Manager

If the Sametime Media Manager components are hosted on separate computers, follow these steps to verify the ports for the SIP Proxy/Registrar component and the Conference Manager component. The procedure is similar for both components--the only difference is when you select which server look at (step 3) and which port to write down (step 5 or 6).

1. On the Sametime System Console, log in to the Integrated Solutions Console as the WebSphere administrator (it may already be open from the last task).

2. In the navigation tree, click **Servers > Server Types > WebSphere application servers**.

3. In the list of WebSphere application servers, click the name of the server where the SIP Proxy/Registrar or the Conference Manager is hosted.

4. On the Configuration page, locate the "Communications" section and click **Ports**.

5. Conference Manager: In the Ports table, look for the port used by the Conference Manager, and write down the value:

   - If you are configuring TCP (unsecured) communications: **SIP_DEFAULTHOST**
   - If you are configuring TLS (secure) communications: **SIP_DEFAULTHOST_SECURE**

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Value</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_DEFAULTHOST</td>
<td>*</td>
<td>5063</td>
</tr>
<tr>
<td>SIP_DEFAULTHOST_SECURE</td>
<td>*</td>
<td>5062</td>
</tr>
</tbody>
</table>

6. SIP Proxy/Registrar: In the Ports table, look for the port used by the SIP Proxy/Registrar, and write the value down:

   - If you are configuring TCP (unsecured) communications: **SIP_ProxyRegHOST**
   - If you are configuring TLS (secure) communications: **SIP_ProxyRegHOST_SECURE**

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Value</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_ProxyRegHOST</td>
<td>*</td>
<td>5080</td>
</tr>
<tr>
<td>SIP_ProxyReg_SECURE</td>
<td>*</td>
<td>5081</td>
</tr>
</tbody>
</table>

7. Skip to section 5, "Disabling SIP security".
4.3 Verifying the ports for a cluster of SIP Proxy/Registrars

In a clustered environment, multiple SIP Proxy/Registrar instances are installed on separate nodes. Each set of nodes is clustered with a WebSphere Proxy servers deployed in front of the cluster to provide load balancing and failover. If you deploy two or more WebSphere proxy servers in front of the cluster, you must additionally deploy a load balancer to front the proxy servers.

For this task, you only need to check the ports used by the SIP Proxy/Registrar cluster. If a load balancer is in use, check its SIP ports; otherwise, check the WebSphere Proxy server's SIP ports.

Determining the SIP ports used by a Load Balancer

Check the port configured for SIP communications. and write down the value. Refer to your vendor documentation for information on configuring ports for the load balancer.

Determining the SIP ports used by WebSphere proxy server

1. Log in to the WebSphere proxy server's Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the proxy servers, click the name of the WebSphere proxy server that operates with the SIP Proxy/Registrar cluster.
4. On the Configuration page, locate the "Communications" section and click Ports.
5. In the Ports table, look for the following port and write down the value:
   - If you are configuring TCP (unsecured) communications: PROXY_SIP_ADDRESS
   - If you are configuring TLS (secure) communications: PROXY_SIPS_ADDRESS
5 Disabling SIP security

TLS encryption is fully supported for secure communications but to simplify configuration of Sametime Unified Telephony Lite Client, you should temporarily disable TLS before configuring the SIP Trunk. You can enable security again after the configuration is complete and verified.

5.1 Changing the security role for the SIP Proxy/Registrar

Modify the WebSphere security setting for the SIP Proxy/Registrar server or cluster.

1. On the computer hosting the complete Sametime Media Manager, the stand-alone SIP Proxy/Registrar component, or the deployment manager for a cluster of SIP Proxy/Registrars, log in to the Integrated Solutions Console as the WebSphere administrator.

2. In the navigation tree, click **Applications > Application Types > WebSphere enterprise applications.**

3. In the list of applications, click **IBM Lotus SIP Registrar.**

4. On the Configuration page, locate the "Detail Properties" section and click **Security role to user/group mapping.**

5. In the mapping table, select **All AuthenticatedUsers.**

6. Click the **Map special Subjects** list at the top of the table, and select **Everyone.**

7. Click **OK.**

8. Save the changes by click the **Save** link in the "Messages" box at the top of the page.
5.2 Disabling TLS on the SIP Proxy/Registrar

Use the Sametime System Console to disable TLS encryption through the Media Manager's administration page.

1. On the Sametime System Console, log in to the Integrated Solutions Console as the WebSphere administrator.

2. Navigate to the Sametime Media Manager's administration pages:
   a. On the navigation tree, click Sametime System Console > Sametime Servers > Sametime Media Manager.
   b. In the list of Deployment Identifiers, click one of the following:
      - If you installed all of the Media Manager components on a single computer, click the Media Manager's name.
      - If you installed the SIP Proxy and Registrar as a stand-alone component or a cluster, click the SIP Proxy and Registrar’s name.

3. On the Configuration page, locate the "SIP proxy registrar" settings in the "Server Integration" section and:
   a. Change the Port to use the unsecured port (typically 5080) that you wrote down in section 3, "Verifying the ports used by the Sametime Media Manager".
   b. Change the Transport Protocol to TCP.

4. In the "Audio Video Media" section, click Disable for the Secure Real-time Transport Protocol (SRTP) Encryption setting.

5. Click OK.
6. Restart the Packet Switcher server.

7. Restart the Conference Manager component's server or cluster:
   - For a stand-alone Media Manager or Conference Manager, restart it now as follows:
     a. In the server’s Integrated Solutions Console, click **Servers > Server Types > server_type**.
     b. In the list of servers, select your server and click the **Restart** button at the top of the table.
     c. Click the **Refresh** button and verify that all of the server components are active.
   - For a cluster of Conference Managers, synchronize and then restart the nodes:
     a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
     b. Select all nodes in the cluster, and then click the **Full Resynchronize** button at the top of the table.
     c. Back in the navigation tree, click **System Administration > Node Agents**.
     d. Select all nodes in the cluster, and then click the **Restart** button at the top of the table.
6 Configuring a custom attribute for authentication

By default, the SIP Proxy/Registrar is configured to use the mail attribute for authentication. If you are using a different attribute for the SIP trunking telephone number, modify the configuration to use that attribute for authentication.

**Note** This step is needed only if you are using an attribute other than mail for authentication.

1. On the computer hosting the deployment manager of SIP Proxy/Registrar, navigate to the server's directory:
   
   DM_install_root/config/cells/Cell_name/nodes/Node_name/servers/Server_name

2. Open the authorization.xml file in a text editor and add the statements to define the property that will be used for authentication against the LDAP directory:

   ```
   <authorizationProperty>
     <description>Telephone number for SIP trunking</description>
     <type>telephoneNumber</type>
     <!-- VMM property name-->
     <repositoryAttr>LDAP_attribute</repositoryAttr>
   </authorizationProperty>
   
   Where **LDAP_attribute** is the LDAP attribute that holds the telephone number used for SIP trunking.

3. Save and close the file.

4. If you are working with a cluster of SIP Proxy/Registrar, make this change to every instance of the file on the Deployment Manager's server (you can copy the modified file to the additional profiles).

5. Restart the SIP Proxy/Registrar server or cluster:
   
   - For a stand-alone Media Manager or SIP Proxy/Registrar, restart it now as follows:
     a. In the server’s Integrated Solutions Console, click **Servers > Server Types > server_type**.
     b. In the list of servers, select your server and click the **Restart** button at the top of the table.
     c. Click the **Refresh** button and verify that all of the server components are active.
   
   - For a cluster of SIP Proxy/Registrars, synchronize and then restart the cluster:
     a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
     b. Select all nodes in the cluster, and then click the **Full Resynchronize** button at the top of the table.
     c. Back in the navigation tree, click **Servers > Clusters > WebSphere application server clusters**.
     d. Select the SIP Proxy/Registrar cluster and click **Stop**.
     e. Wait until the cluster stops.
     f. Click the **Start** button to start the cluster.
7 Configuring the inbound and outbound routes for Sametime

Now that you have enabled the SIP trunking feature and set up the telephoneNumber attribute in the LDAP directory, you are ready to configure inbound routes for calls from third-party SIP endpoints to Sametime, and outbound routes for calls from Sametime to third-party SIP endpoints.

Configuring the call routes is a broad topic and may be dependent on your company's audio/video infrastructure and policies. The example configuration presented in this guide covers the scenario where you configure SIP trunking between Sametime and Cisco UCM to support calls between Sametime clients and Cisco desk phones. This requires that you define one inbound route (from Cisco UCM to Sametime) and one outbound route (from Sametime to Cisco UCM).

Appendix B presents a more complex scenario with trunks configured to multiple third-party PBXes and video conferencing systems.

7.2 Configuring the inbound route to Sametime

The SIP Proxy/Registrar uses inbound routes to receive call requests from third-party audio/video devices and then direct those calls to Sametime clients. For the example configuration, you will set up a static inbound route with a routing rule that tells the SIP Proxy/Registrar to direct all calls from the Cisco UCM's IP address to the Sametime Media Manager's Conference Manager component.

Configure an inbound route from Cisco UCM to Sametime as follows:

1. On the Sametime System Console, log in to the Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. On the SIP main menu page, look in the proxies table and click the Deployment Identifier of the SIP Proxy/Registrar.
4. On the SIP Proxy and Registrar page, click Proxy Administration.
5. In the routing rules table, click New to create a new rule.
6. On the Add New Rule page, type a name and description of the new inbound route in the Name and Description fields.
7. Use the "Conditions" section to configure the routing rule.
   For the example configuration, create a rule that routes all calls from the Cisco UCM to the Sametime Media Manager's Conference Manager component as follows:
   a. Click INVITE in the Method field.
   b. Click Source Address and type the IP address of the Cisco UCM.
   c. Leave the Request URI and Contact Header fields blank.
8. Use the "Destination" section to configure the route from Cisco UCM to Sametime:
   a. Click **Push a Route header field**.
   b. Click **Source Address** and type the IP address of the Cisco UCM.
   c. Click **Using fields** and fill in the fields in that subsection as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>Click <strong>SIP</strong>.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>Type the fully qualified domain name (FQDN) of the Sametime Media Manager's Conference Manager component.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port that the Sametime Media Manager's Conference Manager component is using for SIP communications -- this is the port you looked up in section 3, &quot;Verifying the ports used by the Sametime Media Manager&quot;.</td>
</tr>
<tr>
<td>Transport</td>
<td>Click <strong>TCP</strong>. Supported transport protocols are TCP and TLS over TCP (UDP is not supported). Use the same transport protocol throughout the entire route (from the Sametime client to the SIP Proxy/Registrar to the SIP endpoint). For example, if the Media Manager is configured to use TLS for SIP communications, you must use TLS for all routes. Note The example configuration will use TCP for unsecured communications. For information on configuring TLS encryption, see &quot;Configuring Transport Layer Security for the Sametime Media Manager&quot; in the Sametime documentation wiki.</td>
</tr>
</tbody>
</table>
9. Click OK to save the new inbound route.
7.3 Configuring the outbound route to Cisco UCM

The SIP Proxy/Registrar uses outbound routes to receive call requests from Sametime clients and then direct those calls to third-party SIP endpoints, which in turn route calls to the callee’s audio/video devices. For the example configuration, you will set up a static outbound route with a routing rule that tells the SIP Proxy/Registrar to direct all outgoing calls to the Cisco UCM.

Configure an outbound route from Sametime to Cisco UCM as follows:

1. On the Sametime System Console, log in to the Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.
3. On the SIP main menu page, look in the proxies table and click the **Deployment Identifier** of the SIP Proxy/Registrar.
4. On the SIP Proxy and Registrar page, click **Proxy Administration**.
5. In the routing rules table, click **New** to create a new rule.
6. On the Add New Rule page, type a name and description of the new outbound route in the **Name** and **Description** fields.
7. Use the "Conditions" section to configure the routing rule.
   
   For the example configuration, create a rule that routes all calls from Sametime to the Cisco UCM as follows:
   
   a. Click **INVITE** in the **Method** field.
   b. Click **Request URI** and type `sip:140.*`
This regular expression resolves to the SIP URI of the Sametime users in the example configuration.

c. Leave the Source Address and Contact Header fields blank; in this example you don't need to set conditions on them because you want all outgoing messages to be selected.

8. Use the "Destination" section to configure the route from Sametime to Cisco UCM:

The inbound route was based on values in a header field that was added to the SIP request; the additional values allow Sametime to finish routing the call. The outbound route is more complicated because it must change the Request URI to a format that Cisco UCM will accept before routing the call to the UCM.

The SIP requests for outgoing calls are generated by the Sametime client using the format sip:xxxxx@sip-pr-domain where "xxxxx" is the telephone number to call and sip-pr-domain is the domain name of the SIP Proxy/Registrar; for example: sip:14044614851@st852primary.austin.ibm.com. If the request is routed to Cisco UCM as-is, it will result in a “404-User not found” error because the UCM can only process requests that use its own domain and will reject all other requests.

To resolve this, your route definition will modify the Request URI by replacing the Sametime domain with the UCM's own domain. This is accomplished by specifying the pattern used by a Sametime URI, and then providing a new pattern to replace it. Both patterns include the "sip:" and "@" in the same positions, so there is no need to copy those values; and of course you do not want to copy the Sametime domain name -- only the user name needs to be copied over into the new Request URI. In effect, this drops the Sametime domain from the Request URI and replaces it with the UCM domain.

a. Click Replace a Request-URI.
b. Click **Using a regular expression**.

c. In the **Request-URI pattern** field, type `sip:(.+)?@.*`.

d. In the **Output pattern** field, type `sip:$1@9.3.186.215`

In the **Request URI pattern**, the expression within the parentheses `(.+)` will be assigned to a corresponding variable `$1` in the **Output pattern** (everything between "sip:" and ":@"; everything else is left alone). The **Output pattern** will copy that information into a new URI format that uses the UCM's domain before sending the modified request to the UCM.

For example, if the Sametime Request URI looks like this:

```
sip:14044614851@st852primary.austin.ibm.com
```

then it will be modified to look like this:

```
sip:14044614851@9.3.186.215
```

9. Click **OK** to save the new outbound route.

10. Restart the SIP Proxy/Registrar server or cluster:

    - For a stand-alone Media Manager or SIP Proxy/Registrar, restart it now as follows:
      a. In the server’s Integrated Solutions Console, click **Servers** > **Server Types** > `server_type`.
      b. In the list of servers, select your server and click the **Restart** button at the top of the table.
      c. Click the **Refresh** button and verify that all of the server components are active.

    - For a cluster of SIP Proxy/Registrars, synchronize and then restart the nodes:
      a. In the Deployment Manager's Integrated Solutions Console, click **System Administration** > **Nodes**.
      b. Select all nodes in the cluster, and then click the **Full Resynchronize** button at the top of the table.
      c. Back in the navigation tree, click **System Administration** > **Node Agents**.
      d. Select all nodes in the cluster, and then click the **Restart** button at the top of the table.
8 Configuring Cisco UCM as a SIP endpoint for Sametime calls

The Cisco UCM (Unified Communications Manager) is a software-based call-processing system that manages VoIP telephone calls. In the example configuration, you will configure the Cisco UCM to connect to the Sametime Media Manager's SIP Proxy/Registrar so it can complete IP-based telephony calls.

This section describes the relevant configuration of the Cisco UCM used in this example scenario.

8.1 Launching the UCM Administration Web Page

Cisco UCM provides a web-based administration tool that you will use for this task.

1. Open a browser and navigate to the following URL: https://IP_address_of_UCM:8443/ccmadmin/showHome.do

2. Log in using the UCM administration credentials.

3. Click System > Cisco Unified CM.

4. Click Find and select the CallManager.

8.2 Disabling auto-registration

When auto-registration of phone lines is enabled, UCM will not allow you to add lines manually. Disable auto-registration lines so that you can add phones and Directory Number (DN) lines manually.

1. In the "Auto-registration Information" section, click Auto-registration Disabled on this Cisco Unified CallManager to select it.

2. In the "Cisco Unified CallManager TCP Port Settings for this Server" section, fill in the following fields:
   - SIP Phone Port: type 5060
   - SIP Phone Secure Port: type 5061
3. Click Save.

8.3. Configuring region settings

Configure the region settings to use the audio codec and video call bandwidth supported by Sametime.

1. Select **System > Region**.
2. Click **Find** and select the **Default** region.
3. Verify the following settings:
   - Audio Codec: G.711
   - Video Call Bandwidth: 384
4. If either setting is incorrect, change it as follows:
   a. In the **Modify Relationship to other Regions** field, select **Default**.
   b. In the **Audio Codec** field, click **G.711**.
   c. In the **Video Call Bandwidth** field, click **384**.

8.4. Configuring the SIP trunk security profile

Configure the UCM's SIP trunk to use the same transport setting that you configured in Sametime. In the example configuration, Sametime uses TCP.

1. Select **System > Security > SIP Trunk Security Profile**.
2. On the SIP Trunk Security Profile Configuration page, click **Add New**.
3. Configure the new profile with the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Sametime SIP Trunk profile</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>Non Secure</td>
</tr>
<tr>
<td>Incoming Transport Type</td>
<td>TCP+UDP</td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>TCP</td>
</tr>
<tr>
<td>Incoming Port</td>
<td>5060</td>
</tr>
</tbody>
</table>

4. Click Save.

**8.5 Verifying the Standard SIP Profile configuration**

Verify that the Standard SIP Profile uses the settings required for supporting internet telephony calls to Sametime.

1. Click **Device > Device Settings**
2. Click **SIP Profile**.
3. Click **Find** to list configured SIP Profiles, and then click **Standard SIP Profile**.
4. Verify the following settings, changing them if needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Standard SIP Profile</td>
</tr>
<tr>
<td>Default MTP Telephony Event Payload Type</td>
<td>101</td>
</tr>
<tr>
<td>Disable Early Media on 180</td>
<td>□ Unselected</td>
</tr>
<tr>
<td>Conference Join Enabled</td>
<td>✓ Selected</td>
</tr>
<tr>
<td>RFC 2543 Hold</td>
<td>□ Unselected</td>
</tr>
<tr>
<td>Semi Attended Transfer</td>
<td>✓ Selected</td>
</tr>
<tr>
<td>Fall back to local RSVP</td>
<td>✓ Selected</td>
</tr>
</tbody>
</table>

5. Click Save.
8.6 Adding the SIP Trunk

Now that Cisco UCM is configured for communications with Sametime, add a SIP trunk to connect the two.

1. Click **Device > Trunk**.
2. On the Trunk Configuration page, click **Add New**.
3. Configure the new SIP trunk with the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk Type</td>
<td>Select SIP Trunk</td>
</tr>
<tr>
<td>Device Protocol</td>
<td>Select SIP</td>
</tr>
<tr>
<td>Trunk Service Type</td>
<td>Select &lt;None&gt; (the default)</td>
</tr>
</tbody>
</table>

4. Click **Next**.

5. In the "Device Information" section, fill in the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Type the name of the Sametime SIP Proxy/Registrar server</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief description</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Select <strong>Default</strong></td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>Select <strong>MRGL_1</strong></td>
</tr>
</tbody>
</table>

From Zero to Hero: Sametime Unified Telephony Lite Client 41
6. Click **Next**.

![SIP Information](image)

7. In the "SIP Information" section, fill in the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Address</td>
<td>Type the fully qualified host name of the Sametime SIP Proxy/Registrar.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>5080</td>
</tr>
<tr>
<td>Destination Address is an SRV</td>
<td></td>
</tr>
<tr>
<td>MTP Preferred Originating Codec</td>
<td>711ulaw</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Select <strong>Standard Presence Group</strong></td>
</tr>
<tr>
<td><strong>SIP Trunk Security Profile</strong></td>
<td>Select <strong>Non Secure SIP Trunk Profile</strong></td>
</tr>
<tr>
<td><strong>SIP Profile</strong></td>
<td>Select <strong>Standard SIP Profile</strong></td>
</tr>
<tr>
<td><strong>DTMF Signaling Method</strong></td>
<td>Select <strong>RFC 2833</strong></td>
</tr>
</tbody>
</table>

8. Click **Save**.
8.7 Adding a route pattern for calling Sametime

The route pattern maps the dial string for an outgoing call to the appropriate SIP endpoint; in this case the Sametime SIP Proxy/Registrar. You configure the route pattern using the dial string mappings that you defined in section 2.2, "Mapping dial strings to SIP endpoints". When a Cisco desk phone user dials a string matching this route pattern, Cisco UCM uses the information configured here to determine how to route the call to the Sametime SIP Proxy/Registrar.

1. Click **Call Routing > Route/Hunt > Route Pattern**.

2. On the Route Pattern Configuration page, click **Add New**.

3. In the "Pattern Definition" section, configure the dial string for calling Sametime as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern</td>
<td>512250XXXX</td>
</tr>
<tr>
<td></td>
<td>This is the dial string that you mapped to the Sametime SIP Proxy/Registrar.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>Select &lt;None&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for the route pattern; for example: Sametime</td>
</tr>
<tr>
<td>MLPP Precedence</td>
<td>Select Default</td>
</tr>
<tr>
<td>Gateway/Route List</td>
<td>Select st852primary</td>
</tr>
<tr>
<td></td>
<td>This is the name of the SIP Trunk that you defined in the Device Name field on the SIP Trunk Configuration page.</td>
</tr>
<tr>
<td>Route Option</td>
<td>Select Route this pattern</td>
</tr>
<tr>
<td>Call Classification</td>
<td>Select OffNet</td>
</tr>
</tbody>
</table>

4. Click **Configure Calling Party Transformations**.
5. In the "Calling Party Transformations" section, fill in the following settings to mask the Cisco desk phone number when it is displayed to the Sametime user:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Calling Party's External Phone Number Mask</td>
<td>☑ Selected</td>
</tr>
<tr>
<td>Calling Party Transform Mask</td>
<td>555XXXX</td>
</tr>
<tr>
<td>Calling Line ID Presentation</td>
<td>Select Allowed</td>
</tr>
<tr>
<td>Calling Name Presentation</td>
<td>Select Allowed</td>
</tr>
</tbody>
</table>

When the Cisco desk phone user makes a call, his or her phone number is displayed using the mask. For example, the Cisco desk phone dial string "14044614851" displays to the Sametime user as the nicely formatted "555-4851".
9 Verifying the configuration

Now that Sametime Unified Telephony Lite Client has been configured with the SIP trunking feature, it's time to test the configuration and verify that it works.

9.1 Verifying calls between the different phone systems

At this point, you should be able to make calls between Sametime clients and the third-party phones or devices.

Note The Sametime wiki contains detailed troubleshooting information.

When testing, it is always a good idea to run a packet analyzer such as Wireshark on the computer hosting the Sametime SIP Proxy/Registrar to ensure that SIP traffic is routing as expected.

Here's how to test the example configuration by placing calls between the Sametime client and a Cisco desk phone:

1. Enable Wireshark on the SIP Proxy/Registrar.
2. In Wireshark, add sip or rtp to the Filter.
3. Initiate a call from the Sametime client to a valid Cisco telephone number and verify the outbound route (use one of the calling options described in section 1.4, "Making calls with Sametime Unified Telephony Lite Client").
4. Now initiate a call from a Cisco desk phone to the Sametime client to verify the inbound route.

Tip In the Sametime client, click File > Preferences > Voice and Video to see what phone number is assigned to this client.

Once the basic calls are working over the SIP trunk, you can add more refined routing rules and configure secure communications by enabling TLS and SRTP. For instructions on enabling security, see the Sametime Unified Telephony Lite Client 8.5.2 documentation.
### 9.2 Calling scenarios supported by the example configuration

The example configuration described in this document supports the following call scenarios, which were verified using the applicable systems:

- Making basic calls to/from Cisco SCCP and SIP endpoints connected to Cisco Unified Communications Manager using the G.711 codec set.
  
  These calls were verified using both direct and indirect media. Sametime Unified Telephony Lite Client doesn't support G.729 and Cisco doesn't support other Sametime Unified Telephony Lite Client codecs.
- Transferring call from the Cisco desk phone to the Sametime client
- Putting calls on hold on the Cisco desk phone
- Pausing calls on the Sametime client and on Cisco desk phones
- Abandoning calls made between the two systems
- Hosting a phone conference on Cisco UCM with Sametime Unified Telephony Lite Client client and Cisco SCCP and SIP phones as attendees
- DTMF (dual-tone multi frequency) signals using RFC 2833
- SRTP security
- Display of caller's name and phone number
- Call forking, where an incoming call to a Cisco desk phone is simultaneously routed to the desk phone and to Sametime Unified Telephony Lite Client
Appendix A  Using regular expressions in routing rules

A regular expression is a pattern describing a certain amount of text. Regular expressions must follow a strict notation, different from other notation forms you may use. For example, the operating system shell notation for a wildcard (series of 0 or more characters) is the asterisk character: *, The regular expression equivalent for a wildcard is different: it is a combination of a dot followed by an asterisk, as follows: .*

The table below describes the basic symbols used in regular expressions and their meanings; there are many tutorials on regular expressions available on the web (for example, the Zytrax.com info site, which also includes information on using submatches in your expressions).

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[abc]</td>
<td>Match any character listed between brackets. In this case, a or b or c.</td>
</tr>
<tr>
<td>[^abc]</td>
<td>Match any character except those listed between the brackets. In this case, any characters except a, b and c.</td>
</tr>
<tr>
<td>X-X</td>
<td>A range is indicated by two characters (letters or digits) separated by a &quot;-&quot; sign and matches any element within the range, including the first character and the last character. One or more ranges can be specified inside the character class. For example: 2-7 matches any digit from 2 through 7. azA-CE-Z matches all lower case letters (a-z) and the following upper case letters: A, B, C (A-C) plus all letters from E through Z (E-Z); the letter D is excluded from this set.</td>
</tr>
<tr>
<td>.</td>
<td>Match any character except new-line</td>
</tr>
<tr>
<td>\d</td>
<td>One digit from zero through nine, inclusive (equivalent to: [0-9])</td>
</tr>
<tr>
<td>D</td>
<td>One non-numeric character</td>
</tr>
<tr>
<td>s</td>
<td>One whitespace character</td>
</tr>
<tr>
<td>S</td>
<td>One non-whitespace character</td>
</tr>
<tr>
<td>w</td>
<td>One word character</td>
</tr>
<tr>
<td>W</td>
<td>One non-word character</td>
</tr>
<tr>
<td>X+</td>
<td>Match the preceding element (X, in this case) one or more times</td>
</tr>
<tr>
<td>X*</td>
<td>Match the preceding element (X, in this case) zero or more times</td>
</tr>
<tr>
<td>X{n}</td>
<td>Match the preceding element (X, in this case) n times</td>
</tr>
<tr>
<td>X{n,}</td>
<td>Match the preceding element (X, in this case) at least n times</td>
</tr>
<tr>
<td>X{n,m}</td>
<td>Match the preceding element (X, in this case) at least n times, but no more than m times</td>
</tr>
<tr>
<td>(abc)?</td>
<td>Parentheses indicate an optional match</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

Tip Before configuring a routing rule for a route, you should test the regular expressions using any of the testing engines available online to make sure you have constructed it correctly.
Appendix B  Other example configurations

Sametime Unified Telephony Lite Client is not limited in the number of SIP Trunks that it supports. This appendix provides examples of additional static route configurations in a multi-vendor environment.

This picture expands the configuration diagram showing in section 1.6, "Example Sametime Unified Telephony Lite Client configuration" by adding the following third-party SIP endpoints to the deployment:

- Avaya Session Manager (integrated IP telephony, voice mail, and instant messaging)
- Avaya Communication Manager (VoIP on legacy PBXes)
- Cisco Video Communication Server (provided by Tandberg)
Enabling video calls with an MCU

This scenario configures an inbound route and an outbound route to support video conferencing with the Cisco Video Conferencing Server provided by Tandberg.

The code excerpts shown in the these scenarios are from the `proxy.xml` file, where the configuration changes made in the UI are stored. This file is found in the following location on the Sametime System Console:

\IBM\WebSphere\STSC\AppServer\profiles\STSCDMgrProfile\config\cells\st852primarySSCCell\nodes\st852primSTMSNode1\servers\STMediaServer

Configuring an outbound route from Sametime to Cisco Video Conferencing Server

If you have an MCU and want to enable video calls between room servers/video endpoints and the Sametime client, just set up an outgoing route to handle the `@domain.com` suffix. For example, you can route any traffic with “@vcs.lotus.com” to Cisco's Video Conferencing Server with an outbound route like the one shown in the image below.

![Outbound Route Configuration Image]

Then, when a Sametime Connect user types “sip:ex90@vcs.lotus.com” into QuickFind, this call request will route to the Cisco Video Conferencing Server.

![QuickFind Call Request Image]

Now that the route has been configured, there are many different ways for a user to initiate a call. Two of these options include initiating a call from the QuickFind area or using the Sametime Phonebook that ship with Sametime Unified Telephony Lite Client.
Configuring an inbound route from Cisco Video Conferencing Server to Sametime

This is very straightforward and almost identical to the incoming UCM route; the rule looks like this in the proxy.xml file:

```xml
<rule priority="4" description="" name="VCSIN">
    <condition type="method">INVITE</condition>
    <condition type="sourceAddress">9.32.134.120</condition>
    <destination>
        <output>
            <outputPattern type="header" headerName="Route" value="sip:st852primary.austin.ibm.com:5063;transport=tcp" />
        </output>
    </destination>
</rule>
```

Configuring an inbound route from Avaya Session Manager to Sametime

This is similar to the previous routing rule for incoming calls from VCS but it is assigned a lower priority. The rule looks like this in the proxy.xml file:

```xml
<rule priority="5" description="" name="AvayaIN">
    <condition type="method">INVITE</condition>
    <condition type="sourceAddress">9.51.253.170</condition>
    <destination>
        <output>
            <outputPattern type="header" headerName="Route" value="sip:st852primary.austin.ibm.com:5063;transport=tcp" />
        </output>
    </destination>
</rule>
```

Configuring an outbound route from Sametime to Avaya Session Manager

The desk phone numbers on the Avaya Communication Manager are 5 digits and begin with 513. The rule looks like this in the proxy.xml file:

```xml
<rule priority="6" description="" name="AvayaOUT">
    <condition type="method">INVITE</condition>
    <condition type="requestURI">sip:513.*</condition>
    <destination>
        <output>
            <inputPattern type="requestURI" value="sip:(.+)@.*" />
            <outputPattern type="requestURI" value="sip:9.51.253.170;transport=tcp" />
        </output>
    </destination>
</rule>
```
Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

**Trademarks**

These terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
Lotus
Notes
Sametime
WebSphere
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

---

*From Zero to Hero: Sametime Unified Telephony Lite Client*