HP Network Node Mangager iSPI for IP Telephony Software

For the Microsoft Windows ® operating system

Software Version: 9.10

Online Help for Administrators and Operators

Document Release Date: March 2011

Software Release Date: March 2011

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Oracle and Java are registered trademarks of Oracle and/or its affiliates

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Microsoft IP Telephony

The iSPI for IP Telephony provides the Microsoft IP Telephony workspace to monitor the Microsoft IP telephony entities on your network. The iSPI for IP Telephony monitors the following Microsoft IP Telephony entities on your network and generates incidents on the NNMi console based on the attributes monitored for the entities:

- Microsoft Lync sites
- Microsoft Lync end user groups
- Microsoft Lync end users
- Microsoft Lync servers
- Gateways
- Gateway interfaces
- SIP trunk configurations
- Dial plans
- Voice routes
- Voice policies
- NNMi sites

The iSPI for IP Telephony also allows you to configure the following entities for ease of management:

- Front end pool configuration
- Periodic collection details for CDRs and QoE
- User discovery
- Topology discovery
- End user groups
- NNMi sites
- Polling gateways, gateway channels, and gateway interfaces

The iSPI for IP Telephony provides extension packs that you can use with the iSPI Performance for Metrics to generate reports for the following Microsoft IP telephony entities:

- The iSPI for IP Telephony integrates with HP SiteScope to provide reports based on the metrics collected from the Microsoft unified communication and collaboration applications on the network.
- CDR and QoE details for the Microsoft IP Telephony infrastructure using the iSPI for IP Telephony.
- Gateways deployed on your Microsoft IP telephony network.

Help for Administrators

As an administrator, you can configure attributes listed in the table below for monitoring the Microsoft IP telephony infrastructure discovered on the network.

To access the administration console, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.

The administration console displays configuration options for the following attributes.

Attribute	Description
Frontend	Select this option to configure the discovery of a central Lync site using the front end server pool. You can also use this option to view .the existing front end server pool communication configurations.
Periodic Collection	Select this option to configure periodic collection of CDR and QoE metrics. This page also provides options to configure the interval for user discovery and topology discovery.
Lync End Users	Select this option to configure Lync end user groups. You can configure end user groups, named end users, and end users to be excluded from monitoring on this page.
Site	Select this option to configure NNMi sites. As an administrator, you can map the discovered Lync Server entities (edge servers, gateways, front end servers, registrar pools, and so on) on the network to the site for ease of administration.
Gateway	Select this option to configure the polling interval for gateway interfaces and channels. You can also configure the interval for performance data collection for the gateways using this page.

Note: Before running topology discovery for discovering Microsoft Lync servers and gateways, you must enable SNMP on Lync servers and gateways. You must also configure the read community string for the Lync servers and gateways. See the *NNMi Online Help* and the *iSPI for IP Telephony Installation Guide* for Windows for more information.

Configuring Frontend Server Communication Configuration

The Frontend Communication Configuration page lists the front end server pools configured to discover the corresponding central Lync sites.

To access the Frontend Communication Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Frontend**. This displays the Frontend Communication Configuration page.

The Frontend Communication Configuration page displays the following attributes related to the front end server pools configured by the administrator on the network.

Attribute	Description
Frontend Pool Name	Indicates the name configured for the Frontend server pool configuration.
User Name	The user name configured to access the Frontend server pool configuration.
Tenant Name	The tenant name to be associated with the Frontend server pool configuration.
Description	The description configured for the Frontend server pool configuration.

Adding New Frontend Server Communication Configuration

You can use the Add Frontend Communication Configuration page to add a communication configuration to seed a central Lync site for discovery in the iSPI for IP Telephony. You can do this by adding the details of the front end server pool in the central Lync site.

To access the Add Frontend Communication Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **FrontEnd**. This displays the Frontend Communication Configuration page.
6. Click (New) . This opens the Add Frontend Communication Configuration page.

7. Provide the following details for the new communication configuration:
   - **Pool Name**: The fully qualified domain name for the front end server pool.
   - **User Name**: The user name to access the Frontend server pool. Make sure that you specify the user name in the following format: *domain name\user name*.
   - **User Password**: The password for the user name.
   - **Tenant Name**: The tenant name to be associated with the configuration. You can select a tenant name from the list of tenants configured and displayed in this drop-down list. See the *NNMi Online Help* for information about tenants, user groups, and security groups.
   - **Pool Description**: The description for the communication configuration.
8. Click 💾 (Save) to save the new communication configuration.

Modifying an Existing Frontend Server Communication Configuration

To modify an existing Frontend server communication configuration, do as follows:

1. Select the Frontend server communication configuration that you want to modify from the Frontend Communication Configuration page.
2. Click ✎ (Edit). This displays the Edit Frontend Communication Configuration page.
3. Update the required details listed in step 7 of the section "Adding New Frontend Server Communication Configuration" (on page 11)for the Frontend communication configuration.
4. Click 💾 (Save) to save the updated Frontend communication configuration.

Deleting an Existing Frontend Server Communication Configuration

To delete an existing Frontend server communication configuration, do as follows:

1. Select the Frontend server communication configuration that you want to delete from the Frontend Communication Configuration page.
2. Click ❌ (Delete). This deletes the selected Frontend communication configuration.

Configuring Periodic Collection

You can use the Periodic Collection option on the administration console to configure the following details:

- Call details record collection
- Quality of experience score collection
- User discovery interval
- Topology discovery interval

To access the administration console to configure the listed details, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.

3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Periodic Collection**. This displays the following tabs. Click each tab to configure the required details:
   - CDR
   - QoE
   - Topology Discovery
   - User Discovery.

Configuring Call Detail Record Collection

The CDR Details page allows you to configure the call details record collection on the Microsoft IP telephony network.

To access the CDR Details page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Periodic Collection** This displays the following tabs:
   - CDR
   - QoE
   - Topology Discovery
   - User Discovery.
6. Click the **CDR** tab to configure the required details from the CDR Details page displayed:
   - Enable Collection: Select this option to enable CDR collection.
   - Exclude IM: Select this option to exclude CDR collection for Instant Messaging (IM) sessions.
   - Interval (mins):Select the interval in minutes for CDR collection to be repeated on the network. You can select one of the following intervals:
     - 15
     - 30
     - 45
     - 60
7. Click 💾 (Save) to save the CDR collection configuration changes.

Configuring Quality of Experience Collection

The QoE Details page allows you to configure the QoE score collection on the Microsoft IP telephony network.

To access the QoE Details page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Periodic Collection** This displays the following tabs:
   - CDR
   - QoE
   - Topology Discovery
   - User Discovery.
6. Click the **QoE** tab to configure the required details from the QoE Details page displayed:
   - Enable Collection: Select this option to enable QoE score collection.
   - Interval (mins):Select the interval in minutes for QoE score collection to be repeated on the network. You can select one of the following intervals:
     - 15
     - 30
     - 45
     - 60
7. Click 💾 (Save) to save the QoE score collection configuration changes.

Configuring Topology Discovery Details

The Topology Discovery Details page helps you to enable topology discovery on the network and schedule the interval in hours for the topology discovery to be repeated on the network.

To access the Topology Discovery Details page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Periodic Collection** This displays the following tabs:

- CDR
- QoE
- Topology Discovery
- User Discovery.

6. Click the **Topology Discovery** tab to configure the required details from the Topology Discovery Details page displayed:
   - Enable Collection: Select this option to enable topology discovery.
   - Interval (hrs):Select the interval in hours for topology discovery to be repeated on the network. You can select one of the following intervals:
     - 12
     - 24
     - 48
     - 60
7. Click 💾 (Save) to save the topology discovery configuration changes.

Configuring User Discovery Details

The User Discovery Details page allows you to configure the user discovery details on the Microsoft IP telephony network.

To access the User Discovery Details page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Periodic Collection** This displays the following tabs:
   - CDR
   - QoE
   - Topology Discovery
   - User Discovery.
6. Click the **User Discovery** tab to configure the required details from the User Discovery Details page displayed:
   - Enable Collection: Select this option to enable user discovery on the Microsoft IP telephony network.
   - Interval (hrs):Select the interval in hours for user discovery to be repeated on the network. You can select one of the following intervals:
     - 12
     - 24

   - 48
   - 60

7. Click 💾 (Save) to save the user discovery configuration changes.

Creating End User Groups

As an administrator, you can group end users based on end user attributes. This helps in gathering the CDR details for a required group of users. You can include a user in multiple user groups. In this event, the lowest reporting order number configured for the user in a group is given priority when gathering the CDR details for that user. You can configure the following types of end user groups:

- End user group: to create an end user group based on the end user attributes.
- Named end users: to create an end user group based on end users who have been assigned a name for ease of identification. The CDR/QoE reports display the names of these users. The reports do not display the names of the users who are not included in the named end user group.
- Excluded end users: to create an end user group based on users who must be excluded from being monitored. The iSPI for IP Telephony does not collect the CDR details for such users.

You can use the Lync End Users option on the Microsoft IP telephony Configuration workspace to configure end user groups.

To access the Lync End Users option, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Lync End Users**. This displays the configuration page on the right panel .that you can use to configure end user groups.

Creating End User Groups

You can use the End User Groups tab page to view the existing end user groups configured. You can also use this page to add new end user groups.

To access the End User Groups tab page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Lync End Users**. This displays the configuration page on the right panel .that you can use to configure end user groups.

6. Click the **End User Groups** tab. This displays the End User Groups tab page listing the existing end user groups configured. This page lists the following details for an end user group:

Attribute	Description
End User Group	The end user group name configured for the end user group.
Reporting Order	The reporting order configured for the end user group.

Creating New End User Groups

1. Click (New) on the End Users Group tab page. This opens the End User Group Configuration page.
2. Provide the following details for the new end user group configuration:
   - **Group Name**: The name for the end user group.
   - **Description**: The description for the end user group.
   - **Reporting Order**: The reporting order number to be configured for end user group. The end user group with the lowest order number is given priority.
   - Create a filter to map the required end users under the end user group. See the section "Creating an End User Group Filter" (on page 17) below for more information about defining a filter.
3. Click (Save) to save the end user group.

Creating an End User Group Filter

In this example, as a network administrator, you need to create an end user group based on the following end user group attributes:

- All end users where the company attribute is configured as *XYZ*
- All end users where the display name has the string *Mgmt* prefixed to the display name.

To create an end user configuration based on the conditions listed , you must define an end user configuration filter using the End User Group Configuration Page as follows:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. Select **Company** from the **Attribute** drop-down list under the **Filter Editor** section.
3. Select **like** from the **Operator** drop-down list.
4. Type `XYZ`in the **Value** box.
5. Click **Append**. This displays the following string under the **Filter String** section: `((company like XYZ))`
6. Select the AND condition defined in step 1.
7. Select **displayName** from the **Attribute** drop-down list.
8. Select **like** from the **Operator** drop-down list

9. Type `Mgmt%` in the **Value** box.
10. Click **Append**. This displays the complete filter string in the Filter String section for your requirement in this example as follows: (`(company like XYZ AND displayName like Mgmt%))`

Note:

- You can select one of the following end user attributes from the **Attribute** drop-down list for a filter condition. See the Lync End User Form for a description about the attributes:
  - groupName
  - displayName
  - sipaddress
  - lineURI
  - company
  - countryOrRegionDisplayName
  - department
  - city
  - registrarPool
  - targetRegistrarPool
  - homeServer
  - targetHomeServer
  - enabledForRichPresence
  - audioVideoDisabled
  - voicePolicy
  - conferencingPolicy
  - dialPlan
  - locationPolicy
  - clientPolicy
  - clientVersionPolicy
  - archivingPolicy
  - pinPolicy
  - externalAccessPolicy
  - hostedVoiceMail
  - hostedVoiceMailPolicy
  - hostingProvider

- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: indicates that the filter must be applied to the attributes that do not match the value provided.
  - **like**: indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.
  - **not like**: indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) or asterisk (*) to match a string and the question mark (?) to match a character in the value provided
  - **in**: indicates that the filter must be applied to all the attributes matching the list of values specified. You must specify each value in a separate line when typing multiple values.
  - **not in**: indicates that the filter must not be applied to all the attributes that do not match the list of values specified. You must specify each value in a separate line when typing multiple values.
- You can use the **Insert** option after selecting the relevant AND or OR condition to insert a filter condition (attribute, operator, and value) as required.
- You can select a filter condition and click the **Replace** option to replace that filter condition with the filter condition specified.
- You can select a filter condition or an AND or an OR condition and click **Delete** to delete the required condition.

Modifying an Existing End User Group

To modify an existing end user group, do as follows:

1. Select the end user group that you want to modify from the End User Groups tab page.
2. Click ✎ (Edit). This displays the End User Group Configuration page.
3. Update the required details listed in step 2 of the section "Creating End User Groups" (on page 16)for the frontend communication configuration.
4. Click 💾 (Save) to save the updated end .user group.

Deleting an Existing End User Group

To delete an existing end user group, do as follows:

1. Select the end user group that you want to delete from the End User Groups tab page.
2. Click ✖ (Delete). This deletes the selected end user group.

Creating Named End User Groups

You can use the Named End Users tab page to create end user groups based on the named users discovered on the network. Named users help in ease of identification of users in reports.

To access the Named End Users tab page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Lync End Users**. This displays the configuration page on the right panel .that you can use to configure end user groups.
6. Click the **Named End Users** tab. This displays the Named End Users tab page that you can use to configure new named end user groups.
7. Create a filter to map the required named end users under the named end user group. See the section ""Creating a Named End User Group Filter" (on page 20) below for more information about defining a filter.
8. Click 💾 (Save) to save the named end user group.

Creating a Named End User Group Filter

In this example, as a network administrator, you need to create a named end user group based on the following end user group attributes:

- All end users where the *company* attribute is configured as *XYZ*
- All end users where the *displayName* has the string *_Mktg* suffixed in the display name.

To create an end user configuration based on the conditions listed, you must define an end user configuration filter using the Named End User tab page as follows:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. Select **Company** from the **Attribute** drop-down list under the **Filter Editor** section.
3. Select **like** from the **Operator** drop-down list.
4. Type `XYZ`in the **Value** box.
5. Click **Append**. This displays the following string under the **Filter String** section: `((company like XYZ))`
6. Select the AND condition defined in step 1.
7. Select **displayName** from the **Attribute** drop-down list.
8. Select **like** from the **Operator** drop-down list
9. Type `%_Mktg` in the **Value** box.

10. Click **Append**. This displays the complete filter string in the Filter String section for your requirement in this example as follows: (`(company like XYZ AND displayName like %_Mktg))`

Note:

- You can select one of the following end user attributes from the **Attribute** drop-down list for a filter condition. See the Lync End User Form for a description about the attributes:
  - groupName
  - displayName
  - sipaddress
  - lineURI
  - company
  - countryOrRegionDisplayName
  - department
  - city
  - registrarPool
  - targetRegistrarPool
  - homeServer
  - targetHomeServer
  - enabledForRichPresence
  - audioVideoDisabled
  - voicePolicy
  - conferencingPolicy
  - dialPlan
  - locationPolicy
  - clientPolicy
  - clientVersionPolicy
  - archivingPolicy
  - pinPolicy
  - externalAccessPolicy
  - hostedVoiceMail
  - hostedVoiceMailPolicy
  - hostingProvider

- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: indicates that the filter must be applied to the attributes that do not match the value provided.
  - **like**: indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.
  - **not like**: indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided
  - **in**: indicates that the filter must be applied to all the attributes matching the list of values specified. You must specify each value in a separate line when typing multiple values.
  - **not in**: indicates that the filter must not be applied to all the attributes that do not match the list of values specified. You must specify each value in a separate line when typing multiple values.
- You can use the **Insert** option after selecting the relevant AND or OR condition to insert a filter condition (attribute, operator, and value) as required.
- You can select a filter condition and click the **Replace** option to replace that filter condition with the filter condition specified.
- You can select a filter condition or an AND or an OR condition and click **Delete** to delete the required condition.

Creating Excluded End User Groups

You can use the Excluded End Users tab page to create end user groups that must be excluded from being monitored.

To access the Excluded End Users tab page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Lync End Users**. This displays the configuration page on the right panel .that you can use to configure end user groups.
6. Click the **Excluded End Users** tab. This displays the Excluded End Users tab page that you can use to configure new excluded end user groups.
7. Create a filter to map the required excluded end users under the excluded end user group. See the section "Creating an Excluded End User Group Filter" (on page 23) below for more information about defining a filter.
8. Click 💾 (Save) to save the excluded end user group.

Creating an Excluded End User Group Filter

In this example, as a network administrator, you need to create an excluded end user group based on the following end user group attributes:

- All end users where the *department* attribute is configured as *SrMgmt*
- All end users where the *city* is *Washington*.

To create an end user configuration based on the conditions listed, you must define an end user configuration filter using the Excluded End Users tab page as follows:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. Select **department** from the **Attribute** drop-down list under the **Filter Editor** section.
3. Select **=** from the **Operator** drop-down list.
4. Type `SrMgmt`in the **Value** box.
5. Click **Append**. This displays the following string under the **Filter String** section: `((department=SrMgmt))`
6. Select the AND condition defined in step 1.
7. Select **city** from the **Attribute** drop-down list.
8. Select **=** from the **Operator** drop-down list
9. Type `Washington` in the **Value** box.
10. Click **Append**. This displays the complete filter string in the Filter String section for your requirement in this example as follows: (`(department=SrMgmt AND city=Washington))`

Note:

- You can select one of the following end user attributes from the **Attribute** drop-down list for a filter condition. See the Lync End User Form for a description about the attributes:
  - displayName
  - sipaddress
  - company
  - countryOrRegionDisplayName
  - department
  - city
- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: indicates that the filter must be applied to the attributes that do not match the value provided.

  - **like**: indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.
  - **not like**: indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.

- You can use the **Insert** option after selecting the relevant AND or OR condition to insert a filter condition (attribute, operator, and value) as required.
- You can select a filter condition and click the **Replace** option to replace that filter condition with the filter condition specified.
- You can select a filter condition or an AND or an OR condition and click **Delete** to delete the required condition.

Creating Sites

As an administrator, you can configure sites in NNMi. A site refers to a mapping you can configure in NNMi for the discovered Lync Server entities (edge servers, gateways, front end servers, registrar pools, and so on) on the network. Creating and maintaining sites eases the task of monitoring discovered Lync Server entities.
You can use the Site Configuration tab page to view existing sites and configure new sites. To access this page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Site**. This displays the Site Configuration tab.page that lists all the existing sites configured.

The Site Configuration tab page displays the following details about an existing site configuration.

Attribute	Description
Site Name	Indicates the name of the site.
Reporting Order	Indicates the reporting order configured for the site.

Adding Sites

You can use the Site Configuration page to add a site and map the necessary Lync Server entities to the site..

To access the Site Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Site**. This displays the Site Configuration tab.page that lists all the existing sites configured.
6. Click (New) . This opens the Site Configuration page.
7. Provide the following details for the new site configuration:
   - **Site**: The name for the site.
   - **Order**: The order number to be configured for the site. The site with the lowest order number is given priority.
   - Create a filter to map the required Lync Server entities under the site. See the section "Creating a Site Configuration Filter" (on page 25) below for more information about defining a filter.
8. Click **Test Site Definition** to check if the filter you configured is valid for the Lync Server entities discovered on the network. This opens the Test Site Definition Result window that displays the results of the filter you configured.

Note:

- The Test Site Definition window displays the details in a tabular format with the **Filter** and **Result** columns.
- The status **Pass** indicates that there were matches for the filter criteria among the list of Lync Server entities discovered on the network.
- The status **Fail** indicates that there were no matches for the filter criteria.

4. Click (Save) to save the site configuration.

Creating a Site Configuration Filter

In this example, as a network administrator, you need to create a site configuration that includes the following Lync Server entities:

- All the front end servers that start with the name ipt and msipt
- Associated with a registrar pool named Primary Registrar

To create a site for the condition listed , you must define a site configuration filter using the Site Configuration Page as follows.

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. Click **AND**. This displays the AND condition as a nested condition within the AND condition defined in the previous step.
3. Select the nested AND condition created in the previous step.
4. Select **Frontend Server** from the **Attribute** drop-down list under the **Site Definition** section.

5. Select **like** from the **Operator** drop-down list.
6. Type `ipt%`in the **Value** box.
7. Click **Append**. This displays the following string under the **Filter String** section: `((Frontend Server like ipt%))`
8. Select the nested AND condition again.
9. Repeat steps 4 and 5 listed in this procedure.
10. Type `msipt%` in the **Value** box.
11. Click **Append**. This updates the string under the **Filter String** section as follows: `((Frontend Server like ipt% AND Frontend Server like msipt%))`. This filter string defines the first condition for the site configuration where as an administrator you want to filter all the frontend servers that start with the name ipt and msipt.
12. Select the AND condition defined in step 1.
13. Click **AND**. This inserts the AND condition at the same level where the first AND condition created was placed.
14. Select the AND condition created in the previous step.
15. Select **Registrar Pool** from the **Attribute** drop-down list.
16. Select **=** from the **Operator** drop-down list
17. Type `Primary Registrar` in the **Value** box.
18. Click **Append**. This displays the complete filter string in the Filter String section for your requirement in this example as follows: (`(Frontend Server like ipt% AND Frontend Server like msipt%) AND (Registrar Pool = Primary Registrar))`

Note:

- You can select one of the following Lynd Server entities from the **Attribute** drop-down list for a filter condtion:
  - Edge Server
  - Gateway
  - Registrar Pool
  - Frontend Server
- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: indicates that the filter must be applied to the attributes that do not match the value provided.
  - **like**: indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) or asterisk (*) to match a string and the question mark (?) to match a character in the value provided.

  - **not like**: indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided

- You can use the **Insert** option after selecting the relevant AND or OR condition to insert a filter condition (attribute, operator, and value) as required.
- You can select a filter condition and click the **Replace** option to replace that filter condition with the filter condition specified.
- You can select a filter condition or an AND or an OR condition and click **Delete** to delete the required condition.

Modifying an Existing Site

To modify an existing end user group, do as follows:

1. Select the site that you want to modify from the Site Configuration tab page.
2. Click ✎ (Edit). This displays the Site Configuration page.
3. Update the required details listed in step 7 of the section "Adding Sites" (on page 24)for the frontend communication configuration.
4. Click 💾 (Save) to save the updated end .user group.

Deleting an Existing Site

To delete an existing site, do as follows:

1. Select the site that you want to delete from the Site Configuration tab page.
2. Click ✖ (Delete). This deletes the selected site configuration.

Configuring Gateway Polling

The administration console provides the option to configure polling for the gateway entities discovered on the network.

To access the page to configure the gateway entities, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Gateway**. This displays the following tabs. Click each tab to configure the required gateway entity:
   - Interface: Provides options to enable polling for the gateway interfaces and specify the polling interval.

- Channel: Provides options to enable polling for the gateway channels and specify the polling interval.
- Performance Data Collection: Provides options to enable performance data collection for gateways and specify the interval for data collection to be repeated.

Configuring Gateway Interface Polling

You can use the Interface Polling Configuration page to enable polling for gateway interfaces and specify the polling interval in minutes.

To access the Interface Polling Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Gateway**. This displays the following tabs. Click each tab to configure the required gateway entity:
   - Interface: Provides options to enable polling for the gateway interfaces and specify the polling interval.
   - Channel: Provides options to enable polling for the gateway channels and specify the polling interval.
   - Performance Data Collection: Provides options to enable performance data collection for gateways and specify the interval for data collection to be repeated.
6. Click the **Interface** tab. This opens the Interface Polling Configuration page.
7. Provide the following details on the Interface Polling Configuration page:
   - Enable Polling: Select this option to enable polling for the gateway interfaces discovered on the network.
   - Polling Interval (mins): Specify the interval in minutes to repeat the polling for the gateway interfaces discovered on the network. You can specify one of the following options from the drop-down list:
     - 5
     - 10
     - 15
8. Click 💾 (Save) to save the configuration changes.

Configuring Gateway Channel Polling

You can use the Channel Polling Configuration page to enable polling for gateway channels and specify the polling interval in minutes.

To access the Channel Polling Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Gateway**. This displays the following tabs. Click each tab to configure the required gateway entity:
   - Interface: Provides options to enable polling for the gateway interfaces and specify the polling interval.
   - Channel: Provides options to enable polling for the gateway channels and specify the polling interval.
   - Performance Data Collection: Provides options to enable performance data collection for gateways and specify the interval for data collection to be repeated.
6. Click the **Channel** tab. This opens the Channel Polling Configuration page.
7. Provide the following details on the Channel Polling Configuration page:
   - Enable Polling: Select this option to enable polling for the gateway channels discovered on the network.
   - Polling Interval (mins): Specify the interval in minutes to repeat the polling for the gateway channels discovered on the network. You can specify one of the following options from the drop-down list:
     - 5
     - 10
     - 15
   - Hold Time (mins): Specify the gateway channel hold time in minutes to generate the channel idle incident in the event of a gateway channel staying in the idle state after the specified hold time.
8. Click 💾 (Save) to save the configuration changes.

Configuring Gateway Performance Data Collection

You can use the Performance Data Collection Configuration page to enable performance data collection for gateways and specify the data collection interval in minutes.

To access the Interface Performance Data Collection Configuration page, do as follows:

1. Log on to the NNMi console as an administrator.
2. Click **Configuration** from the workspaces listed.
3. Click **iSPI for IP Telephony Configuration**. This displays the administration console.
4. Click **Microsoft IP Telephony Configuration**. This displays the administration console for Microsoft IP telephony.
5. Click **Gateway**. This displays the following tabs. Click each tab to configure the required gateway entity:

   - Interface: Provides options to enable polling for the gateway interfaces and specify the polling interval.
   - Channel: Provides options to enable polling for the gateway channels and specify the polling interval.
   - Performance Data Collection: Provides options to enable performance data collection for gateways and specify the interval for data collection to be repeated.

6. Click the **Performance Data Collection** tab. This opens the Performance Data Collection Configuration page.
7. Provide the following details on the Performance Data Collection Configuration page:
   - Enable Collection: Select this option to enable performance data collection for the gateways discovered on the network.
   - Collection Interval (mins): Specify the interval in minutes to repeat the performance data collection for the gateways discovered on the network. You can specify one of the following options from the drop-down list:
     - 15
     - 30
     - 60
8. Click 💾 (Save) to save the configuration changes.

Integrating with SiteScope

You can integrate the iSPI for IP Telephony with HP SiteScope to gather performance metrics for the Microsoft unified communication and collaboration applications that include the Lync Server applications and the Exchange Server application on your network. With this integration, you can collect performance metrics and generate reports using the monitors that SiteScope provides for the following applications:

- Microsoft Exchange
- Microsoft Lync Server applications comprising:
  - Audio/Video conferencing server
  - Archiving server
  - Director server
  - Edge server
  - Frontend server
  - Mediation server
  - Monitoring server
  - Registrar server

Integration Considerations

Make sure that you have the completed the following activities to complete this integration:

- Installed and configured SiteScope according to the instructions provided in the SiteScope documentation before attempting this integration.
- Created a data integration connection using the SiteScope console between SiteScope and iSPI for IP Telephony. See the SiteScope documentation to configure the connection between SiteScope and NNMi.
  - You must specify the URL in the following format in the Receiver URL box if you are using an HTTP connection: `http://IPTHostName:10080/nms-spi-uc-sitescope-war/Sample`. `IPTHostName` refers to the system name where you have installed the iSPI for IP Telephony.
  - If you provide an HTTPS link as the Receiver URL for the data integration, make sure that you import the NNMi license file to SiteScope. See the NNMi Deployment Reference Guide for more information.
  - You must specify the URL in the following format in the Receiver URL box if you are using an HTTPS connection:`https://IPTHOSTName:HTTPS PORT NUMBER/nms-spi-uc-sitescope-war/Sample`
- Enable performance monitoring details to be sent for Microsoft unified communication and collaboration applications from SiteScope to the iSPI for IP Telephony as discussed in the following section.

Enabling Performance Monitoring for Microsoft Unified Communication and Collaboration Applications

1. Log on as an administrator to the NNMi console
2. Click **Integration Module Configuration** > **HP SiteScope IP Telephony....** This opens the HP SiteScope IP Telephony tab page.
3. Select **Microsoft UC Applications Performance Monitoring**
4. Click 💾 (Save) to save the integration configuration.

Help for Operators

You can monitor the Microsoft IP telephony network by logging in as an operator (level 1 or level 2) or as a guest. After logging in, you can view the inventory views for the different Microsoft IP telephony devices and entities discovered and monitored.

To access the Microsoft IP Telehony inventory views, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.

Inventory View	Purpose
Lync Sites	Lists the Lync sites discovered on the network.
End User Groups	Lists the end user groups discovered on the network for the Lync Server.
Lync End Users	Lists the end users discovered on the network for the Lync Server.

Inventory View	Purpose
Servers	Lists the servers discovered from all the server pools associated with the Lync server on the network.
Gateways	Lists the gateways discovered on the network.
SIP Trunks	Lists the SIP trunks discovered on the network.
Dial Plans	Lists the dial plans discovered on the network.
Voice Routes	Lists the voice routes discovered on the network.
Voice Policies	Lists the voice policies discovered on the network.

Monitoring Lync Sites

You can use the Lync Sites inventory view to see a list of Lync sites discovered on the network.

To access the Lync Sites inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Lync Sites**. This displays the Lync Sites inventory view.

The Lync Sites inventory view displays the list of Lync sites discovered on the network along with the following attributes for each Lync site.

Attribute	Description
Identity	Indicates the unique identity of the Lync site discovered.
Name	Indicates the name of the Lync site discovered.
Type	Indicates the type of the Lync site discovered. The type can be one of the following: • Remote Site: indicates that the discovered site is a remote site managed by a central site. • Central Site: indicates that the discovered site is a central site that manages remote sites.
Parent Site	Indicates the identity of the site that manages the remote site. This field is applicable only for remote sites.

Attribute	Description
Description	Indicates the description configured for the Lync site discovered..
Management Server	Indicates if the Lync site is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the Lync site is being managed by the NNMi management server console on which you are viewing the IP phone details. • Name of the regional manager that manages the Lync site.

You can view additional details for a discovered Lync site using the Lync site form.

Viewing the Analysis Panel for a Quick Reference

The Analysis panel that appears at the bottom of the Lync Sites inventory view displays the following details. You can select a Lync Site from the Lync Sites inventory view to automatically launch the Analysis panel:

- Left panel: This panel displays the summary for the selected Lync site and displays the following details:

Detail	Description
No. of Branches	The number of branch sites connected to the selected Lync site.
No. of Gateways	The number of gateways discovered in the selected Lync site.
No. of Pools	The number of server pools discovered in the selected Lync site.
No. of Users	The number of users discovered in the selected Lync site.
Parent Site	The name of the parent site associated with the selected Lync site.
Primary Registrar Pool	The primary registrar pool associated with the selected Lync site.
Backup Registrar Pool	The backup registrar pool associated with the selected Lync site.
Last Discovered	The date and time during which the Lync site was last discovered.

- Right panel: The right panel displays pie charts for the following call analysis details:
  - QoE by calling party
  - QoE for called party
  - Calls by Media Type
  - Calls by Call Type
  - Calls by Session Type
  - Top Callers
  - Top Named Callers

Launching Context-sensitive Actions for a Lync Site

You can perform the following context-sensitive actions for a selected Lync site from the Lync Sites inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.
- Discover topology and discover users.

To launch the context-sensitive actions, do as follows:

1. Select the Lync site
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

Note: The pie charts display the details for the past 24 hours. You can click the ⟳ (Refresh) icon to display the pie chart with the latest call analysis details.

Lync Sites Form

You can use the Lync Sites form to view additional details about a discovered Lync site.

To access the Lync Sites form, do as follows:

1. Select a Lync site discovered from the Lync Sites inventory view.
2. Click 📂 (**Open**). This opens the Lync Sites form.

The Lync Sites form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the Lync site discovered.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**

This tab displays the general site attributes as follows.

Attribute	Description
Name	Indicates the name of the site.
Type	Indicates the type of the site. The type can be one of the following: • Remote Site: indicates that the discovered site is a remote site managed by a central site. • Central Site: indicates that the discovered site is a central site that manages remote sites.
Parent Site	Indicates the identity of the site that manages the remote site. This field is applicable only for remote sites.
Primary Registrar Pool	Indicates the name of the primary registrar pool for the site.
Backup Registrar Pool	Indicates the name of the backup registrar pool for the site.
Description	Indicates the description for the site.

- **Pools**

This tab displays the server pools associated with the Lync site as follows

Attribute	Description
Identity	The identity of the server pool associated with the Lync site.
FQDN	The Fully Qualified Domain Name (FQDN) of the server pool.

Select a server pool and click (**Open**). This opens the Pool form.

- **Gateways**: displays the gateways associated with the Lync site as shown in the Gateways inventory view.
- **SIP Trunks**: displays the SIP trunks associated with the Lync site as shown in the SIP Trunk Configuration form.

Pool Form

You can use the Pool form to view additional details about a discovered server pool associated with a Lync site.

To access the Pools form, do as follows:

1. Select a pool associated with a Lync site from the Pools tab page on the Lync Sites form.
2. Click (**Open**). This opens the Pool form.

The Pool form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Identity	Indicates the unique identity of the server pool associated with the Lync site.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general pool attributes as follows.

Attribute	Description
FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server pool.

- **Servers**: displays the servers discovered from all the server pools associated with the Lync site. The Servers tab page displays the following attributes.

Attribute	Description
Identity	The unique identity configured for the server.
FQDN	The FQDN of the server.

Select a server and click 📂 (**Open** to open the Servers form to see the additional details for a discovered server.

Monitoring End User Groups

You can use the End User Groups inventory view to see a list of end user groups configured on the network.

To access the End User Groups inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **End User Groups**. This displays the End User Groups inventory view.

The End User Groups inventory view displays the list of end user groups discovered on the network along with the following attributes for each end user group.

Attribute	Description
Group Name	Indicates the name of the end user group discovered.
Description	Indicates the description of the end user group discovered.
Order	Indicates the order number for the end user group.

Attribute	Description
Number of Members	Indicates the number of end users in the group.

You can view additional details for a discovered end user group using the End User Group form.

Viewing the Analysis Panel for a Quick Reference

The Analysis panel that appears at the bottom of the End User Groups inventory view displays the following details. You can select an end user group from the End User Groups inventory view to automatically launch the Analysis panel:

- Left panel: This panel displays the summary for the selected end user group and displays the following details:

Detail	Description
No. of Members	The number of members in the discovered end user group.
Created on	The data and time at which the end user group was .created.
Modified on	The data and time at which the end user group was .modified last.

- Right panel: The right panel displays pie charts for the following call analysis details:
  - QoE by calling party
  - QoE for called party
  - Calls by Media Type
  - Calls by Call Type
  - Calls by Session Type
  - Top Callers
  - Top Named Callers

Note: The pie charts display the details for the past 24 hours. You can click the 🔄 (Refresh) icon to display the pie chart with the latest call analysis details.

Launching Context-sensitive Actions for a Lync End User Group

You can perform the following context-sensitive actions for a selected Lync end user group from the Lync End User Groups inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the Lync end user group.
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

End User Group Form

You can use the End User Group form to view the additional details of an end user group discovered.

To access the End User Group form, do as follows:

1. Select an end user group from the End User Groups inventory view.
2. Click (**Open**). This opens the End User Group form.

The End User Group form displays the information in two panels, the left panel and the right panel.

The left panel displays the **Basics** drop-down list that displays the name of the end user group.

The right panel displays the following drop-down lists that display the additional details associated with an end user group.

- General

Attribute	Description
Group Name	Indicates the name of the end user group.
Description	Indicates the description provided while configuring the end user group.
Filter String	Indicates the filter string used to group end users in the end user group.
Order	Indicates the order number configured for the user group

- Lync End Users: displays the details of the end users associated with the selected end user group as shown on the Lync End Users inventory view.

Monitoring End Users

You can use the Lync End Users inventory view to see a list of end users discovered on the network.

To access the Lync End Users inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Lync End Users**. This displays the Lync End Users inventory view.

The Lync End Users inventory view displays the list of end users discovered on the network along with the following attributes for each end user.

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Named User	Indicates if the end user is configured as a named user. A named user helps in the easy identification of an end user.
Management Server	Indicates if the end user is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the end users discovered: • Local: If the end user is being managed by the NNMi management server console on which you are viewing the IP phone details. • Name of the regional manager that manages the end user.
Lync Site	Indicates the Lync site associated with the end user.

Launching Context-sensitive Actions for a Lync End User

You can perform the following context-sensitive actions for a selected Lync end user from the Lync End Users inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the Lync end user
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

You can view additional details for a discovered end users using the Lync End User form.

Lync End User Form

You can use the Lync End User form to view the additional details of an end user discovered.

To access the Lync End User form, do as follows:

1. Select an end user from the Lync End Users inventory view.
2. Click 📂 (**Open**). This opens the Lync End User form.

The Lync End User form displays the information in two panels, the left panel and the right panel.

The left panel displays the **Basics** drop-down list that displays following attributes of the end user.

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Home Server	Indicates the home server to which the end user is associated.

The right panel displays the following drop-down lists that display the additional details associated with an end user group.

- General

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Home Server	Indicates the home server to which the end user is associated.
Identity	Indicates the unique identity configured for the end user.
Voice Policy	Indicates the voice policy configured for the end user.
Conferencing Policy	Indicates the conferencing policy configured for the end user.
Dial Plan	Indicates the dial plan configured for the end user.
Location Policy	Indicates the location policy configured for the end user.
Client Policy	Indicates the client policy configured for the end user.

Attribute	Description
Client Version Policy	Indicates the client version policy configured for the end user.
Archiving Policy	Indicates the archiving policy configured for the end user.
Pin Policy	Indicates the pin policy configured for the end user,
External Access Policy	Indicates the external policy configured for the end user.
Hosted Voicemail	Indicates where the voicemail is hosted for the end user.
Hosted Voicemail Policy	Indicates the voice mail policy configured for the end user.
Hosting Provider	Indicates the hosting provider configured for the end user.
Target Registrar Pool	Indicates the target registrar pool configured for the end user.
Target Home Server	Indicates the target home server configured for the end user.
Enabled for Rich Presence	Indicates if the end user is enabled for rich presence. A tick mark in the check box adjacent to this attribute indicates that this attribute is enabled.
Audio Video Disabled	Indicates if audio and video are disabled for the end user. A tick mark in the check box adjacent to this attribute indicates that this attribute is enabled.
Company	Indicates the company name configured for the end user.
Country or Regional Display Name	Indicates the country or regional display name configured for the end user.
Department	Indicates the department configured for the end user.
Country Abbreviation	Indicates the country abbreviation configured for the end user.
City	Indicates the city configured for the end user.
IP Phone	Indicates the IP phone configured for the end user.

Attribute	Description
Created	Indicates the date and time at which the end user was created
Changed	Indicates the date and time at which the end user configuration was modified last.

- Active Endpoints

Attribute	Description
Client Version	Indicates the client version of the active endpoint associated with the end user.
Pool FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the pool to which the end point belongs.

You can view the additional details regarding an active end point using the Active Endpoints form.

Active Endpoints Form

You can use the Active Endpoint form to view additional details about an active endpoint associated with a Lync end user.

To access the Active Endpoints form, do as follows:

1. Select an active endpoint associated with a Lync end user from the Active Endpoints tab page on the Lync End User form.
2. Click (**Open**). This opens the Active Endpoint form.

The Active Endpoint form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Attribute	Description
Client Version	Indicates the client version for the active end point associated with the Lync end user..

The right panel displays the **General** drop-down list that displays the general endpoint attributes as follows.

Attribute	Description
Pool FQDN	The name of the Lync site associated with the SIP trunk.
Edge Server	The edge server associated with the active endpoint.
Manufacturer	The manufacturer for the active endpoint.

Attribute	Description
Hardware Version	Indicates the hardware version of the active endpoint.

Monitoring Lync Servers

You can use the Servers inventory view to see the servers discovered from all the server pools associated with the Lync server on the network.

To access the Servers inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Servers**. This displays the Servers inventory view.

The Servers inventory view displays the list of servers discovered on the network along with the following attributes for each server.

Attribute	Description
Node Status	Indicates the status of the node.
Identity	Indicates the unique identity of the server discovered.
FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server.
Pool	Indicates the server pool to which the server belongs.
Management Server	Indicates if the server is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the server is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the server.
Lync Site	Indicates the Lync site associated with the server.

You can view additional details for a discovered server using the Servers form.

Servers Form

You can use the Servers form to view additional details about a discovered server.

To access the Servers form, do as follows:

1. Select a server discovered from the Servers inventory view.
2. Click 📂 (**Open**). This opens the Servers form.

The Servers form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the server.
Hosted on Node	Indicates the discovered node that hosts the server.

The right panel displays the following tabs:

- **General**: displays the general site attributes as follows.

Attribute	Description
FQDN	Indicates the name of the site.
Pool	Indicates the server pool to which the server belongs.
Management Mode	Indicates if the server is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the server is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the server.

Monitoring Gateways

You can use the Gateways inventory view to see a list of gateways discovered on the network.

To access the Gateways inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Gateways**. This displays the Gateways inventory view.

The Gateways inventory view displays the list of gateways discovered on the network along with the following attributes for each gateway.

Attribute	Description
Node Status	Indicates the status of the node.
Identity	Indicates the unique identity of the gateway discovered.
Name	Indicates the name of the gateway discovered.
IP Address	Indicates the IP address of the gateway discovered.
Site	Indicates the Lync site that includes the gateway.
Description	Indicates the description configured for the gateway discovered..
Management Server	Indicates if the gateway is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the gateway discovered: • Local: If the gateway is being managed by the NNMi management server console on which you are viewing the gateway details. • Name of the regional manager that manages the gateway.

Launching Context-sensitive Actions for a Gateway

You can launch the call details chart detail report for a gateway from the Gateways inventory view

To launch the context-sensitive actions, do as follows:

1. Select the gateway.
2. Click **Actions** > **Microsoft IP Telephony**and select the option to launch the call details chart detail report for the selected gateway.

You can view additional details for a discovered gateway using the Gateway form.

Gateway Form

You can use the Gateway form to view additional details about a discovered gateway.

To access the Gateway form, do as follows:

1. Select a gateway discovered from the Gateways inventory view.
2. Click 📂 (**Open**). This opens the Gateway form.

The Gateway form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Identity	Indicates the unique identity of the gateway discovered.
Hosted Node	Indicates the discovered node that hosts the gateway.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general site attributes as follows.

Attribute	Description
Name	Indicates the name of the gateway.
IP Address	Indicates the IP address of the gateway.
Version	Indicates the version of the gateway.
Pool FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server pool that includes the gateway.
Site	Indicates the Lync site that includes the gateway.
Vendor	Indicates the vendor name for the gateway.
Description	Indicates the description configured for the gateway.
Management Mode	Indicates whether the gateway is managed or unmanaged.

- **Gateway Interface**: displays the gateway interfaces associated with the gateway as follows

Attribute	Description
Operation State	The operation state of the gateway interface. The state can display one of the following values: • Up • Down
Name	The name of the gateway interface.
Type	The type of the gateway interface.
Administrative State	The administrative state of the gateway interface. The state can display one of the following values: • Up

Attribute	Description
	• Down
Description	The description configured for the gateway interface.

- Incidents: Displays the incidents generated for the gateway interfaces discovered on the network as shown on the incidents page.

You can view the additional details for a gateway interface from the Gateway Interface form.

Gateway Incidents

The following table lists the gateway incident generated by the iSPI for IP Telephony for events related to the operational state of the gateways discovered in the Microsoft unified collaboration and communication management environment. You can view this incident using the **Incident Browsing** workspace or the **Incidents** tab page on the Gateway form.

Incident	Message	Severity	Description
GatewayOperStatusDown	The operational state of Gateway : $gwIdentity has changed to critical. Gateway ipaddress : $gwIPAddress	Critical	This incident indicates that operational state of all gateway interface i.e. endpoints hosted on the gateway has changed to down.

Gateway Interface Form

You can use the Gateway Interface form to view additional details about a discovered gateway.

To access the Gateway Interface form, do as follows:

1. Select a gateway interface discovered from the Gateway Interfaces tab on the Gateway form.
2. Click 📂 (**Open**). This opens the Gateway Interface form.

The Gateway Interface form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Name	Indicates the name of the gateway interface.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general gateway interface attributes as follows.

Attribute	Description
Index	Indicates the index number configured for the gateway interface.
Type	Indicates the type of the gateway interface.
Speed	Indicates the speed of the gateway interface.
Physical Address	Indicates the physical address of the gateway interface.
Shelf	Indicates the shelf location configured for the gateway interface.
Slot	Indicates the slot configured for the gateway interface.
Port	Indicates the port number configured for the gateway interface.
Channel Number	Indicates the channel number configured for the gateway interface.
Line Status	Indicates the line status of the gateway interface. The value can be one of the following: • Not Polled • Up • Down
Description	Indicates the description configured for the gateway interface.
Last Change	Indicates when the changes were made last to the gateway channel.

- **Gateway Channel**: displays the gateway channels associated with the gateway interface as follows

Attribute	Description
Operational State	The operational state of the gateway channel. The state can be one of the following values: • Up • Down • Not Polled

Attribute	Description
Usage State	Indicates the usage state of the gateway channel. The state can be one of the following values: • Up • Down • Not Polled
Name	The name configured for the the gateway channel.
Type	The type of the gateway channel.
Description	The description configured for the gateway channel.

- Incidents: Displays the incidents generated for the gateway interfaces discovered on the network as shown on the incidents page.

You can view additional details regarding the gateway channels using the Gateway Channel form.

Gateway Interface Incident

The following table lists the gateway interface incident generated by the iSPI for IP Telephony for events related to the operational state of the gateway interfaces discovered in the Microsoft unified collaboration and communication management environment. You can view this incident using the **Incident Browsing** workspace or the **Incidents** tab page on the Gateway Interfaces form.

Incident	Message	Severity	Description
GatewayInterfaceOperStatusDown	The operational state of Gateway interface : $ifaceName has changed to critical. Gateway ipaddress : $gwIPAddress	Critical	This incident indicates that the operational state of a gateway interface i.e. endpoint hosted on a voice gateway has changed from up to down.

Gateway Channel Form

You can use the Gateway Channel form to view additional details about a discovered gateway channel.

To access the Gateway Channel form, do as follows:

1. Select a gateway channel discovered from the Gateway Channels tab in the Gateway Interface form.
2. Click 📂 (**Open**). This opens the Gateway Channel form.

The Gateway Channel form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Name	Indicates the name configured for the gateway channel.

The right panel displays the following tab.

- **General**: displays the general gateway channel attributes as follows.

Attribute	Description
Index	Indicates the index number configured for the gateway channel.
Type	Indicates the type of the gateway channel.
Speed	Indicates the speed of the gateway channel.
Physical Address	Indicates the physical address of the gateway channel.
Shelf	Indicates the shelf location configured for the gateway channel.
Slot	Indicates the slot configured for the gateway channel.
Port	Indicates the port number configured for the gateway channel.
Channel Number	Indicates the channel number configured for the gateway channel.
Line Status	Indicates the line status of the gateway channel. The value can be one of the following: • Not Polled • Up • Down
Description	Indicates the description configured for the gateway channel.
Last Change	Indicates when the changes were made last to the gateway channel.

- Incidents: Displays the incidents generated for the gateway channels discovered on the network as shown on the incidents page.

Gateway Channel Incident

The following table lists the gateway channel incident generated by the iSPI for IP Telephony for events related to the usage state of gateway channels discovered in the Microsoft unified collaboration and communication management environment. You can view this incident using the **Incident Browsing** workspace or the **Incidents** tab page on the Gateway Channel form.

Incident	Message	Severity	Description
GatewayChannelStatusIdle	The usage state of Gateway channel : $chName has changed to idle. Gateway ipaddress : $gwIPAddress	Critical	Gateway channel usage status is idle.

Monitoring Gateway Interfaces

You can use the Gateway Interfaces inventory view to see the gateway interfaces discovered on the network.

To access the Gateway Interfaces inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Gateway Interfaces**. This displays the Gateway Interfaces inventory view.

The Gateway Interfaces inventory view displays the list of gateway interfaces discovered on the network along with the following attributes for each gateway interface.

Attribute	Description
Operational State	Indicates the operational state of the gateway interface. This column displays one of the following states for the gateway interface: • Polled: indicates that the gateway interface is polled periodically for a state change. • Not Polled: indicates that the gateway interface is not polled for a state change. • Not Applicable: indicates that the gateway interface is discovered, but not configured to be polled for a state change.
Name	Indicates the name configured for the gateway interface.
Type	Indicates the type of the gateway interface discovered.

Attribute	Description
Gateway	Displays the IP address of the gateway associated with the gateway interface.
Administrative State	Indicates the administrative state of the gateway interface discovered. This column displays one of the following states for the gateway interface: • Polled: indicates that the gateway interface is polled periodically. • Not Polled: indicates that the gateway interface is not polled. • Not Applicable: indicates that the gateway interface is discovered, but not configured to be polled.
Description	the description configured for the gateway interface.

You can view additional details for a discovered gateway interface using the Gateway Interfaces form.

Gateway Interface Form

You can use the Gateway Interface form to view additional details about a discovered gateway.

To access the Gateway Interface form, do as follows:

1. Select a gateway interface discovered from the Gateway Interfaces tab on the Gateway form.
2. Click 📂 (**Open**). This opens the Gateway Interface form.

The Gateway Interface form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Name	Indicates the name of the gateway interface.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general gateway interface attributes as follows.

Attribute	Description
Index	Indicates the index number configured for the gateway interface.
Type	Indicates the type of the gateway interface.
Speed	Indicates the speed of the gateway interface.

Attribute	Description
Physical Address	Indicates the physical address of the gateway interface.
Shelf	Indicates the shelf location configured for the gateway interface.
Slot	Indicates the slot configured for the gateway interface.
Port	Indicates the port number configured for the gateway interface.
Channel Number	Indicates the channel number configured for the gateway interface.
Line Status	Indicates the line status of the gateway interface. The value can be one of the following: • Not Polled • Up • Down
Description	Indicates the description configured for the gateway interface.
Last Change	Indicates when the changes were made last to the gateway channel.

- **Gateway Channel**: displays the gateway channels associated with the gateway interface as follows

Attribute	Description
Operational State	The operational state of the gateway channel. The state can be one of the following values: • Up • Down • Not Polled
Usage State	Indicates the usage state of the gateway channel. The state can be one of the following values: • Up • Down • Not Polled

Attribute	Description
Name	The name configured for the the gateway channel.
Type	The type of the gateway channel.
Description	The description configured for the gateway channel.

- Incidents: Displays the incidents generated for the gateway interfaces discovered on the network as shown on the incidents page.

You can view additional details regarding the gateway channels using the Gateway Channel form.

Monitoring SIP Trunk Configurations

You can use the SIP Trunks inventory view to see the SIP trunk configurations discovered on the network.

To access the SIP Trunk Configuration inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **SIP Trunk Configurations**. This displays the SIP Trunk Configuration inventory view.

The SIP Trunk Configuration inventory view displays the list of SIP trunk configurations discovered on the network along with the following attributes for each SIP trunk configuration.

Attribute	Description
Identity	Indicates the unique identity of the SIP trunk configuration discovered.
Site	Indicates the Lync site that includes the SIP trunk configuration.
Description	Indicates the description configured for the SIP trunk configuration.
Management Server	Indicates if the SIP trunk configuration is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the SIP trunk discovered: • Local: If the SIP trunk configuration is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the SIP trunk configuration.

You can view additional details for a discovered server using the SIP Trunk Configuration form.

SIP Trunk Configuration Form

You can use the SIP Trunk Configuration form to view additional details about a discovered SIP trunk configuration.

To access the SIP Trunk Configuration form, do as follows:

1. Select a SIP trunk configuration discovered from the SIP Trunk Configuration inventory view.
2. Click 📂 (**Open**). This opens the SIP Trunk Configuration form.

The SIP Trunk Configuration form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the SIP trunk configuration discovered.

The right panel displays the **General**drop-down list that displays the general SIP trunk configuration attributes as follows.

Attribute	Description
Site	The name of the Lync site associated with the SIP trunk configuration.
Description	The description configured for the SIP trunk configuration.
RTCP Active Calls	Indicates if RTCP Active Calls is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
RTCP Calls on Hold	Indicates if RTCP Calls on Hold is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
SRTP Mode	Indicates if SRTP mode is required for the SIP trunk configuration.
Max Early Dialogs	Indicates the maximum early dialogs configured for the SIP trunk.
Enable Bypass	Indicates if Enable Bypass is enabled or disabled for the SIP trunk. A tick mark indicates that this feature is enabled for the SIP trunk.
Enable Signal Boost	Indicates if Enable Signal Boost is enabled or

Attribute	Description
	disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Concentrated Topology	Indicates if concentrated topology is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Enable Mobile Trunk Support	Indicates if Enable Mobile Trunk Support is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Trunk Enable Refer Support	Indicates if Trunk Enable Refer Support is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.

Monitoring Dial Plans

You can use the Dial Plans inventory view to see the dial plans discovered on the network.

To access the Dial Plans inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Dial Plans**. This displays the Dial Plans inventory view.

The Dial Plans inventory view displays the list of dial plans discovered on the network along with the following attributes for each dial plan.

Attribute	Description
Identity	Indicates the unique identity of the dial plan discovered.
Name	Indicates the name configured for the dial plan.
Description	Indicates the description configured for the dial plan.
Management Server	Indicates if the dial plan is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the dial plan discovered: • Local: If the dial plan is being managed by the NNMi management server console on

Attribute	Description
	which you are viewing the dial plan details. • Name of the regional manager that manages the dial plan.

You can view additional details for a discovered server using the Dial Plans form.

Dial Plan Form

You can use the Dial Plans form to view additional details about a discovered dial plan.

To access the Dial Plans form, do as follows:

1. Select a dial plan discovered from the Dial Plans inventory view.
2. Click 📂 (**Open**). This opens the Dial Plans form.

The Dial Plans form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the dial plan discovered.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general dial plan attributes as follows.

Attribute	Description
Name	Indicates the name of the dial plan.
Description	Indicates the description configured for the dial plan.
Dial in Conferencing Region	Indicates the dial in conferencing region configured for the dial plan.
Country Code	Indicates the country code configured for the dial plan.
State	Indicates the state name configured for the dial plan.
City	Indicates the city configured for the dial plan.
External Access Prefix	Indicates the external access prefix configured for the dial plan.
Optimize Device Dialing	Indicates if this attribute is enabled for the dial plan to support the configuration for an external access prefix. A tick mark next to this attribute indicates that the attribute is enabled for the dial

Attribute	Description
	plan.

- **Normalization Rules**: displays the normalization rules associated with the dial plan as follows

Attribute	Description
Identity	The identity of the normalization rule associated with the dial plan.
Name	The name configured for the normalization rule.
Description	The description configured for the normalization rule.

You can view more details about the normalization rules from the Normalization Rule form.

Normalization Rule Form

You can use the Normalization Rule form to view additional details about a normalization rule associated with a dial plan.

To access the Normalization Rule form, do as follows:

1. Select a normalization rule from the Normalization Rules tab on the Dial Plan form.
2. Click 📂 (**Open**). This opens the Normalization Rule form.

The Normalization Rule form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the normalization rule.

The right panel displays the **General**drop-down list that displays the general normalization rule attributes as follows.

Attribute	Description
Name	The name of the normalization rule.
Description	The description configured for the normalization rule.
Priority	Indicates the priority configured for the normalization rule.
Pattern	Indicates the pattern configured for the normalization rule.
Translation	Indicates the translation string for the normalization rule.

Attribute	Description
Is Internal Extension	Indicates if the phone number is an internal extension. A tick mark next to this attribute indicates that the phone number is an internal extension.
Do Not Use From Device	Indicates if this flag is enabled for the normalization rule. A tick mark next to this attribute indicates that the flag is enabled for the normalization rule.

Monitoring Voice Routes

You can use the Voice Routes inventory view to see the voice routes discovered on the network.

To access the Voice Routes inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Voice Routes**. This displays the Voice Routes inventory view.

The Voice Routes inventory view displays the list of voice routes discovered on the network along with the following attributes for each voice route.

Attribute	Description
Identity	Indicates the unique identity of the voice route discovered.
Name	Indicates the name configured for the voice route.
Description	Indicates the description configured for the voice route.
Priority	Indicates the priority configured for the voice route.
Management Server	Indicates if the voice route is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the voice route discovered: • Local: If the voice route is being managed by the NNMi management server console on which you are viewing the voice route details. • Name of the regional manager that manages the voice route.

You can view additional details for a discovered server using the Voice Routes form.

Voice Routes Form

You can use the Voice Routes form to view additional details about a discovered voice route.

To access the Voice Routes form, do as follows:

1. Select a voice route discovered from the Voice Routes inventory view.
2. Click (**Open**). This opens the Voice Routes form.

The Voice Routes form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the voice route discovered.

The right panel displays the **General**drop-down list that displays the general voice route attributes as follows.

Attribute	Description
Name	Indicates the name of the voice route.
Description	Indicates the description configured for the voice route.
Priority	Indicates the priority configured for the voice route.
Number Pattern	Indicates the number pattern configured for the voice route.
Suppress Caller ID	Indicates if the feature to suppress the caller ID is enabled or disabled. The possible values displayed are as follows: • True • False.
Alternate Caller ID	Indicates the alternate caller ID configured if the Suppress Caller ID feature is enabled for the voice route.
PSTN Gateways	Indicates the PSTN gateway configured for the voice route.
PSTN Usages	Indicates the PSTN usage record associated with the voice route.

Monitoring Voice Policies

You can use the Voice Policies inventory view to see the voice policies discovered on the network.

To access the Voice Policies inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Voice Policies**. This displays the Voice Policies inventory view.

The Voice Policies inventory view displays the list of voice policies discovered on the network along with the following attributes for each voice policy.

Attribute	Description
Identity	Indicates the unique identity of the voice policy discovered.
Name	Indicates the name configured for the voice policy.
Description	Indicates the description configured for the voice policy.
Management Server	Indicates if the voice policy is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the voice policy discovered: • Local: If the voice policy is being managed by the NNMi management server console on which you are viewing the voice policy details. • Name of the regional manager that manages the voice policy.

You can view additional details for a discovered server using the Voice Policy form.

Voice Policy Form

You can use the Voice Policy form to view additional details about a discovered voice policy.

To access the Voice Policy form, do as follows:

1. Select a voice policy discovered from the Voice Policies inventory view.
2. Click 📂 (**Open**). This opens the Voice Policy form.

The Voice Policy form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the voice policy discovered.

The right panel displays the **General**drop-down list that displays the general voice policy attributes as follows.

Attribute	Description
Name	Indicates the name of the voice policy.
Description	Indicates the description configured for the voice policy.
PSTN Usages	Indicates the PSTN usage record associated with the voice policy.
Allow Simul Ring	Indicates if the feature to allow incoming calls to ring simultaneously on additional phones is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Allow Call Forwarding	Indicates if the feature to allow call forwarding is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Allow PSTN Re Routing	Indicates if the feature to allow calls to be routed in the event of a WAN congestion or unavailability is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Delegation	Indicates if the feature to allow calls to be delegated to other users is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Team Call	Indicates if the feature to allow calls to be handled by a team on behalf of other members of the team is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Call Transfer	Indicates if the feature to allow calls to be transferred is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Call Park	Indicates if the feature to allow calls to be parked is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the

Attribute	Description
	voice policy.
Enable Malicious Call Tracing	Indicates if the feature to allow tracing of malicious calls is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable BW Policy Override	Indicates if the feature to allow bandwidth policy override is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Prevent PSTN Toll Bypass	Indicates if the feature to prevent PSTN toll bypass is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.

Monitoring Sites

You can use the Sites inventory view to see the NNMi sites discovered on the network. A site refers to an NNMi site configured by the NNMi administrator. An administrator maps the discovered Lync Server entities (edge servers, gateways, front end servers, registrar pools, and so on) on the network to the site for ease of administration.

To access the Sites inventory view, do as follows:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Sites**. This displays the Sites inventory view.

The Sites inventory view displays the list of sites discovered on the network along with the following attributes for each site.

Attribute	Description
Site Name	Indicates the name of the NNMi site.
Description	Indicates the description configured for the NNMi site.
Order	Indicates the order number configured for the NNMi site.

Launching Context-sensitive Actions for a Site

You can perform the following context-sensitive actions for a selected site from the Sites inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the site.
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

You can view additional details for a discovered server using the Sites form.

Sites Form

You can use the Sites form to view additional details about a discovered NNMi site.

To access the Sites form, do as follows:

1. Select a site discovered from the Sites inventory view.
2. Click (**Open**). This opens the Sites form.

The Sites form displays information in two panels., the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Site Name	Indicates the name of the site discovered.

The right panel displays the **General**drop-down list that shows the general site attributes as follows.

Attribute	Description
Site Name	Indicates the name of the site.
Description	Indicates the description configured for the site.
Site Definition	Indicates the definition configured for the site.
Order	Indicates the order number configured for the site.

Viewing Lync Site Neighborhood

You can use the Lync Topology map to view the sites, branches, and gateways discovered on the network. The topology map displays the connection between the central site, the branch sites, and the gateways discovered on the network.

You can perform the following tasks from the Lync Topology map:

- Launch the call details chart detail report for a selected gateway or Lync site or branch.
- Launch the call quality chart details report for a selected Lync site or branch.

- Discover topology and discover users for a selected Lync site or branch.
- Launch the Analysis panel for a selected Lync site or branch. You can select a Lync site or branch to launch the Analysis pane for the selected Lync site or branch
- View a summary of the details for a Lync site or a branch, or a gateway by placing the cursor on the image that denotes a Lync site, a Lync branch, or a gateway. This displays a pop up that includes the summarized details for the Lync site, Lync branch, or the gateway.

To launch the call details for a Lync site or branch, do as follows:

1. Select the Lync site or branch from the Lync Topology map
2. Click **Actions** > **Microsoft IP Telephony** > **Call Detail by Lync Site**

Note: Follow the steps listed above and select the appropriate option to perform the tasks you can do from the Lync Topology map.

Alternatively, you can also right click a Lync site, Lync branch, or a gateway to launch the context-sensitive menu that lists the options to perform the tasks you can do from the Lync topology map.

We appreciate your feedback!

If an email client is configured on this system, click Send Email

If no email client is available, copy the following information to a new message in a web mail client and send the message to **docfeedback@hp.com**.

Product name and version:

Document title:

Feedback: