CA Unified Communications Monitor

Use Cases for Organizing Your Network Components

Version 3.5

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Creating Location Definitions

By associating network entities with Location definitions, you can quickly locate the sources of performance issues in UC Monitor reports. Location definitions correspond to entities such as branch offices, departments, or buildings.

Many UC Monitor reports are based solely on the Locations you define. Imprecise or incomplete definitions render these reports inefficient, at best, or useless, at worst. Your goal in creating Location definitions is to set up a reporting system in which:

- One problem that affects multiple end users is not reported multiple times.
- More specifically, one problem creates only one incident in the system.
- The IT operator or engineer who receives a notification about an incident is the person most capable of troubleshooting the problem.
- That same operator or engineer receives a minimal number of notifications about any specific performance incident.
- UC Monitor operators see reports that contain only the call data that they have permission to view. Confidential call data is restricted to reports that most operators cannot access.

This use case shows UC Monitor administrators how to create Location definitions, including tips for planning Location definitions and instructions for importing Location definitions from a spreadsheet.

This section contains the following topics:

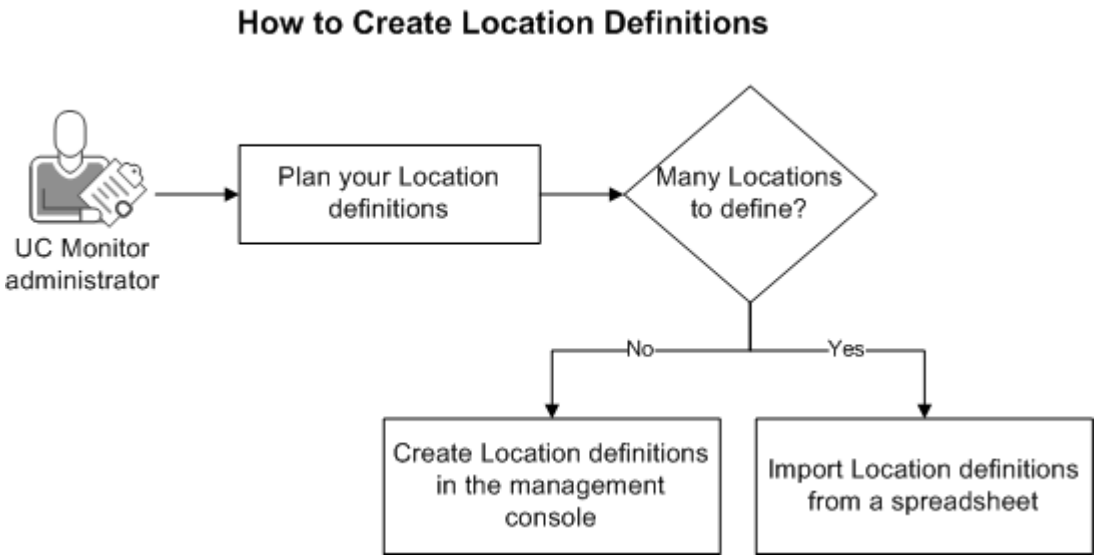
Overview

Creating Location definitions is an essential step to take when setting up your UC Monitor system. Location definitions cannot be applied retroactively to collected data. Create or import definitions when you configure collectors and the management console. Create Location definitions that cover all endpoints in the monitored system.

Call traffic for new subnets is labeled as <Unassigned> until you assign those subnets to a Location definition.

Tip: To define many Locations, you can save time by entering them into a spreadsheet document and importing the spreadsheet into the UC Monitor management console.

The following diagram illustrates the process for creating Location definitions.



The following topics describe how to create Location definitions:

- Tips for planning Locations (see page 8).
- Create Location definitions in the management console (see page 10).
- Import Location definitions from a spreadsheet (see page 12).

Tips for Planning Locations

When properly deployed, Locations help you organize your entire system. This topic provides advice for creating and maintaining Location definitions.

Exclude unwanted data

Some deployments provide more accurate reports when you selectively exclude less-reliable data. For example, the endpoints in laboratory test beds or pilot deployments do not contribute performance metrics to reports that pertain to a production network. When creating a Location definition, you can exclude the Location from monitoring so that metrics from the endpoints in the Location subnets are not collected.

Designate key phones

(*Cisco only*) Location definitions can include key phone designations. By serving as the target for regular traceroute testing, the key phone lets the collector gather more data for baseline traceroute reporting. Key phones are optional, but recommended.

Align UC Monitor Locations and Microsoft locations

The UC Monitor Locations and the locations that are known to the Quality of Experience monitoring server should match each other as closely as possible. The Microsoft concept of locations corresponds to that of UC Monitor: subnets where endpoints are connected.

Use existing IP network regions

(*Avaya only*) IP network regions let you configure IP endpoints in the same segments of the network. For example, you can set QoS parameters, VoIP or video codecs, RTCP monitoring defaults, and call-routing settings. IP network regions can also help you identify the physical or logical locations of endpoints. Use your existing IP network region parameters when setting up Location definitions.

Create Locations for distinct network features

Create a separate Location for network or network segments that have distinctive characteristics, such as an Ethernet LAN segment connected to a Frame Relay network.

Place remote endpoints in a separate Location from endpoints local to the call server cluster. When the branch office telephones undergo an outage or failover, the incident notification provides the Location name of the branch office. The incident report identifies the telephones and equipment for investigation.

Assign similar components to a Location

Assign Locations to groups of unified communications components that, under normal operating conditions, achieve similar performance based on the network links and equipment they access.

Use CA Performance Center to organize Locations in groups or IP domains

Groups permit UC Monitor operators to access only the call data that is required for their jobs. An organizational strategy that leverages groups and Locations to protect sensitive call data is essential.

If you decide to organize Locations and devices into groups or IP domains, the hierarchical structure you require can affect the naming of Locations. For example, you can select an organizational rather than a geographical structure. Plan this structure before you create Location definitions.

Avoid too many Locations

Use Locations to help identify subnets and hosts at a fairly granular level. However, avoid segmenting your enterprise into too many distinct Locations that have the same general networking characteristics. A long list of Locations is difficult to view in reports. In addition, with too many Locations, you might see multiple incidents that stem from the same root issue. For a LAN divided into multiple Locations, problems that affect all endpoints on that LAN create multiple incident reports, one for each Location.

Know your gateways and call servers

As you define Locations, understand which call servers and gateways the endpoints in each subnet or IP network region are using. Doing so makes it easier to configure thresholds and gateways and interpret report data. You can set VoIP and video performance thresholds in the following ways:

- Between pairs of Locations
- Between pairs of Locations and voice gateways.
- Between pairs of voice gateways

Create call quality thresholds for your Locations

You can customize call quality thresholds and then apply the new settings to pairs of Locations. You cannot apply thresholds to groups of Locations.

Create Location Definitions in the Management Console

By associating network entities with Location definitions, you can quickly locate the sources of performance issues in UC Monitor reports. Location definitions correspond to entities such as branch offices, departments, or buildings.

Follow these steps:

1. Click Administration, Data Collection, Locations in the navigation bar.

   The Location List opens.

2. Click New.

   The Location Properties page opens.

3. Complete the following fields.

   - **Name**. A name that makes it easy to identify the Location. For example:
     - Geography, such as *New York* or *Eastern Region*
     - Function, such as *Operations-US*
     - Exact location, such as *Building A*
     - Data center or NOC associated with the subnets in this Location
   - **IP Domain**. The IP domain that is associated with all traffic for this Location. IP domains are created in CA Performance Center. This field is available only when UC Monitor is registered to a CA Performance Center instance where at least one custom IP domain is defined.
   - **Key Phone Address**. (*Cisco only*) The IP address of a key phone for this Location definition. The key phone serves as the target for regular traceroute testing. The collector runs a traceroute test to the key phone every four hours. Baseline traceroute data is then reported in the Traceroute Investigation Details report.

- **Description**. Descriptive terms to help other IT operators identify the Location.
- **Monitoring Status**. Select whether to include data from this Location in reports. The following options are available:
  - Enabled: Monitoring is enabled for subnets you add to this Location.
  - Disabled: The subnets in this Location are not monitored. Data from them is discarded.
  - Enabled (Sending Only): Monitoring is enabled only for calls *from* endpoints in these subnets *to* endpoints in monitored Locations.

4. Click New to add subnets to the Location definition. The Add Subnet in Location page opens.
5. Complete the following fields:
   - **Subnet Name**. A name to identify each subnet when it appears in the Administration pages.
   - **Subnet Address**. The IP network address, in dotted notation, of the subnet to include in this Location definition. For example, 10.11.12.0.

     The subnet address corresponds to the IP addresses for the components in this Location. For a Location, one subnet or multiple subnets can be applicable.
   - **Mask**. Select the number of bits used in the subnet mask to create this subnet. For example, select 27 to indicate that the first 3 bits of the final octet are used to identify or differentiate subnets.
6. Click OK.

   The Location Properties page opens. UC Monitor verifies that the new subnet is unique. Subnets must not share addresses (that is, overlap) with other subnets you defined.
7. Repeat steps 4 through 6 for each subnet that you want to add.
8. Save the Location definition:
   - Click Save. The Location List displays the new Location definition.
   - Click Save & Add Another to save the Location definition and add another definition.

More information:

Understanding Subnets (see page 12)

Understanding Subnets

The key information to supply when creating a Location is the subnet, or list of subnets, that the Location definition includes.

You can enter a 32-bit network address, such as 10.2.3.0. Then select the number of bits to use for the network prefix, such as 27 (to represent 255.255.255.224). For example, you enter 10.2.3.0 for the subnet with a mask of 27. The subnet is stored in the database and shown in the management console with the conventional syntax, 10.2.3.0/27.

Multiple subnets can be added to each Location definition. To extend the previous example, the following valid subnets also use the mask of 27:

```
10.2.3.32
10.2.3.64
10.2.3.96
10.2.3.128
10.2.3.160
10.2.3.192
10.2.3.224
```

Each subnet can contain as many as 30 hosts. The new Location definition is then applied to all valid subnets you add.

Do not add subnets that overlap. Overlapping subnets are not supported.

You can limit a Location to one IP address. The appropriate syntax specifies the IP address with a mask of 32 (all bits). However, avoid defining multiple subnets with a mask of 32 bits. This configuration also restricts the rest of the subnets in that range because of the restriction on overlapping.

Import Location Definitions

You can import Locations and subnets in situations where manually creating them is time-consuming, such as the following examples:

- You need many distinct Locations to organize your unified communications system.
- The network contains many subnets.

You can use the import feature for the initial UC Monitor configuration and for subsequent additions of Locations and subnets. You cannot use the import feature to edit or delete Locations. However, after you import the definitions, you can edit or delete them from the Location List.

Follow these steps:

1. Create a .csv file that contains your Location definitions.
2. Click Administration, Data Collection, Locations in the navigation bar.

   The Location List opens.
3. Click Import.

   The Import Locations wizard opens.
4. (*Optional*) Select a custom domain for the IP Domain field. This field is available only after you create IP domain definitions in CA Performance Center.
5. Click Browse, and navigate to the .csv file that contains your Location and subnet definitions.
6. Click Next.

   UC Monitor analyzes the file and reports any syntax errors.
7. Correct any errors in the file and save it. Then repeat steps 5 and 6.

   When no errors are found, the import operation is completed. A confirmation page appears. The appropriate database objects are created.
8. Click OK.

   The Location List displays the new Locations.

More information:

Understanding Subnets (see page 12)
Syntax for the .CSV File (see page 13)

Syntax for the .CSV File

The import feature imports data from a file in comma-separated values (.csv) format. The correct syntax is to separate items with commas (,) but no spaces. The following list identifies the data type and syntax, and provides examples.

Location definition (complete)

Use quotation marks to enclose strings that contain commas, double quotation marks, or other punctuation.

Syntax: LOCATION,LocationName,"Location Description",Key Phone IP Address

Examples:

- LOCATION,Austin,"All phones,Third Floor",192.168.104.25
- LOCATION,Branch office,"Sales - Milwaukee",10.12.34.2

Subnet definition (complete)

LocationName must correspond to a defined Location. Mask must be a value of 1 to 32, inclusive.

Syntax: SUBNET,LocationName,SubnetName,Subnet IP Address,Mask

Examples:

- SUBNET,Austin,Marketing,192.168.104.0,24
- SUBNET,Branch office,Remote Sales,10.12.34.0,30

Location definition (no description)

Location and Key Phone IP Address are optional.

Syntax: LOCATION,LocationName,,Key Phone IP Address

Examples:

- LOCATION,Marketing - Raleigh Office
- LOCATION,Finance,,10.12.68.2

Subnet definition (no subnet name)

Subnet is optional. LocationName is required for subnets.

Syntax: SUBNET,LocationName,SubnetName,Subnet IP Address,Mask

Examples:

- SUBNET,Marketing - Raleigh Office,,192.168.123.0.24
- SUBNET,Finance,,10.12.68.0.30

Chapter 2: Adding Call Servers

Unified communications deployments rely on specialized server hardware or software to route calls, log quality data, and inventory registered endpoints. No matter which physical server performs the main call processing tasks in a system, UC Monitor labels it a call server.

UC Monitor automatically discovers call servers from monitored call traffic. However, many servers can be the call server in a multi-vendor environment. Therefore, you can also manually supply information to identify the call servers in your network.

Note: You cannot add Microsoft call servers, nor can you change the automatic group assignment for Microsoft call servers that belong to pools.

This use case shows UC Monitor administrators how to add call servers to the UC Monitor database.

This section contains the following topics:

Tips

Adding call servers is recommended in the following situations:

In a Cisco environment that has at least one Cisco TelePresence server.

Adding call servers lets the collector distinguish between the TelePresence server and the Cisco Unified Communications Manager server. The distinction prevents TelePresence traffic from being mistakenly reported as coming from a phone or gateway.

In an Avaya environment where the following are true:

- The identity of the Communications Manager is not easily determined from call data.

  Example: For large environments, the Communication Manager does not usually handle call processing. Instead, Controller-LAN boards (C-LANs) perform call processing. Each board has a dedicated IP address. The IP address appears in call data as the device that handles call processing, and, therefore, the IP address appears in UC Monitor reports as a call server. UC Monitor never discovers the Communication Manager as a call server because:

  - The Communication Manager is installed on a separate media server.
  - The Communication Manager does not participate in call processing.

- You want to collect data from Avaya trunk groups.

  UC Monitor queries the Communication Manager for trunk group data. Therefore, add the Communication Manager as a call server when the Communication Manager is not automatically discovered.

  Tip: To collect trunk group data in an Avaya environment with duplex servers, add only one call server in UC Monitor, using the IP-Alias address. The IP-Alias address is shared between the duplex servers and is sometimes called the Active Server IP address.

  - UC Monitor uses the call server name as part of the trunk group identifier. If you add two call servers, one with the IP-Alias address and one with the actual IP address, then duplicate data is returned for the same trunk group.
  - If you do not add a call server for the IP-Alias address and, instead, add a call server for each duplex server, then only one set of data is returned from the trunk group. Polling to the standby server will fail (because the server is in standby mode), and UC Monitor eventually stops trying to poll that server. If the standby server becomes active again, UC Monitor will not poll it for trunk group data.

Add Call Servers

Take the following steps to add call servers to the UC Monitor database.

Follow these steps:

1. Click Administration, Data Collection, Call Servers in the navigation bar.

   The Call Server List opens.

2. Click New.

   The Call Server Properties page opens.

3. Complete the following fields:

   - **Name**. The DNS host name of the call server. If you do not know the host name, enter the IP address in the Address field and click DNS.
   - **Address**. The IP address of the call server in dotted notation, such as 10.10.2.34. If you do not know the IP address, enter the server DNS host name in the Name field and click IP.

- **IP Domain**. The IP domain that is associated with this device. The IP domain is created in CA Performance Center. This field is available only when UC Monitor is registered to a CA Performance Center instance where at least one IP domain is defined.

  Note: This field is useful when the CA Performance Center administrator creates permission groups that organize call data into separate IP domains. The administrator can grant operator access to call data on a per-domain basis.

- **Description**. (*Optional*) A description to help identify this device, such as its location, capabilities, or past performance.

- **Call Server Group**. The call server group to which the server is assigned. By default, all newly discovered Avaya and Cisco call servers are assigned to the <Unassigned> call server group. Microsoft call servers are automatically assigned to call server groups according to their membership in Enterprise Edition pools.

  Note: For information about creating call server groups, see the online help or the use case titled *Creating Call Server Groups* in the UC Monitor bookshelf on CA Support Online.

4. Save the call server:

   - Click Save. The Call Server List displays the new call server.
   - Click Save & Add Another to save these properties and add another call server.

   Data from the call server is now included in UC Monitor reports.

Chapter 3: Creating and Assigning Call Server Groups

With UC Monitor, you can organize your call servers into call server groups, which mimic the clusters or server pools in your unified communications system. These groups are useful for the following purposes:

- Identifying call server clusters or pools in reports.
- Identifying call servers and call server groups in CA Performance Center when UC Monitor is registered as a data source.
- Helping you to understand call volumes as reported in the Capacity Planning reports.
- Creating valid permission groups so that UC Monitor operators can see the report data in CA Performance Center.
- Letting you assign call server group thresholds to enable incident creation (Cisco only).

All Cisco and Avaya call servers are automatically assigned to the <Unassigned> call server group when they are discovered. Microsoft call servers are automatically assigned to call server groups, according to pool identity, to reflect Enterprise Edition pool structure. You can reassign Cisco and Avaya call servers to custom call server groups. However, you cannot change the assignment for Microsoft call servers.

This use case shows UC Monitor administrators how to create custom call server groups for Cisco and Avaya call servers, and how to assign call servers to a call server group.

This section contains the following topics:

Tips

Consider the following when creating call server groups:

- Avaya and Cisco call servers are placed in the <Unassigned> group when they are discovered. After a day or two of monitoring, most of your call servers are entered into the UC Monitor database. You can verify whether all call servers are discovered by viewing the Call Server List, which displays information about all known call servers.
- When enough call servers are displayed in the list to represent the clusters in your system, you can create call server groups. First, create empty groups. As a best practice, assign these groups names that correspond to their cluster names. Then assign each call server to a group.
- If your environment contains only one cluster, change the name of the <Unassigned> call server group to name of the cluster. This naming convention ensures that call server incidents are reported correctly. New call servers are automatically added to this group because it is the default group.
- You can view call server groups in CA Performance Center after you register UC Monitor as a data source. However, you can manage call server groups only in the UC Monitor management console.

Create a Call Server Group

You can organize your call servers into call server groups, which mimic the clusters or server pools in your unified communications system. Take the following steps to create custom call server groups.

Follow these steps:

1. Click Administration, Data Collection, Call Server Groups in the navigation bar.

   The Call Server Group List opens.

2. Click New.

   The Call Server Group Properties page opens.

3. Complete the following fields:

   - **Name**. A name for the call server group, such as the name of the call server cluster or server pool. This name is sent to CA Performance Center at the next synchronization, where it appears in the Groups tree.
   - **Description**. (*Optional*) The description helps to identify the group when it appears in CA Performance Center.

4. Save the call server group:
   - Click Save to save this group.
   - Click Save & Add Another to save this group and create another call server group.

   You can now assign this group to selected call servers.

Assign a Call Server Group to a Call Server

You can assign Cisco and Avaya call servers to custom call server groups.

Follow these steps:

1. Click Administration, Data Collection, Call Servers in the navigation bar.

   The Call Server List opens.

2. Select the call server to which you want to assign a group and click Edit.

   The Call Server Properties page opens.

3. Select a call server group from the list in the Call Server Group field. The call server group you created appears in the list.

4. Click Save.

   The call server is a member of the call server group.

Chapter 4: Adding Voice Gateways and Other Media Devices

Unified communications systems require specialized devices to route calls from the PSTN, to handle conference calls, and to transcode media streams. Examples include voice gateways, session border controllers, mediation servers, conferencing servers, and unified messaging servers.

- In Cisco or Avaya environments, voice gateways route VoIP calls to and from the PSTN. Voice gateways provide important information about call performance and quality.
- In Microsoft Lync environments, media devices play an essential role in call routing and processing, but do not provide metrics by SNMP. UC Monitor monitors the performance of the call legs that media devices handle and includes their metrics in performance reports.

This use case shows UC Monitor administrators why and how to add voice gateways and other media devices to the UC Monitor database, including instructions for importing voice gateway definitions from a spreadsheet.

This section contains the following topics:

Why Add Voice Gateways?

The collector automatically discovers Cisco or Avaya voice gateways on your network when those devices handle calls. However, you can manually add voice gateways to the database in the following circumstances:

- Analog telephones in your system are connected to Cisco VG-224 gateways. These devices can appear incorrectly in reports unless you add them as voice gateways.
- Your network includes voice gateways that are in different SNMP communities, or that support different versions of SNMP. You can associate a voice gateway definition with an SNMP profile that contains gateway-specific security parameters.

- You suspect that SNMP community information is incorrect. The procedure for adding a voice gateway (see page 24) lets you review the SNMP security parameters and verify that the collector can poll the device.
- You want to create custom groups of devices and Locations in CA Performance Center. Groups let you grant view access to UC Monitor data when you configure user accounts. You can include voice gateways in user permission groups.

Note: You cannot add gateway voice interfaces. UC Monitor automatically polls the gateways and discovers information about available voice interfaces.

Add a Voice Gateway

Take the following steps to manually add additional voice gateways to the UC Monitor database.

Note: If you have many voice gateways to add, you can import their definitions (see page 26) from a spreadsheet.

Follow these steps:

1. Click Administration, Data Collection, Media Devices, Voice Gateways in the navigation bar.

   The Voice Gateway List opens.

2. Click New.

   The Voice Gateway Properties page opens.

3. Complete the following fields:

   - **Name**. A name for the voice gateway. Typically, the DNS host name, although you can enter any name. If you do not know the DNS host name, enter the IP address in the Address field and click DNS.
   - **Address**. The IP address of the device in dotted notation, such as 10.10.2.34. If you do not know the IP address, enter the server DNS host name in the Name field and click IP.
   - **IP Domain**. The IP domain that is associated with this device. The IP domain is created in CA Performance Center. This field is available only when UC Monitor is registered to a CA Performance Center instance where at least one IP domain is defined.

- **SNMP Profile**. Select the SNMP profile to associate with this gateway. The SNMP profile contains security information, such as the SNMP community string, to let the collector query the MIB of this gateway device. The default SNMP profile is used unless you select a custom profile from the list. Unless you changed it, the default SNMP profile uses the "public" community string.

  Click Verify SNMP to instruct the collector to try to contact the gateway using the specified SNMP profile.

  By default, the collector that detected the voice gateway is used for the verification. We recommend using the default collector. If verification fails, select another collector from the "from Collector" list and try again.

  Note: If you are monitoring by IP domain, the IP domain with which the collector associates call data is appended to the collector host name.

- **Monitoring Status**. Whether data from this device is included in reports. The following options are available:

  - Enabled: Monitoring is enabled for calls that are routed by this device.
  - Disabled: Calls that are routed by this device are not monitored. Data from the calls is discarded.
  - Enabled (Sending Only): Monitoring is enabled only for calls that are sent from the PSTN through this device to phones in monitored Locations.

- **Perform routine traceroutes for the baseline**. When enabled, routine traceroutes run to this device every four hours to establish a baseline of data about common paths through the network. Routine traceroute testing is enabled for each new Cisco gateway device. Routine traceroute testing is disabled for Avaya voice gateways, which do not perform call setup. The option is automatically disabled when the monitoring status is Disabled.

- **Description**. (*Optional*) A description to help identify this device, such as its location, capabilities, or past performance.

- **Voice Interfaces**. Click Edit to change the properties of voice interfaces for the gateway. Complete the following fields, and then click OK.

- **Name**. The name for the gateway voice interface. By default, the interface name is based on information from the gateway and the naming convention employed by the trunking equipment. You can supply a more easily remembered name for this field.

- **Discovered Capacity**. The maximum number of simultaneous calls that this interface can support, according to information discovered by the collector. The collector finds information about interface capacity using different methods for each type of gateway device or protocol. The discovered capacity is collected from the gateway MIB.

  Note: In many cases, the collector can retrieve capacity information from its initial polling of the gateway. However, the collector does not retrieve changes in capacity information. Enter any changed information in this field.

- **Override Channel Capacity**. By default, this value is the same as the value in the Discovered Capacity field. You can change, or override, the discovered capacity for reasons that depend on your environment. For example:
  - The device MIB misreports the interface capacity.
  - For capacity-planning purposes, you want to see usage statistics in UC Monitor reports that reflect a different call capacity for an interface.

  Tip: The Voice Interface reports use the channel capacity information to calculate interface usage as a percentage of capacity. These reports are less accurate when the device MIB incorrectly reports channel capacity.

4. Save the voice gateway:
   - Click Save. The Voice Gateway List displays the new voice gateway.
   - Click Save & Add Another to save these properties and add another voice gateway.

   Data from the new voice gateway is now included in UC Monitor reports.

Import Voice Gateway Definitions

When your network contains many voice gateways, use the import feature to add device definitions. Use this feature for the initial UC Monitor configuration and for subsequent additions of gateways.

Note: Only voice gateways that support SNMPv1 or SNMPv2C can be imported. You must manually add voice gateways that support SNMPv3.

The import interface does not let you edit or delete gateways that are already in the system. After you import the definitions, you can edit and delete them from the Voice Gateway List.

For each SNMP community string that you specify in the .csv file, UC Monitor checks for the corresponding SNMP profile. If no corresponding profile is found, UC Monitor creates a profile for the community string.

Tip: Create SNMP profiles before importing voice gateway definitions. For more information, see the "SNMP Profiles" topic in the UC Monitor online help.

For SNMP community strings not specified in the .csv file, the collector uses the default SNMP profile to contact the associated gateway. If you create SNMP profiles, you can set one of them as the default before importing the .csv file. Otherwise, the default profile for SNMP v1/2c is used. The default profile uses the “public” community string.

The monitoring status of imported voice gateways is always set to Enabled. Edit an imported definition to change the monitoring status.

IP domain definitions are not included in the supported syntax. IP domains are determined on a per-collector basis and are assigned to gateways as they are detected during monitoring. The IP Domain field lets you instruct the collector to associate voice gateways with a domain container. To expose the IP Domain field, define an IP domain in CA Performance Center.

The import procedure takes data from a file in comma-separated values (.csv) format. The correct syntax is to separate items with commas (,) and no spaces. The syntax for the data you want to import is described in the following table:

Data Type and Syntax	Notes and Examples
Voice gateway definition (complete): Voice gateway name,IP address,SNMP community,Description,Traceroute	Use quotation marks to enclose strings that contain commas, double quotation marks, or other punctuation. The voice gateway name can be different from its host name. Include the word “Traceroute” to enable the option to “Perform routine traceroutes for baseline.” To disable this option, do not include the word "Traceroute." Examples: ■ Houston Data Center,10.12.34.56,private,"Data center, gateway router",Traceroute ■ HoustonDataCtr01,10.12.34.56,private,Data center gateway router ■ Austin_HQ_FXO,10.123.45.67,ultra5ecur3PW,VGW at HQ,Traceroute
Voice gateway definition (no SNMP community, no description): Voice gateway name,IP address,,,Traceroute	SNMP community, description, and traceroute are optional. The default SNMP profile is used. Examples: ■ Houston Data Center,10.12.34.56,,,Traceroute ■ HoustonDataCtr01,10.12.34.56 ■ Austin_HQ_FXO,10.123.45.67,,,Traceroute
Voice gateway definition (no description): Voice gateway name,IP address,SNMP community,,Traceroute	Voice gateway description and traceroute are optional. Examples: ■ Houston Data Center,10.12.34.56,private ■ HoustonDataCtr01,10.12.34.56,private,,Traceroute ■ Austin_HQ_FXO,10.123.45.67,ultra5ecur3PW,,Traceroute

Data Type and Syntax	Notes and Examples
Voice gateway definition (no SNMP community): Voice gateway name,IP address,,Description,Traceroute	SNMP community string is optional. If no string is supplied, the collector uses the default SNMP profile. Examples: ■ Houston Data Center,10.12.34.56,,"Data center, gateway router",Traceroute ■ HoustonDataCtr01,10.12.34.56,,Data center gateway router ■ Austin_HQ_FXO,10.123.45.67,,VGW at HQ,Traceroute

Follow these steps:

1. Create a .csv file that contains your voice gateway definitions.
2. Click Administration, Data Collection, Media Devices, Voice Gateways in the navigation bar.

   The Voice Gateway List opens.
3. Click Import.

   The first page of the Import Voice Gateways wizard opens.
4. (*Optional*) Select a custom domain for the IP Domain field. This field is available only when you define IP domains in CA Performance Center.
5. Click Browse, and navigate to the .csv file that contains your gateway definitions.
6. Click Next.

   UC Monitor analyzes the file and reports any syntax errors.
7. Correct any errors in the file and save it. Then repeat steps 5 and 6.

   When no errors are found, the import operation is finished. A confirmation page opens. The appropriate database objects are created.
8. Click OK.

   The Voice Gateway List displays the new gateways.

Why Add Other Media Devices?

A unified communications deployment can include many different devices, from various vendors, to support voice and video calls, conferencing, and voice mail. UC Monitor discovers these devices when calls pass through them. You can also manually add devices to the Other Devices category.

The Other Devices category includes the following types of devices:

- Microsoft mediation servers, edge servers, conferencing servers, and unified messaging servers.

  UC Monitor monitors the performance of the call legs that Microsoft devices handle. Both VoIP and video call performance metrics from these call legs are included in the media device views in UC Monitor performance reports. SNMP is not used to contact these servers, therefore:

  - Baseline traceroute data is not available.
  - The servers are not included in performance threshold configuration.

- Devices that do not contribute to call performance reporting, such as unsupported types of voice gateways. You can manually add these devices so that they are included in a device inventory, for example.
- Devices that you want to monitor individually, although they are part of a larger group. For example: You configure a Location that includes the servers that support your high-end video conferencing system, such as Cisco TelePresence or Polycom PVX.

  However, a defined Location provides granularity only to the subnet level in reports. Reports correlate calls to a Location and subnet, but not to the individual servers in that subnet. If you define the video conferencing devices as Other Devices, UC Monitor reports can easily associate video conference calls to their respective devices.

Add Other Media Devices

Take the following steps to add other media devices to the UC Monitor database.

Follow these steps:

1. Click Administration, Data Collection, Media Devices, Other Devices in the navigation bar.

   The Other Device List opens.

2. Click New.

   The Other Device Properties page opens.

3. Complete the following fields:

   - **Name**. A name for the media device. Typically, the DNS host name, although you can enter any name. If you do not know the host name, enter the IP address in the Address field and click DNS.
   - **Address**. Type the IP address of the media device. Use dotted notation, such as 10.10.2.34. If you do not know the IP address, enter the server DNS host name in the Name field and click IP.
   - **IP Domain**. The IP domain that is associated with this device. The IP domain is created in CA Performance Center. This field is available only when UC Monitor is registered to a CA Performance Center instance where at least one IP domain is defined.
   - **Description**. (*Optional*) A description to help identify this device, such as its location, capabilities, or past performance.
   - **Type**. The type of media device, such as IP phone, IP PBX, unified messaging server, mediation server, or session border controller (SBC).

     Use the Type field for identification purposes. For example, you want to create an inventory of servers, including servers that do not contribute to call performance reporting, such as Unified Messaging Servers. These servers are classified as Voice Gateway (Unsupported).

     Note: Some devices play multiple roles. After UC Monitor is registered to CA Performance Center, devices are assigned generic types, such as server or router. If this value is inaccurate for a discovered device, you can edit the device to select another type. Or you can select Unspecified, an option that causes the collector to rediscover the device from monitored call traffic and reassign it a type.
   - **Monitoring Status**. Whether data from this device is included in reports. The following options are available:
     - Enabled: Monitoring is enabled for calls that are routed by this device.
     - Disabled: Calls that are routed by this device are not monitored. Data from the calls is discarded.
     - Enabled (Sending Only): Monitoring is enabled only for calls that are sent from the PSTN through this device to phones in monitored Locations.

4. Save the device:

   - Save. The Other Device List reflects your changes.
   - Save & Add Another to save these properties and add another device.

   Data from the new devices is now included in UC Monitor reports.