PureConnect®

2023 R3

Generated:

09-November-2023

Content last updated:

29-April-2020

See Change Log for summary of changes.

GENESYS™

CIC and SNMP

Technical Reference

Abstract

This document contains information regarding the implementation, configuration, and usage of Simple Network Management Protocol (SNMP) in a Customer Interaction Center environment.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/pureconnect.

Table of Contents

SNMP overview

Simple Network Management Protocol (SNMP) is a standard for monitoring network systems, such as servers, switches, routers, and other network-based devices without requiring physical interaction with the device.

SNMP requires a network management system (NMS) to receive alerts (traps) and to request status messages from the network devices. Using SNMP, you can monitor multiple network devices and react quickly to conditions, problems, or outages with those devices. There are many commercial and open-source NMS products available.

SNMP standards

PureConnect products and the PureConnect SNMP service support SNMPv2c and SNMPv3. The PureConnect SNMP service also supports SNMP agents that use the SNMPv1, SNMPv2, and SNMPv3 standards.

SNMP components

Simple Network Management Protocol (SNMP) requires the following components:

- Host device with a network connection and one or more Management Information Base (MIB) files
- SNMP agent service on host device
- Network
- Network Management System (NMS)
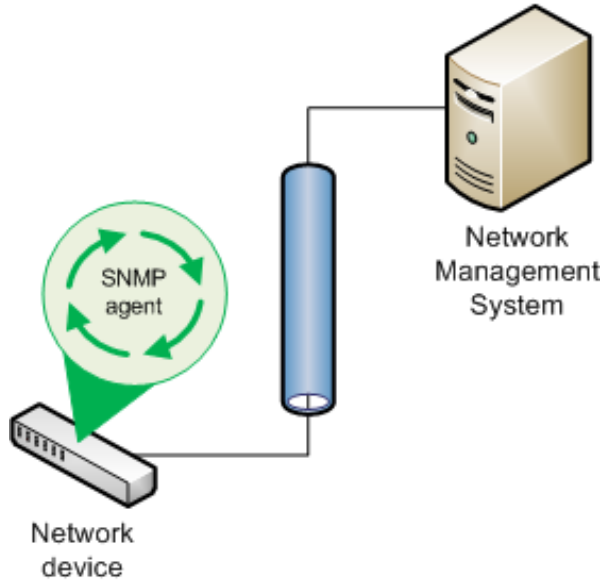
SNMP messages

There are two types of Simplified Network Messaging Protocol (SNMP) messages: requests and traps.
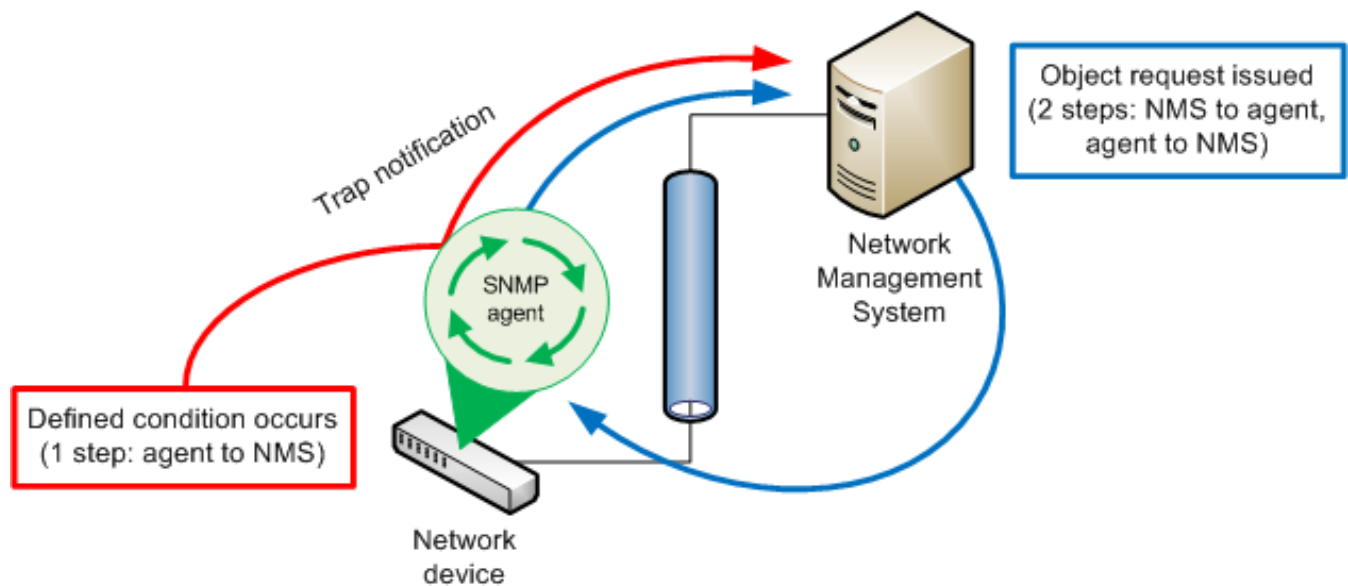
SNMP requests are issued from a Network Management System (NMS) to an SNMP agent service on a host network device. The request can be a query for status of a particular object, as defined in a Management Information Base (MIB) file, of the host network device. A request can also be a command to set a variable, such as a specific value for an object defined in a MIB file. When the request is received, the SNMP agent responds with a message to the NMS that sent the request.

SNMP traps are unsolicited messages from the network device to the NMS. When a monitored condition on the network device reaches a specific value, as defined in a MIB file on the host device, the SNMP agent sends the trap to the NMS.

SNMP network details

The following table provides specific details regarding Simple Network Management Protocol (SNMP) network communications:

Transport layer protocols	The SNMPv2c and SNMPv3 standards support the following network transport layer protocols: • UDP • TLS
Network port numbers	The SNMPv2c and SNMPv3 standards use the following default network port numbers for the specified transport layer protocols: UDP • 161 - SNMP requests • 162 - SNMP traps TLS • 10161 - SNMP requests • 10162 - SNMP traps

Note:
The PureConnect SNMP service (ININ SNMP) does not support TLS.

SNMP Protocol Data Units

The Simple Network Management Protocol v2c (SNMPv2c) and v3 (SNMPv3) standards use protocol data units (PDUs) to contain messages between Network Management Systems (NMSs) and SNMP agents. The following table lists each available message type in the standard and a description.

Message	Description
GetRequest	An NMS sends a GetRequest message to an SNMP agent to request data from one or more variables on the target network device. The SNMP agent returns a Response message with the current data of the requested variables.
SetRequest	An NMS sends a SetRequest message to an SNMP agent to set values for one or more variables on the target network device. The SNMP agent returns a Response message with the current data of the requested variables for validation.
GetNextRequest	An NMS sends a GetNextRequest message to an SNMP agent to query for the next defined variable on the target network device. The SNMP agent returns a Response message with the next defined variable and its current value.
GetBulkRequest	An NMS sends a GetBulkRequest message to an SNMP agent to request data from multiple variables on the target network device. The SNMP agent returns a Response message with the current data of the requested variables. This optimized variation of the GetNextRequest message was introduced in SNMPv2.
Response	An SNMP agent sends a Response message to an NMS after being prompted by a request message from that NMS. The Response message normally contains variable bindings or errors
Trap	An SNMP agent sends an unsolicited Trap message to an NSM when an object defined in the MIB file on a host network device meets or exceeds a specific value.
InformRequest	The InformRequest message can be sent by either SNMP agents or NMSs. Since SNMP typically uses the UDP transport layer protocol, which does not use receipt confirmation messages, the InformRequest message was created to provide receipt confirmation, especially for Trap messages.

SNMP glossary

Simple Network Management Protocol (SNMP) uses specific terms and phrases to describe different aspects in the monitoring of network devices. The following table contains some of these items and the associated definitions:

Agent

> A software service that resides and runs on a network device. This service monitors objects defined through one or more Management Information Base (MIB) files on the host system. The SNMP agent can send unsolicited trap messages to one or more Network Management Systems (NMSs) and respond to SNMP request messages with host device information.

Authentication protocol

> A method of validating SNMPv3 messages.

Community

> A string of characters that represents a group of SNMP-enabled network devices. Only Network Management Systems (NMSs) and SNMP agents that use the same SNMP community name can communicate with each other. Most SNMP agents support multiple community names, which allow the SNMP agents to receive SNMP requests from multiple NMSs.

> The SNMPv1 and SNMPv2c standards support SNMP communities as a method of authorization.

> SNMPv3 uses User-based Security Model (USM) for authentication and encryption. USM uses *user* and *password* for authentication, not a community name. While a community name is not required, supplying one allows communication with systems that use the earlier versions of SNMP.

Destination

> The address of a Network Management System (NMS). The format of the address, such as IP address or fully-qualified domain name (FQDN), is dependent on the application in which you configure the destination.

> An SNMP agent can send traps to one or more destinations.

Management Information Base (MIB)

> A text file, in a specific format, that defines the information available in the host network device.

> The format for MIB files is defined by Structure of Management Information, version 2 (SMIv2), which is included in RFC 2578.

> Genesys has registered its own, unique SNMP MIB object:

> interintelli(2793)

> Objects in MIB files that are created by PureConnect are listed under the following object ID (OID):

> .1.3.6.1.4.1.2793

> Objects in MIB files from other sources use different OIDs. For example, MIBs such as `aus.mib`, `HOST-RESOURCES-MIB.mib`, and `lmmib2.mib`, which are common on host servers, are not created by Genesys and the objects contained within are not members under the .1.3.6.1.4.1.2793 OID.

Manager

> See *Network Management System*.

Network device

> A piece of computerized equipment that is connected to a network.

> Examples of network devices that commonly use SNMP are servers, routers, switches, IP telephones, VoIP gateways, and printers.

Network Management System (NMS)

> Also known as an SNMP manager, a network management system communicates with network devices through the SNMP protocol. An NMS can request status information for one or more variables defined in a MIB located on the network device. An NMS also receives unsolicited *traps* that are also defined in a MIB from SNMP network devices.

Object Identifier (OID)

> Standard: section 3.1 in RFC1155. Every object in a MIB file is assigned an OID. It is through OIDs that SNMP agents and Network Management Systems (NMSs) communicate variable bindings, such as the current amount of free hard drive

space.

Privacy protocol

A method of encrypting and decrypting SNMPv3 messages.

Protocol Data Units (PDU)

The format of an SNMP message. SNMP PDUs contain the following information:
- IP header
- UDP header
- version
- community
- PDU-type
- request-id
- error-status
- error-index
- variable bindings

For information about the messages that can be sent or received through SNMP, see SNMP messages.

Request

A message that a Network Management System (NMS) sends to an SNMP agent. This message requests that the SNMP agent send status information about a specific variable to the NMS.

Traps

Unsolicted messages that an SNMP agent sends to a Network Management System (NMS) as specified in a destination address.

SNMP agents send trap messages when variables, as defined in Management Information Base (MIB) files on the network devices, meet a specific criterion, such as a lack of free hard drive space.

User

The identifier used in conjunction with a password to authenticate SNMPv3 messages.

Variable bindings

An object and one or more values as defined in a Management Information Base (MIB) file.

Each object has a unique object identifier (OID). Within an object, a MIB file can contain one or more values. The pairing of an object and the value is a variable binding.

For example, a MIB file may define an object for free storage space and includes the values of 20%, 10%, and 5%. The SNMP agent on the host network device sends a trap message when the free storage space of the network device reaches each of those defined thresholds.

Variable bindings do not apply only to trap messages. Some MIB files enable a Network Management System (NMS) to set values for an object through variable bindings as well.

Variables

One or more values assigned to an object in a Management Information Base (MIB) file.

Walk

A term that describes the process of a Network Management System (NMS) submitting a succession of `GetNext` SNMP requests to an SNMP agent on a network device. Usually, the succession of requests continues until the end of defined objects in a Management Information Base (MIB) file on the host network device.

Some operating systems contain an `snmpwalk` command that you can use to request data from an SNMP agent on a network device. Most NMS products also provide this functionality.

SNMP and Customer Interaction Center

Customer Interaction Center and its subsystem products use SNMPv2c, SNMPv3, and proprietary protocols for real-time management and reporting of resources on host network devices, such as servers.

Mechanism	Type	Areas of responsibility
Simple Network Management Protocol (SNMP)	Real-time	Hardware: • Status of components in a networked device • Capacities • Configured thresholds • Current utilization
Notifier/Remoco	Real-time	Hardware, software, and contact center interactions: • Errors • Warnings • Information • Status • Current utilization Some Customer Interaction Center subsystem products, such as Interaction Media Server and Interaction Dialer, send errors and events to the Windows Event Log on the Customer Interaction Center server through the Notifier protocol.
Windows Event Log	Historical	Hardware and software Errors and problems encountered by the Windows operating system and other installed software. Some Customer Interaction Center subsystem products, such as Interaction Media Server, send errors and events to the Windows Event Log on the Customer Interaction Center server through the Notifier protocol.
Product-specific log files	Historical	Various errors, problems, and events recorded by software to one or more files on the host device. For some Customer Interaction Center subsystem products, the amount of data

Customer Interaction Center products that support SNMP

Product	Supported SNMP services
Customer Interaction Center server	PureConnect SNMP (through Remoco)
Interaction Media Server	PureConnect SNMP
Interaction SIP Proxy	PureConnect SNMP
Session Manager	PureConnect SNMP
Interaction Recorder	PureConnect SNMP

SNMP requirements for Customer Interaction Center products

- Ensure that Microsoft Windows **SNMP Service** is installed but disabled.
- Using the **Services** control panel, ensure that the following services are set correctly:

- The **ININ SNMP** service is set to start automatically.
- The Microsoft Windows **SNMP Service** is disabled.

- Ensure that all firewalls and network nodes between the host network device and the Network Management System (NMS) allow communications through the necessary protocols and ports. By default, the SNMP ports are UDP 161 and UDP 162.

For more information on the protocols and ports used for SNMP, see SNMP network details.

- Ensure that Domain Name Service (DNS) servers are properly configured so that communications between SNMP entities, such as agents and NMSs, reach the intended targets through fully-quality domain names (FQDN).
- Ensure that the SNMP entities, such as agents and NMSs, are configured to communicate within the same sub-network (subnet).

PureConnect SNMP service

Genesys has developed an SNMP service (ININ SNMP) that provides more control and capabilities with SNMP. For CIC products that include the ININ SNMP service, the installation disables the Windows SNMP service (**SNMP Service** in **Control Panel > Services**). Upon startup, the ININ SNMP service reads all configuration settings for the Windows SNMP service, including accepted communities, registered MIB extension agents, and trap destinations, and binds to the default SNMP port 161.

> **Important!**
> Do not enable the Windows SNMP service while ININ SNMP is enabled as it will create a conflict for port 161.

Leaving the Windows SNMP service installed but disabled also provides the following benefits for ININ SNMP:
- Enables new registrations of any MIB extension agents
- Enables editing of configuration settings through the Microsoft Windows **SNMP Service Properties** dialog box

Functionality of the PureConnect SNMP service

The ININ SNMP service functions as a master agent or agent registry. For CIC and its subsystems, the ININ SNMP service is the default SNMP service. It disables the Windows SNMP Service during installation or an update and binds to UDP port 161, which is the default SNMP port. The ININ SNMP service receives all SNMP requests and pass subrequests to any SNMP subagents that have registered with it (or Windows SNMP Service, previously).

All CIC products that use SNMP register as subagents with the ININ SNMP service and provide variable bindings to their included Management Information Base (MIB) files, such as those installed with the CIC server, Interaction Media Server, and Interaction SIP Proxy.

> **Note:**
> The Windows **SNMP Trap** service listens for trap messages from remote network entitites on UDP port 162. The **SNMP Trap** service is not associated with any SNMP activities that originate on the host computer. The ININ SNMP service is not dependent on or connected to the **SNMP Trap** service in any way.

Customer Interaction Center products that use the PureConnect SNMP service

The PureConnect SNMP agent service is installed with the following Customer Interaction Center (CIC) products:
- Customer Interaction Center server
- Interaction Media Server
- Interaction SIP Proxy
- Session Manager
- Interaction Recorder

Supported SNMP features

- Agent mode for all SNMP versions
- Manager mode for all SNMP versions
- User-based Security Model (USM) (RFC 3414), except for the HMAC-MD5-96 authentication protocol
- SNMPv3 user management through command line utility

Unsupported SNMP features

- View-based Access Control Model (VACM) ([RFC 3415](#))
- SNMP-FRAMEWORK-MIB defintions ([RFC 3411, section 5](#))
- usmUserTable of the SNMP-USER-BASED-SM-MIB ([RFC 3414, section 5](#))
- Transport Security Model (TSM) ([RFC 5591](#))
- Extended Security Options ([ESO](#))
- Discovery ([RFC 5343](#))
- SNMPv3 authentication protocols:

- HMAC-MD5-96
- HMAC-SHA-2

- The snmpSetSerialNo object in the SNMP MIB defined in [RFC 3418](#).
- SNMP MUX protocol and MIB ([RFC 1227](#))
- Agent Extensibility Protocol (AgentX) ([RFC 2741](#))
- SNMP over TCP ([RFC 3430](#))
- SNMP proxying ([RFC 2273](#), [RFC 2573](#), [RFC 3413](#))
- API for Manager or Agent mode for issuing and receiving responses for InformRequest style messages.

Configure SNMP for CIC products and subsystems

> **Note:** If you purchased a packaged server from Genesys, The ININ SNMP service is already installed.

This section contains the following topics:

- Configure PureConnect SNMP service through the command line utility
- Configure ININ SNMP v2c settings through SNMP Service Properties dialog box
- Install MIB files on Customer Interaction Center
- Configure SNMP in Customer Interaction Center products
- Customer Interaction Center server parameters for SNMP
- Customer Interaction Center handlers for SNMP, Notifier, or Remoco

Configure PureConnect SNMP service through the command line utility

Important!

You can configure SNMPv3 settings only through the PureConnect SNMP command line utility. For SNMPv2c settings, you can use either the PureConnect SNMP command line utilty or the **SNMP Service Properties** dialog box.

1. On the Windows server hosting a CIC product and the PureConnect SNMP service, open a command prompt window as **administrator**.
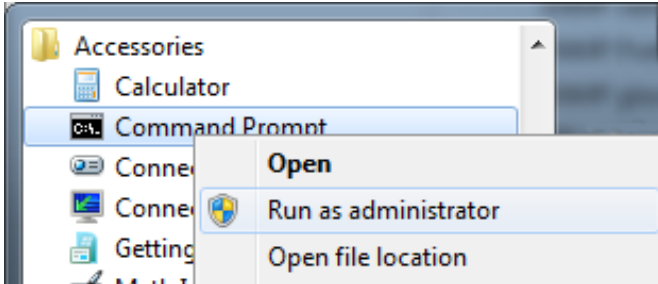
2. Use the `cd` command in the command prompt window to navigate to the `ININ SNMP` subdirectory:

CIC product	Default PureConnect SNMP service directory
Interaction Media Server	`C:\Program Files (x86)\PureConnect\ININ SNMP`
Interaction SIP Proxy	`C:\Program Files (x86)\PureConnect\ININ SNMP`
CIC server	`D:\I3\IC\ININ SNMP\`

Examples:
```
cd "C:\Program Files (x86)\PureConnect\ININ SNMP"
cd "D:\I3\IC\ININ SNMP"
```

3. Enter the following command and press the `Enter` key:
```
ininsnmpconfig-w32r.exe
```
The command prompt window displays the following output and changes the prompt to `ININ SNMP>`.

```
ININ SNMP Configuration
Connecting to ININ SNMP...Connected
ININ SNMP>
```

The `ININ SNMP>` prompt indicates that the PureConnect SNMP service is in configuration mode.

> **Tip:**
> You can enter `h` or `?` at the `ININ SNMP>` prompt and then press the `Enter` key to see a list of commands.

4. At the `ININ SNMP>` command prompt, configure the PureConnect SNMP service by entering the following command with the specified switches and necessary parameter values, and pressing the `Enter` key.
```
ININ SNMP>setup --posture param1 --authmethod param2 --authpassword param3 --engineid param4
```

`posture` **values**

      param1 **represents a secure configuration level**

        `min`

Configures outgoing messages to conform to SNMPv2c

Accepts incoming messages conforming to SNMPv1 (Not secure for incoming message but able to provide security for traps)

Deletes any previously defined SNMPv3 users for the PureConnect SNMP service

Creates a user identifier of `initial` with no privacy method or password (security level: `authNoPriv`)

Sets the `snmpEngineID` to the specified value

Sets `agent.defaultTraUsername` to `initial`

Example:

```
--posture min
```

semi

Configures outgoing messages to conform to SNMPv3

Accepts incoming messages that conform to SNMPv3

Deletes all previously-defined users

Creates a user identity of `initial` with the specified authentication method and password, and the specified privacy method and password (security level: `authPriv`)

Sets the `snmpEngineID` to the specified value

Sets `agent.defaultTrapUsername` to `initial`

Example:

```
--posture semi
```

very

Configures outgoing messages to conform to SNMPv3

Accepts incoming messages that conform to SNMPv3

Deletes all previously-defined users

Sets the snmpEngineID to the specified value

> **Note:**
> The very value does not create the user, initial. The PureConnect SNMP service will not accept any SNMP requests until you define and user and password.

Example:

```
--posture very
```

`authmethod` **values**

param2 represents the user authentication method that the PureConnect SNMP service users for each SNMP message.

No user authentication is done by the PureConnect SNMP service.

Example:

```
--authmethod none
```

sha

The PureConnect SNMP service users the HMAC-SHA-96 (SHA) protocol to create a message digest with an algorithm. The authentication keys used by the service are generated locally with the Engine ID and the password of the defined SNMPv3 user.

Example:

```
--authmethod sha
```

`authpassword` **values**

param3 represents a password that you enter for the defined SNMPv3 user. The PureConnect SNMP service uses this password for user authentication of SNMP messages.

Example:

```
--authpassword mypassword
```

`engineid` **values**

param4 represents three components in a colon-separated string:

○ A number specifying an identifying method (IP address, MAC address, character string)

○ The Internet Assigned Numbers Authority (IANA)-assigned organization identifier

2793 is the IANA private enterprise identifer for "Interactive Intelligence", which was acquired by Genesys.

- A value conforming to the specified method

IPv4 address

`1:`*`IANA org number:`*`4 octets`

Example:

`--engineid 1:2793:192.168.10.45`

IPv6 address

`2:`*`IANA org number:`*`16 octets`

Example:

`--engineid 2:2793:2001:db8:3c4d:15::1a2f:1a2b`

MAC address

`3:`*`IANA org number:`*`MAC address`

Example:

`--engineid 3:2793:782bcb8d6987`

Text

`4:`*`IANA org number:`*`text` (27 character maximum)

Example:

`--engineid 4:2793:thisisatest`

Octets

`5:`*`IANA org number:`*`octets` (27 character maximum)

Example:

`--engineid 5:2793:38a63b9d76df893a`

After you press the `Enter` key, the command prompt window displays the following messages:

```
Setting up ININ SNMP...
Completed, ININ SNMP setup.
```

5. At the `ININ SNMP>` command prompt, add an SNMP user by entering the following command with the specified switches and necessary parameter values, and then pressing the `Enter` key:

`ININ SNMP>au -u`*`param1`* `-a` *`param2`* `--authpassword` *`param3`* `-p` *`param4`* `--privpassword` *`param5`*

`u` **(username) values**

param1 represents the name of an SNMP user to add to the PureConnect SNMP service for SNMPv3 authentication.

Example:

`-u johnsmith`

`a` **(authmethod) values**

param2 represents the user authentication method that the PureConnect SNMP service users for each SNMP message for this user.

`none`

No user authentication is done by the PureConnect SNMP service.

`sha`

The PureConnect SNMP service uses the HMAC-SHA-96 (SHA) protocol to create a message digest with an algorithm. The authentication keys used by the service are generated locally with the Engine ID and the password of the defined SNMPv3 user.

Example:

`-a sha`

`authpassword` **values**

param3 represents a password that you enter for the defined SNMPv3 user. The PureConnect SNMP service users this password for user authentication of SNMP messages.

Example:

`--authpassword mypassword`

`p` (privmethod) values

> *param4* represents the privacy protocol that the PureConnect SNMP service uses for this SNMP user.

> none
>> No privacy protocol is used.
>>
>> Example:
>>
>> `-p none`

> des
>> The PureConnect SNMP service uses the CBC-DES Symmetric Encryption Protocol for this SNMP user.
>>
>> Example:
>>
>> `-p des`

> aes128
>> The PureConnect SNMP service uses the Advanced Encryption Standard (AES) Cipher Algorithm for this SNMP user.
>>
>> Example:
>>
>> `-p aes128`

`privpassword` values

> *param5* represents the password that the PureConnect SNMP service uses to generate keys with the specified privacy protocol for this SNMP user.

> **Note:**
> If you specify the privacy method (`-p`) as `none`, the `--privpassword` parameter is not required.

> Example:
>
> `--privpassword mypassword`

After you press the `Enter` key, the command prompt window displays the following messages:

```
Adding user "username"...
Completed, user added.
```

> **Tip:**
> To see a list of all users while using the PureConnect SNMP configuration tool, enter `lu` and then press the `Enter` key.

6. At the `ININ SNMP>` prompt, add a trap destination by entering the following command with the specified switches and necessary parameter values, and pressing the `Enter` key:

   `ININ SNMP> atd --community param1 --uri param2`

`community` values

> *param1* represens a name that you define as an SNMP community identifier for SNMPv2c communications. This name is not used with SNMPv3 messages or authentication.
>
> Supply a community name so that the PureConnect SNMP service can exchange message with multiple Network Management System (NMS) instances that support the range of SNMPv1, SNMPv2c, SNMPv3.
>
> Example:
>
> `--community myexamplecommunity`

`uri` values

> *param2* represents a Uniform Resource Identifier (URI) destination, which is used for SNMP messages.

> **Note:**
> You can specify more separate destination URIs for differing protocols. For exaple, you can set the default URI as `localhost` and the SNMPv3 destination as `username@myhost.com`.

> **Tip:**
> Using the `uri` switch, you can specify additional information in the value, such as the SNMP user name and the network port to use.

> default
>> This value configures the PureConnect SNMP service to send all SNMP messages to the specified URI of an NMS.

If you use multiple SNMP agents that use differing versions (v1, v2c, v3), setting this value to the URI of an NMS that is capable of processing messages from all versions provides the simplest configuration.

Examples:

```
--uri default://mynms.example.com
--uri default://192.168.1.100
```

> **Note:**
> If you do not use the `default` value, the trap destination is not saved so that it appears in the Windows **SNMP Service** dialog box. The **PureConnect SNMP** service will save and use trap destinations that use values other than default but they are not displayed in the Widnows **SNMP Service** dialog box.

`snmp`

At this time, this value is equivalent to using the `default` value in that it sends messages for all SNMP versions to the specified URI of an NMS.

Examples:

```
--uri snmp://mynms.example.com
--uri snmp://192.168.1.100
```

`snmpv1`

This value configures the PureConnect SNMP service to send all SNMPv1 messages are sent to the specified URI of an NMS.

Examples:

```
--uri snmpv1://mynms1.example.com
--uri snmpv2://192.168.1.102
```

`snmpv2`

This value configures the PureConnect SNMP service to send all SNMPv2c messages are sent to the specified URI of an NMS.

Examples:

```
--uri snmpv2://mynms.example.com
--uri snmpv2://192.168.1.102
```

`snmpv3`

This value configures the PureConnect SNMP service to send all SNMPv3 messages are sent to the specified URI of an NMS.

You can specify an SNMP user and network port number as part of the URI in the following format:

`snmpuser@uri:port`

Examples:

```
--uri snmpv3://testuser@mynms3.example.com:8161
--uri snmpv3://192.168.1.103
```

> **Note:**
> You can add multiple trap destination URIs for each protocol version. For example, you can specify one SNMPv2c trap destination and five or more SNMPv3 trap destinations. To see a list of all defined trap destinations while using the PureConnect SNMP configuration tool, enter `ltd` at the `ININ SNMP>` prompt, and then press the `Enter` key.

7. At the `ININ SNMP>` prompt, set a default user to associate with SNMPv3 traps by entering the following command and then pressing the `Enter` key:

`ININ SNMP>sdtu --username param1`

param1 represents an SNMP user that you have already added with the `au -u username` command in the PureConnect SNMP configuration tool.

After you press the `Enter` key, the command prompt window displays the following messages:

```
Setting the default trap user to "username"...
Completed, default trap user changed.
```

8. At the `ININ SNMP>` prompt, add an accepted host for which the PureConnect SNMP service will receive and process SNMP messages by entering the following command with the specified switch and then pressing the `Enter` key:

`ININ SNMP>aah --host param1`

param1 represents the fully-qualified domain name (FQDN) or IP address of a host from which the PureConnect SNMP service will receive and process SNMP messages.

> **Tip:**
> You can add multiple hosts through a single `aah` command by adding multiple `--host` *param* switches.
> Example:
> `aah --host 192.168.1.90 --host 192.168.1.91`

After pressing the `Enter` key, the command prompt window displays the following messages:

```
Adding the accept host(s)...
Completed, host(s) added.
```

> **Tip:**
> You can list all defined accepted hosts by entering the `lah` command at the `ININ SNMP>` prompt and then pressing the `Enter` key.

9. If you need to set a minimum SNMP version that is acceptable to the PureConnect SNMP service, enter the following command with the specified switches and parameters and then press the `Enter` key:

> **Note:**
> This command is required only if you previously set the `setup --posture` command to a value of `min`. For the `semi` and `very` values, the PureConnect SNMP service automatically sets the accepted and outgoing SNMP version to 3.

`ININ SNMP>smv --snmpversion` *param1*

param1 represents a single digit that corresponds to an SNMP version as defined in the following table:

1	SNMPv1
2	SNMPv2c
3	SNMPv3

The PureConnect SNMP service will accept SNMP messages for the specific version and any later version, if one exists.

After you press the `Enter` key, the command prompt window display the following messages:

```
Setting the default accepted SNMP version to version-n (n)
Completed, default accepted SNMP version changed.
```

10. If you need to set a minimum SNMP version that the PureConnect SNMP service is allowed to send, enter the following command with the specified switches and parameters and then press the `Enter` key:

> **Note:**
> This command is required only if you set the `setup --posture` command to a value of `min`. For the `semi` and `very` values, the ININ SNMP service automatically sets the accepted and outgoing SNMP version to 3.

`ININ SNMP>sdv --snmpversion` *param1*

param1 represents a single digit that corresponds to an SNMP version as defined in the following table:

1	SNMPv1
2	SNMPv2c
3	SNMPv3

The PureConnect SNMP service will send SNMP that conform to the specific version and any later version, if one exists.

After you press the `Enter` key, the command prompt window displays the following messages:

```
Setting the default outgoing SNMP version to version-n (n)...
Completed, default outgoing SNMP version changed.
```

11. To check the status of the SNMP configuration, enter `s` at the `ININ SNMP>` prompt and then press the `Enter` key.

The command prompt window displays the following messages and the associated values (examples shown):

```
Getting ININ SNMP status...
Configured SNMP port: 161
In use SNMP port: 161
SNMP Port bind status: Both IPv4 and IPv6 ports successfully bound
In packets: 523
Out packets: 957
Minimum accepted SNMP version: version-3 (3)
Default outgoing SNMP version: version-3 (3)
Default trap username: myexampleuser
```

12. To exit the `ininsnmpconfig` utility, enter `x` at the `ININ SNMP>` prompt and then press the `Enter` key.

> **Note:**
> Ensure the Windows Firewall allows ports 161 and 162 for SNMP and traps to the Network Management Servers that you specified as trap destinations.

Configure ININ SNMP v2c settings through SNMP Service Properties dialog box

You can configure the SNMPv1 and SNMPv2c settings of the ININ SNMP service through the interfaces of the CIC products that install the service. Additionally, you can use the dialog box for the disabled Windows **SNMP Service**.

> **Important!**
> Microsoft Windows **SNMP Service** does not support SNMPv3. As such, you cannot configure SNMPv3 users, passwords, or authentication methods through the **SNMP Service Properties** dialog box. To configure users and authentication for SNMPv3, the ININ SNMP service includes the `ininsnmpconfig-w32r.exe` command line utility. For more information, see [Configure ININ SNMP service through the command line utility](#).

> **Note:**
> If the Windows **SNMP Service** is not installed, Genesys recommends that you add this feature but ensure that it is disabled.

1. At the Windows host machine, log on with an administrative account.
2. Select **Start > Run**.
3. Enter `services.msc` and select **OK**.
4. In the **Services** window, double-click the **SNMP Service** entry.
5. On the **General** tab of the **SNMP Service Properties (Local Computer)** dialog box, set the **Startup type** box to **Automatic**.
6. Select the **Agent** tab.
7. In the **Contact** box, enter the name of the Customer Interaction Center administrator account.
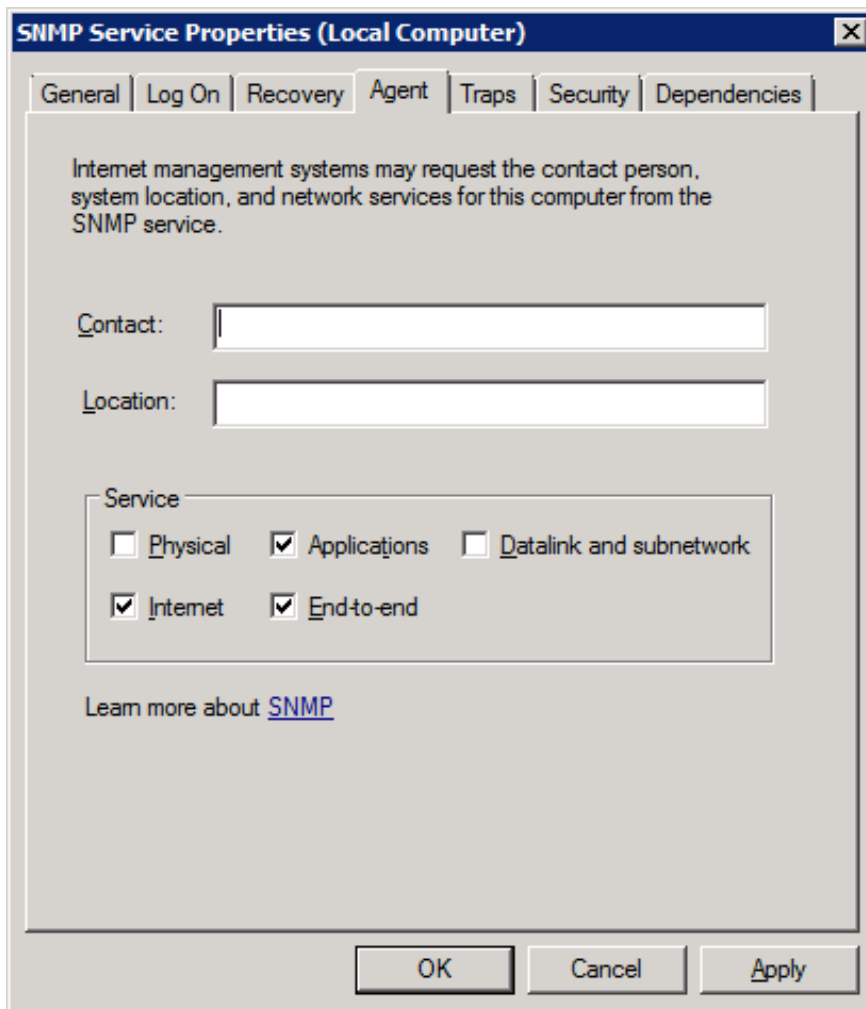
8. In the **Services** section, enable the following check boxes:
   - **Applications**
   - **Internet**
   - **End-to-end**
9. Select the **Traps** tab.

SNMP Service Properties (Local Computer)

General | Log On | Recovery | Agent | Traps | Security | Dependencies

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name

[   ] ▼   Add to list

Remove from list

Trap destinations:

[   ]

Add...   Edit...   Remove

Learn more about SNMP

OK   Cancel   Apply

10. In the **Community name** box, enter the name of an SNMP community in which this server will participate and then select the **Add to list** button.

11. Below the **Trap destinations** box, select the **Add** button.

12. In the **Host name, IP or IPX address** box of the **SNMP Service Configuration** dialog box, enter the address of the Network Management System (NMS) that will receive SNMP traps from this server.

SNMP Service Configuration

Add

Cancel

Host name, IP or IPX address:

[   ]
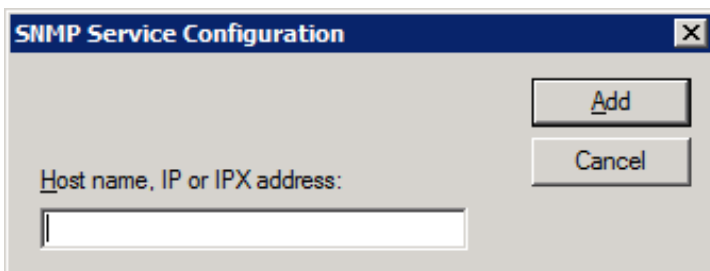
You can use a host name, fully-qualified domain name, or IP address to specify the destination server.

13. In the **SNMP Service Configuration** dialog box, select the **Add** button.

14. In the **SNMP Service Properties (Local Computer)** dialog box, select the **Security** tab.
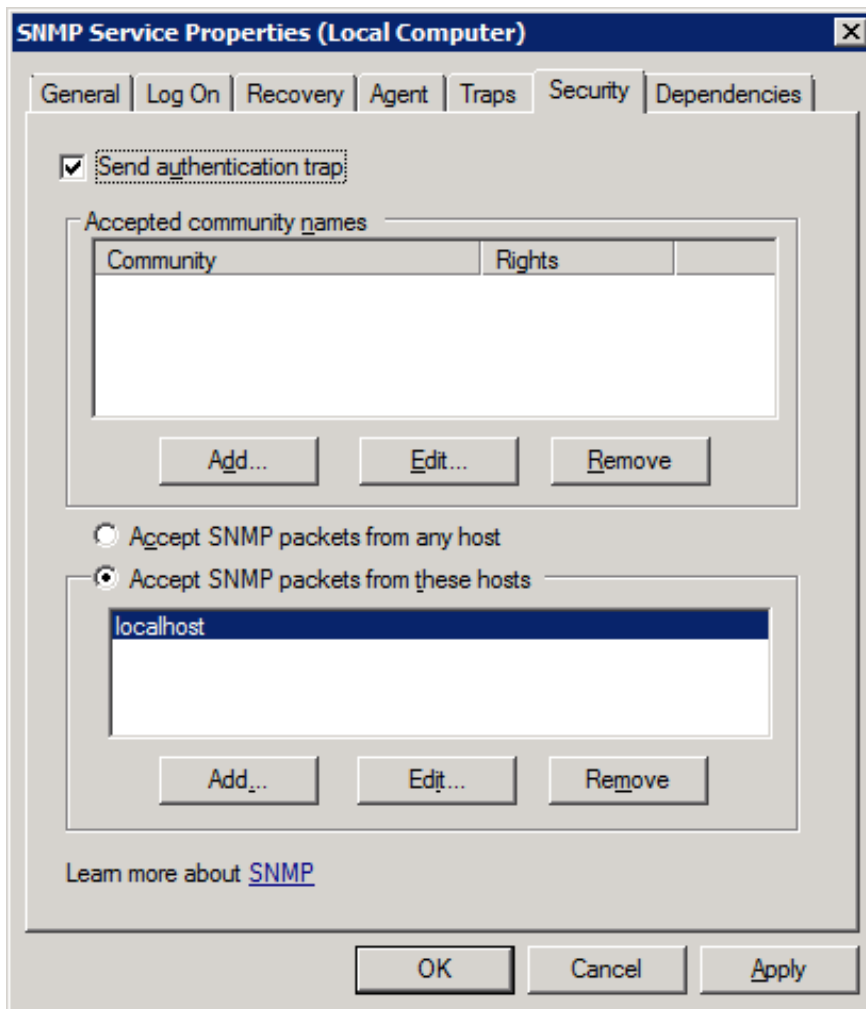
15. Ensure that the **Send authentication trap check box** is enabled.

16. In the **Accepted community names** group box, select the **Add** button.

17. In the **Community rights** box of the **SNMP Service Configuration** dialog box, select the rights that the community will have for SNMP objects on this server.
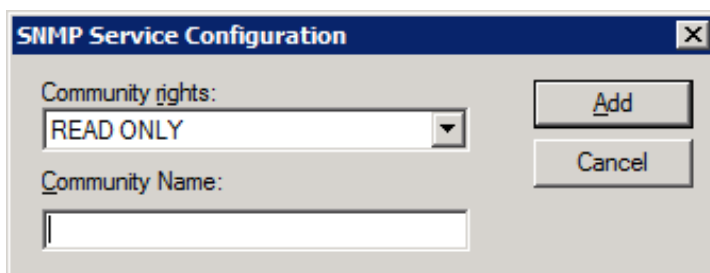
NONE

> The host system will not process any SNMP requests from the specified community.

NOTIFY

> The host system will send SNMP traps to the specified community.

READ ONLY

> The host system will send SNMP traps and fulfill SNMP object data GET requests from systems in the specified community.

READ WRITE

> The host system will send SNMP traps, fulfill SNMP object data GET requests, and process SET requests on existing SNMP objects from systems in the specified community.

READ CREATE

> The host system will send SNMP traps, fulfill SNMP object data GET requests, process SET requests on existing SNMP objects, and fulfill creation requests for new entries in SNMP tables from systems in the specified community.

18. In the **Community Name** box, enter the name of the SNMP community to have the specified rights.

> **Caution!**
> Do not use **Public** as an SNMP community name as it is the default community name for many SNMP products. Because of the security concerns with SNMPv2c, you should protect your SNMP community names as though they were passwords.

19. Select the **Add** button.

    To add more communities and rights, repeat steps 16 through 19.

20. In the **SNMP Service Properties (Local Computer)** dialog box, select the the appropriate option for receiving SNMP packets.

21. If you choose to limit which systems can send SNMP packets to this host, those systems must still be members of an allowed SNMP community.

> **Important!**
> Genesys recommends that you specify which systems can send SNMP messages to this host server by using the **Accept SNMP packets from these hosts** option and specifying the necessary addresses through the **Add** button.

22. Select the **OK** button.

Install MIB files on Customer Interaction Center

1. If you have not done so already:
   a. Download the CIC `.iso` file from the PureConnect product information site at the following URL address:
      https://help.genesys.com/pureconnect/secure/Downloads.aspx
   b. Copy the `.iso` file to a non-Customer Interaction Center file server with a high bandwidth connection to the machines on which you will install CIC products.
   c. Mount the `.iso` file and share the contents to make them accessible to the machines on which you will install CIC products.
2. Navigate to the `\Additional Files\SNMP` directory of the mounted `.iso` image.
3. Copy the `i3ic.mib` and `i3icrecorder.mib` files to the `\I3\IC\Server` directory on the Customer Interaction Center server.

Configure SNMP in Customer Interaction Center products

To configure SNMPv2c settings for a specific Customer Interaction Center product, see the documentation listed for that product.

Customer Interaction Center product	Product documentation
Customer Interaction Center server	*CIC and SNMP Technical Reference*
Interaction Media Server	*Interaction Media Server Technical Reference*
Interaction SIP Proxy	*Interaction SIP Proxy Technical Reference* *Interaction SIP Proxy Help*
Session Manager	Session Manager has no direct user interface and is configured through Interaction Administrator, which connects the SNMP features with the CIC Remoco subsystem (IC System Manager) for reporting information and traps. You can edit the `i3icsessionmanager.mib` and `i3icstatalertserver.mib` files to change thresholds and other MIB object values.
Interaction Recorder	For SNMP, Interaction Recorder has no direct user interface and is configured through Interaction Administrator, which connects the SNMP features with the CIC Remoco subsystem (IC System Manager) for reporting information and traps. Statistics about recordings gathered through SNMP are displayed in Interaction Supervisor. You can edit `i3icrecorder.mib` to change thresholds and other MIB object values.

> **Important!**
>
> To use the SNMPv3 features of the PureConnect SNMP service, you configure the users and encryption settings through the ININ SNMP configuration command line utility in a command prompt window with administrator privileges. For more information on the ININ SNMP configuration command line utility, see Configure ININ SNMP service through the command line utility.

Customer Interaction Center server parameters for SNMP

The Customer Interaction Center server supports the following server parameters:

Server parameter	Values	Description
`Allow SNMP Process Restarts`	• 0 (default) • 1	This server parameter enables stopping and restarting Customer Interaction Center server processes through SNMP `SETRequest` messages. Set this server parameter to `1` to enable this functionality.
`SNMPTrapEnterprise`	• All • I3 • ININ (default) • None	This server parameter, set by default on packaged servers, enables the Customer Interaction Center server to send SNMP trap messages to handlers, which can be customized. The value indicates which SNMP trap messages to send to handlers.

For information on how to set server parameters, see *Interaction Administrator Help*.

Customer Interaction Center handlers for SNMP, Notifier, or Remoco

The following initiators and tools in Customer Interaction Center handlers support SNMP, Notifier, or Remoco:

- Receive Log Events initiator
- Receive Trap initiator
- Get Process Information tool
- Merge Log Event Messages tool
- Merge Log Event ID and Insertion Strings tool
- Restart IC Subsystem tool
- Stop IC Subsystem tool

For more information on these initiators and tools, see *Interaction Designer Help*.

Customer Interaction Center Management Information Base files

Several Customer Interaction Center products use Simple Network Management Protocol (SNMP) to provide information about a host server and its software to a Network Management System (NMS).

This section contains the following topics about base files:

- General
- Customer Interaction Center
- Interaction Recorder
- Interaction Media Server
- Interaction SIP Proxy
- Session Manager
- StatAlert Server

General

The MIB files in this section apply to multiple Customer Interaction Center products.

- HOST-RESOURCES-MIB.mib
- hrSystem objects
- hrStorage objects
- hrDevice objects
- hrSWRun objects
- hrSWRunPerf objects
- hrSWInstalled objects

HOST-RESOURCES-MIB.mib

The following Customer Interaction Center products use the `HOST-RESOURCES-MIB.mib` file:

- Interaction Media Server
- Interaction SIP Proxy

The `HOST-RESOURCES-MIB.mib` file contains the following SNMP object types:

SNMP object type	Description
hrSystem	This object contains information about running time, date, parameters, users, and processes on the host system. See hrSystem objects.
hrStorage	This object contains information on available memory space and local storage space on the host system. See hrStorage objects.
hrDevice	This object contains information on hardware installed on the host system. See hrDevice objects.
hrSWRun	This object contains information on software processes that are running on the host system. See hrSWRun objects.
hrSWRunPerf	This object contains information on the CPU and memory impacts of software processes that are running on the host system. See hrSWRunPerf objects.
hrSWInstalled	This object contains information on the versions of software installed on the host system. See hrSWInstalled objects.

hrSystem objects

hrSystemUptime

Type	Access	Description
TimeTicks	read-only	The amount of time since this host was last initialized. Note that this is different from sysUpTime in MIB-II [3] because sysUpTime is the uptime of the network management portion of the system.

hrSystemDate

Type	Access	Description
DateAndTime	read-write	The host's notion of the local date and time of day.

hrSystemInitialLoadDevice

Type	Access	Description
Integer	read-write	The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.

hrSystemInitialLoadParameters

Type	Access	Description
InternationalDisplayString	read-write	This object contains the parameters (e.g. a pathname and parameter) supplied to the load device when requesting the initial operating system configuration from that device.

hrSystemNumUsers

Type	Access	Description
Gauge	read-only	The number of user sessions for which this host is storing state information. A session is a collection of processes requiring a single act of user authentication and possibly subject to collective job control.

hrSystemProcesses

Type	Access	Description
Gauge	read-only	The number of process contexts currently loaded or running on this system.

hrSystemMaxProcesses

Type	Access	Description
Integer	read-only	The maximum number of process contexts this system can support. If there is no fixed maximum, the value should be zero. On systems that have a fixed maximum, this object can help diagnose failures that occur when this maximum is reached.

hrStorage objects

hrMemorySize

Type	Access	Description
KBytes	read-only	The amount of physical main memory contained by the host.

hrStorageTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of logical storage areas on the host. An entry shall be placed in the storage table for each logical area of storage that is allocated and has fixed resource limits. The amount of storage represented in an entity is the amount actually usable by the requesting entity, and excludes loss due to formatting or file system reference information. These entries are associated with logical storage areas, as might be seen by an application, rather than physical storage entities which are typically seen by an operating system. Storage such as tapes and floppies without file systems on them are typically not allocated in chunks by the operating system to requesting applications, and therefore shouldn't appear in this table. Examples of valid storage for this table include disk partitions, file systems, ram (for some architectures this is further segmented into regular memory, extended memory, and so on), backing store for virtual memory (`swap space').  This table is intended to be a useful diagnostic for `out of memory' and `out of buffers' types of failures. In addition, it can be a useful performance monitoring tool for tracking memory, disk, or buffer usage.

hrStorageEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one logical storage area on the host. As an example, an instance of the hrStorageType object might be named hrStorageType.3 Each entry contains data for the following objects: hrStorageIndex hrStorageType hrStorageDescr hrStorageAllocationUnits hrStorageSize hrStorageUsed hrStorageAllocationFailures

hrStorageIndex

Type	Access	Description
Integer	read-only	A unique value for each logical storage area contained by the host.

hrStorageType

Type	Access	Description
Object Identifier	read-only	The type of storage represented by this entry.

hrStorageDescr

Type	Access	Description
DisplayString	read-only	A description of the type and instance of the storage described by this entry.

hrStorageAllocationUnits

Type	Access	Description
Integer	read-only	The size, in bytes, of the data objects allocated from this pool. If this entry is monitoring sectors, blocks, buffers, or packets, for example, this number will commonly be greater than one. Otherwise this number will typically be one.

hrStorageSize

Type	Access	Description
Integer	read-write	The size of the storage represented by this entry, in units of hrStorageAllocationUnits.

hrStorageUsed

Type	Access	Description
Integer	read-only	The amount of the storage represented by this entry that is allocated, in units of hrStorageAllocationUnits.

hrStorageAllocationFailures

Type	Access	Description
Counter	read-only	The number of requests for storage represented by this entry that could not be honored due to not enough storage. It should be noted that as this object has a SYNTAX of Counter, that it does not have a defined initial value. However, it is recommended that this object be initialized to zero.

hrDevice objects

hrDeviceTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of devices contained by the host.

hrDeviceEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one device contained by the host. As an example, an instance of the hrDeviceType object might be named hrDeviceType.3 Each entry contains data for the following objects: hrDeviceIndex hrDeviceType hrDeviceDescr hrDeviceID hrDeviceStatus hrDeviceErrors

hrDeviceIndex

Type	Access	Description
Integer	read-only	A unique value for each device contained by the host. The value for each device must remain constant at least from one re-initialization of the agent to the next re-initialization.

hrDeviceType

Type	Access	Description
Object Identifier	read-only	An indication of the type of device. If this value is `hrDeviceProcessor { hrDeviceTypes 3 }' then an entry exists in the hrProcessorTable which corresponds to this device.  If this value is `hrDeviceNetwork { hrDeviceTypes 4 }', then an entry exists in the hrNetworkTable which corresponds to this device. If this value is `hrDevicePrinter { hrDeviceTypes 5 }', then an entry exists in the hrPrinterTable which corresponds to this device.  If this value is `hrDeviceDiskStorage { hrDeviceTypes 6 }', then an entry exists in the hrDiskStorageTable which corresponds to this device.

hrDeviceDescr

Type	Access	Description
DisplayString	read-only	A textual description of this device, including the device's manufacturer and revision, and optionally, its serial number.

hrDeviceID

Type	Access	Description
ProductID	read-only	The product ID for this device.

hrDeviceStatus

Type	Access	Description
Integer	read-only	The current operational state of the device described by this row of the table. A value unknown(1) indicates that the current state of the device is unknown. running(2) indicates that the device is up and running and that no unusual error conditions are known. The warning(3) state indicates that agent has been informed of an unusual error condition by the operational software (e.g., a disk device driver) but that the device is still 'operational'. An example would be a high number of soft errors on a disk. A value of testing(4), indicates that the device is not available for use because it is in the testing state. The state of down(5) is used only when the agent has been informed that the device is not available for any use. This object supports the following values: 1 = unknown 2 = running 3 = warning 4 = testing 5 = down

hrDeviceErrors

Type	Access	Description
Counter	read-only	The number of errors detected on this device. It should be noted that as this object has a SYNTAX of Counter, that it does not have a defined initial value. However, it is recommended that this object be initialized to zero.

hrProcessorTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of processors contained by the host. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the hrDeviceType object is `hrDeviceProcessor'.

hrProcessorEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one processor contained by the host. The hrDeviceIndex in the index represents the entry in the hrDeviceTable that corresponds to the hrProcessorEntry. As an example of how objects in this table are named, an instance of the hrProcessorFrwID object might be named hrProcessorFrwID.3 Each entry contains data for the following objects: hrProcessorFrwID hrProcessorLoad

hrProcessorFrwID

Type	Access	Description
ProductID	read-only	The product ID of the firmware associated with the processor.

hrProcessorLoad

Type	Access	Description
Integer	read-only	The average, over the last minute, of the percentage of time that this processor was not idle. Implementations may approximate this one minute smoothing period if necessary.

hrNetworkTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of network devices contained by the host. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the hrDeviceType object is `hrDeviceNetwork'.

hrNetworkEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one network device contained by the host. The hrDeviceIndex in the index represents the entry in the hrDeviceTable that corresponds to the hrNetworkEntry. As an example of how objects in this table are named, an instance of the hrNetworkIfIndex object might be named hrNetworkIfIndex.3. Each entry contains data for the following objects: hrNetworkIfIndex

hrNetworkIfIndex

Type	Access	Description
Integer	read-only	The value of ifIndex which corresponds to this network device.

hrPrinterTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of printers local to the host. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the hrDeviceType object is `hrDevicePrinter'. Each entry contains data for the following objects: HrPrinterEntry

hrPrinterEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one printer local to the host. The hrDeviceIndex in the index represents the entry in the hrDeviceTable that corresponds to the hrPrinterEntry. As an example of how objects in this table are named, an instance of the hrPrinterStatus object might be named hrPrinterStatus.3 Each entry contains data for the following objects: hrPrinterStatus hrPrinterDetectedErrorState

hrPrinterStatus

Type	Access	Description
Integer	read-only	The current status of this printer device. This object supports the following values: 1 = other 2 = unknown 3 = idle 4 = printing 5 = warmup

hrPrinterDetectedErrorState

Type	Access	Description
Octet String	read-only	This object represents any error conditions detected by the printer. The error conditions are encoded as bits in an octet string, with the following definitions: | Condition	Bit	hrDeviceStatus
lowPaper	0	warning(3)
noPaper	1	down(5)
lowToner	2	warning(3)
noToner	3	down(5)
doorOpen	4	down(5)
jammed	5	down(5)
offline	6	down(5)
serviceRequested	7	warning(3) | If multiple conditions are currently detected and the hrDeviceStatus would not otherwise be unknown(1) or testing(4), the hrDeviceStatus shall correspond to the worst state of those indicated, where down(5) is worse than warning(3) which is worse than running(2). Bits are numbered starting with the most significant bit of the first byte being bit 0, the least significant bit of the first byte being bit 7, the most significant bit of the second byte being bit 8, and so on. A one bit encodes that the condition was detected, while a zero bit encodes that the condition was not detected. This object is useful for alerting an operator to specific warning or error conditions that may occur, especially those requiring human intervention.

hrDiskStorageTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of long-term storage devices contained by the host. In particular, disk devices accessed remotely over a network are not included here. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the hrDeviceType object is `hrDeviceDiskStorage'.

hrDiskStorageEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one long-term storage device contained by the host. The hrDeviceIndex in the index represents the entry in the hrDeviceTable that corresponds to the hrDiskStorageEntry. As an example, an instance of the hrDiskStorageCapacity object might be named hrDiskStorageCapacity.3 Each entry contains data for the following objects: hrDiskStorageAccess hrDiskStorageMedia hrDiskStorageRemoveble hrDiskStorageCapacity

hrDiskStorageAccess

Type	Access	Description
Integer	read-only	An indication if this long-term storage device is readable and writable or only readable. This should reflect the media type, any write-protect mechanism, and any device configuration that affects the entire device. This object supports the following values: 1 = readWrite 2 = readOnly

hrDiskStorageMedia

Type	Access	Description
Integer	read-only	An indication of the type of media used in this long-term storage device. This object supports the following values: 1 = other 2 = unknown 3 = hardDisk 4 = floppyDisk 5 = opticalDiskROM 6 = opticalDiskWORM 7 = opticalDiskRW 8 = ramDisk

hrDiskStorageRemoveble

Type	Access	Description
Boolean	read-only	Denotes whether or not the disk media may be removed from the drive. This object supports the following values: 1 = true 2 = false

hrDiskStorageCapacity

Type	Access	Description
KBytes	read-only	The total size for this long-term storage device.

hrPartitionTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of partitions for long-term storage devices contained by the host. In particular, partitions accessed remotely over a network are not included here.

hrPartitionEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one partition. The hrDeviceIndex in the index represents the entry in the hrDeviceTable that corresponds to the hrPartitionEntry. As an example of how objects in this table are named, an instance of the hrPartitionSize object might be named hrPartitionSize.3.1 Each entry contains data for the following objects: hrPartitionIndex hrPartitionLabel hrPartitionID hrPartitionSize hrPartitionFSIndex

hrPartitionIndex

Type	Access	Description
Integer	read-only	A unique value for each partition on this long-term storage device. The value for each long-term storage device must remain constant at least from one re-initialization of the agent to the next re-initialization.

hrPartitionLabel

Type	Access	Description
InternationalDisplayString	read-only	A textual description of this partition.

hrPartitionID

Type	Access	Description
Octet String	read-only	A descriptor which uniquely represents this partition to the responsible operating system. On some systems, this might take on a binary representation.

hrPartitionSize

Type	Access	Description
KBytes	read-only	The size of this partition.

hrPartitionFSIndex

Type	Access	Description
Integer	read-only	The index of the file system mounted on this partition. If no file system is mounted on this partition, then this value shall be zero. Note that multiple partitions may point to one file system, denoting that that file system resides on those partitions. Multiple file systems may not reside on one partition.

hrFSTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of file systems local to this host or remotely mounted from a file server. File systems that are in only one user's environment on a multi-user system will not be included in this table.

hrFSEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one file system local to this host or remotely mounted from a file server. File systems that are in only one user's environment on a multi-user system will not be included in this table. As an example of how objects in this table are named, an instance of the hrFSMountPoint object might be named hrFSMountPoint.3 Each entry contains data for the following objects: hrFSIndex hrFSMountPoint hrFSRemoteMountPoint hrFSType hrFSAccess hrFSBootable hrFSStorageIndex hrFSLastFullBackupDate hrFSLastPartialBackupDate

hrFSIndex

Type	Access	Description
Integer	read-only	A unique value for each file system local to this host. The value for each file system must remain constant at least from one re-initialization of the agent to the next re-initialization.

hrFSMountPoint

Type	Access	Description
InternationalDisplayString	read-only	The path name of the root of this file system.

hrFSRemoteMountPoint

Type	Access	Description
InternationalDisplayString	read-only	A description of the name and/or address of the server that this file system is mounted from. This may also include parameters such as the mount point on the remote file system. If this is not a remote file system, this string should have a length of zero.

hrFSType

Type	Access	Description
Object Identifier	read-only	The value of this object identifies the type of this file system. This object supports the following values:

Value	File system type
1	hrFSOther
2	hrFSUnknown
3	hrFSBerkeleyFFS
4	hrFSSys5FS
5	hrFSFat
6	hrFSHPFS
7	hrFSHFS
8	hrFSMFS
9	hrFSNTFS
10	hrFSVNode
11	hrFSJournaled
12	hrFSiso9660
13	hrFSRockRidge
14	hrFSNFS
15	hrFSNetware
16	hrFSAFS
17	hrFSDFS
18	hrFSAppleshare
19	hrFSRFS
20	hrFSDGCFS
21	hrFSBFS

hrFSAccess

Type	Access	Description
Integer	read-only	An indication if this file system is logically configured by the operating system to be readable and writable or only readable. This does not represent any local access-control policy, except one that is applied to the file system as a whole. This object supports the following values: 1 = readWrite 2 = readOnly

hrFSBootable

Type	Access	Description
Boolean	read-only	A flag indicating whether this file system is bootable.

hrFSStorageIndex

Type	Access	Description
Integer	read-only	The index of the hrStorageEntry that represents information about this file system. If there is no such information available, then this value shall be zero. The relevant storage entry will be useful in tracking the percent usage of this file system and diagnosing errors that may occur when it runs out of space.

hrFSLastFullBackupDate

Type	Access	Description
DateAndTime	read-write	The last date at which this complete file system was copied to another storage device for backup. This information is useful for ensuring that backups are being performed regularly.
		If this information is not known, then this variable shall have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

hrFSLastPartialBackupDate

Type	Access	Description
DateAndTime	read-write	The last date at which a portion of this file system was copied to another storage device for backup. This information is useful for ensuring that backups are being performed regularly.
		If this information is not known, then this variable shall have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

hrSWRun objects

hrSWOSIndex

Type	Access	Description
Integer32	read-only	The value of the hrSWRunIndex for the hrSWRunEntry that represents the primary operating system running on this host. This object is useful for quickly and uniquely identifying that primary operating system.

hrSWRunTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of software running on the host.

hrSWRunEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for one piece of software running on the host Note that because the installed software table only contains information for software stored locally on this host, not every piece of running software will be found in the installed software table. This is true of software that was loaded and run from a non-local source, such as a network-mounted file system.
		As an example of how objects in this table are named, an instance of the hrSWRunName object might be named hrSWRunName.1287
		Each entry contains data for the following objects:
		hrSWRunIndex
		hrSWRunName
		hrSWRunID
		hrSWRunPath
		hrSWRunParameters
		hrSWRunType
		hrSWRunStatus

hrSWRunIndex

Type	Access	Description
Integer32	read-only	A unique value for each piece of software running on the host. Wherever possible, this should be the system's native, unique identification number.

hrSWRunName

Type	Access	Description
InternationalDisplayString	read-only	A textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software was installed locally, this should be the same string as used in the corresponding hrSWInstalledName.

hrSWRunID

Type	Access	Description
ProductID	read-only	The product ID of this running piece of software.

hrSWRunPath

Type	Access	Description
InternationalDisplayString	read-only	A description of the location on long-term storage (e.g. a disk drive) from which this software was loaded.

hrSWRunParameters

Type	Access	Description
InternationalDisplayString	read-only	A description of the parameters supplied to this software when it was initially loaded.

hrSWRunType

Type	Access	Description
Integer	read-only	The type of this software.
		This object supports the following values:
		1 = unknown
		2 = operatingSystem
		3 = deviceDriver
		4 = application

hrSWRunStatus

Type	Access	Description
Integer	read-write	The status of this running piece of software. Setting this value to invalid(4) shall cause this software to stop running and to be unloaded. Sets to other values are not valid.
		This object supports the following values:
		1 = running
		2 = runnable
		3 = notRunnable
		4 = invalid

hrSWRunPerf objects

hrSWRunPerfTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of running software performance metrics.

hrSWRunPerfEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry containing software performance metrics. As an example, an instance of the hrSWRunPerfCPU object might be named hrSWRunPerfCPU.1287
		Each entry contains data for the following objects:
		hrSWRunPerfCPU
		hrSWRunPerfMem

hrSWRunPerfCPU

Type	Access	Description
Integer32	read-only	The number of centi-seconds of the total system's CPU resources consumed by this process. Note that on a multi-processor system, this value may increment by more than one centi-second in one centi-second of real (wall clock) time.

hrSWRunPerfMem

Type	Access	Description
KBytes	read-only	The total amount of real system memory allocated to this process.

hrSWInstalled objects

hrSWInstalledLastChange

Type	Access	Description
TimeTicks	read-only	The value of sysUpTime when an entry in the hrSWInstalledTable was last added, renamed, or deleted. Because this table is likely to contain many entries, polling of this object allows a management station to determine when re-downloading of the table might be useful.

hrSWInstalledLastUpdateTime

Type	Access	Description
TimeTicks	read-only	The value of sysUpTime when the hrSWInstalledTable was last completely updated. Because caching of this data will be a popular implementation strategy, retrieval of this object allows a management station to obtain a guarantee that no data in this table is older than the indicated time.

hrSWInstalledTable

Type	Access	Description
N/A	not-accessible	The (conceptual) table of software installed on this host.

hrSWInstalledEntry

Type	Access	Description
N/A	not-accessible	A (conceptual) entry for a piece of software installed on this host. As an example of how objects in this table are named, an instance of the hrSWInstalledName object might be named hrSWInstalledName.96 Each entry contains data for the following objects: hrSWInstalledIndex hrSWInstalledName hrSWInstalledID hrSWInstalledType hrSWInstalledDate

hrSWInstalledIndex

Type	Access	Description
Integer32	read-only	A unique value for each piece of software installed on the host. This value shall be in the range from 1 to the number of pieces of software installed on the host.

hrSWInstalledName

Type	Access	Description
InternationalDisplayString	read-only	A textual description of this installed piece of software, including the manufacturer, revision, the name by which it is commonly known, and optionally, its serial number.

hrSWInstalledID

Type	Access	Description
ProductID	read-only	The product ID of this installed piece of software.

hrSWInstalledType

Type	Access	Description
Integer	read-only	The type of this software. This object supports the following values: 1 = unknown 2 = operatingSystem 3 = deviceDriver 4 = application

hrSWInstalledDate

Type	Access	Description
DateAndTime	read-only	The last-modification date of this application as it would appear in a directory listing. If this information is not known, then this variable shall have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

Customer Interaction Center

Using Simple Network Management Protocol (SNMP) on a Customer Interaction Center server is optional. To use SNMP on a Customer Interaction Center server, you must install the Microsoft Windows SNMP service through the **Programs and Features** object in the **Control Panel**.

This section contains information about the following .mib files and SNMP object types:

- i3ic.mib
- i3IcGeneral objects
- i3IcInfo objects
- i3IcCommands objects
- i3IcTrapInfo objects
- i3IcTraps objects
- reporting_plugin.mib

i3ic.mib

The `i3ic.mib` file contains SNMP object definitions for a Customer Interaction Center server. By default, this file is located in the `D:\I3\IC\Server` directory.

The `i3ic.mib` file contains the following SNMP object types:

SNMP object type	Description
i3IcGeneral	These objects contain information about the Customer Interaction Center software. See i3IcGeneral objects.
i3IcInfo	These objects contain host system information such as CPU usage, memory usage, elapsed run time, and thread count. See i3IcInfo objects.
i3IcCommands	These objects are responsible for stopping and restarting various subsystems. See i3IcCommands objects.
i3IcTrapInfo	These objects contain the information that is displayed with trap messages. See i3IcTrapInfo objects.
i3IcTraps	These objects are the trap messages when a warning or error threshold has been met on the host system. These objects can contain one or more i3IcTrapInfo objects. See i3IcTraps objects.

i3IcGeneral objects

i3IcGenVersion

Type	Access	Description
DisplayString	read-only	This object displays the version of the Customer Interaction Center server software on the host network device.

i3IcGenBuild

Type	Access	Description
DisplayString	read-only	This object displays the build number that produced the Customer Interaction Center server software on the host network device.

i3IcGenTimeStarted

Type	Access	Description
DisplayString	read-only	This object displays the chronological time when the Customer Interaction Center server on the host network device was last started.

i3IcGenMibVersion

Type	Access	Description
DisplayString	read-only	This object displays the version of the `i3ic.mib` Management Information Base (MIB) file that is used by the Customer Interaction Center server on the host network device.

i3IcGenSwitchoverRole

Type	Access	Description
Integer	read-only	This object displays the switchover role for this CIC server: • 1 = NotApplicable because the Server is not in a Primary/Backup configuration. • 2 = Primary • 3 = Backup • 4 = Failed

i3IcGenSwitchoverBackupState

Type	Access	Description
Integer	read-only	This object displays the switchover backup state for this CIC server: • 1 = Not Applicable. Not in a Primary/Backup configuration • 2 = Not Ready. The backup server is either not active or is starting • 3 = Ready

i3IcGenSwitchoverSwitchMode

Type	Access	Description
Integer	read-only	This object displays the switchover mode for this CIC server pair: • 0 = Not Applicable. Not in a Primary/Backup configuration • 1 = Auto. Switchovers occur automatically between the two CIC servers. • 2 = Manual. Switchovers between the two CIC servers must be initiated manually.

i3IcGenSwitchoverReplicationMode

Type	Access	Description
Integer	read-only	This object displays the switchover replication mode for this CIC server pair: • 0 = Unknown • 1 = Normal • 2 = Upgrade

i3IcGenSwitchoverPeer

Type	Access	Description
DisplayString	read-only	This object displays the name of the peer machine in the switchover pair.

i3IcInfo objects

i3IcSubsysInfoTable

Type	Access	Description
N/A	not-accessible	This SNMP information object contains entries for various Customer Interaction Center subsystems.

i3IcSubsysInfoTableEntry

Type	Access	Description
N/A	not-accessible	This SNMP information object contains the following SNMP information objects for a Customer Interaction Center subsystem: Each entry contains data for the following objects: i3IcSubsysInfoIndex i3IcSubsysInfoCpuUsage i3IcSubsysInfoMemUsage i3IcSubsysInfoRuntime i3IcSubsysInfoThreadCount i3IcSubsysInfoAvailable i3IcSubsysInfoName

i3IcSubsysInfoIndex

Type	Access	Description
Integer	N/A	Each item represents a Customer Interaction Center subsystem. This object supports the following values: 1 = Notifier 2 = FileMonitor 3 = IonNotifier 4 = DSServer 5 = HttpPluginHost 6 = ClusterConnector 7 = Mail Account Monitor 8 = SwitchoverService 9 = Transaction Server 10 = AdminServer 11 = AccServer 12 = Compressor Manager 13 = DataManager 14 = DSSink 15 = HostServer 16 = IPDBServer 17 = Mrcp Subsystem 18 = Post Office 19 = Prompt Server 20 = Provision Server 21 = Reco Subsystem 22 = VXIHostServer 23 = Client Services 24 = Feedback Server 25 = Optimizer Server 26 = Recorder Server

27 = Resource Broker

28 = Tracker Server

29 = AcdServer

30 = OutOfProcCustomDLL

31 = QueueStatProvider

32 = Session Manager

33 = TsServer

34 = EMS Server

35 = FaxServer

36 = FileRouter

37 = IpServer

38 = RCCServer

39 = SMSServer

40 = StatAlertServer

41 = StatServer

42 = VPIM Receiver

43 = WebProcessor

44 = WebProcessorBridge

45 = IP

46 = Process Automation Server

47 = Set SIP NAT

48 = Thin IP Bridge

49 = DialerServer (Dialer)

50 = CampaignServer (Dialer)

51 = UpdateServer (Dialer)

52 = DialerStatRepeater (Dialer)

53 = DialerStatServer (Dialer)

54 = DialerTranServer (Dialer)

55 = DialerHistoryWriter (Dialer)

56 = DirectorServer(Director)

57 = MicServer (Communite)

58 = InteractionRecoveryService

59 = WebPortalServer

60 = ICSecureTokenServer

i3IcSubsysInfoCpuUsage

Type	Access	Description
Integer	read-only	The amount of central processing unit (CPU) resources currently in use by the Customer Interaction Center subsystem product.

i3IcSubsysInfoMemUsage

Type	Access	Description
Integer	read-only	The amount of random access memory (RAM) resources currently in use by the Customer Interaction Center subsystem product.

i3IcSubsysInfoRuntime

Type	Access	Description
DisplayString	read-only	The amount of time that has elapsed since the Customer Interaction Center subsystem product was last started.

i3IcSubsysInfoThreadCount

Type	Access	Description
Integer	read-only	The total number of CPU threads on the host network device of the Customer Interaction Center subsystem product.

i3IcSubsysInfoAvailable

Type	Access	Description
Integer	read-only	An integer value that indicates if the Customer Interaction Center subsystem product is available for use. This object supports the following values: 1 = available 2 = unavailable

i3IcCommands objects

i3IcSubsysCmdTable

Type	Access	Description
N/A	not-accessible	This SNMP control object contains status information from the designated system or commands to run on the designated system.

i3IcSubsysCmdTableEntry

Type	Access	Description
N/A	not-accessible	This SNMP control object contains the following SNMP control objects for a Customer Interaction Center subsystem: Each entry contains data for the following objects: i3IcSubsysCmdIndex i3IcSubsysCmdRestart i3IcSubsysCmdStop i3IcSubsysCmdFilterEvents

i3IcSubsysCmdIndex

Type	Access	Description
Integer	read-only	An integer that represents a PureConnect subsystem for which the SNMP command is issued.

This object supports the following values:

1 = Notifier

2 = FileMonitor

3 = IonNotifier

4 = DSServer

5 = HttpPluginHost

6 = ClusterConnector

7 = Mail Account Monitor

8 = SwitchoverService

9 = Transaction Server

10 = AdminServer

11 = AccServer

12 = Compressor Manager

13 = DataManager

14 = DSSink

15 = HostServer

16 = IPDBServer

17 = Mrcp Subsystem

18 = Post Office

19 = Prompt Server

20 = Provision Server

21 = Reco Subsystem

22 = VXIHostServer

23 = Client Services

24 = Feedback Server

25 = Optimizer Server

26 = Recorder Server

27 = Resource Broker

28 = Tracker Server

29 = AcdServer

30 = OutOfProcCustomDLL

31 = QueueStatProvider

32 = Session Manager

33 = TsServer

34 = EMS Server

35 = FaxServer

36 = FileRouter

37 = IpServer

38 = RCCServer

39 = SMSServer

40 = StatAlertServer

41 = StatServer

42 = VPIM Receiver

43 = WebProcessor	
44 = WebProcessorBridge	
45 = IP	
46 = Process Automation Server	
47 = Set SIP NAT	
48 = Thin IP Bridge	
49 = DialerServer (Dialer)	
50 = CampaignServer (Dialer)	
51 = UpdateServer (Dialer)	
52 = DialerStatRepeater (Dialer)	
53 = DialerStatServer (Dialer)	
54 = DialerTranServer (Dialer)	
55 = DialerHistoryWriter (Dialer)	
56 = DirectorServer(Director)	
57 = MicServer (Communite)	
58 = InteractionRecoveryService	
59 = WebPortalServer	
60 = ICSecureTokenServer	

i3IcSubsysCmdRestart

Type	Access	Description
Integer	read-write	An integer that represents the SNMP status or command for the PureConnect subsystem. This object supports the following values: 1 = running 2 = restart

i3IcSubsysCmdStop

Type	Access	Description
Integer	read-write	An integer that represents the SNMP status or command for the PureConnect subsystem. This object supports the following values: 1 = running 2 = stop

i3IcSubsysCmdFilterEvents

Type	Access	Description
Integer	read-write	An integer that represents which SNMP event messages that the SNMP agent sends for the PureConnect subsystem.
		The integers use a binary mask, which enables you to add two or more items for inclusion. For example, a value of 3 enables the SNMP events for 1 and 2 (1+2=3). A value of 7 enables the SNMP events for 1, 2, and 4 (1+2+4=7).
		This object supports the following values or their inclusion in a binary mask:
		0 = Don't send any event messages
		1 = Send Error level event messages
		2 = Send Warning level event messages
		4 = Send Information level event messages
		8 = Unable to get filter data

i3IcTrapInfo objects

i3IcTrapInfoSubsys

Type	Access	Description
Integer	N/A	This SNMP trap message indicates which Customer Interaction Center subsystem has restarted.
		This SNMP trap message supports the following values:
		1 = Notifier
		2 = FileMonitor
		3 = IonNotifier
		4 = DSServer
		5 = HttpPluginHost
		6 = ClusterConnector
		7 = Mail Account Monitor
		8 = SwitchoverService
		9 = Transaction Server
		10 = AdminServer
		11 = AccServer
		12 = Compressor Manager
		13 = DataManager
		14 = DSSink
		15 = HostServer
		16 = IPDBServer
		17 = Mrcp Subsystem
		18 = Post Office
		19 = Prompt Server
		20 = Provision Server
		21 = Reco Subsystem
		22 = VXIHostServer
		23 = Client Services
		24 = Feedback Server

25 = Optimizer Server

26 = Recorder Server

27 = Resource Broker

28 = Tracker Server

29 = AcdServer

30 = OutOfProcCustomDLL

31 = QueueStatProvider

32 = Session Manager

33 = TsServer

34 = EMS Server

35 = FaxServer

36 = FileRouter

37 = IpServer

38 = RCCServer

39 = SMSServer

40 = StatAlertServer

41 = StatServer

42 = VPIM Receiver

43 = WebProcessor

44 = WebProcessorBridge

45 = IP

46 = Process Automation Server

47 = Set SIP NAT

48 = Thin IP Bridge

49 = DialerServer (Dialer)

50 = CampaignServer (Dialer)

51 = UpdateServer (Dialer)

52 = DialerStatRepeater (Dialer)

53 = DialerStatServer (Dialer)

54 = DialerTranServer (Dialer)

55 = DialerHistoryWriter (Dialer)

56 = DirectorServer(Director)

57 = MicServer (Communite)

58 = InteractionRecoveryService

59 = WebPortalServer

60 = ICSecureTokenServer

i3IcTrapInfoRestartReason

Type	Access	Description
Integer	read-only	An integer that identifies the reason why Customer Interaction Center was restarted. This SNMP trap message supports the following values: 1 = maintenance 2 = unknown

i3IcTrapInfoEventLogSubsys

Type	Access	Description
DisplayString	read-only	A string that identifies the PureConnect subsystem that caused Customer Interaction Center to write an SNMP trap information message to the Windows Event Log of the Customer Interaction Center host server.

i3IcTrapInfoEventLogMsgID

Type	Access	Description
Integer	read-only	An integer that provides the numerical identifier of the Windows Event Log entry that was the Customer Interaction Center server wrote to the Windows Error Log for an SNMP trap information message on behalf of a Customer Interaction Center subsystem.

i3IcTrapInfoEventLogMsg

Type	Access	Description
DisplayString	read-only	The SNMP trap information message that was written to the Windows Event Log of the Customer Interaction Center server on behalf of a Customer Interaction Center subsystem.

i3IcTrapWarningEventLogSubsys

Type	Access	Description
DisplayString	read-only	A string that identifies the PureConnect subsystem that caused Customer Interaction Center to write an SNMP trap warning message to the Windows Event Log of the Customer Interaction Center host server.

i3IcTrapWarningEventLogMsgID

Type	Access	Description
Integer	read-only	An integer that provides the numerical identifier of the Windows Event Log entry that was the Customer Interaction Center server wrote to the Windows Error Log for an SNMP trap warning message on behalf of a Customer Interaction Center subsystem.

i3IcTrapWarningEventLogMsg

Type	Access	Description
DisplayString	read-only	The SNMP trap warning message that was written to the Windows Event Log of the Customer Interaction Center server on behalf of a Customer Interaction Center subsystem.

i3IcTrapErrorEventLogSubsys

Type	Access	Description
DisplayString	read-only	A string that identifies the PureConnect subsystem that caused Customer Interaction Center to write an SNMP trap error message to the Windows Event Log of the Customer Interaction Center host server.

i3IcTrapErrorEventLogMsgID

Type	Access	Description
Integer	read-only	An integer that provides the numerical identifier of the Windows Event Log entry that was the Customer Interaction Center server wrote to the Windows Error Log for an SNMP trap error message on behalf of a Customer Interaction Center subsystem.

i3IcTrapErrorEventLogMsg

Type	Access	Description
DisplayString	read-only	The SNMP trap error message that was written to the Windows Event Log of the Customer Interaction Center server on behalf of a Customer Interaction Center subsystem.

i3IcTrapYellowAlarmTSInterface

Type	Access	Description
DisplayString	read-only	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives a yellow PSTN alarm from the carrier.

i3IcTrapRedAlarmTSInterface

Type	Access	Description
DisplayString	read-only	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives a red PSTN alarm from the carrier.

i3IcTrapAlarmClearedTSInterface

Type	Access	Description
DisplayString	read-only	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives an alarm clearance message from the carrier.

i3IcTrapDChannelDownTSInterface

Type	Access	Description
DisplayString	read-only	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the interface that receives, from the carrier, an error message that the D-channel for a Time Division Multiplexer (TDM) span is not functional.

i3IcTrapVariableHostName

Type	Access	Description
DisplayString	read-only	This object displays the host name of this CIC server that is associated with a trap message.

i3IcTrapVariableSubsystemName

Type	Access	Description
DisplayString	read-only	This object displays the name of the subsystem on this CIC server for which a trap message pertains.

i3IcTrapVariablePluginName

Type	Access	Description
DisplayString	read-only	This object displays the optional name of the HttpPluginHost if it is associated with a trap message.

i3IcTrapVariableErrorDesc

Type	Access	Description
DisplayString	read-only	This object contains the condition or reason for which a trap message was generated.

i3IcTrapVariableHealthLevel

Type	Access	Description
Integer	read-only	This object indicates the health level of the subsystem on the CIC server that is associated with a trap message: • 0 = Recovered - The subsystem of the CIC server has resumed normal functionality • 3 = Warning - The subsystem of the CIC server is in a limited state of functionality as some problems are still present • 5 = Error - The subsystem of the CIC server is not functioning

i3IcTraps objects

i3IcTrapRestart

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that a Customer Interaction Center subsystem has restarted. This SNMP trap message contains the following objects: i3IcTrapInfoSubsys i3IcTrapInfoRestartReason

i3IcTrapInformationalEventLog

Type	Access	Description
N/A	N/A	This SNMP trap information message indicates that the Customer Interaction Center server has written an information entry in the Windows Event Log of the host server. **Important!** To use this trap on the CIC server (or both in a switchover pair) and the subsystems, you must set the following keys in the specified path to `1`: ``` HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432 \Node \Interactive Intelligence \EIC \Remoco \EIC Subsystems[subsystem_name] \Log Event Filter ``` **Error Log Event** **Info Log Event** **Warning Log Event** After modifying these Registry keys, you must restart the server for these changes to take effect. This SNMP trap message contains the following objects: i3IcTrapInfoEventLogSubsys i3IcTrapInfoEventLogMsgID i3IcTrapInfoEventLogMsg

i3IcTrapWarningEventLog

Type	Access	Description
N/A	N/A	This SNMP trap warning message indicates that the Customer Interaction Center server has written a warning entry in the Windows Event Log of the host server. **Important!** To use this trap on the CIC server (or both in a switchover pair) and the subsystems, you must set the following keys in the specified path to `1`: ``` HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432 \Node \Interactive Intelligence \EIC \Remoco \EIC Subsystems[subsystem_name] \Log Event Filter ``` **Error Log Event** **Info Log Event** **Warning Log Event** After modifying these Registry keys, you must restart the server for these changes to take effect. This SNMP trap message contains the following objects: i3IcTrapWarningEventLogSubsys i3IcTrapWarningEventLogMsgID i3IcTrapWarningEventLogMsg

i3IcTrapErrorEventLog

Type	Access	Description
N/A	N/A	This SNMP trap error message indicates that the Customer Interaction Center server has written an error entry in the Windows Event Log of the host server. **Important!** To use this trap on the CIC server (or both in a switchover pair) and the subsystems, you must set the following keys in the specified path to `1`: ```\nHKEY_LOCAL_MACHINE\n \SOFTWARE\n \Wow6432\n \Node\n \Interactive Intelligence\n \EIC\n \Remoco\n \EIC Subsystems[subsystem_name]\n \Log Event Filter\n``` **Error Log Event** **Info Log Event** **Warning Log Event** After modifying these Registry keys, you must restart the server for these changes to take effect. This SNMP trap message contains the following objects: i3IcTrapErrorEventLogSubsys i3IcTrapErrorEventLogMsgID i3IcTrapErrorEventLogMsg

i3IcCommenceSwitchoverEvent

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that a switchover from a primary Customer Interaction Center server to a backup Customer Interaction Center server has been initiated.

i3IcTSInterfaceYellowAlarm

Type	Access	Description
N/A	N/A	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives a yellow PSTN alarm from the carrier. This SNMP trap message contains the following object: i3IcTrapYellowAlarmTSInterface

i3IcTSInterfaceRedAlarm

Type	Access	Description
N/A	N/A	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives a red PSTN alarm from the carrier. This SNMP trap message contains the following object: i3IcTrapRedAlarmTSInterface

i3IcTSInterfaceAlarmCleared

Type	Access	Description
N/A	N/A	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the Time Division Multiplexer (TDM) interface that receives an alarm clearance message from the carrier. This SNMP trap message contains the following object: i3IcTrapAlarmClearedTSInterface

i3IcTSInterfaceDChannelDown

Type	Access	Description
N/A	N/A	For Customer Interaction Center subsystems that provide connectivity to the Public Switched Telephone Network (PSTN), this object provides the identifier of the interface that receives, from the carrier, an error message that the D-channel for a Time Division Multiplexer (TDM) span is not functional. This SNMP trap message contains the following object: i3IcTrapDChannelDownTSInterface

i3IcDiscontinueSwitchoverEvent

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that a switchover from a primary Customer Interaction Center server to a backup Customer Interaction Center server has been stopped before completion.

i3IcHighLatencyState

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that the Customer Interaction Center server is experiencing significant delays between network packets resulting in delayed interactions, such as receiving calls or chat messages, transferring calls, or placing a call on hold.

i3IcHighLatencyStateClear

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that the Customer Interaction Center server is no longer experiencing significant delays between network packets.

i3IcTracingStoppedInsufficientDiskSpace

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that the Customer Interaction Center is no longer monitoring system resources because the host server has insufficient free storage space to ensure continued core functionality.

i3IcTracingStoppedInsufficientDiskSpaceCleared

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that the Customer Interaction Center server has re-enabled the monitoring of system resources as the host server has adequate free storage space.

i3IcSubsystemInTroubleTrap

Type	Access	Description
N/A	N/A	This SNMP trap message indicates that a subsystem of the Customer Interaction Center server is not functioning optimally or has recovered from a trap.

reporting_plugin.mib

The reporting_plugin.mib enables you to monitor plugin status through your MIB browser.

reportingplugin objects

reportingpluginTotalReportingTunnelConnections

Type	Access	Description
Unsigned32	read-only	The number of open http tunnel connections against this instance of the Reporting Plugin. The number of this value is intended for use by Genesys personel and software.

reportingpluginLongestActiveConnection

Type	Access	Description
TimeTicks	read-only	The duration that the longest active reporting tunnel has been open. The number of this value is intended for use by Genesys personnel and software.

reportingpluginHighestDataTransferConnection

Type	Access	Description
Unsigned32	read-only	The amount of data in KB transferred over the most heavily used connection in the last 30 seconds. The number of this value is intended for use by Genesys personel and software.

reportingpluginTotalReportingTunnelErrorConnections

Type	Access	Description
Unsigned32	read-only	The number of open http tunnel connections against this instance of the Reporting Plugin that have reported an error status. The number of this value is intended for use by Genesys personel and software.

Interaction Recorder

This section contains information about the following .mib file and SNMP object types:

- i3icrecorder.mib
- i3RecGeneral
- i3RecContentServerInfo
- i3RecTrapVars objects
- I3RecTraps objects

i3icrecorder.mib

The `i3icrecorder.mib` file contains the following SNMP object types:

SNMP object type	Description
General objects	These objects contain version information of the CIC subsystem. See i3RecGeneral.
Interaction Recorder Remote Content Service information objects	These objects provide information on the configuration of Interaction Recorder Remote Content Service servers.See i3RecContentServerInfo.
Trap variables	These object provide the configurable settings as they relate to trap messages for Interaction Recorder Remote Content Service servers. See i3RecTrapVars objects.
Traps	These objects contain informational, error, or warning messages that occur for Interaction Recorder Remote Content Service servers. See I3RecTraps objects.

i3RecGeneral

i3RegGenFileVersion

Type	Access	Description
DisplayString	read-only	The file version information for Interaction Recorder.

i3RecContentServerInfo

i3RecContentServerInfoTable

Type	Access	Description
N/A	not-accessible	Table containing information about Interaction Recorder Remote Content Service servers.

i3RecContentServerInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3ContentServerInfoTable. Each entry is applicable for each Interaction Recorder Remote Content Service server.
		Each entry contains data for the following objects:
		i3RecContentServerId
		i3RecContentServerHostFqdn
		i3RecContentServerHostPort
		i3RecContentServerRegistered
		i3RecContentServerMemoryUsage
		i3RecContentServerCpuUsage
		i3RecContentServerLocalFreeSpace
		i3RecContentServerSharedFreeSpace
		i3RecContentServerConfiguredForS3
		i3RecContentServerAvailableHttpClientConnections
		i3RecContentServerSuccessfulRecordingsLastHour
		i3RecContentServerFailedRecordingsLastHour
		i3RecContentServerInfoTracingFreeSpace

i3RecContentServerId

Type	Access	Description
Unsigned32	read-only	The unique identifier for this Interaction Recorder Remote Content Service server, which Customer Interaction Center persists in the DS subsystem. The Interaction Recorder server identifier is always 0.

i3RecContentServerHostFqdn

Type	Access	Description
DisplayString	read-only	The Fully-Qualified Domain Name (FQDN) of this Interaction Recorder Remote Content Service server.

i3RecContentServerHostPort

Type	Access	Description
Integer	read-only	The port number used on this Interaction Recorder Remote Content Service server for moving files and communicating the other systems.
		For HTTPS operations, the port number is one value higher (+1).

i3RecContentServerRegistered

Type	Access	Description
TruthValue	read-only	This object indicates if the Interaction Recorder Remote Content Service server is connected and registered with a Customer Interaction Center. If this value is false, the values for other MIB objects for this server will not update.

i3RecContentServerMemoryUsage

Type	Access	Description
Gauge32	read-only	The amount of Random Access Memory (RAM) that this Interaction Recorder Remote Content Service server is using.

i3RecContentServerCpuUsage

Type	Access	Description
Gauge32	read-only	The percentage of CPU that this Interaction Recorder Remote Content Service server is using.

i3RecContentServerLocalFreeSpace

Type	Access	Description
Gauge32	read-only	The total amount, in gigabytes, of all free local storage space that is available to this Interaction Recorder Remote Content Service server.

i3RecContentServerSharedFreeSpace

Type	Access	Description
Gauge32	read-only	The total amount, in gigabytes, of all free shared storage lcoations that are available to this Interaction Recorder Remote Content Service server.

i3RecContentServerConfiguredForS3

Type	Access	Description
TruthValue	read-only	This value indicates if this Interaction Recorder Remote Content Service server is configured to access storage space through Amazon Simple Storage Service (Amazon S3).

i3RecContentServerAvailableHttpClientConnections

Type	Access	Description
Gauge32	read-only	The number of HTTP client connections that this Interaction Recorder Remote Content Service server supports before it rejects additional connections.

i3RecContentServerSuccessfulRecordingsLastHour

Type	Access	Description
Gauge32	read-only	The number of recordings that this Interaction Recorder Remote Content Service server successfully processed in the last 60 minutes.

i3RecContentServerFailedRecordingsLastHour

Type	Access	Description
Gauge32	read-only	The number of recordings that this Interaction Recorder Remote Content Service server failed to process in the last 60 minutes.

i3RecContentServerInfoTracingFreeSpace

Type	Access	Description
Gauge32	read-only	The amount of free storage space, in gigabytes, that is available to this Interaction Recorder Remote Content Service server for the purpose of storing trace logs.

i3RecContentServerStorageInfoTable

Type	Access	Description
N/A	not-accessible	Table containing information about all storage locations that are accessible by this indexed Interaction Recorder Remote Content Service server. This value is updated at every directory stat update interval.

i3RecContentServerStorageInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3RecContentServerStorageInfoTable. Each entry is applicable for each Interaction Recorder Remote Content Service server.
		Each entry contains data for the following objects:
		i3RecContentServerStorageId
		i3RecContentServerIndexFqdn
		i3RecContentServerStoragePath
		i3RecContentServerStorageFreeSpace

i3RecContentServerStorageId

Type	Access	Description
Unsigned32	read-only	The numeric identifier assigned to this Interaction Recorder Remote Content Service server's storage location.

i3RecContentServerIndexFqdn

Type	Access	Description
DisplayString	read-only	The Fully-Qualified Domain Name (FQDN) of this Interaction Recorder Remote Content Service server storage index entry.

i3RecContentServerStoragePath

Type	Access	Description
DisplayString	read-only	The path of the storage location for this Interaction Recorder Remote Content Service server.
		This object supports the specification of an Amazon Simple Storage Service (Amazon S3) location.

i3RecContentServerStorageFreeSpace

Type	Access	Description
Gauge32	read-only	The amount of free storage space for the location specified by the i3RecContentServerStoragePath object.
		Note: This object is not set if the i3RecContentServerStoragePath object is set to an Amazon S3 location.

i3RecTrapVars objects

i3RecSpecificTrapType

Type	Access	Description
Integer	accessible-for-notify	This variable object specifies the type of trap notification: • 1 - transferFailure • 2 - regionLowDiskSpace • 3 - sharedStorageNotAccessible

i3RecMediaSourcePath

Type	Access	Description
DisplayString	accessible-for-notify	This variable object specifuies the path of the media source that is associated with the i3RecTrapTransferFailure trap.

i3RecMediaDestinationPath

Type	Access	Description
DisplayString	accessible-for-notify	This variable object specifies the path of the media source that is associated with the i3RecTrapTransferFailure trap.

i3RecRegionName

Type	Access	Description
DisplayString	accessible-for-notify	This variable object specifies the region name that is associated with the i3RecRegionLowDiskSpace trap.

I3RecTraps objects

I3RecTrapsPrefix

Type	Access	Description
N/A	N/A	This object is a container for the following traps of the `i3icrecorder.mib` file.

i3RecTrapTransferFailure

Type	Access	Description
N/A	N/A	This trap is generated when an Interaction Recorder Remote Content Service server fails to transfer a file. To prevent SNMP message flooding, this trap provides subsequent failures to transfer a specific file once every 5 minutes. This trap includes the following objects: • i3RecContentServerId • i3RecMediaDestinationPath • i3RecMediaSourcePath

i3RecTrapRegionLowDiskSpace

Type	Access	Description
N/A	N/A	This trap is generated when the available storage space for all Interaction Recorder Remote Content Service servers in a configured region is less than 5 gigabytes. This trap is generated at each directory stat update interval until the problem is correct. This trap includes the following objects: • i3RecRegionName

i3RecTrapSharedStorageNotAccessible

Type	Access	Description
N/A	N/A	This trap is generated when a Interaction Recorder Remote Content Service servers cannot access a shared storage space. This trap is generated at each directory stat update interval until the problem is correct. This trap includes the following objects: • i3RecMediaDestinationPath

Interaction Media Server

This section contains information about the following .mib files and SNMP object types:
- INTERACTION-MEDIASERVER.mib
- i3MsGeneral objects
- i3MsInfo objects
- i3MsTraps objects
- HOST-RESOURCES-MIB.mib

INTERACTION-MEDIASERVER.mib

The `INTERACTION-MEDIASERVER.mib` file contains the following SNMP object types:

SNMP object type	Description
General objects	These objects contain information of the host system such as operational status, product version, memory usage, and other configuration details. See i3MsGeneral objects.
Information objects	These objects contain information on media engines, which facilitate communications by Interaction Media Server, and configured Customer Interaction Center servers with which this Interaction Media Server can communicate. See i3MsInfo objects.
Traps	These objects contain informational, error, or warning messages that occur on the Interaction Media Server host system. See i3MsTraps objects.

i3MsGeneral objects

i3MsGeneralInfoCurrentTimeStamp

Type	Access	Description
DisplayString	read-only	The current time as reported by Media Server, in GMT.

i3MsGeneralInfoOperStatus

Type	Access	Description
Integer	read-only	Operational status of Interaction Media Server. This object supports the following values: 1 = unknown 2 = up 3 = down 4 = congested 5 = restarting 6 = quiescing 7 = testing

i3MsGeneralInfoOperStatusDuration

Type	Access	Description
Unsigned32	read-only	The duration of the current status in seconds

i3MsGeneralInfoFileVersion

Type	Access	Description
DisplayString	read-only	Current product file version

i3MsGeneralInfoBuildDescription

Type	Access	Description
DisplayString	read-only	Current product build description

i3MsGeneralInfoLicenseType

Type	Access	Description
DisplayString	read-only	Current product license type.

i3MsGeneralInfoLicenseExpiration

Type	Access	Description
DisplayString	read-only	Expiration date of current license

i3MsGeneralInfoFqdn

Type	Access	Description
DisplayString	read-only	The Fully Qualified Domain Name (FQDN) of the Media Server.

i3MsGeneralInfoSnmpTrapDestinations

Type	Access	Description
DisplayString	read-only	A comma-separated list of hostnames and IP addresses which are currently configured as SNMP trap destinations.

i3MsGeneralInfoMemoryUsage

Type	Access	Description
Gauge32	read-only	Memory usage of Interaction Media Server, in bytes.

i3MsGeneralInfoTracelogFilePath

Type	Access	Description
DisplayString	read-only	Local file path where tracelogs are kept.

i3MsGeneralInfoTracelogFreeDiskSpace

Type	Access	Description
Gauge32	read-only	Amount of remaining (free) space on the disk available for tracelog files, in MiB

i3MsGeneralInfoTracelogTotalDiskSpace

Type	Access	Description
Gauge32	read-only	Total amount of disk space reserved for tracelog files, in MiB

i3MsGeneralInfoHttpCacheFilePath

Type	Access	Description
DisplayString	read-only	Local file path where HTTP cache files are kept.

i3MsGeneralInfoHttpCacheFreeDiskSpace

Type	Access	Description
Gauge32	read-only	Amount of remaining (free) space on the disk available for HTTP cache files, in MiB

i3MsGeneralInfoHttpCacheTotalDiskSpace

Type	Access	Description
Gauge32	read-only	Total amount of disk space reserved for HTTP cache files, in MiB

i3MsInfo objects

i3MsAudioEngineInfoTable

Type	Access	Description
N/A	not-accessible	Table containing all media engine parameters.

i3MsAudioEngineInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3MsAudioEngineInfoTable. Each entry is applicable for each activated media engine. Each entry contains data for the following objects: i3MsAudioEngineId i3MsAudioEngineThreadID i3MsAudioEngineCPUID i3MsAudioEngineLocation i3MsAudioEngineCurrentLoad i3MsAudioEngineAverageLoad i3MsAudioEngineGraphCount i3MsAudioEngineElementCount

i3MsAudioEngineId

Type	Access	Description
Integer	read-only	Index into Audio Engine Table

i3MsAudioEngineThreadID

Type	Access	Description
DisplayString	read-only	The local thread ID of this media engine

i3MsAudioEngineCPUID

Type	Access	Description
Integer	read-only	The local CPU ID of this media engine

i3MsAudioEngineLocation

Type	Access	Description
DisplayString	read-only	The Location ID of this media engine

i3MsAudioEngineCurrentLoad

Type	Access	Description
DisplayString	read-only	The current load of this media engine, in percent capacity

i3MsAudioEngineAverageLoad

Type	Access	Description
DisplayString	read-only	The average load of this media engine, in percent capacity, over last 30 seconds

i3MsAudioEngineGraphCount

Type	Access	Description
Gauge32	read-only	The number of active graphs within this media engine

i3MsAudioEngineElementCount

Type	Access	Description
Gauge32	read-only	The total number of active graph elements within this media engine

i3MsCommandServerInfoTable

Type	Access	Description
N/A	not-accessible	Table containing all listed Command Servers.

i3MsCommandServerInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3MsCommandServerInfoTable. Each entry represents a single defined Command Server.
		Each entry contains data for the following objects:
		i3MsCmdSrvId
		i3MsCmdSrvStatus
		i3MsCmdSrvStatusLabel
		i3MsCmdSrvStatusDetail
		i3MsCmdSrvNotifierHost
		i3MsCmdSrvClient
		i3MsCmdSrvClientId
		i3MsCmdSrvAcceptSessions
		i3MsCmdSrvResourceCount
		i3MsCmdSrvLogicalCapacity
		i3MsCmdSrvRecFilePath
		i3MsCmdSrvRecFreeDiskSpace
		i3MsCmdSrvRecTotalDiskSpace
		i3MsCmdSrvResourceAgeHistogram

i3MsCmdSrvId

Type	Access	Description
Gauge32	read-only	Unique Command Server identifier

i3MsCmdSrvStatus

Type	Access	Description
Integer	read-only	Enumeration indicating broad classification of status.
		This object supports the following values:
		0 = unknown
		1 = ready
		2 = notready
		3 = error

i3MsCmdSrvStatusLabel

Type	Access	Description
DisplayString	read-only	Extra status information

i3MsCmdSrvStatusDetail

Type	Access	Description
DisplayString	read-only	More detailed status information

i3MsCmdSrvNotifierHost

Type	Access	Description
DisplayString	read-only	DNS name or IP address of the Notifier for the primary Notifier connection.

i3MsCmdSrvClient

Type	Access	Description
DisplayString	read-only	Name of the Customer Interaction Center server to which the subsystem is connected (empty if not connected)

i3MsCmdSrvClientId

Type	Access	Description
DisplayString	read-only	Unique identifier of the client API instance (empty if not connected)

i3MsCmdSrvAcceptSessions

Type	Access	Description
TruthValue	read-only	Indicates if Command Server can host more resources. This object supports the following values: 1 = true 2 = false

i3MsCmdSrvResourceCount

Type	Access	Description
Gauge32	read-only	The number of resources allocated to this command server

i3MsCmdSrvLogicalCapacity

Type	Access	Description
DisplayString	read-only	The logical capacity of this server (frequency of CPUs multiplied by number of CPUs)

i3MsCmdSrvRecFilePath

Type	Access	Description
DisplayString	read-only	The local file path where recordings are kept.

i3MsCmdSrvRecFreeDiskSpace

Type	Access	Description
Gauge32	read-only	The amount of remaining (free) storage space that is available for recordings, in MiB

i3MsCmdSrvRecTotalDiskSpace

Type	Access	Description
Gauge32	read-only	The total amount of storage space reserved for recordings, in MiB

i3MsCmdSrvResourceAgeHistogram

Type	Access	Description
DisplayString	read-only	The aggregated age of all active resources on this command server, separated into raw histogram bands defined in a comma-separated list of elements of [max_age_in_seconds]:[resource_count]

i3MsTraps objects

i3MsSpecificTrapType

Type	Access	Description
Integer	accessible-for-notify	Contains the type of trap notification. This SNMP trap message supports the following values: 2 = operStatus 3 = adminCredentials 4 = configChange 5 = dnsQueryAlarm 6 = diskLogSpace 7 = memoryUsage 8 = diskRecSpace 9 = dosAttack 10 = i3MsTrapAudioQuality 11 = i3MsTrapAudioFault 12 = i3MsTrapHttpCacheDiskSpace

i3MsTrapOperStatus

Type	Access	Description
N/A	N/A	This trap is generated when the Interaction Media Server changes its own state. If the SNMP service is running, but the Interaction Media Server application is unresponsive, this trap will be sent repeatedly every 30 seconds until the condition is cleared.

i3MsTrapAdminCredentials

Type	Access	Description
N/A	N/A	This trap is generated when the administrator login credentials are changed.

i3MsTrapCmdSrvConfigChange

Type	Access	Description
N/A	N/A	This trap is generated when the configuration of any Command Server within the Media Server is changed. This SNMP trap message contains data for the following object: i3MsCmdSrvId

i3MsTrapDNSQueryAlarm

Type	Access	Description
N/A	N/A	This trap is currently not implemented.

i3MsTrapLogDiskSpace

Type	Access	Description
N/A	N/A	This trap is generated when the amount of free space for tracelog files drops below 100 MiB. Tracing will be disabled until more storage space is provided to the application.

i3MsTrapMemoryUsage

Type	Access	Description
N/A	N/A	This trap is generated when overall memory usage of Interaction Media Server exceeds 1.825 Gb (85 percent of 2Gb process limit).

i3MsTrapRecDiskSpace

Type	Access	Description
N/A	N/A	This trap is generated when the amount of free space available on the recording drive falls below 10 percent and again below 2 percent. Recordings are disabled if the recording drive free space falls to 2 percent or below. This SNMP trap message contains data for the following object: i3MsCmdSrvId

i3MsTrapDOSAttack

Type	Access	Description
N/A	N/A	This trap is currently not implemented.

i3MsTrapAudioQuality

Type	Access	Description
N/A	N/A	This trap is currently not implemented.

i3MsTrapAudioFault

Type	Access	Description
N/A	N/A	This trap is generated when a media engine enters an error or exception state.

i3MsTrapHttpCacheDiskSpace

Type	Access	Description
N/A	N/A	This trap is generated when the amount of free space for HTTP cache files drops below 500 MiB.

i3MsTrapLogDiskSpaceClear

Type	Access	Description
N/A	N/A	This trap is generated after i3MsTrapLogDiskSpace was previously sent and the amount of free space for tracelog files reaches or exceeds 100 MiB.

i3MsTrapMemoryUsageClear

Type	Access	Description
N/A	N/A	This trap is generated after i3MsTrapMemoryUsage was previously sent and overall memory usage of Interaction Media Server drops below 85 percent of the process limit.

i3MsTrapRecDiskSpaceClear

Type	Access	Description
N/A	N/A	This trap is generated after i3MsTrapRecDiskSpace was previously sent and the amount of free space available on the audio recording drive meets or exceeds 10 percent.

i3MsTrapHttpCacheDiskSpaceClear

Type	Access	Description
N/A	N/A	This trap is generated ater i3MsTrapHttpCacheDiskSpace was previously sent and the amount of free space for HTTP cache files meets or exceeds 500 MiB.

i3MsTrapAudioEngineLoadLimitClear

Type	Access	Description
N/A	N/A	This trap is generated after i3MsTrapAudioEngineLoadLimit was previously sent and the running average of the audio engine load has fallen below the load limit.

HOST-RESOURCES-MIB.mib

For a list of SNMP objects in this Management Information Base (MIB) file, see HOST-RESOURCES-MIB.mib in the General section.

Interaction SIP Proxy

This section contains information about the following .mib files and SNMP object types:

- INTERACTION-SIP-PROXY.mib
- i3SpGeneral objects
- i3SpInfo objects
- i3SpTraps objects
- HOST-RESOURCES-MIB.mib

INTERACTION-SIP-PROXY.mib

The `INTERACTION-SIP-PROXY.mib` file contains the following SNMP object types:

SNMP object type	Description
General objects	These objects contain information of the host system such as operational status, product version, memory usage, and other configuration details. See i3SpGeneral objects.
Information objects	These objects contain information regarding IP routes, call counts, destination status, and media engine parameters. See i3SpInfo objects.
Traps	These objects contain informational, error, and warning messages for events that occur on the Interaction SIP Proxy host system. See i3SpTraps objects.

i3SpGeneral objects

i3SpGeneralInfoTable

Type	Access	Description
N/A	not-accessible	Table containing general information about Interaction SIP Proxy server.

i3SpGeneralInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3SpGeneralInfoTable.
		Each entry contains data for the following objects:
		i3SpGeneralInfoIndex
		i3SpGeneralInfoProductVersion
		i3SpGeneralInfoOperStatus
		i3SpGeneralInfoLastOperStatusChange
		i3SpGeneralInfoActiveSessions
		i3SpGeneralInfoSIPQueueLength
		i3SpGeneralInfoLicenseType
		i3SpGeneralInfoHostAddress
		i3SpGeneralInfoMemoryAddress
		i3SpGeneralInfoCurrentTimeStamp
		i3SpGeneralInfoDiskFreeSpace
		i3SpGeneralInfoSnmpTrapDestinations
		i3SpGeneralInfoAlertServerStatus
		i3SpGeneralInfoAlertAdminCredentials
		i3SpGeneralInfoAlertConfigChanges
		i3SpGeneralInfoAlertCallDuration
		i3SpGeneralInfoAlertDNSQueryTimeout
		i3SpGeneralInfoAlertSIPQueueLength

i3SpGeneralInfoIndex

Type	Access	Description
Integer	read-only	Index into General Plan Table.

i3SpGeneralInfoProductVersion

Type	Access	Description
DisplayString	read-only	The Interaction SIP Proxy version and build number.

i3SpGeneralInfoOperStatus

Type	Access	Description
Integer	read-only	Operational status of Interaction SIP Proxy. This object supports the following values: 1 = unknown 2 = up 3 = down 4 = congested 5 = restarting 6 = quiescing 7 = testing

i3SpGeneralInfoLastOperStatusChange

Type	Access	Description
Counter32	read-only	The duration of the current status, in seconds.

i3SpGeneralInfoActiveSessions

Type	Access	Description
Gauge32	read-only	Count of currently active sessions.

i3SpGeneralInfoSIPQueueLength

Type	Access	Description
Gauge32	read-only	Count of pending SIP transactions.

i3SpGeneralInfoLicenseType

Type	Access	Description
DisplayString	read-only	The Interaction SIP Proxy license type.

i3SpGeneralInfoHostAddress

Type	Access	Description
InetAddress	read-only	The IPv4 host address on which Interaction SIP proxy is listening.

i3SpGeneralInfoMemoryUsage

Type	Access	Description
Gauge32	read-only	Memory usage of Interaction SIP Proxy, in bytes.

i3SpGeneralInfoCurrentTimeStamp

Type	Access	Description
DisplayString	read-only	The current timestamp reference of Interaction SIP Proxy server.

i3SpGeneralInfoDiskFreeSpace

Type	Access	Description
Gauge32	read-only	Amount of remaining free space on the disk used for trace logging, in GiB.

i3SpGeneralInfoSnmpTrapDestinations

Type	Access	Description
DisplayString	read-only	A comma-separated list of hostnames and IP addresses which are currently configured to as SNMP trap destinations.

i3SpGeneralInfoAlertServerStatus

Type	Access	Description
TruthValue	read-only	Indicates whether alerts will be sent when destination server status changes from UP to DOWN. This object supports the following values: 1 = true 2 = false

i3SpGeneralInfoAlertAdminCredentials

Type	Access	Description
TruthValue	read-only	Indicates whether an alert will be sent if the Administrator credentials are changed. This object supports the following values: 1 = true 2 = false

i3SpGeneralInfoAlertConfigChanges

Type	Access	Description
TruthValue	read-only	Indicates whether an alert will be sent if any configuration item, such as protocols, routes, certificates, server plans, etc. are changed. This object supports the following values: 1 = true 2 = false

i3SpGeneralInfoAlertCallDuration

Type	Access	Description
TruthValue	read-only	Indicates whether an alert will be sent if any single call session exceeds a preset duration. This object supports the following values: 1 = true 2 = false

i3SpGeneralInfoAlertDNSQueryTimeout

Type	Access	Description
TruthValue	read-only	Indicates whether an alert will be sent if any single DNS lookup query requires more than 2 seconds. This object supports the following values: 1 = true 2 = false

i3SpGeneralInfoAlertSIPQueueLength

Type	Access	Description
TruthValue	read-only	This alert parameter is currently disabled. It may be implemented in a future release.

i3SpLicenseInfo

i3SpLicenseVersion

Type	Access	Description
DisplayString	read-only	The license version number.

i3SpLicenseDetail

Type	Access	Description
DisplayString	read-only	The license type and details.

i3SpLicenseCompanyName

Type	Access	Description
DisplayString	read-only	The name of the Company to which this license was issued.

i3SpLicenseServerName

Type	Access	Description
DisplayString	read-only	The server name associated with this license

i3SpLicenseFeatureLoadBalancing

Type	Access	Description
TruthValue	read-only	Indicates whether the load-balancing license feature has been activated. This object supports the following values: 1 = true 2 = false

i3SpLicenseRegistrationsCount

Type	Access	Description
Gauge32	read-only	The maximum number of SIP devices allowed to concurrently register with this Interaction SIP Proxy server.

i3SpLicenseMediaPortCount

Type	Access	Description
Gauge32	read-only	The maximum number of concurrent media recordings enabled on this Interaction SIP Proxy server.

i3SpLicenseG723Count

Type	Access	Description
Gauge32	read-only	The maximum number of concurrent G.723 media recordings enabled on this Interaction SIP Proxy server.

i3SpLicenseG729Count

Type	Access	Description
Gauge32	read-only	The maximum number of concurrent G.729 media recordings enabled on this Interaction SIP Proxy server.

i3SpManagedProxyInfo

i3SpManagedProxyState

Type	Access	Description
Integer	read-only	Operational status of Managed Proxy feature. This object supports the following values: 0 = disconnected 1 = pending 2 = activated 3 = rejected

i3SpManagedProxyLastUpdate

Type	Access	Description
DisplayString	read-only	The local time at which the last update message was received from the Customer Interaction Center server.

i3SpManagedProxyRegion

Type	Access	Description
DisplayString	read-only	The geographical region name which has been assigned to this Interaction SIP Proxy server by the Customer Interaction Center administrator.

i3SpManagedProxyHostname

Type	Access	Description
DisplayString	read-only	The local host name of this Interaction SIP Proxy server.

i3SpManagedProxyFqdn

Type	Access	Description
DisplayString	read-only	The fully qualified domain name (FQDN) of this Interaction SIP Proxy server.

i3SpManagedProxyStationCount

Type	Access	Description
Counter32	read-only	The number of local stations which are currently being remotely managed by the Customer Interaction Center server. The stations are enumerated in the i3SpAuthenticationTable.

i3SpManagedProxyProvisionProxyRunning

Type	Access	Description
TruthValue	read-only	Indicates if the Provision Proxy feature is currently running. This object supports the following values: 1 = true 2 = false

i3SpMediaManagerInfo

i3SpMediaRecFilePath

Type	Access	Description
DisplayString	read-only	The local file path destination where recordings are kept.

i3SpMediaRecFreeDiskSpace

Type	Access	Description
Gauge32	read-only	The amount of remaining free storage space used for recordings, in MiB.

i3SpMediaRecTotalDiskSpace

Type	Access	Description
Gauge32	read-only	The total allocated storage size used for recordings, in MiB. This value includes free space and used space.

i3SpmediaResourceAgeHistogram

Type	Access	Description
DisplayString	read-only	The aggregated age of all active audio resources on this Interaction SIP Proxy server, separated into raw histogram bands defined in a comma-separated list of elements of [max_age_in_seconds]: [resource_count].

i3SpTracelogInfo

i3SpTracelogFilePath

Type	Access	Description
DisplayString	read-only	The local file path destination where tracelog files are kept.

i3SpTracelogFreeDiskSpace

Type	Access	Description
Gauge32	read-only	The amount of remaining free space on the hard drive used for trace logging, in MiB.

i3SpTracelogTotalDiskSpace

Type	Access	Description
Gauge32	read-only	The total allocated size of the hard drive used for tracelog files, in MiB. This value includes free space and used space.

i3SpDiagnostics

i3SpDiagCpuTimeTotalPct

Type	Access	Description
Gauge32	read-only	The overall CPU usage of this server, across all cores and processes, in percent capacity.

i3SpDiagProcessTimeTotalPct

Type	Access	Description
Gauge32	read-only	The CPU usage of this server due to the Interaction SIP Proxy process only, in percent capacity.

i3SpDiagPrivateBytes

Type	Access	Description
Gauge32	read-only	The amount of memory current in use by the Interaction SIP Proxy process, in Kilobytes.

i3SpDiagIOBytesPerSec

Type	Access	Description
Gauge32	read-only	The rate at which the Interaction SIP Proxy process is reading and writing bytes in I/O operations. This value represents all I/O activity generated by the process to include file network and device I/Os.

i3SpDiagTCPConnectionCount

Type	Access	Description
Gauge32	read-only	The number of currently active TCP connections to this Interaction SIP Proxy server.

i3SpDiagTLSConnectionCount

Type	Access	Description
Gauge32	read-only	The number of currently active TLS connections to this Interaction SIP Proxy server.

i3SpDiagSIPSessionCount

Type	Access	Description
Gauge32	read-only	The total number of all SIP sessions being managed, in ALL of their various states (not just 'connected').

i3SpDiagSIPQueueLength

Type	Access	Description
Gauge32	read-only	The number of SIP messages waiting to be processed.

i3SpTrapVars

i3SpSpecificTrapType

Type	Access	Description
Integer	accessible-for-notify	Contains the type of trap notification This object contains one of the following values: 1 = operStatus 2 = destServerStatus 3 = adminCredentials 4 = configChange 5 = dnsQueryAlarm 6 = sipQueueLength 7 = sessionDuration 8 =- memoryUsage 9 = diskSpace 10 = dosAttack 11 = recDiskSpace

i3SpSessionCallID

Type	Access	Description
DisplayString	accessible-for-notify	Specific call ID value associated with i3SpTrapSessionDuration.

i3SpSessionConnectDuration

Type	Access	Description
Counter32	accessible-for-notify	Call duration, in minutes, associated with i3SpTrapSessionDuration.

i3SpInfo objects

i3SpServerPlanInfoTable

Type	Access	Description
N/A	not-accessible	Table containing all destination IP addresses, call counts, and Up/Down status for each destination.

i3SpServerPlanInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3SpServerPlanInfoTable. Each entry is applicable for each destination server of all active Server Plans. Each entry contains data for the following objects: i3SpServerPlanInfoIndex i3SpServerPlanInfoName i3SpServerPlanInfoIPAddress i3SpServerPlanInfoProtocol i3SpServerPlanInfoCallCount i3SpServerPlanInfoStatus i3SpServerPlanInfoStatusSince i3SpServerPlanInfoStatusDuration

i3SpServerPlanInfoIndex

Type	Access	Description
Integer	read-only	Index into Server Plan Table.

i3SpServerPlanInfoName

Type	Access	Description
DisplayString	read-only	The server plan name to which this server belongs.

i3SpServerPlanInfoIPAddress

Type	Access	Description
DisplayString	read-only	The address or hostname of this destination server.

i3SpServerPlanInfoProtocol

Type	Access	Description
Integer	read-only	Protocol type.
		This object supports the following values:
		0 = notSet
		1 = udp
		2 = tcp
		3 = tls
		4 = sctp
		5 = other

i3SpServerPlanInfoCallCount

Type	Access	Description
Counter32	read-only	The number of calls currently in progress.

i3SpServerPlanInfoStatus

Type	Access	Description
Integer	read-only	Destination server status up/down.
		This object supports the following values:
		0 = none
		1 = up
		2 = down

i3SpServerPlanInfoStatusSince

Type	Access	Description
DisplayString	read-only	Timestamp when status last changed.

i3SpServerPlanInfoStatusDuration

Type	Access	Description
Counter32	read-only	Duration of current status, in seconds.

i3SpAudioEngineInfoTable

Type	Access	Description
N/A	not-accessible	Table containing all audio engine parameters.

i3SpAudioEngineInfoTableEntry

Type	Access	Description
N/A	not-accessible	Entry in the i3SpAudioEngineInfoTable. Each entry is applicable for each activated media engine. Each entry contains data for the following objects: i3SpAudioEngineId i3SpAudioEngineThreadID i3SpAudioEngineCPUID i3SpAudioEngineLocation i3SpAudioEngineCurrentLoad i3SpAudioEngineAverageLoad i3SpAudioEngineGraphCount i3SpAudioEngineElementCount

i3SpAudioEngineId

Type	Access	Description
Integer	read-only	Index into Audio Engine Table.

i3SpAudioEngineThreadID

Type	Access	Description
DisplayString	read-only	The local thread ID of this media engine.

i3SpAudioEngineCPUID

Type	Access	Description
Integer	read-only	The local CPU ID of this media engine.

i3SpAudioEngineLocation

Type	Access	Description
DisplayString	read-only	The Location ID of this media engine.

i3SpAudioEngineCurrentLoad

Type	Access	Description
DisplayString	read-only	The current load of this media engine, in percent capacity.

i3SpAudioEngineAverageLoad

Type	Access	Description
DisplayString	read-only	The average load of this media engine, in percent capacity, over the last 30 seconds.

i3SpAudioEngineGraphCount

Type	Access	Description
Gauge32	read-only	The number of active graphs within this media engine.

i3SpAudioEngineElementCount

Type	Access	Description
Gauge32	read-only	The total number of active graph elements within this media engine.

i3SpTraps objects

i3SpTrapOperStatus

Type	Access	Description
N/A	N/A	This trap is generated when the Interaction SIP Proxy changes its own state. If the SNMP service is running, but the Interaction SIP Proxy application is unresponsive, this trap will be sent repeatedly every 30 seconds until the condition is cleared. This SNMP trap message contains the following objects: i3SpGeneralInfoOperStatus

i3SpTrapDestServerStatus

Type	Access	Description
N/A	N/A	This trap is generated when a destination server listed in any active server plan changes state from UP to DOWN or vice-versa. This trap message contains the following objects: i3SpServerPlanInfoIPAddress i3SpServerPlanInfoCallCount i3SpServerPlanInfoStatus

i3SpTrapAdminCredentials

Type	Access	Description
N/A	N/A	This trap is generated when the administrator login credentials are changed. This trap message contains the following objects: i3SpGeneralInfoCurrentTimeStamp

i3SpTrapConfigChange

Type	Access	Description
N/A	N/A	This trap is generated when any Interaction SIP Proxy configuration items are changed. This trap message contains the following objects: i3SpGeneralInfoCurrentTimeStamp

i3SpTrapDNSQueryAlarm

Type	Access	Description
N/A	N/A	This trap is generated when any DNS name lookup duration exceeds 2 seconds. This trap message contains the following objects: i3SpGeneralInfoCurrentTimeStamp

i3SpTrapSIPQueueLength

Type	Access	Description
N/A	N/A	Deprecated. This item is currently under review.
		This trap message contains the following objects:
		i3SpGeneralInfoSIPQueueLength
		i3SpGeneralInfoCurrentTimeStamp

i3SpTrapSessionDuration

Type	Access	Description
N/A	N/A	This trap is signaled if any call exceeds the Excessive Call Duration threshold that is configured in the Alerts setup.
		This trap message contains the following objects:
		i3SpSessionCallID
		i3SpSessionConnectDuration

i3SpTrapMemoryUsage

Type	Access	Description
N/A	N/A	This trap is generated when overall memory usage of Interaction SIP Proxy exceeds 1.825 Gb (85% of 2Gb process limit).
		This trap message contains the following objects:
		i3SpGeneralInfoMemoryUsage

i3SpTrapDiskSpace

Type	Access	Description
N/A	N/A	This trap is generated when the amount of free space on the drive used for trace logging falls below 2 GiB (gigabytes).
		This trap message contains the following objects:
		i3SpTracelogFreeDiskSpace

i3SpTrapDOSAttack

Type	Access	Description
N/A	N/A	This trap is currently disabled.
		This trap message contains the following objects:
		i3SpGeneralInfoCurrentTimeStamp

i3SpTrapRecFreeDiskSpace

Type	Access	Description
N/A	N/A	This trap is signaled when the amount of free disk space for audio recordings falls below 2 GiB (gigabytes).
		This trap message contains the following objects:
		i3SpMediaRecFreeDiskSpace

HOST-RESOURCES-MIB.mib

For a list of SNMP objects in this Management Information Base (MIB) file, see HOST-RESOURCES-MIB.mib in the General section.

Session Manager

This section contains information about the following .mib file and SNMP object type:

- i3icsessionmanager.mib
- sessionmanagerInfo objects

i3icsessionmanager.mib

The `i3icsessionmanager.mib` Management Information Base (MIB) file was introduced in CIC 2016 R1. It provides the ability of network and telephony administrators to monitor and determine the current health of a Session Manager instance. See sessionmanagerInfo objects.

sessionmanagerInfo objects

sessionmanagerTotalSessionsInfoTable

Type	Access	Description
N/A	not-accessible	Table containing the total number of current sessions by CIC subsystem with this Interaction Session Manager instance

sessionmanagerTotalSessionsInfoTableEntry

Type	Access	Description
N/A	not-accessible	An entry in sessionmanagerTotalSessionsInfoTable. Each entry represents a CIC subsystem and its number of current sessions with this Interaction Session Manager instance. Each entry contains data for the following objects: sessionmanagerProductId sessionmanagerProductName sessionmanagerProductTotalSessions

sessionmanagerProductId

Type	Access	Description
Integer	read-only	The index number of a CIC subsystem that has current sessions with this Interaction Session Manager instance.

sessionmanagerProductName

Type	Access	Description
DisplayString	read-only	The name of the CIC subsystem that has current sessions with this Interaction Session Manager instance.

sessionmanagerProductTotalSessions

Type	Access	Description
Unsigned32	read-only	The number of current sessions for the associated CIC subsystem with this Interaction Session Manager instance.

sessionmanagerTotalNumberStatisticsCached

Type	Access	Description
Unsigned32	read-only	The number of alerts that Interaction Session Manager has encountered and saved for statistical purposes. This value is intended for use by Genesys personnel and software.

sessionmanagerTotalNumberStatisticsWatched

Type	Access	Description
Unsigned32	read-only	The number of statistics that Session Manager is watching. This MIB object is closely related to the sessionmanagerTotalNumberStatisticsCatched object as it also correlates to the amount of memory used in the process of monitoring, caching, and averaging usage statistics.

sessionmanagerTotalSessionsWatchingStatistics

Type	Access	Description
Unsigned32	read-only	The number of sessions from typical CIC products that are watching at least one statistic on this Session Manager host. This value can help you determine if one or more CIC products are dominating this instance of Session Manager.

sessionmanagerTotalAlertsCached

Type	Access	Description
Unsigned32	read-only	In CIC, alerts are notifications of contact center problems, such as having too few agents available for a large number of interactions. This object provides the number of alerts that Session Manager has encountered and saved for statistical purposes. This value is intended for use by Genesys personnel and software.

sessionmanagerTotalAlertsWatched

Type	Access	Description
Unsigned32	read-only	In CIC, alerts are notifications of contact center problems, such as having too few agents available for a large number of interactions. This object provides the number of alerts that Session Manager has encountered and is actively monitoring for statistical purposes. This value is intended for use by Genesys personnel and software.

sessionmanagerTotalSessionsWatchingAlerts

Type	Access	Description
Unsigned32	read-only	In CIC, alerts are notifications of contact center problems, such as having too few agents available for a large number of interactions. This object provides the number CIC subsystems that are actively monitoring these alerts through connections to Interaction Session Manager. This value is intended for use by Genesys personnel and software.

sessionmanagerTopBandwidthUsers

Type	Access	Description
Octet String	read-only	A list of the top 20 bandwidth users of this Session Manager instance over the last 5 minutes. Users and the amount of associated bandwidth are separated by the | character.

StatAlert Server

This section contains information about the following .mib file and SNMP object type:

- i3icstatlaertsserver.mib
- StatalertserverObjects objects

---

i3icstatalertsserver.mib

The `i3icstatalertserver.mib` Management Information Base (MIB) file was introduced in CIC 2016 R1. It enables network and telephony administrators to monitor system health of StatAlert Server through SNMP. See StatalertserverObjects objects.

StatalertserverObjects objects

statisticsByConnections

Type	Access	Description
N/A	not-accessible	This table contains the number of statistics requested of StatAlertServer from various CIC products.

statisticByConnection

Type	Access	Description
N/A	not-accessible	Each entry represents a CIC product connection and the number of statistics that it has requested. Each entry contains data for the following objects: connectionIdentifier statisticsWatched

connectionIdentifier

Type	Access	Description
Unsigned32	read-only	The unique identifier for the associated CIC product connection

statisticsWatched

Type	Access	Description
Unsigned32	read-only	The number of statistics requested by the associated CIC product connection

statisticsByProviders

Type	Access	Description
N/A	not-accessible	Table containing the number of statistics provided by each CIC product.

statisticsByProvider

Type	Access	Description
N/A	not-accessible	Each entry represents a CIC product and the number of statistics that it provided. Each entry contains data for the following objects: providerIdentifier statisticsProvided

providerIdentifier

Type	Access	Description
DisplayString	read-only	The name of the associated CIC product

statisticsProvided

Type	Access	Description
Unsigned32	read-only	The number of statistics provided by the associated CIC product

Change log

The following changes have been made to this document since release:

Date	Changes
11-November-2011	GA release
09-January-2012	• Updated document formatting to current standards • Updated "Copyright and Trademark information" page
09-February-2012	Removed incorrect statement regarding installation sequence
20-March-2014	• Updated content for 4.0 • Added Management Information Base (MIB) file objects and traps for Customer Interaction Center products and Interaction Edge/Interaction Gateway • Added content for PureConnect SNMP agent service
05-September-2015	• Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to PureConnect Product Information site URLs, and copyright and trademark information. • IC-115103 - Rename i3TracelogFreeDiskSpace to i3SpTracelogFreeDiskSpace • IC-114101 - Remove ServerURI and RemoteURI objects from the Interaction SIP Proxy MIB • IC-115289 - i3SpProvisionProxyRunning element should be renamed
16-April-2015	• Updated "Copyright and Trademark information" page • Updated formatting to conform to new corporate standards
28-July-2015	• DP-1272 Support for SNMPv3 on our products • Updated to reflect the ININ SNMP service is now installed as the default SNMP service • Removed obsolete content for the previous SNMP solution • Reorganized content to reflect new default SNMP service (ININ SNMP) and configuration process

24-September-2015	• Added new reporting subsystems for `i3ic.mib` in the following MIB objects:
	  ○ i3IcSubsysInfoIndex
	  ○ i3IcSubsysCmdIndex
	  ○ i3IcTrapInfoSubsys
	• Added new MIB objects for `i3ic.mib`:
	  ○ i3IcGenSwitchoverRole
	  ○ i3IcGenSwitchoverBackupState
	  ○ i3IcGenSwitchoverSwitchMode
	  ○ i3IcGenSwitchoverReplicationMode
	  ○ i3IcTrapVariableHostName
	  ○ i3IcTrapVariableSubsystemName
	  ○ i3IcTrapVariablePluginName
	  ○ i3IcTrapVariableErrorDesc
	  ○ i3IcTrapVariableHealthLevel
	• Removed the following MIB objects for `i3ic.mib`:
	  ○ i3IcTrapCommenceSwitchoverEvent
	  ○ i3IcTrapDiscontinueSwitchoverEvent
	  ○ i3IcTrapHighLatencyState
	  ○ i3IcTrapHighLatencyStateClear
	  ○ i3IcTrapTracingStoppedInsufficientDiskSpace
	  ○ i3IcTrapTracingStoppedInsufficientDiskSpaceCleared

21-October-2015	• Added new `i3icsessionmanager.mib` file and its objects • Added new `i3icstatalertserver.mib` file and its objects

08-January-2016	- IC-134501 Rewrite confusing sentence regarding the ININ Object ID The definition for "Management Information Base (MIB)" was rewritten for clarity. - IC-134846 Include registry tweaks necessary for App log trap messages to work for subsystems - Added admonitions for the following traps: - i3IcTrapInformationalEventLog - i3IcTrapWarningEventLog - i3IcTrapErrorEventLog
06-July-2016	- Updated "Copyright and trademark information" page - Added content for Session Manager support for SNMP - Added content for Interaction Recorder Remote Content Service support for SNMP
29-July-2016	IC-138711 - Some traps need corresponding trap that clears the alarm state when the respective condition is alleviated. Added five traps for clearing conditions in i3MsTraps objects.
02-June-2017	Added new MIB object for `i3ic.mib` i3IcGenSwitchoverPeer
18-October-2017	Rebranding terminology, updated title page and copyright page.
23-January-2018	Conversion to HTML.
15-March-2018	Added content for `reporting_plugin.mib`.
01-October-2018	Updated i3IcSubSysInfoAvailablecontent object to 2=unavailable.
03-January-2019	Updated "Configure PureConnect SNMP service through the command line utility" to correct ININ SNMP> atd --community param1 --uri param2 and "D:\I3\IC\ININ SNMP".
23-July-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section...".
13-December-2019	Removed references to Interaction Gateway and Interaction Edge as they are EOL.
02-April-2020	Updated values for i3IcGenSwitchoverRole.
09-April-2020	Updated values for i3IcGenSwitchoverBackupState.
29-April-2020	Updated links from my.inin.com to new locations.