DeviceListX Report

DeviceListX Report Overview

Note The DeviceListX Report is no longer supported as of Cisco Unified Communications Manager Release 5.0. Retrieving real-time information from Cisco Unified Communications Manager is now supported using the Cisco Unified Communications Manager AXL Serviceability API.

The DeviceListX Report provides a list of the services-capable devices along with basic information about the device to identify or classify the devices based on specific criteria. The report also includes the current device status and the IP address information that is obtained from the Real-Time Information Service.

Note DeviceListX does not support all devices. If you have a device that you need to support, contact Cisco Developer Support to verify whether it is supported:

https://developer.cisco.com/site/devnet/home/index.gsp

When a third-party developer initiates an *HTTP GET* request for the DeviceListX.asp report page, the system retrieves the following information about phones that are registered to a Cisco Unified Communications Manager server from the database:

- Device Type

- Device Name

- Device Description

- Calling Search Space

- Device Pool

- IP Address

- Real-Time Information

The completed list of data gets formatted into a simple XML object and gets returned in the HTTP Response to the developer.

Benefits

DeviceListX provides access to critical real-time data that was previously unavailable to third-party developers. In particular, the ability to list currently registered devices along with their IP address allows developers to easily build push, broadcast, and CTI-type applications.

Restrictions

Only users with administrative privileges to the Cisco Unified Communications Manager Administration can access the report.

Note To minimize processing overhead on the Cisco Unified Communications Manager server, access to the DeviceListX report gets rate-limited to once per minute. Any attempt to pull the report more frequently will fail. In practice, the developer application should pull and cache the DeviceListX report, refreshing only as often as required, typically every few hours or daily.

Integration Considerations and Interoperability

The interface allows HTTP 1.1 or HTTP 1.0 *GET* requests for the report. The report returns data that is encapsulated by using XML version 1.0.

Performance and Scalability

You can run this report on the largest supported Cisco Unified Communications Manager cluster size for the targeted release without impacting core features, such as delaying dial tone. On multiserver Cisco Unified Communications Manager clusters, the report can access only from the publisher server. In large clusters where the publisher is not a Cisco Unified Communications Manager server, no possibility exists of impacting the system performance as perceived by a user.

This report is not intended for use during real time, so this interface should provide a mechanism for developers to poll for the data on a daily or hourly basis. Give consideration to the frequency of polling and the time of day to prevent unnecessary burden on the system during peak usage times.

Security

This report, which is within the Cisco Unified Communications Manager Administration, inherits its security from that web site, so no security issues directly relate to this report. If the Cisco Unified Communications Manager Administration changes how it implements security with additions, such as SSL, this report benefits from that enhancement.

Related Features and Technologies

DeviceListX acts as an independent interface, which is a real-time complement to the XML-Layer Database API (AXL), where AXL provides access to static, persisted data, and DeviceListX provides access to dynamic, volatile information.

Supported Platforms

For the DeviceListX.asp page to function requires Cisco Unified Communications Manager Administration reporting infrastructure. The following releases support DeviceListX.asp:

- Cisco CallManager Release 3.2(3)SPB

- Cisco Unified Communications Manager Release 4.0(1) and later

Prerequisites

You can access this feature when devicelistX.asp resides in the C:\ciscoWebs\Admin\reports directory of the Cisco Unified Communications Manager publisher server.

Message and Interface Definitions

Use the following URL to access the report using HTTP:

http://x.x.x.x/CCMAdmin/reports/devicelistx.asp

where

x.x.x.x can either be the IP address or hostname of the Cisco Unified CallManager system that contains the report.

Note Beginning with Cisco Unified CallManager 4.1 release, the DeviceListX report can only be accessed using secure HTTP (HTTPS), so the URL must begin with "https:" rather than "http:".

DeviceList XML Object

Third-party applications that reside elsewhere on the network commonly use the interface. The application makes an HTTP request for the report and gets a response that contains a DeviceList XML object. The XML object follows:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<DeviceList>
<Device t="" n="" d="" c="" p="" i="" s="" />
</DeviceList>
```

Table 1: DeviceList XML Object Attributes

Attribute name	Field name	Description
t	Device Type	Numeric enumeration value that is specified in the database.
n	Device Name	String value that specifies the device name.
d	Device Description	String value that is specified in the database.
c	Device Calling Search Space	String value that is specified in the database.
p	Device Pool	String value that is specified in the database.
i	Device IP Address	Last known IP address as reported by the Real-Time Information Service "" = No known IP address "x.x.x.x" = Last known IP address
s	Device Status	Numeric enumeration for the current device status as reported by the Real-Time Information Service "" = Device not found "1" = Device registered "2" = Device found but not currently registered

DeviceList Object Example with Data

```
<?xml version="1" encoding="iso-8859-1"?>
<DeviceList>
<Device t="35" n="SEP000123456789" d="Auto 2010" c="" p="Default" i="10.1.1.1" s="1"/>
</DeviceList>
```

Troubleshooting DeviceListX Reports

These sections can assist you in troubleshooting DeviceListX Reports.

Error Codes

The error codes that are specific to this report interface are:

Error message 1001

Message

```
Error Message 1001 Too many simultaneous requests for Device List.
Please wait at least 60 seconds and try again.
```

Explanation

When two or more clients attempt to get the list at the same time, or if the list is long, overlapping requests can result (first request is processing when the second request attempts processing).

Recommended action

Request information only as often as necessary.

Note Cisco recommends that you wait longer than 60 seconds between requests.

Error message 1002

Message

```
Error Message 1002 Too many consecutive requests for Device List.
Please wait at least 60 seconds and try again.
```

Explanation

Because the system is busy, it cannot process a Device List.

Recommended action

Request information only as often as necessary. Because the real-time status of every device gets checked, Device List represents a CPU-intensive process.

Note Cisco recommends that you wait longer than 60 seconds between requests.

Determine Interface Problems

Use the following procedure to determine whether a problem exists with the interface and determine the root cause of the problem.

Procedure

Step 1   Check the Windows NT Event Logs for error messages that pertain to the IIS server and the SQL server:

Start > **Programs** > **Administrative Tools** > **Event Viewer**

Step 2   Check for error messages or successful completion of a request in the IIS log files, which are typically located in

C:\WINNT\System32\LogFiles\W3SVC1

The date of the log provides part of the log name. All times in the log files specify GMT for noted events. The IIS logs appear in chronological order and can easily be searched by specific query event.

Step 3   Use a web browser, such as Internet Explorer, to request the URL of the devicelistx.asp web page. A successful request yields a well-formed XML object of all the device information.

Step 4   Use a Sniffer trace to view the HTTP GET request and response transaction between the third-party application and the report.