ClarusIPC®

User Guide

Revision: 2.5.0
Date: October 7, 2008

Clarus Systems, Inc.
2200 Bridge Parkway, Suite 101
Redwood City, CA 94065
http://www.clarussystems.com
Voice: 650-632-2800
Fax: 650-632-2810

TABLE OF CONTENTS

CHAPTER 1 GETTING STARTED

ClarusIPC® is used by enterprises, systems integrators and managed service providers to support the lifecycle of Cisco Unified Communications, from deployment through ongoing operations. ClarusIPC offers remote certification, configuration analysis, and troubleshooting; further validating operational integrity while building the foundation for a Unified Communications network.

ClarusIPC allows you to validate that all aspects of a Cisco IP Communications environment work together to meet user functionality requirements at deployment and during ongoing operations. Tests may be scheduled around the clock, and may be monitored live, or reviewed later as health checks, to identify and correct issues before they impact end-users.

ClarusIPC currently supports Cisco Unified CallManager versions 4.X, and Cisco Unified Communications Manager versions 5.X and 6.X.

NOTE: Please note that this user guide will use the term “Cisco Unified Communications Manager” or “CUCM” when referring to all Cisco cluster versions, as well as for the Cisco Unified CallManager Administration tool.

This chapter provides an introduction to the ClarusIPC user interface, and instructions for system configuration. It covers:

Network Connectivity Requirements

ClarusIPC required ports must be open for each required interface. The ports required for ClarusIPC to interface to Cisco Unified Communications Manager are shown in the Figure below:

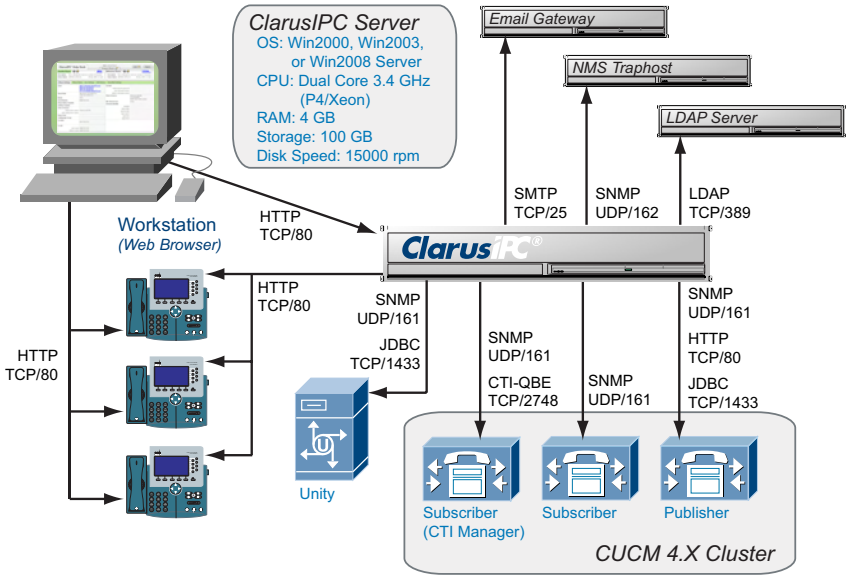


Figure 1-1 ClarusIPC Network Connectivity Requirements for CUCM 4.X

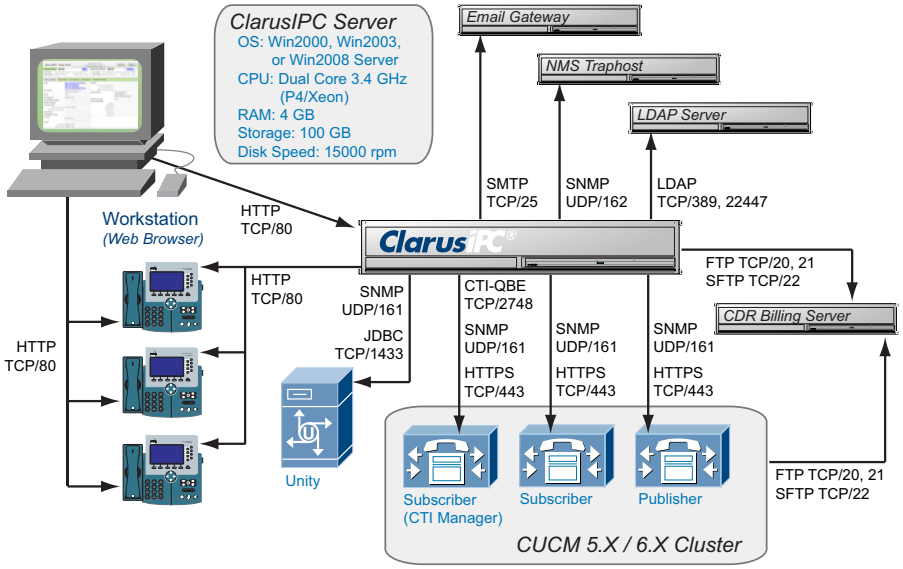


Figure 1-2 ClarusIPC Network Connectivity Requirements for CUCM 5.X and 6.X

Preparing CUCM

Some configuration changes to Cisco Unified Communications Manager (CUCM) are required to support ClarusIPC. To enable ClarusIPC to connect to the CUCM Cluster:

1. Create two CUCM user accounts reserved for use by ClarusIPC. One account will be used to for Test execution; the other to access the Remote Hands remote control feature.
2. Enable the SNMP service on each CUCM Server in your cluster. SNMP is used to gather some real-time information during Sync.
3. Configure CDR access. (CDR access is required for viewing Call History from the Help Desk module.)

As Cisco Unified Communications Manager differs significantly from version 4.X to version 5.X, the setup for these two cluster types is described separately below. (Please note that ClarusIPC supports CUCM versions 4.X, 5.X, and 6.X.)

NOTE: To simplify setup, use the same accounts for all customers, whenever possible.

Enable SNMP Service

To view server process information in some reports, you must configure SNMP for each of your CUCM servers. Each Communications Manager Server in the Cluster must have an SNMP Community String configured with Read-Only permission.

To create an SNMP Community String:

1. Access the CUCM server:
   - **Start > Programs > Administrative Tools > Services**
2. Select **SNMP Service**.
3. Right click on **SNMP** and select **Properties** from the drop down menu.
4. Select the **Security** tab.
5. Select **Add** for the **Accepted Community** names.
   - Ensure that **Community Rights** is set to **Read-Only**.
   - Add the **Community** name.
6. Check to see if **Accept SNMP packets** is set to **from any host.**
7. If **Accept SNMP packets from these hosts** is checked, verify that the system with ClarusIPC installed is included. If not then add it.
   - Select **Add**.
   - Enter Host Name or IP Address.
   - Select **Add**.
8. Click **OK**.
9. Start or restart the SNMP service.

10. Repeat these steps for each CUCM server in the Cluster.
    - Open **Services** from Control Panels.
    - Find **SNMP Service,** verify that it is Started and set to Automatic.
    - Click Properties on the Security tab, verify there is a community string with Read-Only privileges.
    - You may wish to restrict SNMP access to only the ClarusIPC host IP.
    - If you made ANY changes you must restart the SNMP service for them to take effect.
    - Repeat for remaining CUCM servers.

Create CUCM 4.X User Accounts

ClarusIPC requires that one CUCM user be created for each Cluster. Use the Communications Manager Administration UI to create a user.

1. Access the Communications Manager Administration page through your browser by entering:

   ```
   http(s)://<ccm hostname or IP Address>/ccmadmin
   ```

2. Create a CUCM user for Remote Hands.
   - From the CUCM Administration UI, select **User > Add a New User.**
   - Complete the following fields:
     - **First Name:** Clarus
     - **Last Name:** Remote Hands Account
     - **User ID:** clarusrh
     - **Enable CTI Super Provider:** No
     - **Controlled Devices:** Use the Device Association link to associate all phones that you may wish to control using Remote Hands, up to the Cisco max recommended limit of 2000. (If more than 2000 phones are to be supported using Remote Hands, create additional accounts, such as "clarusrh2," "clarusrh3," and "clarusrh4.")

3. Create a CUCM user for Test execution.
   - From the CUCM Administration UI, select **User > Add a New User.**
   - Complete the following fields:
     - **First Name:** Clarus Systems
     - **Last Name:** Test Exec Account
     - **User ID:** clarustest
     - **User Password:** 12345
     - **Confirm Password:** 12345
     - **PIN:** 12345
     - **Confirm PIN:** 12345
     - **Enable CTI Application Use:** Yes
     - **Enable CTI Super Provider:** Yes
     - **Call Park Retrieval Allowed:** Yes
     - **Controlled Devices:** none

Use Multi-Level Access

If you have implemented Multi-Level Access (MLA) to authenticate CUCM users, then a single account may be used for both the CUCM User ID and the CUCM Admin ID. First, create the CUCM User ID; then, add administrative privileges for the account.

- From the CUCM Administration UI, select **User > Access Rights > User Group**.
- Click **Server Maintenance**, then **Add a User to Group**.
- Add the *clarustest* user to the group, and click **Add Selected**.

The *clarustest* user account will be used for both the CUCM Admin ID and the CUCM User ID when defining ClarusIPC Clusters.

NOTE: If MLA is not enabled, the Windows Administrator account will be used for AXL, RIS, and Perfmon setup.

Create CUCM 5.X+ User Accounts

ClarusIPC® requires that one CUCM user be created for each Cluster. Use the Communications Manager Administration UI to create a user.

1. Access the CUCM Administration page through your browser by entering:

   `http(s)://<CUCM hostname or IP Address>/ccmadmin`

2. Create a CUCM user for Remote Hands.

   - From the CUCM Administration UI, select **User Management > End User,** click **Add New,** and complete the following fields:
     - **User ID:** clarusrh
     - **Password:** 12345
     - **Confirm Password:** 12345
     - **PIN:** 12345
     - **Confirm PIN:** 12345
     - **Last Name:** Remote Hands
     - **Presence Group:** (leave the default setting)
     - Click **Save.**
   - Click the **Device Association** button to associate all phones that you may wish to control using Remote Hands, up to the Cisco max recommended limit of 2000. (If more than 2000 phones are to be supported using Remote Hands, create additional accounts, such as “clarusrh2,” “clarusrh3,” and “clarusrh4.”)

3. Create a CUCM user for Test Execution

   - From the CUCM Administration UI, select **User Management > Application User,** click **Add New,** and complete the following fields:
     - **User ID:** clarustest
     - **Password:** 12345
     - **Confirm Password:** 12345
     - **Presence Group:** (leave the default setting)
     - Click **Save**.

To enable 3rd party call control for Test Execution, your user must be included in four Cisco User Groups:

- Standard CTI Allow Call Park Monitoring,
- Standard CTI Allow Control of All Devices,
- Standard CTI Enabled, and
- Standard CCM Super Users.

4. Add your test user to these groups.

   - Go to **User Management > User Group.**
   - Click **Find.**
   - In the Search Results returned list, click **Standard CTI Allow Call Park Monitoring.**
   - Click **Add Application Users to Group.**
   - In the Search Options field, enter **Find Application User where User ID contains clarustest** (the user created above), and click **Find.**
   - When the user *clarustest* appears in the Search Results pane, select the checkbox, and click **Add Selected.**

NOTE: Repeat for **Standard CTI Allow Control of All Devices,** and **Standard CTI Enabled.**

Configure CDR Access for CUCM 4.X

To view Call History from within Help Desk, you must provide ClarusIPC access to Call Detail Records (CDR). If you do not configure the CDR section, you may still use Help Desk, but will not be able to view Call History.

CDR access is also required for the Voice Monitor. Without Call Detail Records, the Voice Monitor will have no data with which to work.

Please note that CUCM 4.X requires that TCP Port 1433 be open between ClarusIPC and the Publisher, to allow CDR records to be extracted.

Service Parameters

To enable CDR/CMR logging for the Help Desk and Voice Monitor options, log into Cisco Unified Communications Manager Administration.

1. Go to **Service > Service Parameters.**
2. Select the CDR/CMR server, then select **Service: Cisco CallManager**.
3. Under **System**, set **CDR Enabled Flag** to **True**.
4. Under **Clusterwide Parameters (Device – General)**, set **Call Diagnostics Enabled** to **True.**

Set Up CDR SQL User

Create a CDR SQL User. This username and ID will be entered in the Database User ID and Database Password fields in the Cluster Details window for CUCM 4.X clusters. (For more information, see *Creating Clusters* on page 2-3.)

1. Create a new Windows user (claruscdr, or reuse an existing, non-Administrator) account on the CUCM Publisher server. (For clarity, use *claruscdr* as the username.) This user is not required to belong to any special Windows groups other than Users.

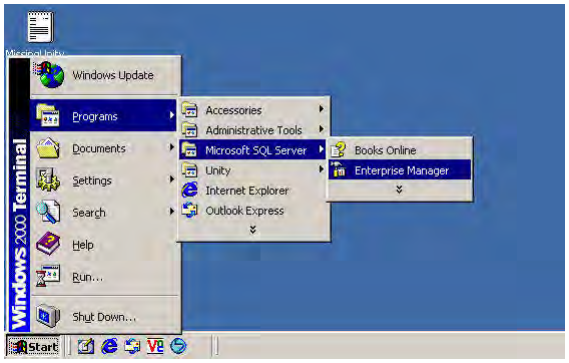


Figure 1-3 Open Enterprise Manager

2. From the CUCM Publisher console, click **Start Menu** and open **Microsoft SQL Server > Enterprise Manager**.

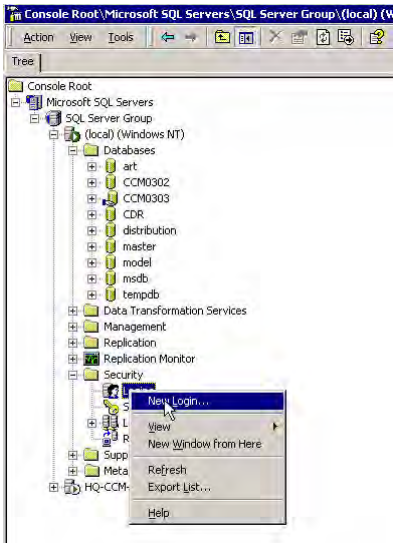


Figure 1-4 Create Login

3. From the Security folder in the Publisher Database folder, right-click **Login** and select **New Login** from the menu.

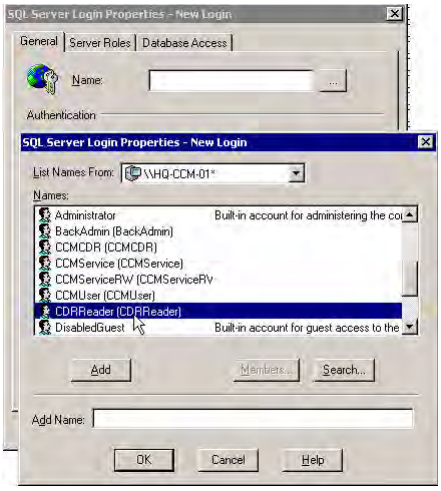


Figure 1-5 New User

From the **General** tab of the **New Login** window, click the "**...**" button next to the **Name** field. In the window that is invoked, select the *claruscdr* user created in Step1. Click **Add** followed by **OK**.

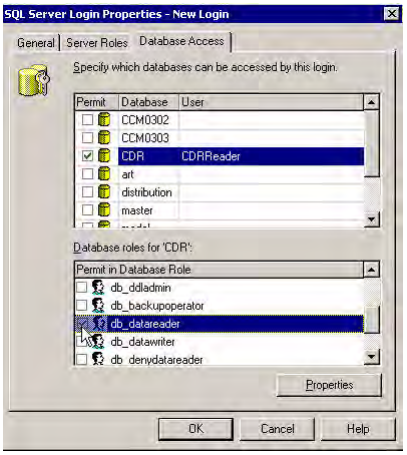


Figure 1-6 SQL Server Login

4. From the New Login window, select the **Database Access** tab. In the upper window displayed, check the **CDR Database Entry**. In the lower window, check the **db_datareader** database role. (Leave the **public** role item checked.) When finished, click **OK**.

5. Click **OK** to add the new user.

Configure CDR Access for CUCM 5.X+

To view Call History from within Help Desk, you must provide ClarusIPC access to Call Detail Records (CDR). If you do not configure the CDR section, you may still use Help Desk, but will not be able to view Call History.

CDR access is also required for the Voice Monitor. Without Call Detail Records, the Voice Monitor will have no data with which to work.

Service Parameters

To enable CDR/CMR logging for the Help Desk and Voice Monitor options, log into Cisco Unified Communications Manager Administration.

1. Go to **System > Service Parameters.**
2. Select the CDR/CMR server, then select **Service: Cisco CallManager.**
3. Under **System**, set **CDR Enabled Flag** to **True**.
4. Under **Clusterwide Parameters (Device – General)**, set **Call Diagnostics Enabled** to “Enabled Only When CDR Enabled Flag is True,” or “Enabled Regardless of CDR Enabled Flag.”

CDR Collection

To enable the Help Desk module to display Call History, you must grant access to your CDR data.

In previous versions of CUCM 4.X, CDR data was accessible directly through the CUCM database. With CUCM 5.X and 6.X, a billing server (FTP or SFTP) must be configured, which will periodically receive CDR flat files. To allow Call History information to be displayed in Help Desk, ClarusIPC must be configured to periodically fetch these files from the billing server.

With CUCM 5.X and 6.X:

1. Calls are made.
2. CUCM sends the CDR/CMR records to *all* preconfigured billing servers.
3. ClarusIPC polls a billing server regularly, looking for new CDR/CMR files, then imports them to the ClarusIPC database.
4. ClarusIPC removes all imported files from the billing server.

NOTE: Because ClarusIPC will automatically remove all imported CDR/CMR files from their original directory, it is strongly recommended that you define a dedicated Billing Server, or Billing Server directory, exclusively for this purpose. Do not use a Billing server that serves other applications because ClarusIPC will delete CDR files during the collection process.

The frequency with which ClarusIPC will poll the Billing Server, as well as how long CDR/CMR records will be retained, may be specified using the Cluster Details page. For more information, see Chapter 2, *Creating Clusters*.

To grant access to your CDR data for CUCM version 5.X and 6.X:

1. Set up an SFTP or FTP server to serve as the CUCM CDR Billing server. The user account will need Read, Write, and Delete permissions on the path configured.

NOTE: If you do not yet have an (S)FTP server in place, you may wish to use the open source FTP server FileZilla (http://sourceforge.net/projects/filezilla/), or the SFTP server OpenSSH (http://sshwindows.sourceforge.net/).

2. Log into Cisco Unified Communications Manager Administration.
3. Select Cisco Unified Communications Manager Serviceability from the Navigation dropdown menu in the top right corner of the CM Administration window, and click **Go**.
4. From the **Serviceability** window, select **Tools > CDR Management**.

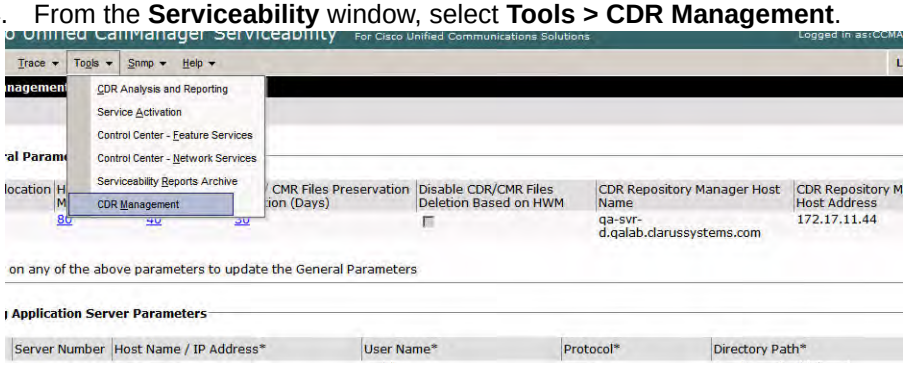


Figure 1-7 CDR Management Access

5. To add a new billing (S)FTP server, click the **Add New** button directly beneath the CDR Management header:

Add New

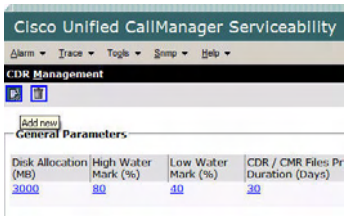


Figure 1-8 Add New CDR Management Server

6. Complete the Billing Server fields (examples are in *italics*):

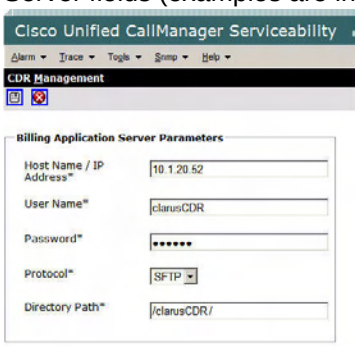


Figure 1-9 Billing Server Parameters

- Host Name/IP Address: the IP address of your (S)FTP server.
- User Name: *claruscdr*.
- Password: *12345*.
- Protocol: select *SFTP* or *FTP*, depending upon how you configured the server.
- Directory Path: */claruscdr/* (subdirectory under the home directory for user claruscdr). (Please note that a forward slash, "/", is required at the end of the directory path.)

7. Save your new Billing server.

   - The CUCM allows a maximum of 3 Billing servers per CUCM cluster.

Enable Call Statistics for SIP Phones

If you have SIP phones deployed in your network, you must enable Call Statistics reporting on the SIP Profile in order to view K-factor voice quality scores (MVTQav) for both the Help Desk and Voice Monitor modules.

To enable Call Statistics Reporting:

1. Log into CUCM Admin.
2. From the *CUCM Administration UI,* select **Device > Device Settings > SIP Profile.**
3. Create or modify an existing SIP Profile.
4. Select the **Call Stats** checkbox, and click **Save** or **Reset**.
5. If required, change the SIP Profile assigned to your SIP phones to use this new profile, then reset each.

CUCM IP Addresses and Administrator Credentials

To configure ClarusIPC, obtain the following from the CUCM System Administrator:

- CTI Manager IP Address: IP Address of the CUCM server(s) running the CTI Manager Service within the Cluster.

NOTE: For best performance, choose the least loaded server, and one upon which other CTI applications do not rely.

- Publisher CUCM IP Address: IP Address of the CUCM Publisher server within the Cluster.

6. CUCM Administrator Credentials: Username and Password for the Administrator login.

Preparing Unity

To access Unity data for Reports and Tasks, you must provide ClarusIPC access to the Unity Server. Access may be through either a Unity SQL or Unity Windows user account.

Set Up Unity SQL User

Create a Unity SQL User. This username and ID will be entered in the Username and Password fields in the Unity Details window. (For more information, see *Unity Systems* on page 1-27.)

1. Create a new Windows user (clarusunity, or reuse an existing, non-Administrator) account on the Cisco Unity server. (For clarity, use *clarusunity* as the username.) This user is not required to belong to any special Windows groups other than Users.
2. From the Unity Server console, click **Start Menu** and open **Microsoft SQL Server > Enterprise Manager**.

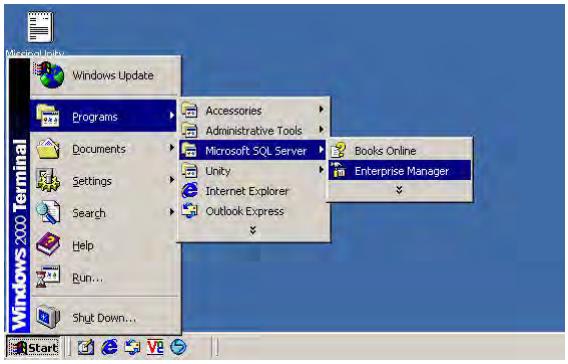


Figure 1-10 Open Enterprise Manager

3. From the Security folder, right-click **Logins** and select **New Login** from the menu.

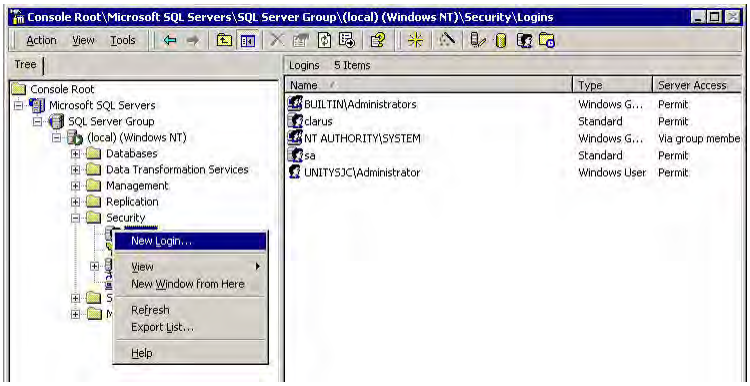


Figure 1-11 Create Login

4. From the **General** tab of the **New Login** window, click the "**...**" button next to the **Name** field. In the window that is invoked, select the *clarusunity* user created in Step1. Click **Add** followed by **OK**.

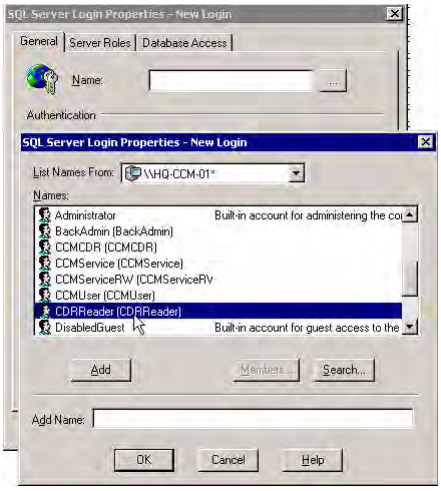


Figure 1-12 New User

5. From the New Login window, select the **Database Access** tab. In the upper window displayed, check the **UnityDb**. In the lower window, check the **db_datareader** database role. (Leave the **public** role item checked.) When finished, click **OK**.

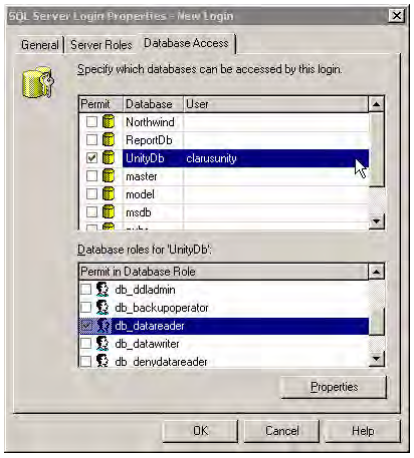


Figure 1-13 SQL Server Login

6. Click **OK** to add the new user.

License Installation

To enable ClarusIPC:

1. Open a web browser to:

```
http://<hostname or IP of ClarusIPC server>
```

The following screen displays:

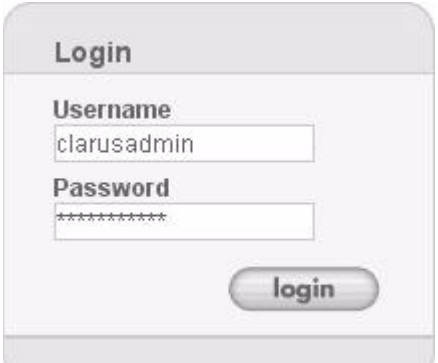


Figure 1-14 Login Window

2. Enter **clarusadmin**, the default password **clarusadmin** and click **login**. To change the password, see *Users* on page 1-18.
3. If this is the first time you have run the program, or if your license has expired, the following screen displays:

Figure 1-15 License Window

4. Enter the license key given to you by Clarus Systems Technical Support, and click **save**. If you have not received a license key, click the **Request New License Key** button to generate an email to Clarus, requesting a new key.
5. After entering the license key and clicking **save**, the main **Clusters** screen displays. You are now ready to use ClarusIPC.

Please note that your ClarusIPC installation is locked to the installed host, and cannot be moved to another machine without first contacting Clarus Systems.

Navigating the System

The ClarusIPC application screens are composed of the following sections:

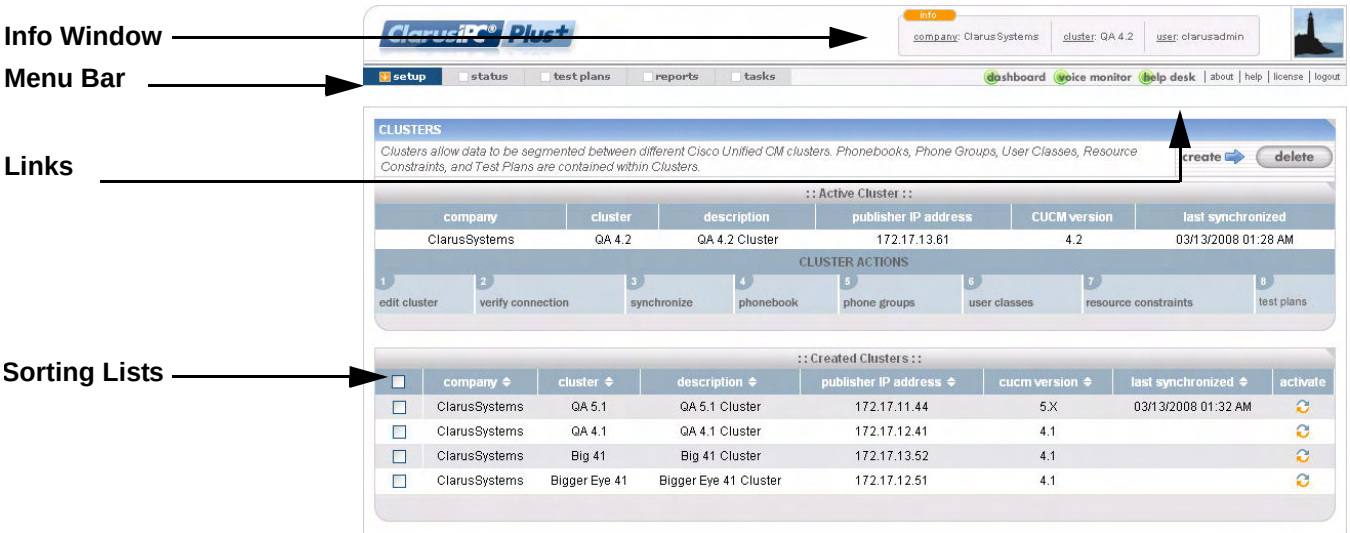


Figure 1-16 Clusters

Info Window

This window displays the current status of the system, such as the currently active Cluster and whether or not a test plan is running. The lighthouse light rotates during test plan execution and other ClarusIPC activities. This information is available for all users. When you log into a ClarusIPC system, the status of your tests and Clusters is reflected in this area.

Menu Bar

This contains the main menus for the ClarusIPC system.

Setup

Use Setup to create a Cluster or Collector definition; to set up user accounts and roles; to set up Unity systems; or to modify the Test Constraints (Phonebook, Phone Group, User Classes, Resource Constraints) for the active Cluster. A Cluster must be active to be used; and only one Cluster may be active per user. (For more information about Clusters, see Chapter 2, *Managing Clusters*.)

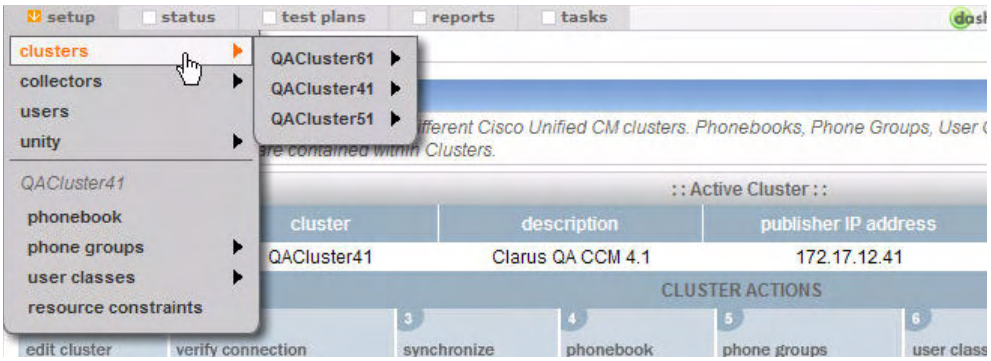


Figure 1-17 Setup Pulldown Menu

You may edit, verify, sync, augment data, or activate Clusters from the Clusters submenu.

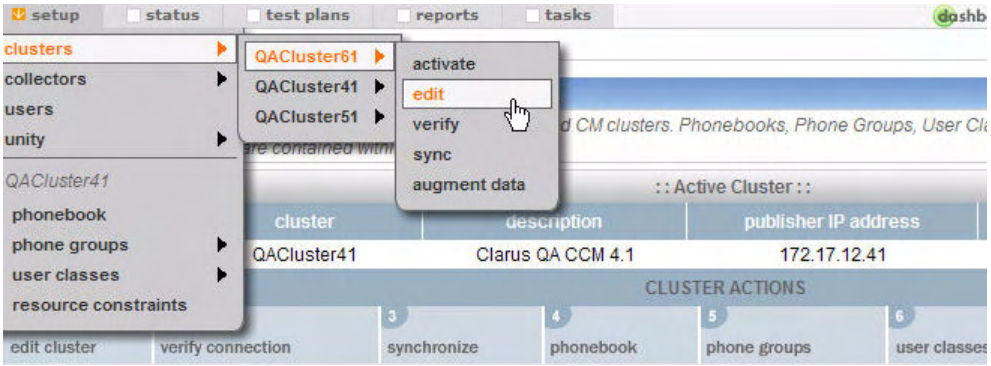


Figure 1-18 Edit Cluster Submenu

The bottom half of the Setup menu, available below the division line, displays the active Cluster, and allows you to access its Phonebook, Phone Groups, User Classes, and Resource Constraints.

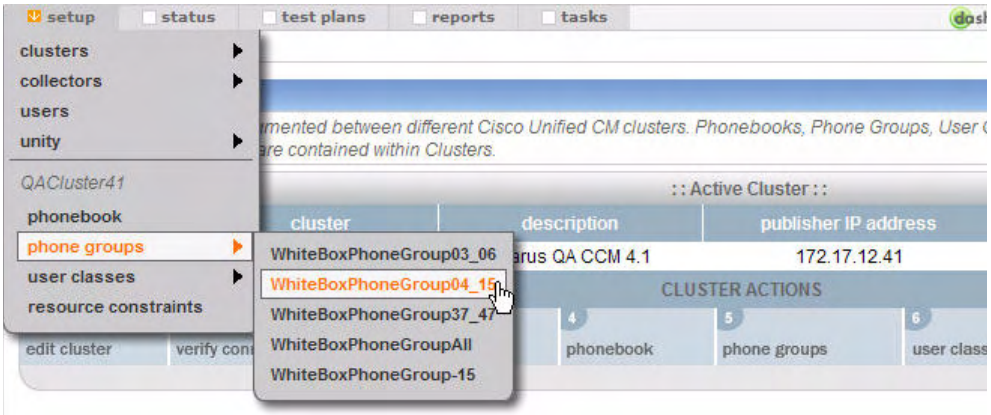


Figure 1-19 Phonegroups Submenu

Clusters

Use the **clusters** item to activate, edit, verify, sync, or augment the data of individual clusters.

For more information, see *Managing Clusters* on page 2-2.

Collectors

Use the **collectors** item to create or view Collectors, which allow you to monitor the registration status of phones at any given moment, within selected Device Pools, and across different CUCM Clusters.

For more information, see *Performance Data Collection* on page 3-1.

Users

Users allows you to change the administrator's login password, enable LDAP authentication, and define user roles. Click **users** to open the **User Accounts** window.

For more information, see *Managing Users* on page 1-22.

Unity

The **unity** item allows you to edit, verify, or sync Unity Systems associated with your ClarusIPC installation.

For more information, see *Unity Systems* on page 1-27.

Phonebook

The Phonebook stores all test phone numbers set to answer automatically. These entries will be used as test parameters for certain test types. Organize them by their call classification and include all access code digits in the dialing string.

For more information, see *Phonebook* on page 2-16.

Phone Groups

Phone Groups define sets of phones to be used by tests and reports. *Static groups* define a set list of phones that will not change as a result of a sync operation. *Dynamic groups* are created by a stored set of queries and may change after a sync operation.

For more information, see *Phone Groups* on page 2-20.

User Classes

User Classes define logical groupings of phones based on calling permissions. Tests use User Classes to verify the Class of Service assigned to each user.

For more information, see *User Classes* on page 2-28.

Resource Constraints

Resource Constraints allow you to restrict the set of phones that can serve as a supporting role in a test. Supporting phones help perform a test, but their performance is not an objective of the test.

For more information, see *Resource Constraints* on page 2-30.

Status

The Status menu lists running activities, and allows you to view their status.

Jobs

Jobs include Synchronization, Test Plan Execution, and Test Plan Staging. Jobs consume system resources, making it advisable to monitor concurrent Jobs to stay within the resource constraints of your system.

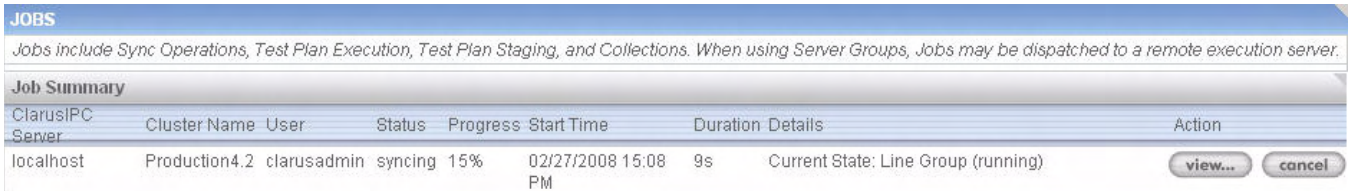


Figure 1-20 Jobs Window

Test Plans

Use Test Plans to create, edit, stage, and execute test plans. Test Plans contain tests that may be executed against your IPC environment. Test Plans must be staged before being executed, to assign appropriate resources to each test. (For more information, see *Creating Test Plans* on page 4-3.) This menu lists all defined test plans for the active Cluster.

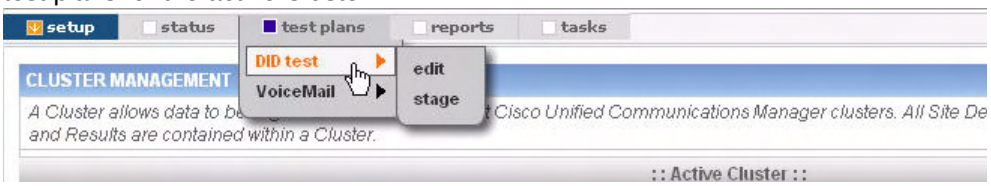


Figure 1-21 Test Plans Pulldown Menu

Selecting a specific test from the pull-down allows you to edit the test plan, stage its execution, or view the results of its last run.

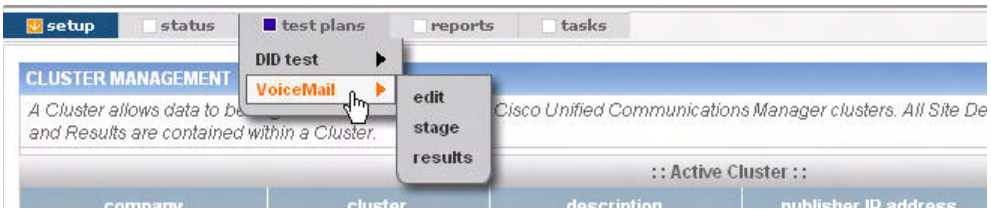


Figure 1-22 Edit / Stage / Results Submenu

Reports

Use Reports to organize and display data collected from various portions of your UC system. (For more information, see Chapter 6, *Reports*.)

Tasks

Tasks contain groups of operations (tests, synchronizations, collections, or reports), that are scheduled to occur on a one-time or recurring basis. Notification of their operational status is available via SNMP or email before, during, and upon completion of a Task. Use Tasks to schedule tests and other ongoing events. (For more information, see Chapter 7, *Tasks*.)

Links

The following links are also available:

- **Dashboard** allows you to access the Dashboard (if licensed), which offers graphic representation of your system's configuration and performance indicators. For more information, see the ClarusIPC Dashboard Guide.
- **Voice Monitor** allows you to access the Voice Monitor (if licensed), which offers the ability to monitor the configuration, performance and status information for your system. For more information, see the ClarusIPC Voice Monitor Guide.
- **Help Desk** allows you to access the Help Desk (if licensed) for remote troubleshooting. For more information, see the ClarusIPC Help Desk Guide.
- **About** displays the Release and Build numbers and Build date of the current ClarusIPC installation.
- **Help** opens the ClarusIPC User's Guide.
- **License** displays the current status of your license.
- **Logout** logs you out of ClarusIPC.

Sorting Lists

Screens with lists of items, such as Phonebook listings and available test plans, may be rearranged by header field. Each field name contains white arrows to its right, as shown in the Phonebook window below. Clicking on the arrows sorts the list in descending alphabetical order by that column's topic. A double arrow image indicates that the list has not yet been sorted by that column; a single arrow indicates the direction in which the list is sorted by that column. For example: in the image below, the list has been sorted by Name, but not by Call Classification.

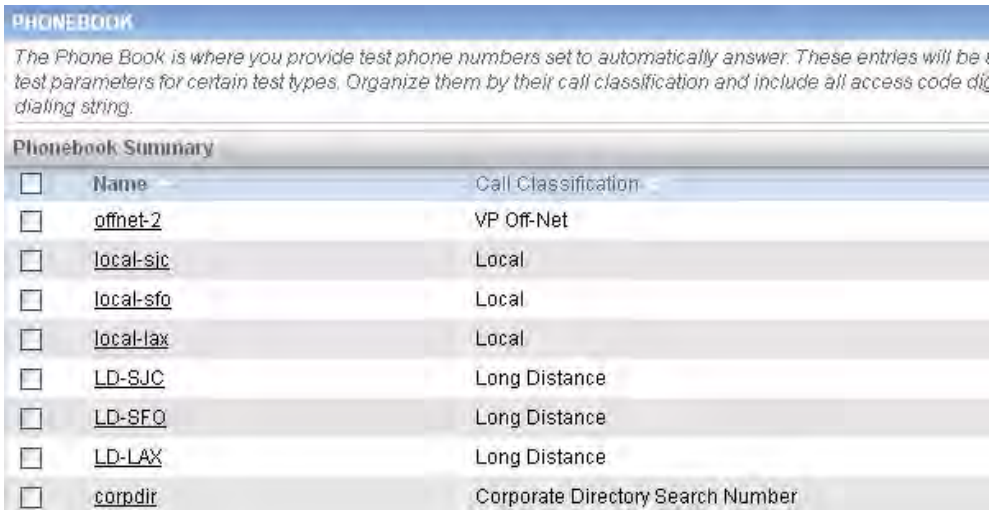


Figure 1-23 Sort by Name

Managing Users

In addition to the local clarusadmin account, access to ClarusIPC may also be controlled using a remote LDAP server. ClarusIPC uses LDAP authentication to allow you to organize and authenticate users and groups. Access to the ClarusIPC interface is controlled through the User Accounts and User Roles panes of this window.

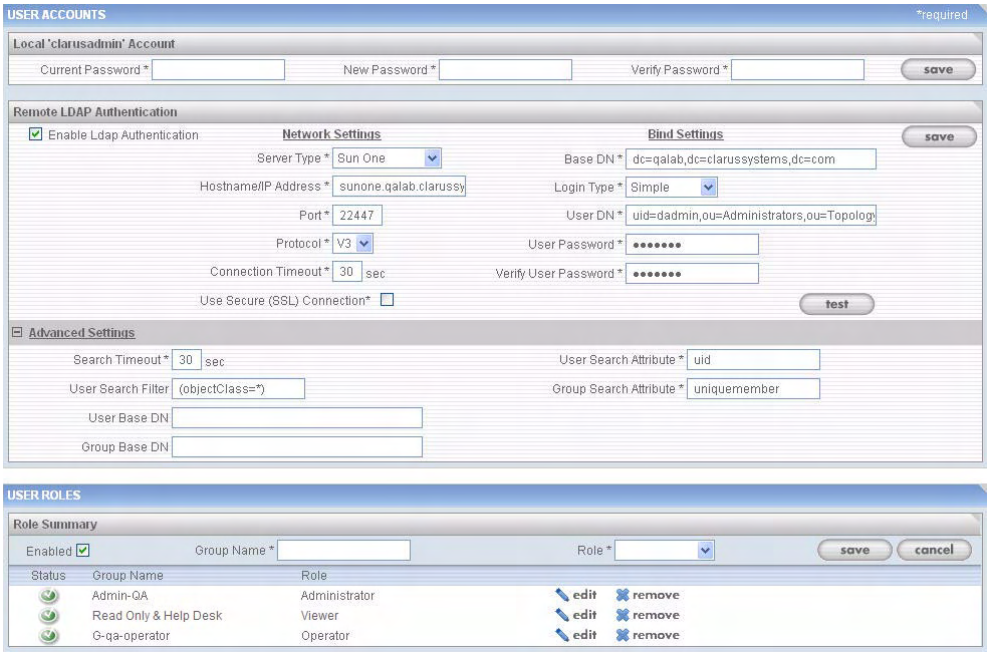


Figure 1-24 User Accounts Window

User Accounts

The User Accounts pane allows you to change the local clarusadmin account's password, and enable and configure LDAP authentication for other ClarusIPC users, if desired.

Local "clarusadmin" Account

Each ClarusIPC installation includes a default administrative account: *clarusadmin*. This pane allows the ClarusIPC Administrator to change the password for this account.

This account cannot be removed. It is useful both if you do not plan to integrate with an existing LDAP server, or if you must login when there is a problem with authenticating with your LDAP server.

(Please note that Individual users, who log in using the LDAP settings, may also be given administrative privileges.)

To change the *clarusadmin* password, enter the current password, then enter and confirm the new password, and click **save**.

Remote LDAP Authentication

Remote LDAP authentication allows you to integrate with an existing LDAP server to handle user authentication and authorization, allowing users to access ClarusIPC through their existing LDAP username and password.

NOTE: These LDAP settings are not tied to the LDAP implementation described in *Preparing CUCM* on page 1-3.

Enable LDAP Authentication

Clicking this checkbox enables LDAP authentication, and allows you to access ClarusIPC using your local accounts.

Network Settings

Network Settings define LDAP Server settings, and allow ClarusIPC to connect.

- **Server Type:** Active Directory; Sun One; or Other. Selecting Active Directory or Sun One from this dropdown menu will populate the Port, User Search Attribute, and Group Search Attribute fields with default values for the selected server.
- **Hostname/IP Address:** The hostname or IP Address of the LDAP server.
- **Port:** The port on which your LDAP server runs. The default values, based on the Server Type and SSL connection, may be overridden if desired.
- **Protocol:** The protocol version your LDAP server supports (V2 or V3).
- **Connection Timeout:** The period after which the system will stop trying to connect to the LDAP server.
- **Use Secure (SSL) Connection:** Click this checkbox if your LDAP server requires a secure connection (ldaps:). If checked, the system will update the port number, based on the server type. (The port number selected may then be overridden.)

Bind Settings

Bind Settings are required for ClarusIPC to interface with the LDAP application, and to perform queries to validate user credentials and authorization levels.

- **Base DN:** The “Distinguished Name” top level of the LDAP directory tree.
- **Login Type:** Anonymous, or Simple. The LDAP server uses a search user that navigates the LDAP tree to find a match. This user may be “Anonymous,” which means they do not need to log into the LDAP server in order to perform a search; or “Simple,” which means they must first log into the LDAP server to perform the search. (Selecting Simple enables the User DN, User Password, and Verify User Password fields described below.)
- **User DN:** The User Distinguished Name defines the login name of the search user in the case of Simple login type. (For example: *dc=subdomain,dc=domain,dc=com*. Please note that there are no spaces between text, equal signs, and commas in this string.)
- **User Password/Verify User Password:** The password for the User DN.
- **Test:** Clicking Test will verify that all required fields have a value, and issue a warning if any required fields are blank. The system then checks if a connection may be made to the LDAP server using the entered criteria, and issues an appropriate warning message if the connection fails. If all tests pass, the system will issue the message: LDAP Connection Successful!
- **Save:** Saves your settings.

Advanced Settings

Advanced Settings are used to refine search criteria for user and group login verification.

- **Search Timeout:** The amount of time (in seconds) the search should attempt to find a user before timing out. (A large LDAP might require prohibitive amounts of time to search for a user. This field allows you to set a limit on search times.)
- **User Search Filter:** Allows you to define user search filters, using standard LDAP attribute settings. For example, to limit the search to users with objectClass equal to "user," enter *(objectClass=user)* in this field.
- **User Base DN:** Allows you to define the base-location of users on your LDAP server, relative to your base DN.
  - Please note that terms containing commas and/or spaces must be enclosed with quotation marks. For example, if users are located at ou=Users, enter *ou=Users* in this field; if they are located at ou=Users, Local, you must enter *ou="Users, Local"* in the field.
- **Group Base DN:** Allows you to define the base-location of groups on your LDAP server, relative to your base DN. This field has the same rules for data entry as the User Base DN field.
- **User Search Attribute:** Defines the unique attribute of each LDAP user account. By default, this value is *sAMAccountName* for Active Directory, and *uid* (the username) for SunOne.
- **Group Search Attribute:** Defines the LDAP attribute used to contain the users who belong to the group defined in the User Role pane. When login is performed, first the user is found and authenticated, then their group memberships are found by searching through all defined groups. By default, this attribute is "member" for Active Directory, and "uniqueMember" for SunOne.

User Roles

To associate LDAP users to ClarusIPC roles, a ClarusIPC administrator must create User Roles. User Roles allow you to map the LDAP group settings to a ClarusIPC role: Administrator, Operator, or Viewer. The active Role Summary defined in this pane is assigned to all users contained in the directory defined in the Remote LDAP Authentication settings pane above.

A single user may have one or many User Roles. For example, the group AllEmployees may be assigned the Operator role, while the group Development may be granted the Administrator role. Any employee that is a member of both the AllEmployees group and the Development group will be granted both the Operator and Administrator roles.

ClarusIPC offers three User Roles from which to choose:

- **Administrators** may access all aspects of ClarusIPC, including
  - entering updated ClarusIPC license information,
  - administering User Accounts, and
  - creating and editing clusters.
- **Operators** are allowed use of all of ClarusIPC, except the ability to:
  - enter a new user license,
  - administer User Accounts, or
  - create, remove, or update a cluster.
- **Viewers** may:
  - view published Dashboards,
  - view published reports, and
  - access the Help Desk interface.
- **Change Managers** may
  - view published Dashboards,
  - view published reports,
  - access the Help Desk interface, and
  - access Line Manager.

Role Summary

- **Enabled:** Selecting this checkbox enables the User Role described in the Role Summary pane.
- **Group Name:** Maps to the Group Name field on the LDAP server.
- **Role:** Assigns a predefined Role to all members of the group defined by the Group Name field.
- **Save:** Saves any additions or changes made in the Role Summary pane.
- Cancel: Cancels any changes made, and clears the Group Name and Role fields.
- **Edit:** Loads the appropriate Group Name data in the fields above, where it may be edited.
- **Remove:** Deletes the group from the Role Summary data.

NOTE: Please note that the Group Name entered in ClarusIPC must ***exactly match*** that created on your LDAP server: the Group Names are case sensitive, and ClarusIPC does not poll the LDAP server for available Group Names.

Cisco DC Directory Integration

Although the directory is not listed, it is possible to interface directly to the DC Directory using the following default settings:

Network Settings

- **Server Type:** Other
- **Port:** 8404
- **Protocol:** V2

Bind Settings

- **Base DN:** o=cisco.com
- **Login Type:** Anonymous

Advanced Settings

- **User Search Filter:** (objectClass=*)
- **User Base DN:** ou=Users
- **Group Base DN:** ou=MultiLevelAdmin,ou=Admins
- **User Search Attribute:** cn
- **Group Search Attribute:** member

User Roles

- **Group Name:** SuperUserGroup (for example)
- **Role:** Administrator

Add the LDAP user to the SuperUserGroup MLA group.

NOTE: MLA need not be enabled to use DC Directory for ClarusIPC authentication and authorization.

Unity Systems

To include Unity Unified Messaging system data in Reports, you must configure the system in ClarusIPC, and associate it with the required Clusters.

Creating Unity Systems

To define a Unity system, select **setup > unity**, and click **create**.

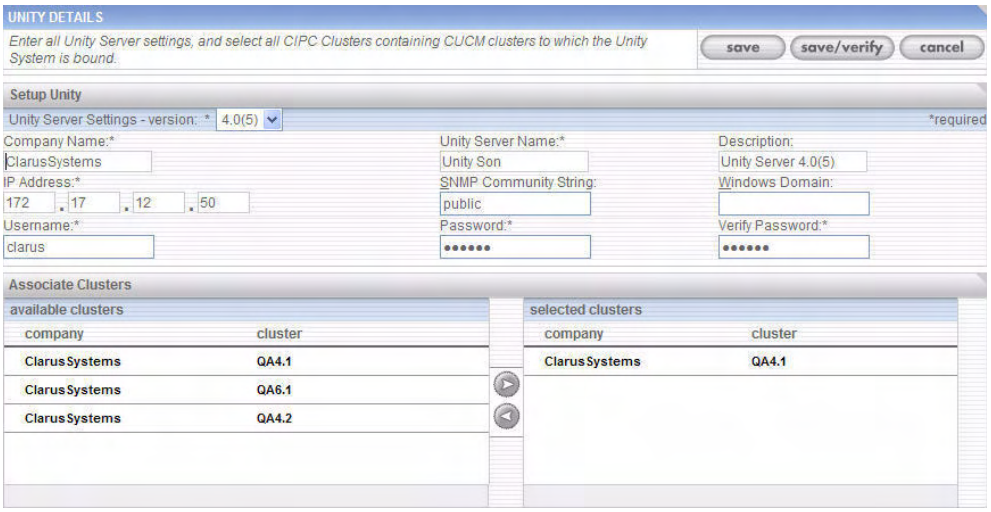


Figure 1-25 Unity Details Window

Select the Unity Server version, and enter the required information.

- **Company Name:** Name of the company at which the System is installed.
- **Unity Server Name:** User-defined name.
- **Description:** User-defined description.
- **IP Address:** IP address of the Unity Server.
- **SNMP Community String:** Read-only SNMP community string on the Unity server.
- **Windows Domain:** The Windows Domain or workgroup of your Unity System.
- **Username:** Username defined in *Set Up Unity SQL User* **on page 1-13**: *clarusunity*.
- **Password:** Password defined for the *clarusunity* user, described above.

Select Clusters with which the Unity System is associated. The system uses this mapping to generate reports. A Unity System may be mapped to multiple Clusters; and a single Cluster may be associated with multiple Unity Systems.

Click **save** to save the system as defined. Click **cancel** to cancel your work, and return to the **Unity Systems** window.

Click **save/verify** to verify the server settings by checking for JDBC access using the supplied credentials, and save the System. After clicking **save/verify**, the Verify Unity System Configuration window is opened, which lists the results of the verification.

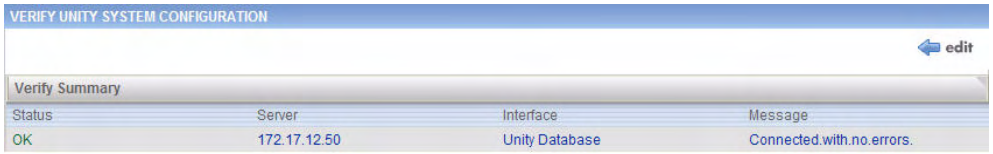


Figure 1-26 Verify Unity System Configuration Window

Synchronize

Synchronizing allows ClarusIPC to gather and store information about the Unity System, for use in Report generation. To Sync with a Unity system, select **unity > *unity system* > sync** from the **setup** menu, or click **sync** for the desired Unity System from the Unity Configurations window.

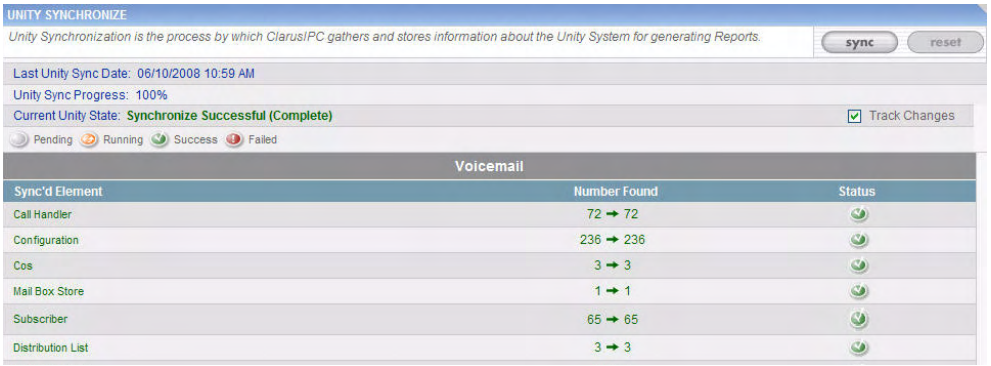


Figure 1-27 Unity Synchronize Window

Select **Track Changes** to audit changes between one Sync and the next.

Editing

To edit a System, select the System from the **setup > unity** pulldown menu, then **edit** from its pulldown menu. This will open the Unity System Configuration window. Make the required changes, and click **save**.

Deleting

To delete a Unity System, select **setup > unity** from the main menu bar, click the checkboxes to the left of the Systems you wish to delete, and click **delete**.

CHAPTER 2 CLARUSIPC CLUSTERS

ClarusIPC Clusters allow users to segment data from different Cisco Unified Communications Manager (CUCM) Clusters. This chapter outlines the steps and requirements to configure customers and Clusters within ClarusIPC. Once created, ClarusIPC allows users to easily navigate between Clusters to perform tasks, such as reporting the CUCM database; and creating, executing, and evaluating test plans.

Managing Clusters

ClarusIPC uses the concept of a Cluster, which allows a user to segment data and execute test plans. ClarusIPC allows users to create several Clusters that may be activated as needed to perform required tasks. All major sections of ClarusIPC (i.e., Test Plans), change to correspond to the active Cluster. For example, you may only edit and run test plans associated with the active Cluster. To change the active Cluster, see *Activating Clusters* on page 2-6.

When ClarusIPC is installed, a Cluster must be created before any other components of the product can be accessed. The first time you run ClarusIPC the Cluster Details screen displays:

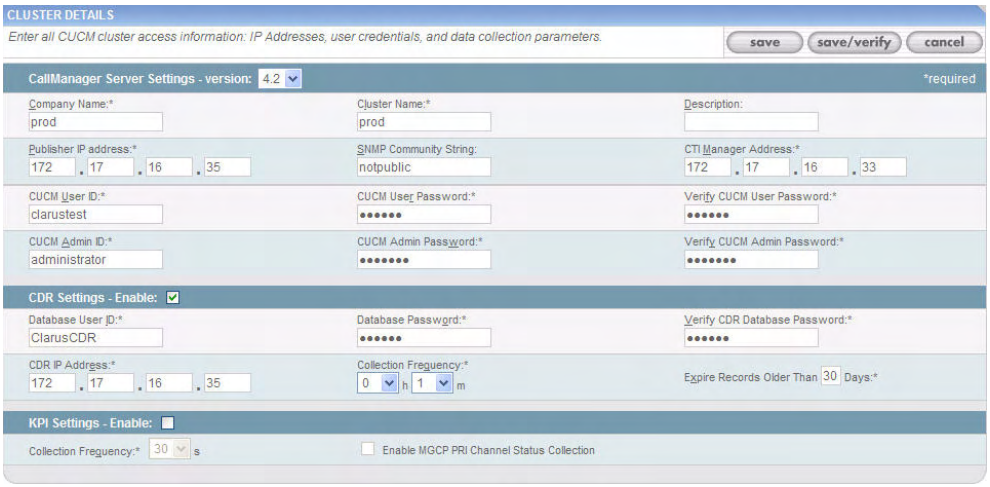


Figure 2-1 CUCM 4.X Cluster Details

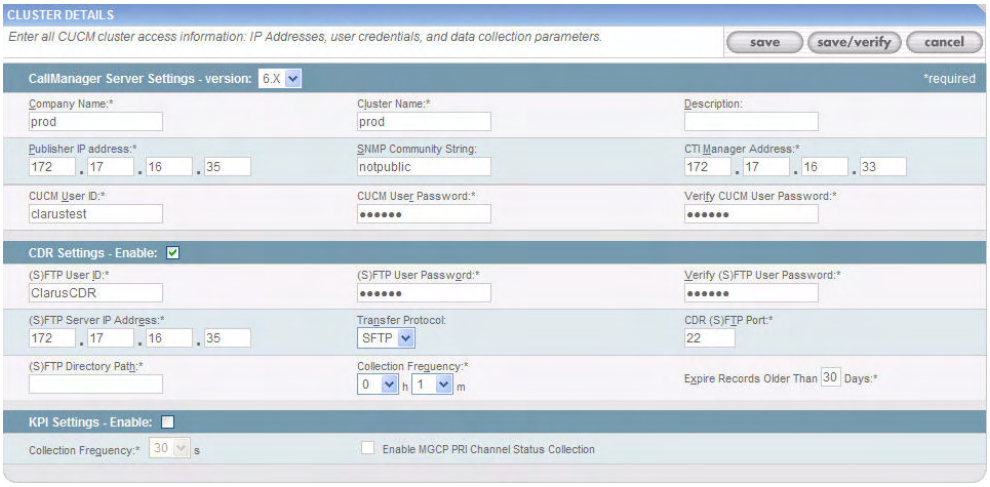


Figure 2-2 CUCM 5.X+ Cluster Details

Creating Clusters

To create a Cluster, select **setup > clusters**, then click **create**, and enter the following information:

ClarusIPC Fields	Required for CUCM: 4.X	5.X+	Cluster Details Parameters
CUCM Server Settings			**Defines Cisco Unified Communications Manager settings.**
Company Name	X	X	Name of the company at which the Cluster is installed.
Cluster Name	X	X	User-defined name; must be unique within the company.
Description	X	X	User-defined description.
Publisher IP Address	X	X	IP address of Publisher CUCM.
SNMP Community String	X	X	Read-only SNMP community string on all CUCM servers.
CTI Manager Address	X	X	IP address of the CUCM server running CTI Manager Service.
CUCM User ID	X		CUCM username with the following credentials: • Enable CTI Super Provider. • Enable CTI Application Use. • Call Park Retrieval Allowed. (This is the *clarustest* user created in *Create CUCM 4.X User Accounts* on page 1-4.)
CUCM User ID		X	CUCM username with the following credentials: • Username must be a member of the Cisco Standard CTI Allow Control of All Devices and Standard CTI Enabled groups. • Enable CTI Application Use. • Call Park Retrieval Allowed. (This is the *clarustest* user created in *Create CUCM 5.X+ User Accounts* on page 1-5.)
CUCM User Password	X	X	CUCM username password.
CUCM Admin ID	X		CUCM Administrator user ID or LDAP user ID when MLA is enabled.
CUCM Admin Password	X		CUCM Administrator password or LDAP password when MLA is enabled.

ClarusIPC Fields	Required for CUCM: 4.X	5.X+	Cluster Details Parameters
CDR Settings Enable			**Enables use of CDR parameters.**
Database User ID	X		SQL server user with read-access for the CDR database. (This is the *claruscdr* user created in *Configure CDR Access for CUCM 4.X* on page 1-6.)
Database Password	X		Password for SQL server user.
CDR IP Address	X		IP address of CDR database server.
(S)FTP User ID		X	(S)FTP User with Read/Write/Delete access to the directory where CDR/CMR records are to be written. (This is the *claruscdr* user created in *Configure CDR Access for CUCM 5.X+* on page 1-9.)
(S)FTP User Password		X	Password for the (S)FTP User ID.
(S)FTP Server IP Address		X	IP address of (S)FTP Billing server.
Transfer Protocol		X	Transfer protocol for the Billing server: secure FTP (SFTP) or insecure FTP.
CDR (S)FTP Port		X	TCP port of (S)FTP Billing server. Recommend using default values.
(S)FTP Directory Path		X	Absolute (S)FTP directory for the location of CDR files on the Billing server.
Collection Frequency	X	X	Frequency with which ClarusIPC will collect data from the (S)FTP server.
Expire Records Older Than			Number of days that CDR records will be saved.
KPI Settings Enable			**Enables KPI record collection.**
Collection Frequency	X	X	Frequency with which ClarusIPC will collect Key Performance Indicator counters, for use by Voice Monitor and Dashboard.
Enable MGCP PRI Channel Status Collection			Enables collection of status for all channels on all MCGP PRI Devices.

NOTE: To use Voice Monitor, Dashboard, or to view Call History from Help Desk, CDR and KPI collection must be enabled. For more information about these ClarusIPC applications, please see the appropriate Guides.

NOTE: KPI collection can generate a large amount of data. Adding the status of all PRI channels for gateways in selected Device Pools can increase the amount of data, and therefore the load, substantially. Unless you must monitor the specific state of a particular gateway PRI channel, leave the MGCP PRI Channel Status Collectors option unchecked to avoid unnecessary collection and improve performance.

Saving Clusters

You may save a Cluster, or save and verify a Cluster simultaneously.

Save stores the Cluster without verifying the parameters and configuration against the CUCM Cluster. **Save / Verify** saves the Cluster, and verifies that the user accounts are configured properly for the created Cluster. See *Verifying the Connection* on page 2-6 for more information.

After saving, the **Clusters** screen opens:

Figure 2-3 Clusters Window

Cancel discards any changes you may have made to the information on the screen, and returns you to the **Clusters** page.

Editing Clusters

A Cluster must be active to be edited. To edit a Cluster:

1. Select the Cluster from the **setup > clusters** pulldown menu, then **edit** from its pulldown menu. This will activate the selected cluster, and open the Cluster Details window. Make the required changes, and click **save**.
2. Or, from the Clusters window, click the **activate** button for the Cluster you wish to edit, then click **edit cluster** to open the Cluster Details window.

Deleting Clusters

You may delete Clusters that are no longer required, but a Cluster must be inactive to be deleted. Upon deleting the Cluster, all information specific to that Cluster will be deleted (test plans, and results). There must always be one Cluster defined; therefore, you cannot delete the only Cluster. From the Clusters screen, check the box for each inactive Cluster you wish to delete and click **delete** in the top right of the Clusters window. Select **confirm** from the displayed window.

Activating Clusters

To activate a Cluster, click the activate button to the right of the Cluster's row in the Clusters window, or select **clusters > *cluster name* > activate** from the **setup** menu. The Cluster will now be displayed as active in the **setup** menu, and will be listed in the bottom half of the menu, with its associated Phone Groups, Resource Constraints, Phonebook, and Test Plans for easy access.

Activating the Cluster recalls its status from your last synchronization. It is recommended that you synchronize reactivated Clusters with CUCM to insure that you are working with the latest CUCM data. See *Synchronizing With CUCM* on page 2-9 for more information.

Verifying the Connection

To help avoid configuration issues, ClarusIPC allows you to verify that the Cluster Details parameters are correct by attempting to connect to the CUCM. The verification process includes the CUCM server, interface (protocol), and the verification status message. It is performed for each CUCM server within a Cluster as follows:

Table 2-1 Interfaces

Interface	Verify Action
AXL	Verifies the ClarusIPC application has connectivity to the CUCM Publisher database with the provided user credentials
SNMP	Verifies the SNMP community string is configured correctly for all CUCM Servers within the Cluster
CTI Manager	Authenticates using JTAPI to the designated CTI Manager
CDR	CUCM 4.X: Verifies the connection using SQL. CUCM 5.X+: Logs into the (S)FTP server to verify the connection.

For CUCM 5.X+ clusters, the verification process will attempt to connect to the defined (S)FTP server, defined in the cluster details. It will not use SQL for verification.

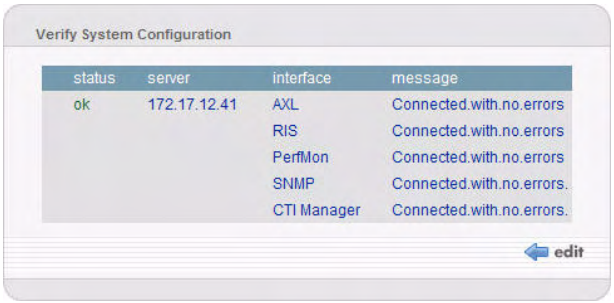
NOTE: You must be connected to the network that allows access to all interfaces for the verify connection to complete without error.

1. To verify a Cluster, select **clusters > *cluster* > verify** from the **setup** menu, or click **save/verify** on the **Cluster Details** window.

The following screen displays:

Figure 2-4 Verifying Cluster

After verification completes, the following screen displays:



status	server	interface	message
ok	172.17.12.41	AXL	Connected.with.no.errors
		RIS	Connected.with.no.errors
		PerfMon	Connected.with.no.errors
		SNMP	Connected.with.no.errors.
		CTI Manager	Connected.with.no.errors.

Verify that all interfaces have passed. Click **edit** to return to the Clusters page to correct your configuration. In most cases the configurations are set correctly and the verification will return “Connected with no errors” in the message column.

Error Messages

A failure can occur if network connectivity between ClarusIPC and the designated server is blocked for the specified protocol. (For network connectivity requirements, see *Network Connectivity Requirements* on page 1-2.)

Some common failures and possible causes include:

AXL Failure

- The AXL Service is not running on the Publisher CUCM server.
- The CUCM Admin user or password was entered incorrectly.
- The AXL service is not reachable.

To test AXL failures, enter the following URLs in a browser, as appropriate:

AXL - RIS failure (device registration status or IP addresses are not collected)

For CUCM version 4.X, enter

```
http://<ccmserver>/soap/astsvc.dll
```

For CUCM version 5.X or 6.X, enter

```
https://<ccmserver>/realtimeservice/services/RisPort
```

AXL - PerfMon failure (key performance indicators are not collected)

For CUCM version 4.X, enter

```
http://<ccmserver>/soap/astsvc.dll
```

For CUCM version 5.X or 6.X, enter

```
https://<ccmserver>/perfmonservice/services/PerfmonPort?wsdl
```

AXL - Database failure (configuration data is not collected during Sync)

For CUCM version 4.X, enter

```
http://<ccmserver>/CCMApi/AXL/V1/SOAPISAPI.dll
```

For CUCM version 5.X or 6.X, enter

```
https://<ccmserver>/axl
```

This will prompt you for a username and password, then redirect you to an XML page similar to the one below:

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encod-
ing/">
SOAP-ENV:Body>
- <SOAP-ENV:Fault>
  <faultcode>SOAP-ENV:Client</faultcode>
  <faultstring>The AXL API service only accepts the HTTP POST
  request type.</faultstring>
  </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

CDR Failure (CUCM 4.X)

- The CDR database user or password was entered incorrectly.
- The CDR IP address was entered incorrectly.
- The CDR database user does not have at least Read-Only access to the CDR database.

CDR Failure (CUCM 5.X+)

- The IP address of the (S)FTP server was entered incorrectly.
- The User/Password of the (S)FTP server does not have permission to read from (S)FTP server.
- The path specified on the (S)FTP server cannot be accessed or does not exist.
- The port for the (S)FTP server is incorrect.

CTI Failure

- The CUCM User or password was entered incorrectly.
- The Enable CTI Application Use flag is not set on the CUCM User account provided.
- The CTI Manager Service is not running on or responsive from the designated CUCM Server.

SNMP Failure

- The SNMP service is not running on one or more CUCM servers.
- The community string entered is not configured for, at minimum, Read-Only permissions

If you have made any changes to your Cluster, verify and adjust the Cluster until it passes. Additional Clusters may be created at any time by selecting **create** from the **Clusters** screen, and following the steps described in this chapter. New Clusters appear in the **Clusters** window and the **setup > clusters** submenu.

After making changes to existing Clusters, or creating a new Cluster, you should synchronize with CUCM.

Synchronizing With CUCM

The Synchronization operation (Sync) allows ClarusIPC to gather critical data from the Communications Manager database and registered IP Phones within the CUCM Cluster. The data gathered during this process supports Test Plan creation, staging, and execution reports. Sync updates the data on your testing machine to match the current configuration of the network you are testing.

ClarusIPC supports synchronization against a CUCM Cluster. As this process requires gathering a large amount of data, it may take a significant amount of time. When only a portion of the CUCM Cluster has been changed since the last Sync, you may perform a Targeted Sync to reduce the time required.

A Sync with CUCM collects the following data:

Table 2-2 Sync Data Collected

Target Sync	Interface	Data Collected
CUCM DB Elements	AXL	Configuration data from the CUCM Publisher database
Real-time Information	AXL/SNMP	Real-time status information such as device registration and server process lists
Phone Details	HTTP	Status information from each phone Web interface.

Sync should be performed for the following conditions:

- Following the creation of a new Cluster.
- Following changes to the CUCM Cluster, including phone addition, subtraction, or editing.
- Following the addition of new phones registered to the CUCM Cluster.

To execute synchronization, the following conditions must be present:

- ClarusIPC must be connected to the CUCM network. See *Network Connectivity Requirements* on page 1-2 for more information.
- Cluster Details parameters must be correct and verified. See*Creating Clusters* on page 2-3 for more information.

If the Active Cluster has been synchronized, the date and time will be displayed in the **last synchronized** column. This field is blank if no Sync has been executed.

Initiating a Sync

1. To initiate a Sync, select **synchronize** from the **Clusters** window, or select **setup > clusters > *cluster* > sync** from any screen:

The following screen displays:

Synchronize

Target Synchronize

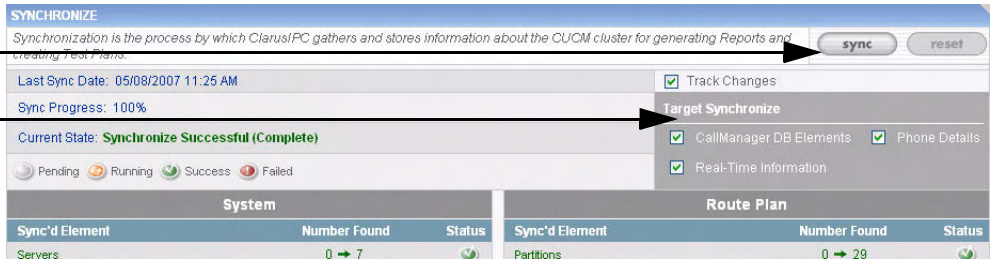


Figure 2-5 Sync

NOTE: If this is the first synchronize operation after Cluster creation, Sync element counts found will be zero, and Last Sync Date and Current Status will be blank.

2. Click **sync** to begin synchronization. If you wish to perform a more selective sync, uncheck data you do not wish to track in the **Target Synchronize** pane.

During Sync, the window displays synchronization progress, as shown below:

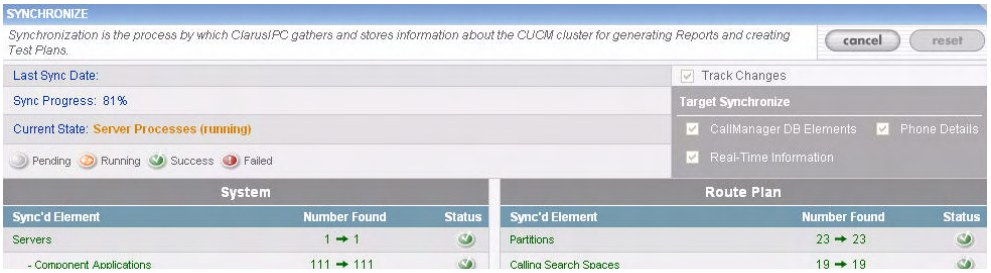


Figure 2-6 Synchronization Status

As the Sync progresses, a synced element's status will change from **Pending** (grey) to **Running** (orange) to **Success** (green) or **Failed** (red).You can see which element is currently running in the **Current State** field. The **Sync Progress** field contains the percentage of completion.

NOTE: The time required to run a Sync will vary depending upon the size and complexity of the CUCM Cluster, the number of devices configured and registered, and whether you have chosen to perform a Targeted Sync or a complete Sync.

NOTE: If any item fails to successfully synchronize, your ability to view reports, or create and execute test plans, may be affected. Troubleshoot this problem immediately, and, if you cannot resolve it, contact the Clarus Systems Customer Support Group for assistance.

Track Changes

Selecting **Track Changes** generates a *Snapshot* of this sync operation for subsequent Change Tracking reports. Note that Snapshots include all aspects of the cluster configuration. Snapshots are not selective, nor may they be customized.

All device configuration changes, with the exception of the following volatile attributes, will be tracked:

- Last registration time
- Last status update time
- Status reason code

NOTE: For greater time efficiency, do not select **Track Changes** unless you plan to use the Change Tracking reports.

Target Synchronization

Target Synchronization allows you to synchronize only selected types of information. Performing a Targeted Sync, rather than a Complete Sync, will collect a much smaller dataset, and consume much less time.

In a Targeted Sync, selecting both Real-Time Information and Phone Detail will query ***only*** those phones which have reregistered since the last Sync for new information. Selecting Phone Detail and not Real-Time Information will collect ***all*** Phone Detail from ***all*** available registered phones. Please note that selecting both Real-Time Information and Phone Detail enables the more efficient Sync.

Viewing Sync Details

After synchronization completes, you can display a list of phones that did not respond to the request for phone detail data, were not registered, or which had web access disabled. To view this information, click the **view details** button

View Details

System

Sync'd Element	Number Found	Status
Servers	7 → 7	
- Component Applications	817 → 817	
- Process Status	58 → 58	
Call Managers	7 → 7	
Call Manager Groups	12 → 12	
Date/Time Groups	9 → 9	
Regions	13 → 13	
Device Pools	20 → 20	
Locations	9 → 9	
Device Defaults	71 → 71	
Enterprise Parameters	69 → 69	
SRST	8 → 8	

Route Plan

Sync'd Element	Number Found	Status
Partitions	29 → 29	
Calling Search Spaces	30 → 30	
Route Filters	20 → 20	
Route Groups	10 → 10	
Route Lists	11 → 11	
Route Patterns	16 → 16	
Translation Patterns	487 → 487	
Directory Numbers	486 → 486	
AAR Groups	10 → 10	
Time Period	7 → 7	
Time Schedule	6 → 6	
Line Group	7 → 7	
Hunt List	7 → 7	
Hunt Pilot	8 → 8	

Devices

Sync'd Element	Number Found	Status
Phones view details	123 → 123	
- Registration	3 → 3	
- Details	3 → 3	
Device Models	76 → 76	

Features

Sync'd Element	Number Found	Status
Call Park Numbers	7 → 7	
Call Pickup Numbers	8 → 8	
MeetMe Patterns	8 → 8	
Voice Mail Profiles	10 → 10	

Figure 2-7 Synchronization Completion

The following screen displays:

Phone Summary	
Category	Count
Installed	42
No Longer Registered	1
Unreachable	3
Web Access Disabled	0
Recently Discovered	0

Phone Detail						
Device Name	Description	DN	IP Address	Model	Discovered	Last Registration

Figure 2-8 Phone Details Summary

Clicking on the following items will provide more detailed information:

- **Installed:** number of phones installed in the CUCM database.
- **No Longer Registered:** phones where the registration status has changed from the previous sync.
- **Unreachable:** phones whose web server did not respond, preventing collection of Phone Detail information.
- **Web Access Disabled:** phones that are configured with Web Access disabled preventing ClarusIPC from collecting detail information.
- **Recently Discovered:** phones discovered online since the last Synch.

NOTE: Phones which are shown as No Longer Registered, Web Access Disabled, or Unreachable, might be excluded from participating in certain tests, and will not have complete information in Phone Reports.

Device Detail						
Name	Description	Directory Number	IP Address	Phone Model	Date Discovered	Last Registration Date
ATA0006D7A5798B	QA Phone 29 - ATA 186	01029		Cisco ATA 186		
ATA06D7A5798B01	QA Phone ATA Line 2	02041		Cisco ATA 186		
SEP000CF1406ADF	Auto 82005	82005		Cisco IP Communicator		
SEP000D288E48A4	QA Wireless 32 - 7920	430321		Cisco 7920		
SEP000D288E5978	QA Wireless 30 - 7920	430301		Cisco 7920		
SEP000D288E597A	QA Wireless 31 - 7920	430311		Cisco 7920		
SEP000D603A44AE	Auto 82008	82008		Cisco IP Communicator		
SEP000DBDBEF5D1	QA Phone 05 - 7960	440051		Cisco 7960		
SEP000DBDBEF6DE	QA Phone 08 - 7960	440081		Cisco 7960		
SEP000DBDBEF703	QA Phone 48 - 7960	440481		Cisco 7960		

Figure 2-9 Phone Summary Details

Cancelling a Sync

If you cancel a Sync in progress, the database will be rolled back to its previous state and you can continue using the application. If this is the first Sync, there will be no available data. Following the completion of the **cancel**, select **reset** to refresh your display with the most current available data. The **Last Sync Date** will contain the date and time of the last completed sync.

Cancel / Reset

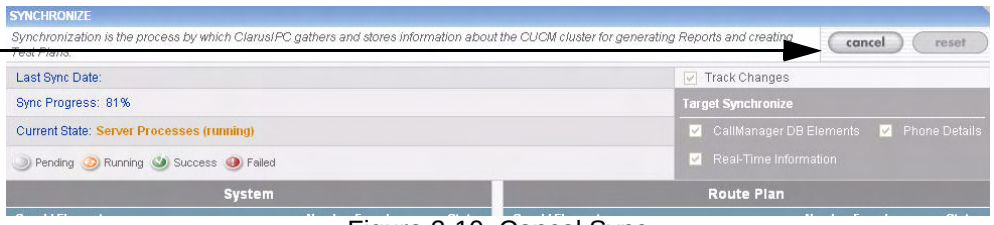


Figure 2-10 Cancel Sync

Synchronization and Upgrading from CUCM 4.X to 5.X+

Due to significant changes in the Windows and Linux CUCM platforms, it is necessary to first perform a Sync against the intermediate 4.1, 4.2, 4.3 upgrade versions (4.1u, 4.2, 4.3u) before moving to CUCM 5.X+. Doing so will preserve all data for Change Tracking reports between these versions, and prevent the loss of previously built test plans.

For more tips on upgrading from CUCM 4.X to CUCM 5.X+, please contact *ClarusIPC Customer Support*.

Augmenting Device Data

Data Augmentation allows you to add extra data fields to the system on a per-phone basis. This option is often necessary to support the Direct Inward Dial test, and may also be useful in the Call Handling and Detailed Phone Inventory reports. Fields that may be added to existing data include:

- Alternate DID 1: Use when your internal directory numbers do not have any overlap with the assigned direct inward dial numbers.
- Alternate DID 2: Use when you have additional DID numbers (such as 800 numbers) which also route to your user directory numbers.
- User Data 1
- User Data 2
- User Data 3
- User Data 4
- User Data 5

Augmented data may be added before the initial Sync, and is stored independently of the Sync data. You may import these extra fields even before the phones themselves have been discovered during Sync. In addition, if a phone is removed from the CUCM system, and from ClarusIPC as a result of a Sync, the augmented data for that phone will remain in the ClarusIPC system until it is explicitly removed.

Please see *Direct Inward Dial* on page 4-26 for more information on the Alternate DID fields.

Importing Data

To augment data, download the SampleAlternateDIDData.xml template file from the **Augment Data** window, and edit it in Excel as desired. Available fields may be populated, or left blank, as needed. The only requirement is that a given row contain:

- DN
- Device Name
- Partition Name

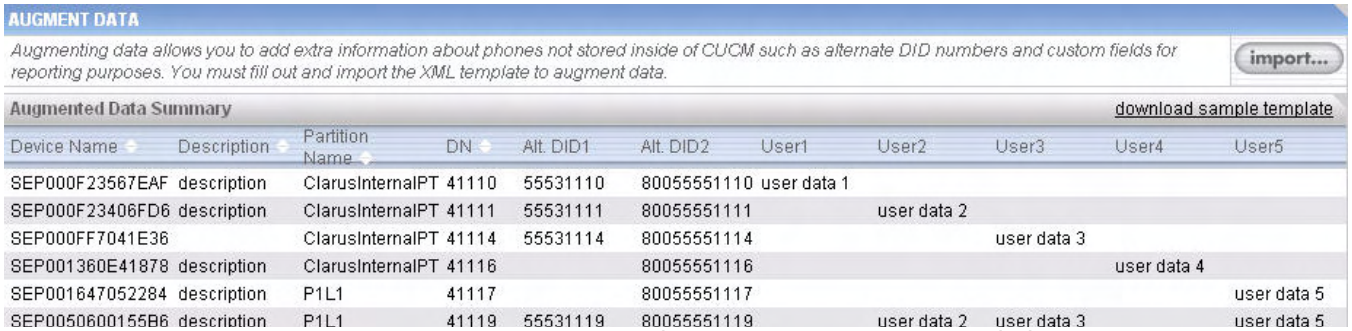
You may also generate the **Reports > Special > Augment Data** report, and use it as a starting point for populating the SampleAlternateDIDData.xml file. This report lists all Device Names, and their DNs and Partition Names for the selected Phone Group. Simply copy and paste the original data from the Augment Data report into the SampleAlternate file, make any necessary changes, and upload the saved file.

	A	B	C	D	E	F	G	H	I	J	
1	DN	Device Name	Partition Name	Alternate DID 1	Alternate DID 2	Description	User Data 1	User Data 2	User Data 3	User Data 4	Use
2	41110	SEP000F23567EAF	ClarusInternalPT	55531110	80055551110	description	user data 1				
3	41111	SEP000F23406FD6	ClarusInternalPT	55531111	80055551111	description	"	user data 2			
4	41114	SEP000FF7041E36	ClarusInternalPT	55531114	80055551114	"	"	"	user data 3		
5	41116	SEP001360E41878	ClarusInternalPT	"	80055551116	description	"	"	"	user data 4	
6	41117	SEP001647052284	P1L1	"	80055551117	description	"	"	"	"	user
7	41119	SEP0050600155B6	P1L1	55531119	80055551119	description	"	user data 2	user data 3	"	user
8											

Figure 2-11 Augmenting Data File

NOTE: The DN, Device Name, Partition Name, Alternate DID 1 and 2, and Description columns must be used as described, as these fields have a specific use in the Direct Inward Dial test, to allow calling DID numbers which do not directly overlap with the phone Directory Number. The User Data 1-6 fields may be used for any purpose desired, such as Site Name, Building, Floor, Jack Number, or Asset ID. User Data 1-5 fields will appear in Reports such as Call Handling and Detailed Phone Inventory.

Once imported, ClarusIPC performs basic validation to ensure that the field values are acceptable. A confirmation window is opened to show that the file was successfully imported, and the data is displayed in a tabular layout.



Device Name	Description	Partition Name	DN	Alt. DID1	Alt. DID2	User1	User2	User3	User4	User5
SEP000F23567EAF	description	ClarusInternalPT	41110	55531110	80055551110	user data 1				
SEP000F23406FD6	description	ClarusInternalPT	41111	55531111	80055551111		user data 2			
SEP000FF7041E36		ClarusInternalPT	41114	55531114	80055551114			user data 3		
SEP001360E41878	description	ClarusInternalPT	41116		80055551116				user data 4	
SEP001647052284	description	P1L1	41117		80055551117					user data 5
SEP0050600155B6	description	P1L1	41119	55531119	80055551119		user data 2	user data 3		user data 5

Figure 2-12 Augment Data Window

NOTE: If an invalid combination is entered (i.e. the DN doesn't exist on the Device Name), no error will be posted. Please be certain to manually validate any augmented data.

Updating Imported Data

To update an entry, simply import an edited XML file. Existing entries with the same Device Name, Partition, and DN will be overwritten with the new fields.

To remove a record, import an edited XML file with only the Device Name, Partition, and DN fields populated for the selected device.

Creating System Elements

System Elements include:

- Phonebook
- Phone Groups
- User Classes
- Resource Constraints

Phonebook

The Phonebook stores all dialing strings used for tests. Each Phonebook entry consists of a name, a description, a call classification, and dialing strings. These are calling permissions that may be assigned to User Classes.

Call Classifications

The following default call classifications are available:

- Local
- Long Distance
- International
- Toll-Free (800,866,877,888)
- Service numbers (311,411,911)
- Pay-per-call (976,900, some Caribbean)
- Emergency

System call classifications are also available for use by specific tests, as follows:

- **VP OffNet:** Voice protocol OffNet tests
- **AutoAttendant Number:** Directory Handler tests
- **Corporate Directory Search Number:** Softkey functions corporate directory tests

The Phonebook also allows you to create custom call classifications.

Dialing Strings

The dialing string represents the exact sequence of key strokes entered by an enduser, and may include:

- 0-9
- #
- , (one-second pause per each comma)
- *

NOTE: You may add multiple dialing strings for each call classification.

Adding a Phonebook Entry

You may add Phonebook entries manually or by importing a file. For information about importing, see *Importing a Phonebook* on page 2-19.

1. To create a new Phonebook entry, select **phonebook** from the **Clusters** screen, or select **setup > phonebook** from any screen.

NOTE: The Cluster must be active to add a Phonebook. The active Cluster is listed in the bottom half of the setup menu, above the **phonebook** entry. If this is not the Cluster to which you wish to add a Phonebook, select **setup > clusters > *cluster* > activate** to activate the appropriate Cluster.

The following screen displays:

Create

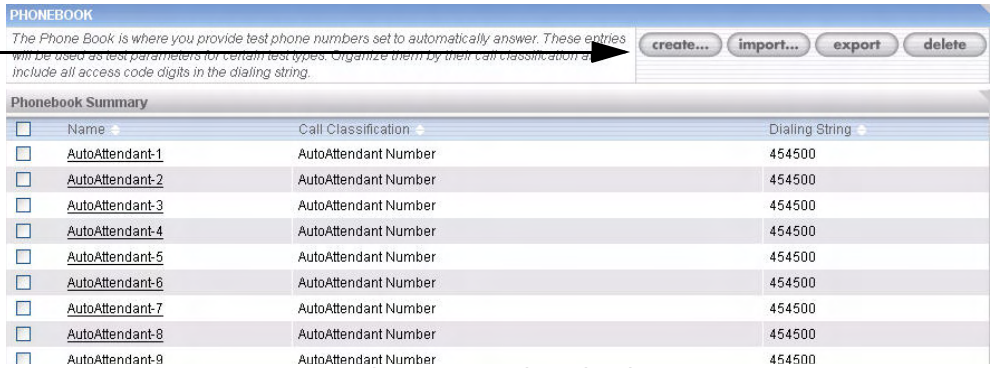


Figure 2-13 Phonebook

2. Select **create** to open the **Create Phonebook Entry** window.

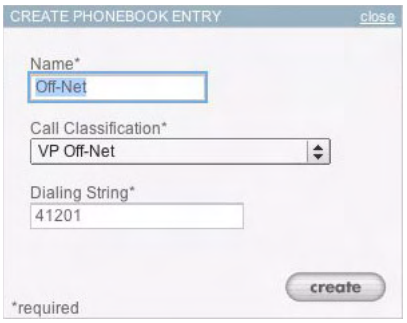


Figure 2-14 Create Phonebook Entry

3. Complete the following fields:

Table 2-3 Phonebook Descriptions

Field Name	Values	Description
Name	Up to 30 Alphanumeric Characters	This name must be unique; for example, sf415-info.
Call Classification	Up to 30 Alphanumeric Characters	Select from the menu of provided Call Classifications. To add a new one, scroll to the bottom of the list and select **New Classification.** Enter the new classification. To return to the list of existing Call Classifications, select **Choose**.
Dialing String	• Maximum Number of digits = 30 • 0-9 • # • , (one-second pause) • *	Example: 9,01144207552345#

When you are finished, click **create**.

Editing a Phonebook

1. To edit an existing Phonebook, you must first activate the Cluster to which the Phonebook is assigned. Click **setup > clusters > *cluster name* > activate** to activate the Cluster, and display its name in the bottom half of the **setup** menu.
2. Select **setup > phonebook** to open the Phonebook window.
3. Click the Phonebook entry you wish to edit in the main **Phonebook** window to open the **Create Phonebook Entry** window.

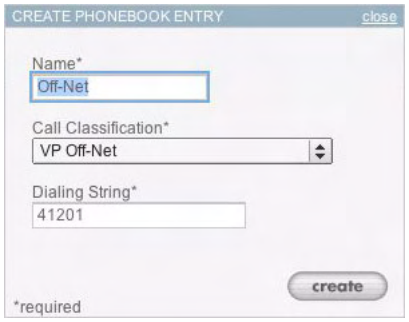


Figure 2-15 Edit Phonebook

4. Change the information and click **create**. You are returned to the **Phonebook** screen.

NOTE: Changing the call classification can affect existing Call Permission tests.

Exporting a Phonebook

ClarusIPC allows you to export a Phonebook, which may be imported to other Clusters on the same or another system. This eliminates the need to create new Phonebook entries for each newly created Cluster. The export option will export all entries created within a Phonebook.

1. Select **setup > phonebook.**
2. Click **export** to open the **File Download** window:

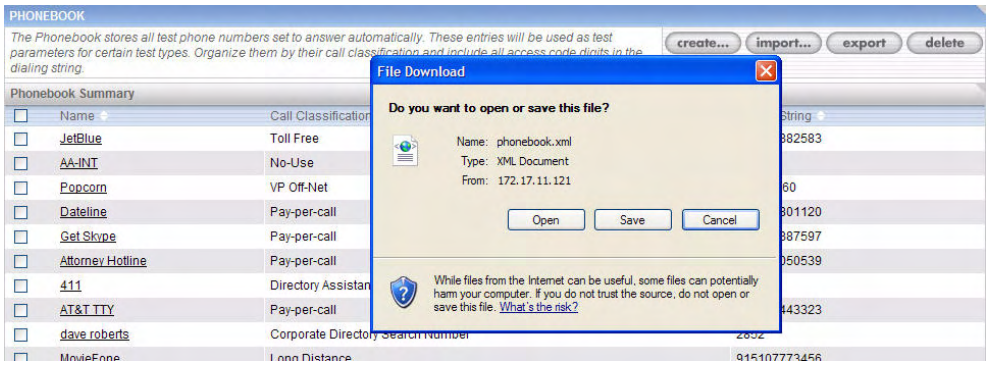


Figure 2-16 Export Phonebook

3. Click **Save**.
4. Select a location to save the exported file, and click **Save**.

NOTE: Exported Phonebooks are stored in XML. These files may be edited before importing.

Importing a Phonebook

ClarusIPC allows you to import a Phonebook from another Cluster or from another ClarusIPC user, eliminating the need to create Phonebooks for each Cluster.

NOTE: The import option overwrites all entries previously contained within a Phonebook.

1. Select **setup > phonebook**, and click **import** to open the **File Upload** window.

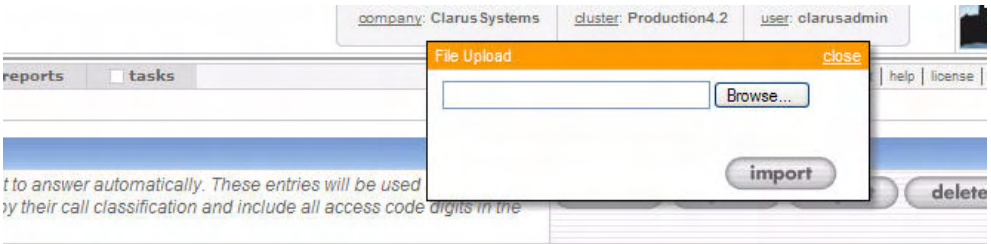


Figure 2-17 Import Phonebook

2. Use **browse...** to locate the desired Phonebook file and click **update**. The imported Phonebook is now shown in the Phonebook window.

Deleting Phonebook entries

1. Select **setup > phonebook** to open the **Phonebook** window.

Delete

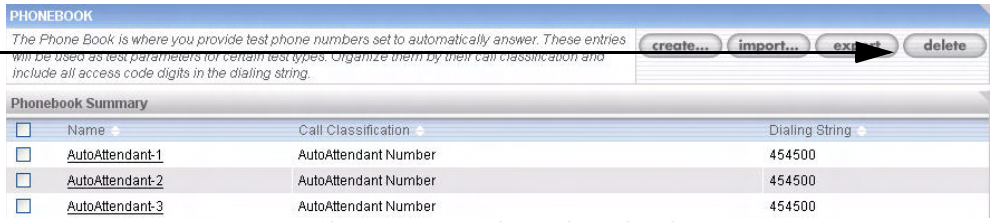


Figure 2-18 Delete Phonebook

2. Select the checkboxes of the items you wish to delete, and click **delete**.
3. To delete all entries within the Phonebook, select the checkbox in the top left, next to the name column, then click **delete**.

NOTE: A confirm window will be launched for all deletions.

Phone Groups

A Phone Group is a logical grouping of phones, created by the ClarusIPC user.

Phone Groups can serve a multitude of functions and can be created using dynamic or static phone selection methods.

Static Phone Groups

Static phone selection allows you to select a specific group of phones, which will remain unchanged through subsequent sync operations. If a Phone Group is created using the static method, modifications to the Group may be required when new phones are added to or removed from the ClarusIPC cluster. To edit the Phone Group, select and deselect the specific set of phones desired.

Pros: This grouping allows the user to identify groups in the phone populations by phone, rather than by attribute. If the phones' configurations are changed, it will not be reflected in a Static Phone Group. If the list of phones to be included in this group changes, you must make those changes manually. For example, Phone Groups can be used for the DID test. Likely, the list of phones to be used for the test is known in advance; no CUCM configuration phone or DN parameter identifies DID. Phones in this group will change only if you update the group manually.

Cons: This grouping is more time consuming to set up and maintain, in that a list of individual phones must be maintained, rather than a list of phone attributes. It is not recommended in volatile rollout environments, where configurations are constantly changing, and you want to perform regression testing with the same group of phones. It is also not recommended when Phone Group selection options are insufficient to identify a set of phones (i.e. if more than two queries are needed to identify the group).

Dynamic Phone Groups

Dynamic phone selection allows you to select phones based upon attributes: ClarusIPC automatically discovers and selects phones matching the specified attributes, recreating the group after every Sync. With the dynamic method for device selection, you do not need to add new phones to the Phone Group as they are installed and come into service. ClarusIPC automatically discovers and adds new phones that match the selected attributes.

Pros: This grouping allows for reduced maintenance over group members, as the list of members is automatically updated following each Sync. It requires less vigilance to maintain the Phone Group over continuing upgrades, as the user simply reruns a stored query.

Cons: This grouping offers a limited ability to identify phones from the population (compound query plus filters). If specific phones should always remain in the group, regardless of whether their configuration changes, then Static Phone Groups must be used. Dynamic Phone Groups will change each time the Discovered or Last Registered filter options are used.

Phone Group Uses

Phone Groups may be defined for the following purposes:

Table 2-4 Phone Group Uses

Purpose	Description
User Class	A User Class is comprised of a Phone Group and a set of Calling Permission expectations (e.g. allowed to call Long Distance, blocked from calling International). When creating a Phone Group for this purpose, it is recommended that you use the CSS-Phone and CSS-DN phone/DN attributes for selection.
Test Element	Some Tests (DID, Directory Handler, and the entire Phone Feature category) require a Phone Group as the Test Element. These tests concentrate on some aspect of the phones in the group (have a DID mapping, are listed in the Directory Handler, etc.). It is suggested that you create a group reflective of and specific to the test you wish to run.
Resource Constraints	One or more Phone Groups may be added to either the On or OffNet Resource Pools. Phones in these Pools will be used as supporting resources, and can help achieve the goal of the test. The main consideration in whether to include phones in these Phone Groups is whether they are available to be accessed during tests without disturbing endusers.
Reports	Reports may be generated based on selected Phone Groups. Phone Groups allow you to target specific Phones for specific Reports.

Creating a Phone Group

1. To create Phone Groups. Select **phone groups** from the active Cluster's Clusters window, or from the **setup** menu.

NOTE: A Cluster must be active to create a new, or edit an existing Phone Group.

The following screen displays:

Create

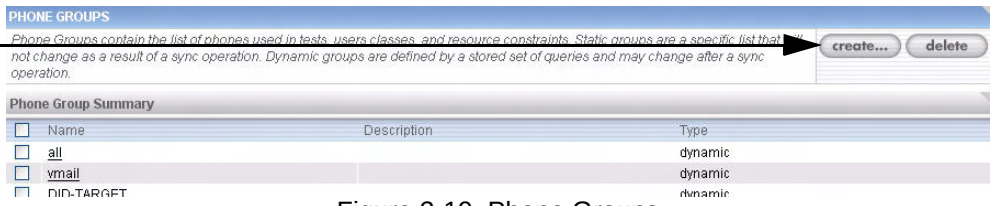


Figure 2-19 Phone Groups

2. Click **create** to open the Create Phone Group window:

Figure 2-20 Create Phone Group

3. Enter a name and description for the Phone Group, and select a type.
4. Click **create**. The following screen displays:

Filters

And /Or Functions

Show Details

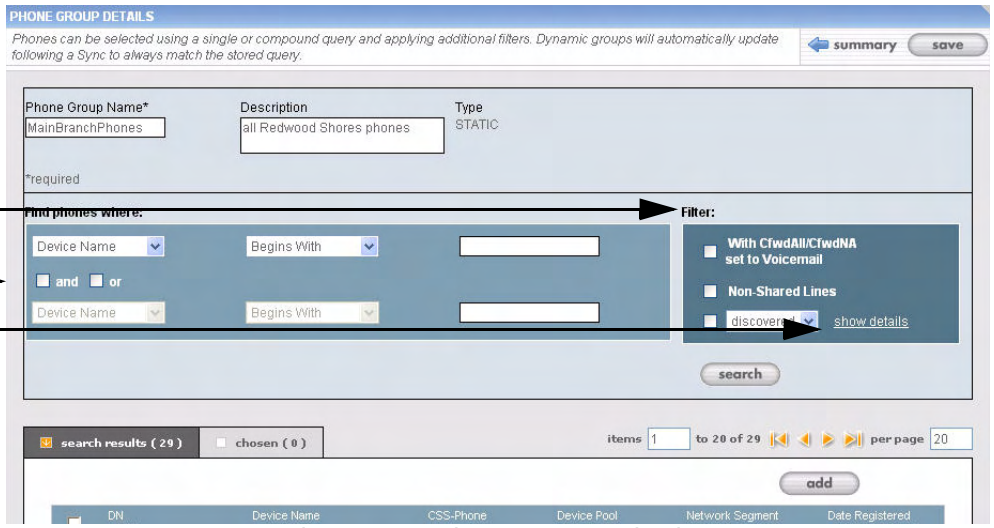


Figure 2-21 Phone Group Selection

5. Select the phone attributes for your search.

The following attributes are available for selection:

Table 2-5 Phone Attributes

Attribute	Value
Device Name	A text field containing all or part of a phone device name (e.g. SEP00AFAC013).
DN	A text field containing all or part of a directory numberline 1 only (e.g. 41211).
Partition	A drop down list to choose from the existing route Partitions. The selected item will be compared with the partition assigned to the DN of the primary line of each phone.
Description	A text field containing all or part of a phone description (e.g. Jon Smith).
CSS-Phone	A drop down list to choose from the existing Calling Search Spaces. The selected item will be compared with the CSS assigned to each phone.
CSS-DN	A drop down list to choose from the existing Calling Search Spaces. The selected item will be compared with the CSS assigned to the primary line/ DN of each phone.
Device Pool	A drop down list to choose from the existing Device Pools.The selected item will be compared with the Device Pool assigned to each phone.
Model (Device Type)	A drop down list to choose from the existing phone models (e.g.7960).
Location	A drop down list to choose from the existing Locations. The selected item will be compared with the Location assigned to each phone.
Network Segment	A drop down list to choose from the existing network segments (e.g. 172.17.16.0/24). The selected item will be compared with the network segment of all registered phones' user input string.

The Following Filters are available for use:

Table 2-6 Filters

Filter	Use
With CfwdAll/CfwdNA set to Voice Mail	When selected, only phones with their primary line set to forward to the Voice Mail Profile for either NA or All will be displayed.
Non-Shared Lines	When selected, only phones whose primary line is not shared will be displayed.
Registered	When selected, only phones that have *registered* within a specific time period will be displayed. Note that only the "last" registered timestamp will be used. The options are: • since the last Sync operation. • within the last N hours (N is an integer). • between a starting and ending date.
Discovered	When selected, only phones that have been *discovered* within a specific time period will be displayed. Discovery indicates that the phones have been found to be registered during a Sync. Note that phones that have since reregistered will not be considered Discovered. The options are: • since the last Sync operation. • within the last N hours (N is an integer). • between a starting and ending date.

NOTE: Most tests run more quickly if no shared lines are used. ClarusIPC recommends that if Shared Lines are not required, they not be included in a test.

6. To view filter choices for **discovered** or **registered**, click **show details** to expand the options.

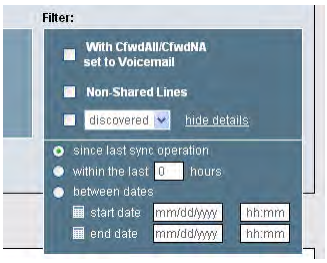


Figure 2-22 Search Filters

The Phone Group Details page allows you to search for phones using either a single or compound query. A single query simply applies a phone's attribute against a matching value. For example:

Find phones where Device Pool equals "Bldg2A"

If this criteria is not sufficient to identify the specific group of phones, you may use a compound query by using the **And** or **Or** functions. For example:

Find phones where Device Pool equals "Bldg2A"
AND
where Description contains "Floor 2"

The search results will contain only phones where both the Device Pool is "Bldg2A" and where the *Description* contains the phrase "Floor 2", a smaller set than either query applied independently. For example:

Single Query:

Find phones where Device Pool equals "Bldg2A" ==> 272 phones

Single Query:

Find phones where Description contains "Floor 2" ==> 42 phones

Compound query:

Find phones where Device Pool equals "Bldg2A"
AND
where Description contains "Floor 2" ==> 13 phones

Similarly, sometimes a single query does not allow you to match the entire set of phones you wish to group. In this case, by applying the OR compound function, you can extend the list. For example:

Single Query:

Find phones where Device Pool equals "Bldg2A" ==> 272 phones

Single Query:

Find phones where Description contains "Floor 2" ==> 42 phones

Compound query:

Find phones where Device Pool equals "Bldg2A"
OR
where Description contains "Floor 2" ==> 301 phones

Remember that the compound results will not always equal the totals of the single queries (272+42) because there may be overlap where some phones with Device Pool or Bldg2A also have a Description containing "Floor 2." In fact, we know that 13 phones fit this description from the previous example:

(272 + 42 - 13=301)

Select **Close** to save your selections and return to the search screen.

Static Phone Groups

The following steps are required to complete a Static Phone Group using attributes:

1. After all phones that match the selected attributes have been returned, use the check boxes to the left of each phone to select the desired phone to include in this Phone Group and select **add**. This will move the selected phones into **Chosen**. To view the phone selected (chosen) for the Static Phone Group, click **chosen**.
2. You can repeat the attribute selection process as necessary. After each query, you can add the required phones.
3. When all required phones have been added to the static Phone Group, select **save**.
4. Select **search**. The following screen displays:

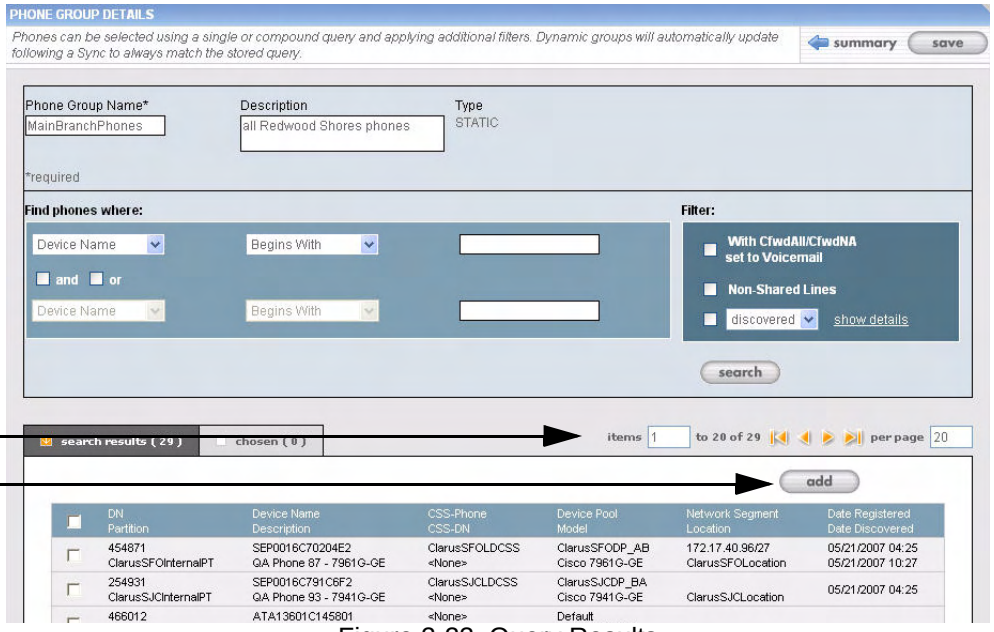


Figure 2-23 Query Results

The results displayed at the bottom of the screen are the phones that are now part of this group. Results are displayed 20 items per page. Use the arrows at the top right of the returned items to scroll through the list. Each time this Static Phone Group is used for a test, these are the phones that will be tested. Add to the group by checking the box next to the phone and clicking **add**. (A Dynamic Phone Group would be updated automatically based upon the search criteria you used in its query.)

Dynamic Phone Groups

To create a Dynamic Phone Group using phone attributes:

1. Select **search.**
2. After all phones that match the selected attributes have been returned, select **save query,** then **save**.

Editing a Phone Group

1. To edit a Phone Group, activate its Cluster, then select **setup > phone groups > *phone group name*** to open the Phone Group Details window.

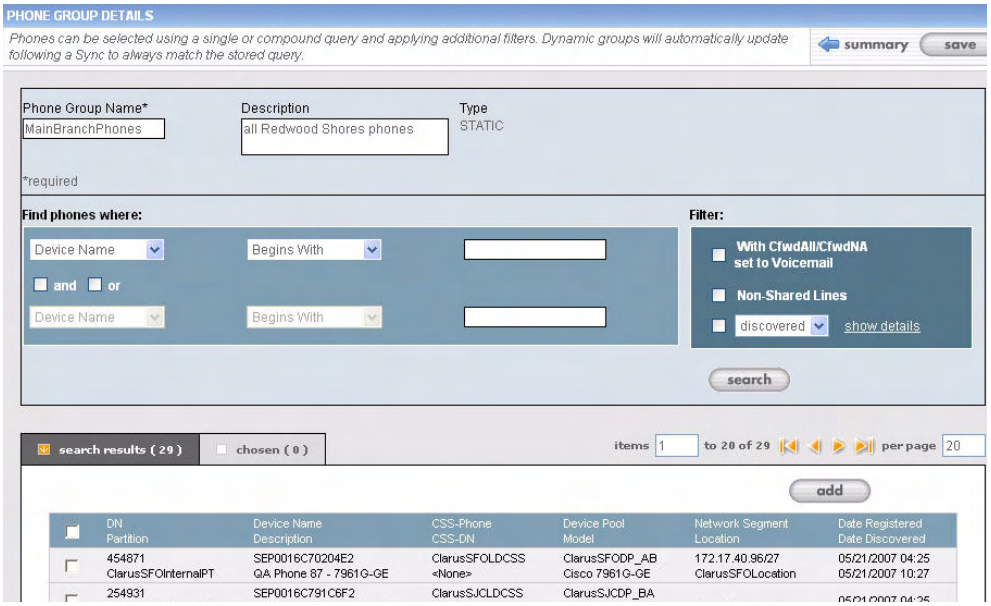


Figure 2-24 Phone Group Details

2. Click the **chosen** tab to view devices included in the Phone Group.
3. Make changes to the Group as desired, then click **save**.

NOTE: Any changes made to existing Phone Groups may affect test plans. You must execute a Sync after making changes to a Phone Group if you wish the new settings to be reflected in the next test.

Deleting a Phone Group

1. Select **setup > phone groups** to open the Phone Groups window.

Delete

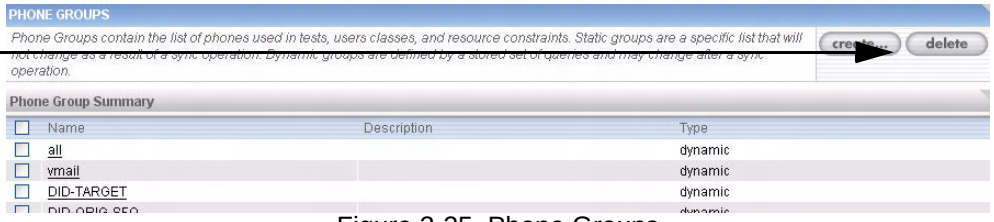


Figure 2-25 Phone Groups

2. Check the Phone Groups you wish to delete, and click **delete**.

NOTE: It is possible to delete a Phone Group that is assigned to a test plan or Resource Constraint. Verify that the Phone Group is unassigned before it is deleted.

User Classes

User Classes allow you to establish a logical grouping of users based on their intended calling permissions. This grouping allows the ClarusIPC user to group similar classes of users together, and to indicate which call classifications they should be allowed or denied. Some examples of User Classes include:

- **Lobby Phone:** call permissions support only internal calling and block external calling such as Local, Long Distance, or International, calls.
- **Executive:** call permissions support all internal and external calling, but block Pay-per-Call numbers such as 900, and 976.

The following call classifications apply to User Classes:

- Local
- Long Distance
- International
- Toll Free
- Pay-per-call
- Service
- Emergency
- New Classification - user-defined call classification

NOTE: Phone Groups must be configured before configuring User Classes. User Classes use Phone Groups, so create Phone Groups based on the Calling Search Space of the phone or directory number.

Creating a User Class

1. To create a User Class, select **user classes** from the **Clusters** screen, or from the **setup** menu for the active Cluster.

The following screen displays:

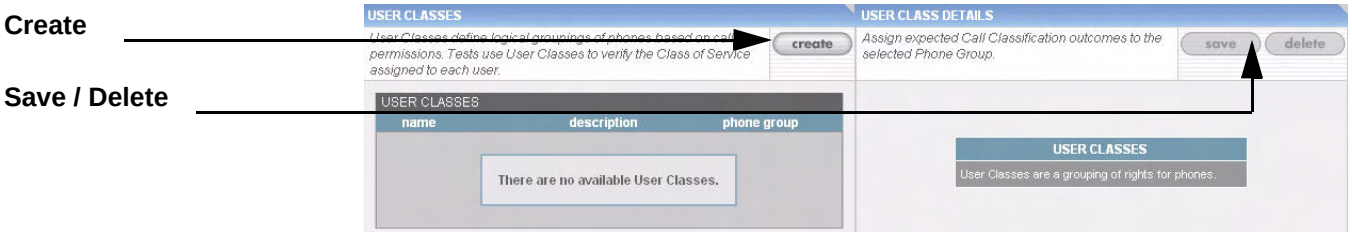


Figure 2-26 Create User Class

2. Select **create** in the left column. The options for the new User Class display in the right column.

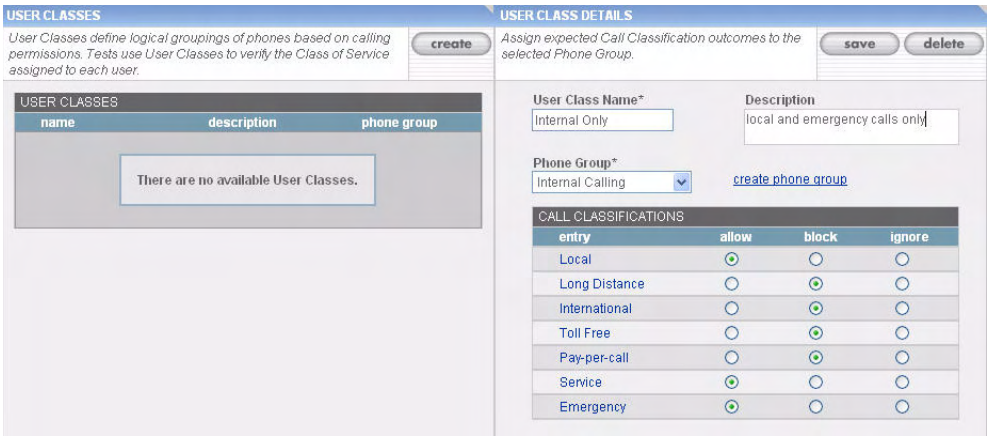


Figure 2-27 User Class Details

3. Complete the following fields:

Table 2-7 User Class Field Descriptions

Field Name	Values	Description
User Class Name	Up to 30 Alphanumeric characters	Enter a unique name for the User Class.
Description	Up to 30 Alphanumeric characters	Enter a description of the User Class. This field is optional.
Phone Group	One Phone Group	Select the appropriate Phone Group created in support of this User Class. In many cases the Phone Groups created for User Classes will be based on Calling Search Spaces assigned to either the phone (CSS-Phones), primary Directory Number (Calling Search Spaces-DN), or both. If you need to create a new phone, click **create group.** For more information about creating Phone Groups, see *Phone Groups* on page 2-20.
Call Classifications	• Allowed: if selected, the test will be executed using the selected call classification, which is expected to complete • Block: if selected, the test will be executed using the selected call classification, which is expected to be blocked • Ignore: if selected, this call classification will not be executed	Select an action for each item. Ignore is the default, no calls to any Phonebook entry assigned to this call classification will be made.

4. Click **save** when you are done.

Editing a User Class

You can edit a User Class at any time. If the name of a User Class is changed, the Call Permission tests that had the original User Class assigned will be automatically updated when Staged. For more information about Staging, see *Staging Test Plans* on page 4-15.

1. Select **setup > user classes >** ***user class name.***
2. Make the desired changes.
3. Click **save** to update the User Class.

Deleting a User Class

To delete a User Class, select the class from **setup > user classes >** ***user class name,*** and click **delete**:

NOTE: Make certain that the User Class you wish to delete is not assigned to a Test Plan. Remove the User Class from the Test Plan before it is deleted.

Resource Constraints

A resource is a phone that is used to perform one of the roles required to execute a test component. Resources are broken up into *target* and *supporting resources*. A *target* resource is a phone that must come from the test element itself, and will fulfill the target role of the test component. *Supporting* resources fill the remaining roles of a test component, and are provided to help execute the tests. Resource Constraints provide the ability to control the supporting resources, and allow you to limit the phones used in test plans so as not to disturb production users.

Resource Constraints consist of two Resource Pools: OnNet and OffNet. A phone may be selected from one of these pools according to the required supporting role.

OnNet Resource Pool

The following tests require supporting resources from the OnNet Resource Pool.

Network

- **Device Registration:** Requires one supporting resource per test component. These resources must belong to the selected test element. (Device Pool, Network Segment or Location)
- **Signaling Delay:** Requires one supporting resource per test component. These resources must belong to the selected test element. (Device Pool, Network Segment or Location)
- **Voice Protocol OnNet:** Requires one supporting resource per test component. These resources must belong to the selected test element. (Device Pool, Network Segment or Locations)

Application

- **Meet-Me Conference:** Requires multiple (user-configured) supporting resources.

Phone Feature

- **Softkey Functions:** Requires multiple supporting resources (depending upon the softkey option selected).
- **Forward To Voice Mail:** Requires one supporting resource.
- **Rollover:** Requires two supporting resources.

OffNet Resource Pool

The following tests require supporting resources from the OffNet Resource Pool. Ensure that the phones added to this pool can call OffNet (to the PSCN).

Network

- **Voice Protocol OffNet:** Requires one supporting resource per test component. These resources must also belong to the selected test element. (Device Pool, Network Segment or Location)

Route Plan

- **Direct Inward Dial:** Requires one supporting resource.

Application

- **Directory Handler Lookup:** Requires one supporting resource.

Updating Resource Constraints

1. To access this section, select **resource constraints** from the Clusters window, or **setup > resource constraints** for the active Cluster.

The following screen displays:

Figure 2-28 Resource Constraints Window

2. Use the left arrow buttons to move the desired Phone Groups from the right column to the OnNet or OffNet support resource pool. Use the right arrow buttons to remove a Phone Group from testing. Click **save** when you are done.

CHAPTER 3 PERFORMANCE DATA COLLECTION

ClarusIPC allows you to monitor the performance of the CUCM system by collecting Key Performance Indicators (KPI) such as active calls, available media resources, and server health, as well as device registration status. Collectors are used to control which data is polled; the Dashboard allows you to view both current and historic information graphically; and the Voice Monitor rules allow you to be automatically alerted when thresholds are violated.

Configuring Collectors

Collectors allow you to control which KPI and registration status data is polled. The KPI collection frequency is determined on the Cluster Details page, while the registration status collection frequency is a fixed 60 second interval. (If the CUCM system or ClarusIPC is unable to keep up with the polling frequency, it will automatically slow down by waiting for a collection in progress to finish before starting the next.)

Clusters and their Device Pools must be included in a *running* collector for KPI and registration data to be collected. Selecting a Cluster with KPI enabled in the Cluster Details page runs KPI collection for that Cluster *only* while the Collector is running. Selecting a Device Pool enables device registration status collection for that Device Pool *only* while the Collector is running.

If you wish to monitor the Cluster's Device Pools' registration data, without collecting the Cluster's KPI data, Clusters may be included in a collector with KPI collection disabled. KPI data collection need not be enabled for Device Pools to be added to the Collector.

NOTE: Collectors collect KPI data only for Clusters with KPI collection *enabled* (see *Creating Clusters* on page 2-3). Registration status data for *all* selected Device Pools is collected while the Collector is running.

To create a Collector, click **setup > collectors** in the menu bar.

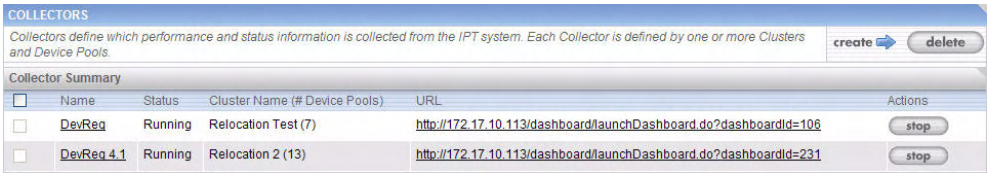


Figure 3-1 Collectors Window

Multiple Collectors may be created, each identified by a Name. The Collectors summary page displays:

- the Collector's **Name**
- its **Status** (Running / Not Running)
- the **Cluster Name** and number of **Device Pools**
- the **URL** used to access the Collector's view in the Dashboard
- an **Action** button to Stop or Start the Collector

To change a Collector's configuration, click on its name in the Collectors window, make changes as desired, and click **save**. Changes to Collectors are implemented instantly.

To delete a Collector, select its checkbox, and click **delete**. A Collector must be stopped to be deleted, but running Collectors may be edited.

To create a new Collector, click **create** to launch the Collector Details window.

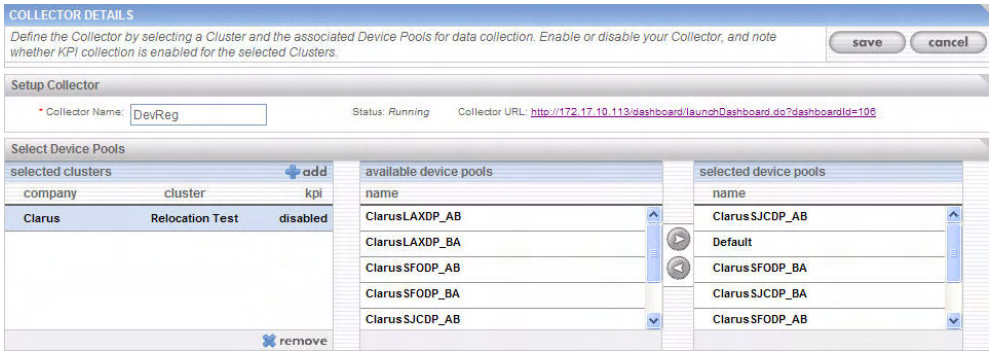


Figure 3-2 Collector Details Window

1. Enter a **Name** to describe the function of the Collector.
2. In the **selected clusters** pane, click **add** to add the Clusters you wish to monitor. (Select the Cluster and click **remove** to remove it from the list.)
3. If you wish to collect KPI data for the selected Clusters, check that **KPI** is **enabled** in the **selected clusters** pane. If **disabled**, return to the **Cluster Details** page for the selected Cluster, and select the **KPI Settings - Enable** checkbox.
4. Select specific Device Pools to enable registration status collection for the selected Pools. For each added Cluster:

NOTE: Collectors are not dependent on Sync. The list of Device Pools presented for selection is dynamically retrieved, and does not reflect Device Pools collected as a result of the last Sync.

a. Click the name of the Cluster in the **selected clusters** window to generate a list of **available device pools**.

b. Click on a Device Pool you wish to monitor, and click the right arrow to move it into the **selected device pools** pane.

c. Repeat for each Cluster you wish to monitor.

NOTE: Selecting the same Device Pools for multiple Collectors may cause CUCM to reach throttling limits, and prevent it from returning device registration information for all Collectors. To avoid these limits, create separate Collectors for each Device Pool you wish to monitor.

5. To start the Collector on save, select the **Enable Collector** checkbox.

When your Collector is configured, click **save** in the upper right hand corner of the window. The **Saving Collector** progress window will open as the Collector is created. When completed, the **Collectors** window will open, listing all Collectors and their current status.

Viewing Collectors

Once configured and saved, Collectors may be viewed in the ClarusIPC Dashboard. The URL for each Collector allows you to quickly access the Dashboard view, filtered against data from the selected Collector. You may also send the URL to others to view the Dashboard in any browser window. They will not be able to alter your settings, nor will they be able to start, stop, or otherwise control your Collector.

To access the Dashboard, click on the **dashboard** link from ClarusIPC, or enter

```
http://<clarus_server>/dashboard/launchDashboard.do
```

into any browser window. If more than one Collector is running, the Dashboard will list all results. You may access individual Collectors by opening the Dashboard, then selecting the Collector by name from the drop down menu shown.

Device Registration

The **Device Registration** window displays registration status for devices managed by Clusters included in the selected Collector. Use the pulldown menu to select the device type for which data will be shown: Phones, MGCP Endpoints, Voice Mail, CTI, H.323 Gateways, or Media Resources. (You may exclude registration status for a particular Cluster by unchecking the box to the left of the Cluster name.)

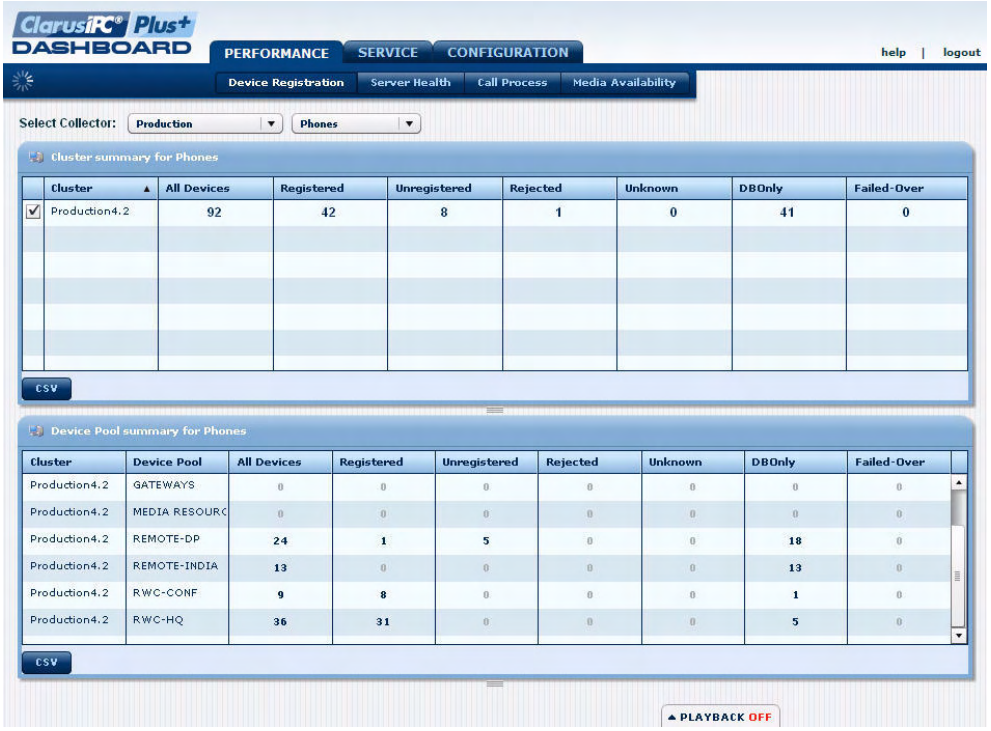


Figure 4 Device Registration Window

The two main panes summarize registration status by Cluster and by Device Pool, for the selected Device type. Counts are listed for registration status:

- **Registered:** devices registered to a CUCM.
- **Unregistered:** devices not registered to any CUCM.
- **Rejected:** devices for which the registration attempt was rejected by CUCM.
- **Unknown:** devices for which CUCM was unable to determine status.
- **DBOnly:** devices which do not have a registration state, but which exist in the CUCM database. These devices have either never been registered, or their registration status with the CUCM has expired.
- **Failed-Over:** devices currently registered to their non-primary CUCM.

Clicking a count in the **Device Pool summary** pane opens a third pane, in which details for that count are listed. The Details pane displays the Device's DN, Name, Description, IP Address, Status, Last Registered, Model, Active CM, and Primary CM.

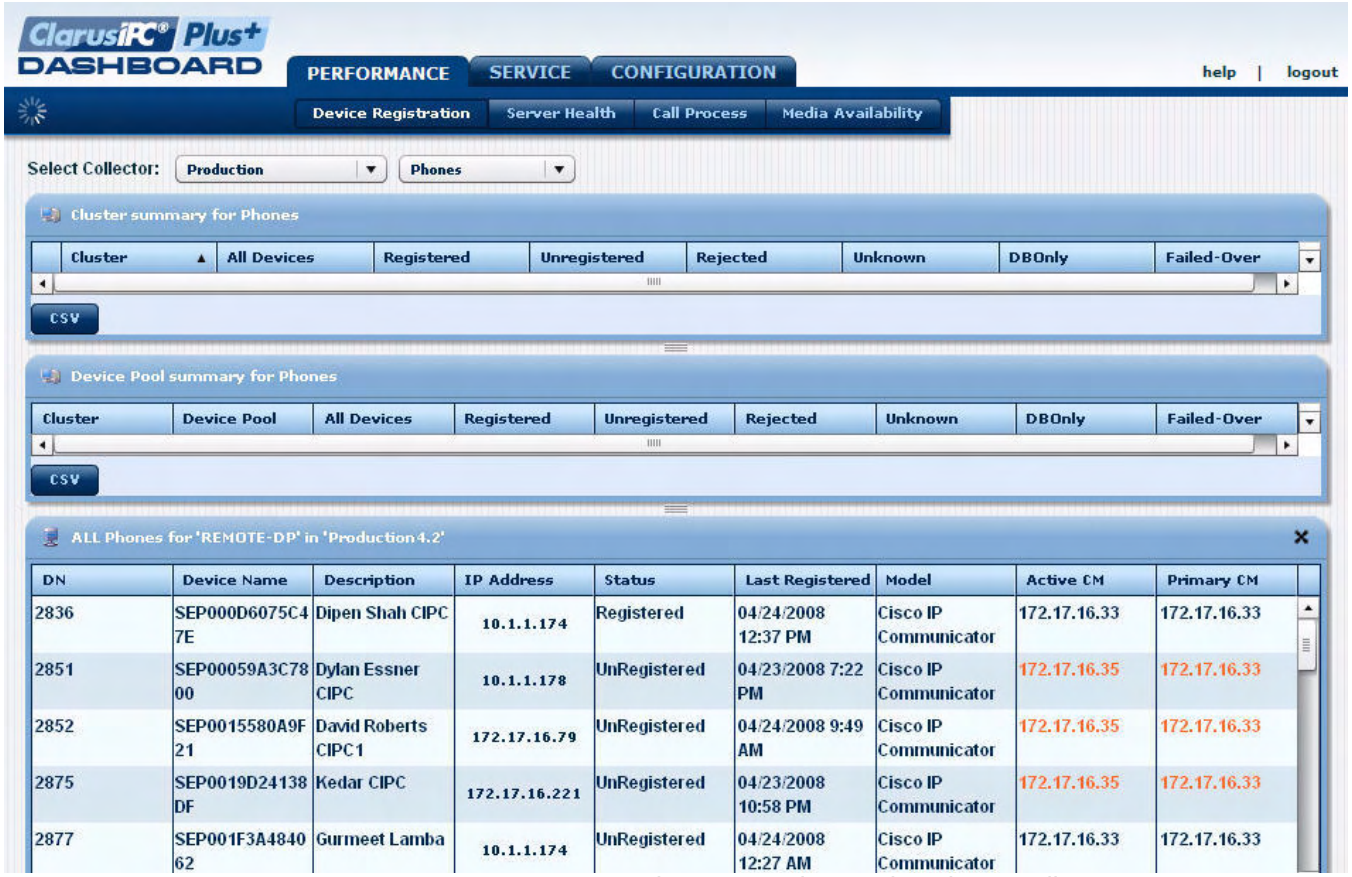


Figure 5 Device Registration Details

A question mark (?) indicates that data is not available for the field. The display of the Active and Primary CM fields in orange indicates that the phone is no longer registered to its Primary Communications Manager. IP addresses of listed phones link to the phone's Device Information web page.

NOTE: The Device Registration timestamp is generated by the CUCM server, and will reflect the time zone in which the CUCM server is located. For example, a registration event which occurs at 3:00pm Eastern Standard Time will appear in a Pacific Standard Time zone browser shortly after noon PST, with a 3:00pm timestamp.

CHAPTER 4 TEST DESIGN

To execute tests, you must create Test Plans which contain a set of tests applied to a set of test elements (devices). In a previous chapter, you learned how to create some test element types: Phone Groups and User Classes. Test Plans can be designed to exercise a particular aspect of your IPC environment, such as verifying voice network availability or user calling permissions. Test Plans must be staged before being executed, to assign appropriate resources to each test.

You may have one or more tests within a Test Plan, but the entire Test Plan must be executed at one time. Test Plans can be exported and imported into the same or different ClarusIPC Systems.

The Test Plan Process

To build, stage and execute a Test Plan:

1. Create the Test Plan by selecting tests that will exercise certain functionalities of your communications system.
2. Select one or more test elements. Test elements are phones that can be identified by Device Pools, Locations, Network Segments, Phone Groups, User Classes, etc.
3. Stage the Test Plan to assign test resources (phones) to each role in your Test Plan. These phones are assembled from the resources defined in Step 2. The staging process builds the test components based on the data available from the latest Sync. Test Components are the specific resource activities that are performed for each test element (phone). It can involve a simple call from one phone to another phone, such as used in Voice Protocol OnNet. It can also involve more complex activities, such as performing a Call Transfer using an originating, transfer, and a terminating phone.
4. Select resource constraints for the individual tests. Resource Constraints allow you to restrict the set of phones that can serve a supporting role in a test. Supporting phones help perform a test, but their performance is not the objective of the test.
5. Execute the Test Plan and monitor the Test Components.
6. Review the test results of each Test Component.
7. Troubleshoot problems and rerun the test as necessary.
8. Produce a certification report that can be given to your customer as proof the IPC system is fully operational.
9. Schedule the test to run on a recurring schedule.

Creating Test Plans

Before creating a test Plan you must configure a Cluster. See *Managing Clusters* on page 2-2 for more information.

NOTE: Some steps may not be available depending upon the tests selected, or the state of the database. Tests created within a Test Plan cannot be shared or used outside of their Test Plan.

To create a new Test Plan:

1. Click **test plans.** The following screen displays:

Create

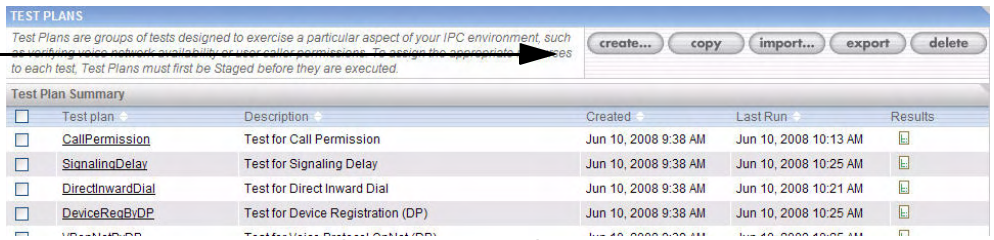


Figure 4-1 Test Plans Create

2. Click **create**. The following screen displays:

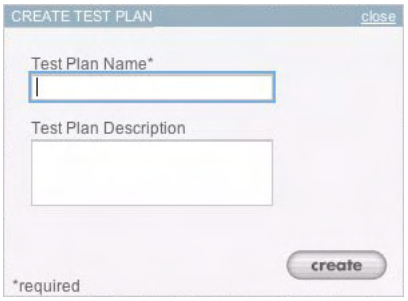


Figure 4-2 Create Test Plan

3. Enter a name and description for the new Test Plan, and click **create**. The following screen displays:

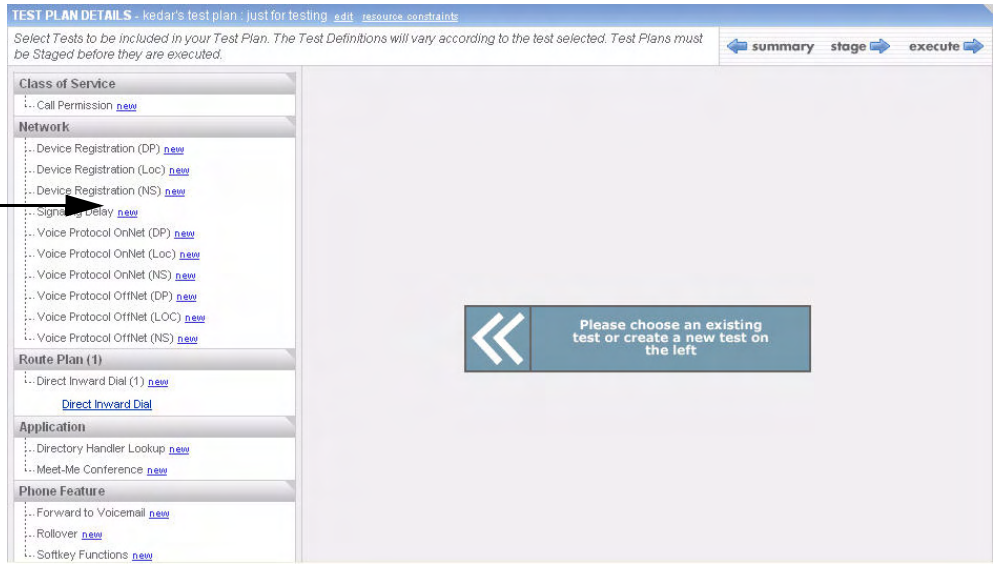


Figure 4-3 Select Test Type

NOTE: Create names that allow you to easily identify the purpose of the Test Plan, portion of the IPC system being tested, location, etc.

4. Click **new** next to the test type you wish to add to your test plan in the left column. The following screen displays:

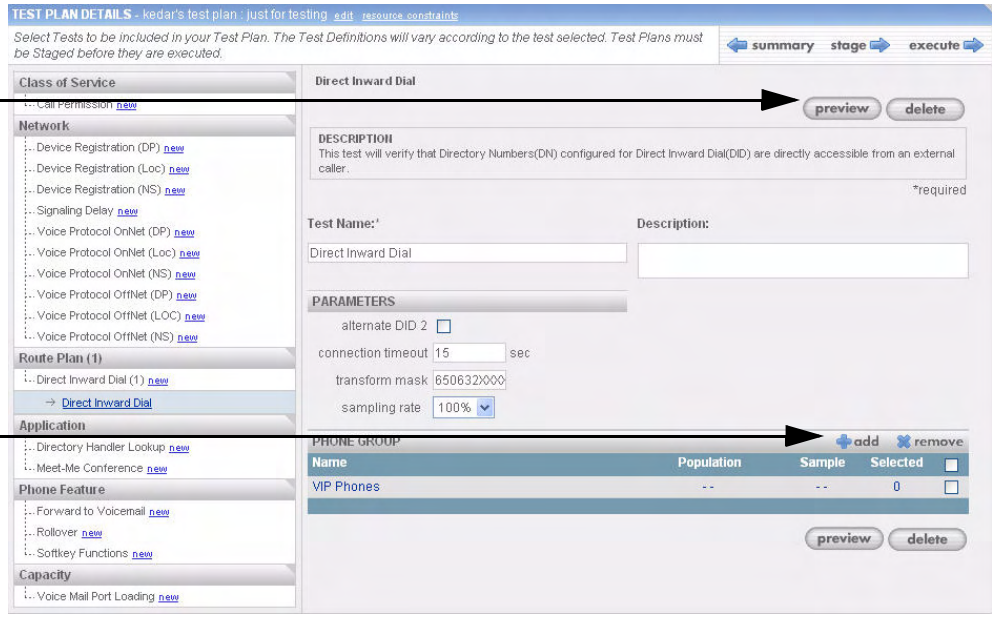


Figure 4-4 Edit Test Plan

5. Complete all fields for each test selected. Refer to Table 4-1 for required fields and suggested input. Make changes to the test default parameters as required.

Table 4-1 Create Test Field Descriptions

Field Name	Values	Description
Test Name	Up To 30 Alpha-numeric Characters	A unique name, such as sigdelay20 for a signaling delay test run against 20% of the phones.
Description	Up To 30 Alpha-numeric Characters	A description of the test.
Test Parameters	Specific to each test type.	This information is detailed under each specific test type in the rest of this chapter.
Sampling Rate	10 - 100%, in increments of 10%.	A sufficient number of target resources are randomly selected from the defined (Phone Group, User Class, network path) group to meet the sampling requirement. Meet-Me Conference and Voice Mail Port Loading replace Sampling Rates with Counts.
Test Elements	Specific to each test type.	These are the User Classes, Phone Groups and Network Path Endpoints (Device Pools, Locations, Network Segments) defined during the Cluster definition phase. Select resources to run the test against. See below for more information.

6. Select at least one Test Element for each test. The bottom pane of the Edit Test Plan window will automatically update to reflect the requirements of the selected Test type:

   - Device Pool
   - Location
   - Meet-Me Pattern
   - Network Segment
   - Network Path Endpoints
   - Phone Group
   - User Class
   - Voice Mail Profile

Elements are selected by clicking the **add** button in the Test Element bar, and selecting from a list of available elements.

To add a test element, select **add** in the right column. The following screen displays:

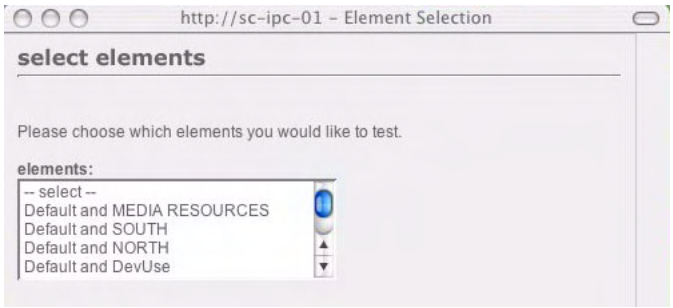


Figure 4-5 Test Elements

7. Select elements from the menu box and click **close**.
8. To delete an element from a Test Plan, select the element's checkbox and click **remove**.
9. When you have completed configuring test parameters, click **save** to update the plan.

Abbreviated Dialing

Abbreviated Dialing allows intra-office callers to dial only the last 5 digits of a 10-digit Directory Number. For example, a branch office may have 40 users with a 10-digit Directory Number. If Abbreviated Dialing is enabled, they need only dial the last 5 digits of the user DN to ensure that the call is properly routed within the office.

If, in another branch office, a second phone exists, with its own unique 10-digit DN containing the same last 5 digits, Translation Patterns may be used to prefix the appropriate local digits, to ensure that the call is routed within the corresponding branch. The combination of Abbreviated Dialing and Translation patterns allows a multi-office company to enable 5 digit intra-office calls, while maintaining a single network for the multiple locations.

ClarusIPC tests are designed with the assumption that direct DN-to-DN dialing, using the entire 10-digit string, is the standard user behavior. In the situation above, Direct Dialing DN-to-DN is not the likely user behavior. In some environments, it may be prohibited. If the Calling Search Space of user phone/DN does not permit dialing the complete Directory Number of other lines in the same office, only in other remote offices, users must dial the truncated extension number for internal calls.

For tests involving a call from an OnNet originator to an OnNet terminator, Test Plan staging selects originating phones which have permission to call the terminating phones. Because Test Plan staging assumes dialing DN to DN, in environments where abbreviated dialing is used, staging will either produce undesired results, or find no legitimate test components.

To overcome this problem, the following test options must be set:

- **Transform mask:** enter the mask that would be applied to the dialed number to perform an abbreviated dial. For example, if the actual DN is 6506322800, but abbreviated dialing allows users to dial simply 2800, then the transform mask would be XXXX.

- **Enable Abbreviated Dialing:** check this box to remove the permission checks performed during staging, and allow abbreviated dialing to be used. Note that it is possible to introduce more test failures if your environment has tight intra-office controls on which internal numbers users may dial.

NOTE: When discarding the CSS check, you must ensure that your selected Resource Constraints have the appropriate permissions to call terminators.

Transform Mask

The Transform Mask field allows you to enter a numeric string which will be used to transform all targeted Directory Numbers within the selected test from an internal-only number, to an external, OffNet number. For example, if the DID number is 914155435223 and the internal directory number is 5223, then the Transform Mask would be 91415543XXXX.

Please note that ClarusIPC does not validate Transform Mask data; if inaccurate data is entered, all tests will fail without error message.

Augmented Data

The Direct Inward Dial test is limited in that it expects an overlap of the DID number with part of the existing Directory Number for the line. In some cases, such as with 1-800 numbers, there is no overlap. Some users may also have multiple numbers that route to a single line.

One workaround is to create a single DID test for each user in the office, in which the Transform Mask field is used to fully identify the 1-800 number.

To provide a less cumbersome solution, ClarusIPC offers the ability to augment data, and define an alternate DID number for each device.

For more information, see *Augmenting Device Data* on page 2-14.

If the Cluster data has been augmented, and there is a number in the AltNumber1 field of the augmented data file, it will be used instead of the DN for line 1 of the target phone. The transform mask will remain in place (to allow users to dial 9 to attain an outside line.) If the Cluster data has been augmented, and there is no number in this field, the test will use the device's original DN.

If the "Use Alternate Number 2" checkbox is selected, the AltNumber2 value will be used instead of AltNumber1. If this parameter is selected but no number exists for this field, the device will be skipped.

Test Result Display

For greater clarity, the Transform Mask, the Dialed Number, and the Directory Number, are all displayed in the Test Results details window.

Resource Selection

After saving the test, the number of available and selected phones that will be used during the test are displayed in the Test Elements pane.

Figure 4-6 Resource Selection

Population: shows the number of phones eligible to participate in the test. Each phone considered as a test component must first pass a strict set of resource selection rules. See Appendix C, *Resource Selection Rules* for more information.

Sample: indicates the sampled subset of phones from the Population count that will be used to represent the test element, based on the selected sampling rate.

View Resource Selection Details

To view the specifics of the resources selected for your test, click **details** in the Population column of the Test Elements pane, to open the Resource Details window.

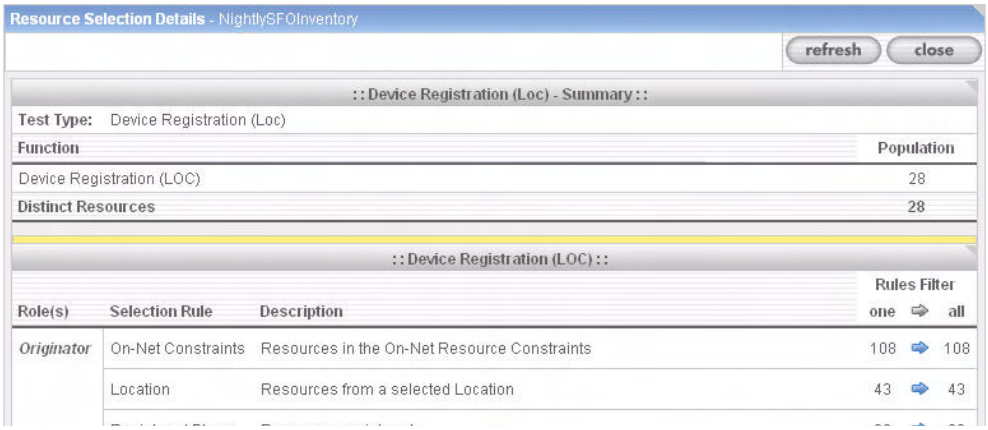


Figure 4-7 Resource Details

Starting from the top of the list, a specific rule is applied to the resource. In the above example, the first rule, OnNet Constraints is applied. The Rules Filter shows how many phones still qualify for this test after the rule has been applied. In the above example, 108 out of the original 108 phones qualified for this test after this rule was applied. As each rule listed is applied to the resource, the number of phones available to the test may change if some no longer fit the requirements of the test.

Custom Resource Constraints

If the default Resource Constraints are not appropriate for all Test Plans, they may be overridden with custom Resource Constraints. By default, Test Plans are assigned the Resource Constraints defined for the system under **clusters > resource constraints.** While creating a test plan, you may choose to alter the default resource assignments.

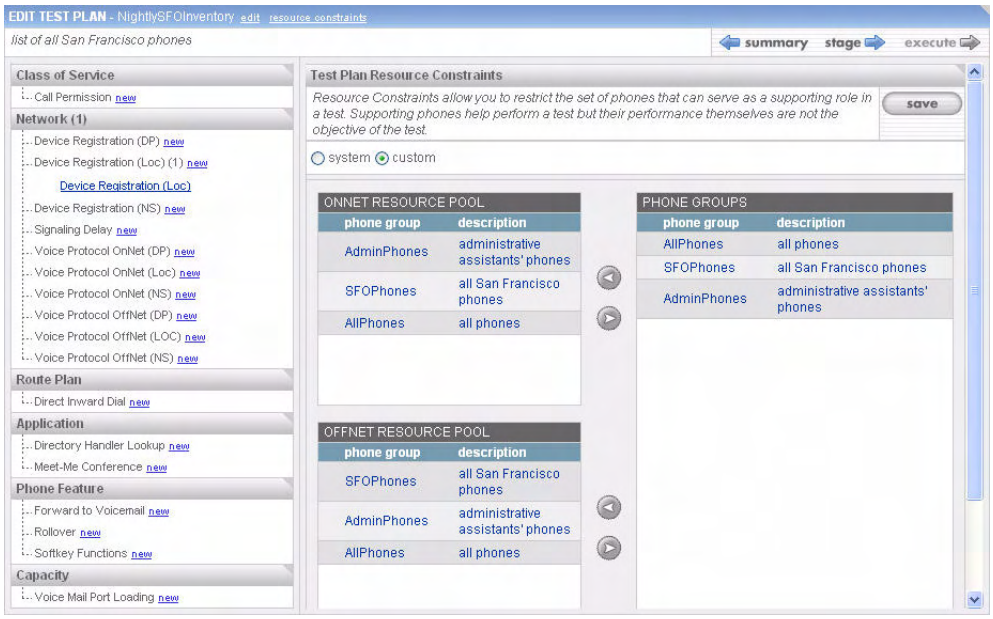


Figure 4-8 Test Plan Resource Constraints

Click **resource constraints** in the upper left corner of the Edit Test Plan window to open the Test Plan Resource Constraints pane.

- **system** indicates that the Test Plan will be run using the Resource Constraints defined for the Cluster; that is, the OnNet and OffNet Resource Pools as defined using **setup > *cluster* > resource constraints.**
- **custom** indicates that the Test Plan will be run using custom Resource Constraints; that is, Resource Constraints defined specifically for this Test Plan.

To force Test Plans defined with custom Resource Constraints to use the Resource Constraints defined at the Cluster level, click the system toggle button. To allow the tests listed to be defined using custom resource constraints, select **custom**.

To customize Resource Constraints for a Test Plan:

1. Click **resource constraints** in the Test Plan Details header of the page.
2. Use the right and left arrows to move Phone Groups in and out of the **OnNet** and **OffNet resource pools**, as desired.

(For more information, see *Resource Constraints* on page 2-30.)

When you have finished customizing resource constraints for the Test Plan, click **save** to save your changes.

Editing Test Plans

You can modify an existing test plan or tests within the test plan. To edit a test plan:

1. Select either **test plans** or the specific test from the **test plans** pull-down menu and select the desired test plan name. If you used the pull-down menu, skip to Step 2. The following screen displays:

Sorted by Creation Date

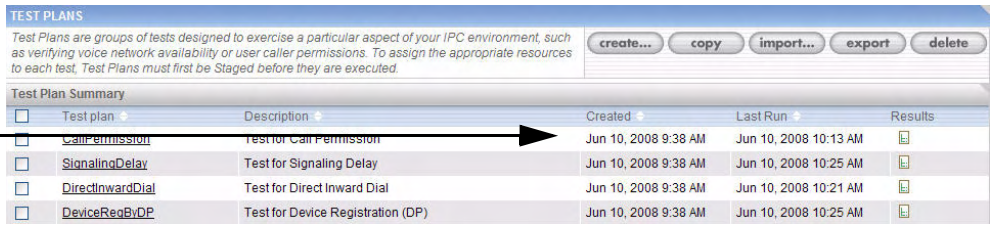


Figure 4-9 Test Plans

The following screen displays:

Test Plan Name

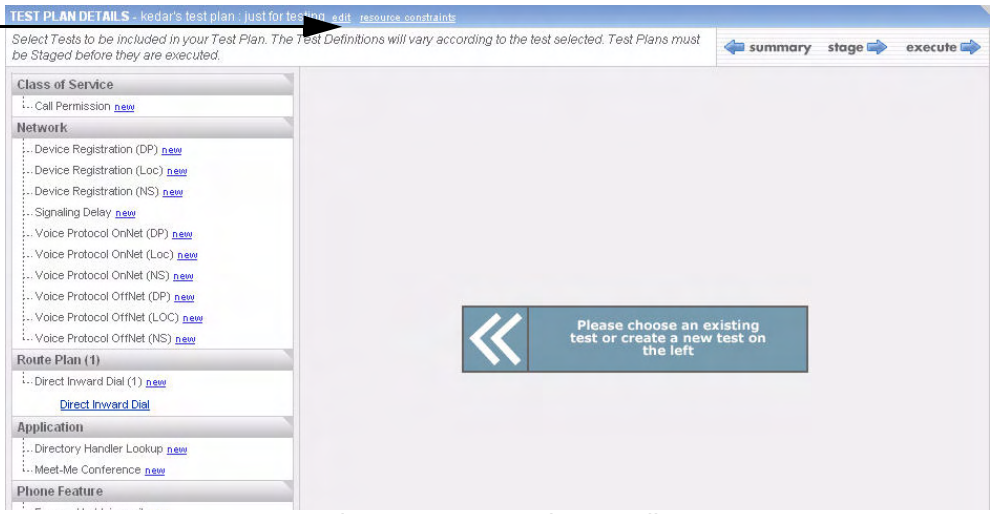


Figure 4-10 Test Plan Details

1. To edit the name of the Test Plan, select **edit** next to **Test Plan Details: <name>** in the top left corner, as shown in Figure 4-9. Change the test name or description, and click **create** to return to the full Edit Test Plan screen.
2. The Test Plan Details view displays a list of all available tests, as well as all tests currently in your test plan, listed below the test type. You might have multiple tests of the same type in a single test plan. To edit a test, click its name in the left column. Its details display in the right column.

NOTE: A appearing next to any test indicates that there is a problem with some portion of the test (missing required parameters, test elements have been removed from the system, etc.). These tests must be edited to run properly.

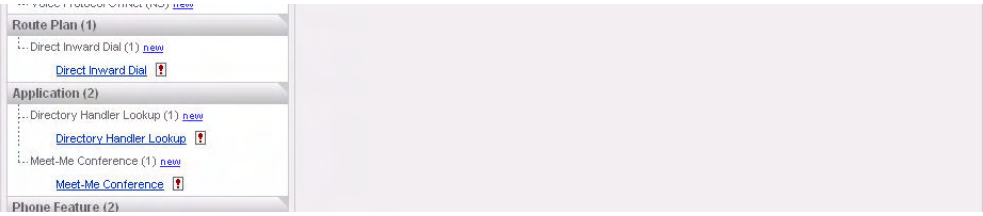
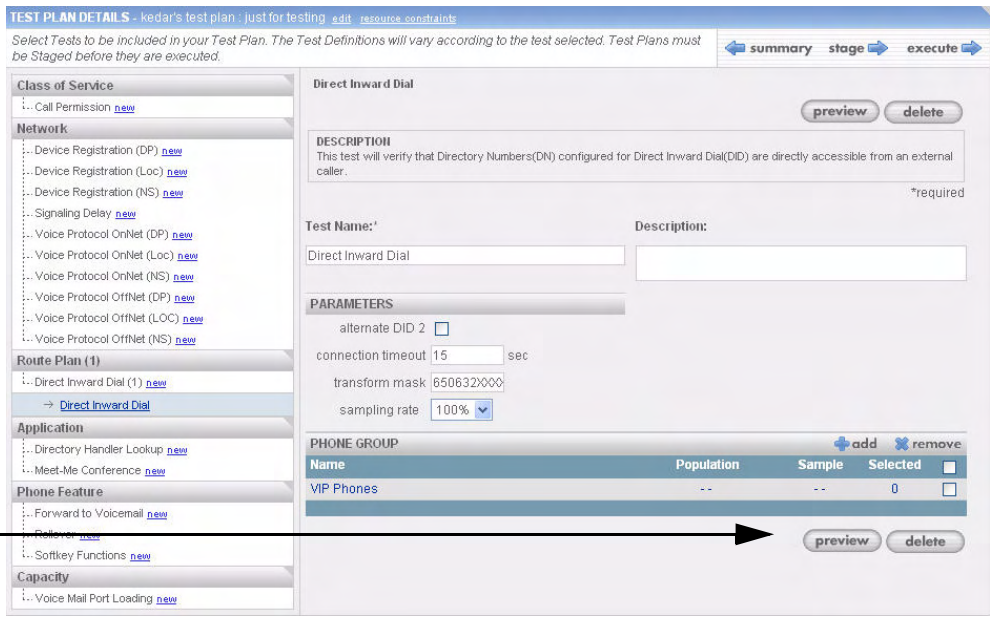


Figure 4-11 Test Plan List Populated

3. To add a new test to the Test Plan, click **new** next to the type of test you would like to add.



Preview

Figure 4-12 Preview Test Elements

4. On first selecting a test to edit, the display contains no values for the existing fields. Click **preview** to acquire values based on the most recently performed sync. The Staging column will contain values only if this test has already been staged. For more information, see *Staging Test Plans* on page 4-15.

NOTE: A ⚠ in the Population column indicates that the preview function was unable to identify any resources appropriate for the test in the selected Device Pool.

Figure 4-13 Device Pool Population Warning

5. To add test elements, click **add** in the elements section. Select the elements from the menu box, and click **close**. To remove test elements from the test, select the checkbox next to the element name then click **remove**. After making changes, the **preview** button reverts to **save**. You must click **save** for any modifications to be saved in the test. (You may select multiple elements using the Shift or Ctrl key.)
6. Repeat Step 5 for all the tests you wish to edit.

Copying Test Plans

Copying test plans can be useful if you wish to make a small modification to an existing Test Plan, but save the original. In addition, since all test results are overwritten each time a Test Plan is executed, you can use the Copy function to preserve the original results and run the copied plan instead. To copy a Test Plan:

1. From the **Test Plans** screen, click the checkbox(s) next to the test plan(s) you wish to copy and select **copy**. All selected test plans are copied and automatically renamed by appending a digit to the name. For example, the copy of a test plan called *My Test Plan* would become *My Test Plan1*.

Copy

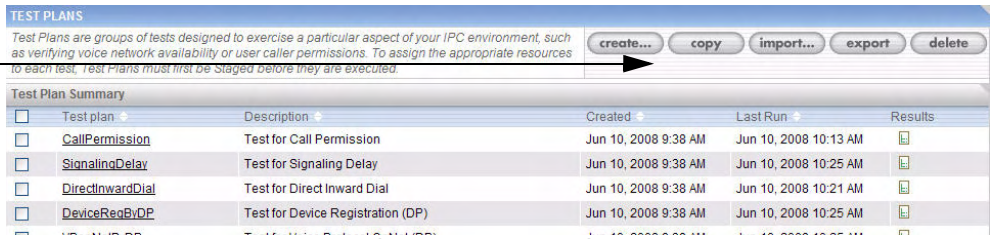


Figure 4-14 Test Plans

Importing Test Plans

You may import an existing Test Plan and customize it for a specific Cluster environment. The following properties may be imported:

- Test Plan Name
- Test Plan Description
- List of included tests

For each test, its

- Type
- Name
- Sampling Rate
- Parameters, and
- Dependencies may also be imported (Phonebook entries)

NOTE: Test elements, which are Cluster-specific data, will not be preserved across the export/import operation.

To import a Test Plan:

1. From the Test Plans screen, select **import**.

Import

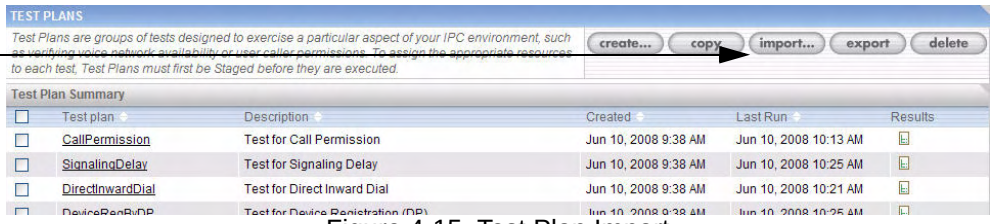


Figure 4-15 Test Plan Import

Figure 4-16 Import Test Plan

2. Use the **browse** button to locate the required Test Plan input file.
3. Click **import**. Your imported test plan displays on the **Test Plans** screen.

NOTE: If you attempt to import a Test Plan that has the same name as an existing Test Plan, the imported Test Plan will be automatically renamed by appending a digit to the end of the name. For example, if there is an existing Test Plan with name *My Test Plan,* the imported Test Plan with the same name will be imported with the name *My Test Plan1.*

Exporting Test Plans

You may export existing Test Plans to files for later import into either the same or another ClarusIPC system. Test elements, however, are not exported along with Test Plans, because they are applicable only to a specific Cluster.

Exporting Test Plans allows you to standardize your testing processes, and enable your deployment engineers to exercise a consistent set of certification procedures when performing a IPC installation. To export a Test Plan:

1. From the **Test Plans** screen click on the plan you wish to export, and click **export**.

Export

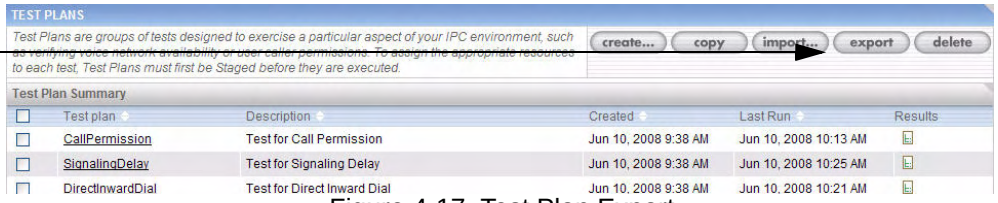


Figure 4-17 Test Plan Export

2. When the download dialog appears, click **Save**.

Deleting Test Plans

To delete a Test Plan:

1. From the **Test Plans** screen, click on the test plan checkbox you wish to delete, and click **delete** in the top right of the screen.

Delete

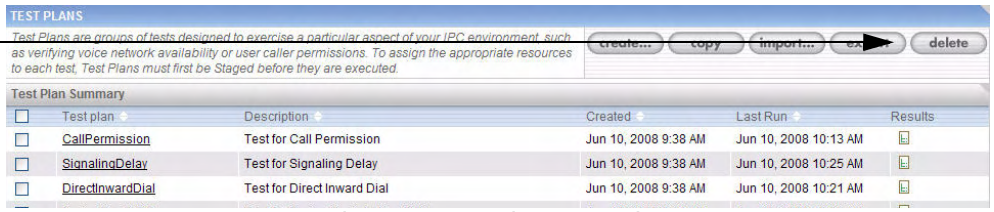


Figure 4-18 Delete Test Plan

The following warning displays:

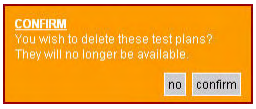


Figure 4-19 Confirm Test Plan Deletion

2. ClarusIPC requests confirmation for deletions. Click **confirm** to complete the deletion or **no** if you do not wish to complete the deletion.

NOTE: Only Test Plans that are not currently staging or executing may be deleted.

Staging Test Plans

The last step in preparing a test plan for execution is to *stage* the Test Plan. Staging is the process by which ClarusIPC assigns resources to each of the roles of each test in your Test Plan. For example, a Voice Protocol OnNet test requires two roles: an originator and terminator to verify that calls can be made between two network path endpoints. If you chose the network segments form of the test, then ClarusIPC must find one or more phones, depending upon the sampling rate, to represent each network segment pair selected as test elements. Phones assigned a role during the staging process are known as test resources.

The staging process builds the test components based on the data available from the latest Sync. (See *Synchronizing With CUCM* on page 2-9 for more information.) It also displays all tests in the Test Plan on one screen. When a previously executed Test Plan is staged, test results from that previous test run will be deleted, and will no longer be available to view. (Note that the **Execution** button is greyed out until a successful stage has been performed.)

Once you have staged a Test Plan, you are ready to execute it. For more information about executing test plans, see *Executing Test Plans* on page 4-17.

To begin staging, click **stage** in the **Edit Test** window:

Stage

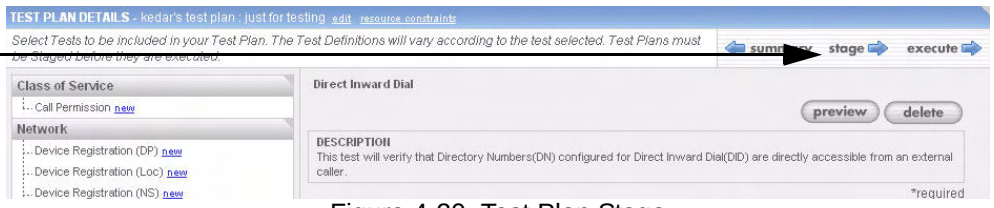


Figure 4-20 Test Plan Stage

The following screen displays:

Stage / Preview

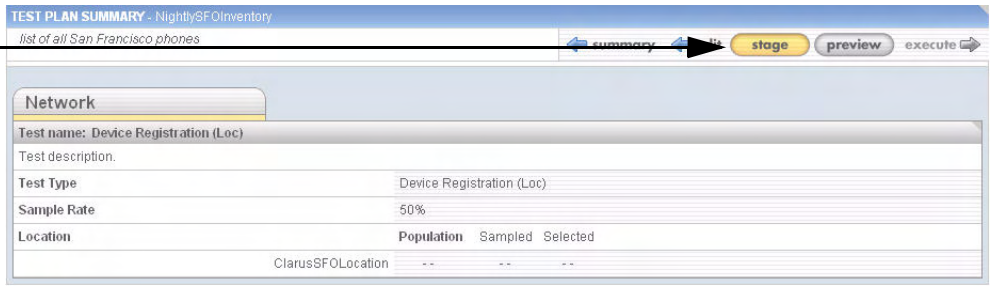


Figure 4-21 Test Plan Summary

1. Note that the Test Plan has not yet been staged. You must first select **preview** to check that there are no errors with your resources. Click **preview**.

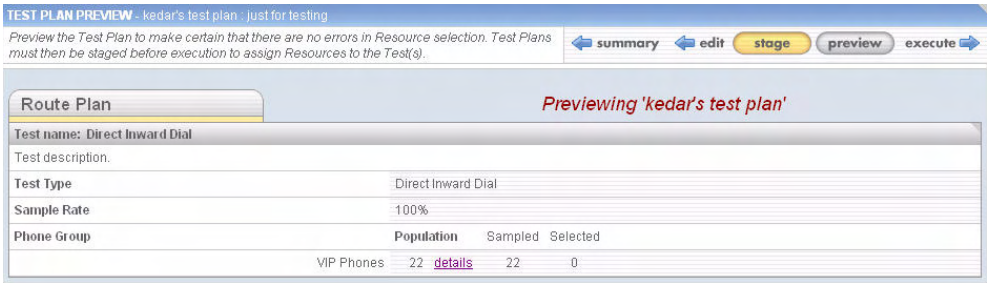


Figure 4-22 Preview

2. If a Preview is successful, you are ready to commit these test components for execution by staging. If this test has never been Staged, the **Selected** column will be empty. If you have no resources in your population to create a required test component, it will be marked with a warning icon ⚠ for that test. Click **edit** and edit the affected areas of your Test Plan.

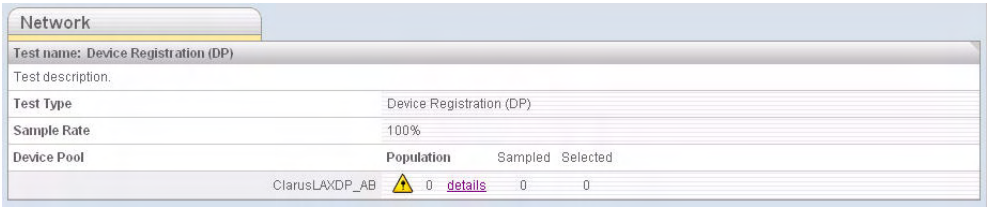


Figure 4-23 Test Plan Staging Error

3. To stage the Test Plan, click **stage**. The system may take some time assembling and committing the test components. When staging is complete, results are displayed:

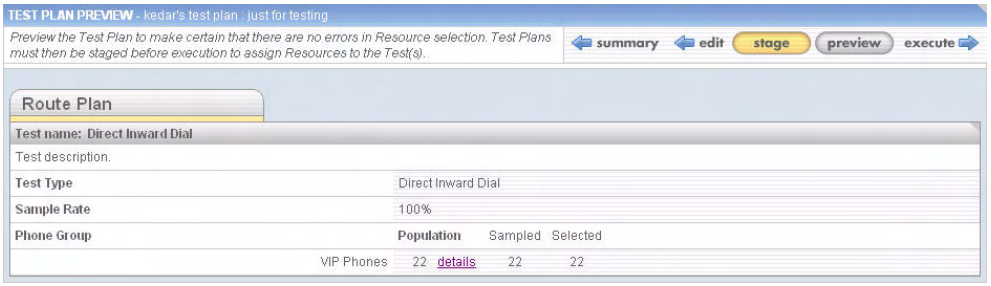


Figure 4-24 Stage Values

Note that there are values listed in the **Selected** column. You are now ready to execute the test.

Executing Test Plans

Test Plans must be staged prior to execution. If Test Plans that have been executed are rerun without staging, they will be run using the same resources as the previous test run. If Test Plans that have been previously executed are re-staged, they will have new resources allocated, if available. For more information about staging, see *Staging Test Plans* on page 4-15.

1. To execute a Test Plan, select **execute** from either the **Test Plan Preview** or the **Test Plan Details** window.

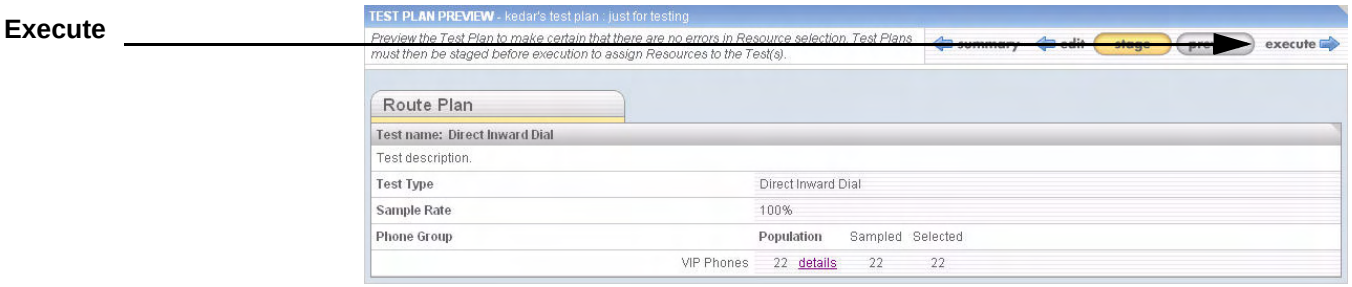


Figure 4-25 Execute Test Plan

The following screen displays, showing the test with **status: pending**:

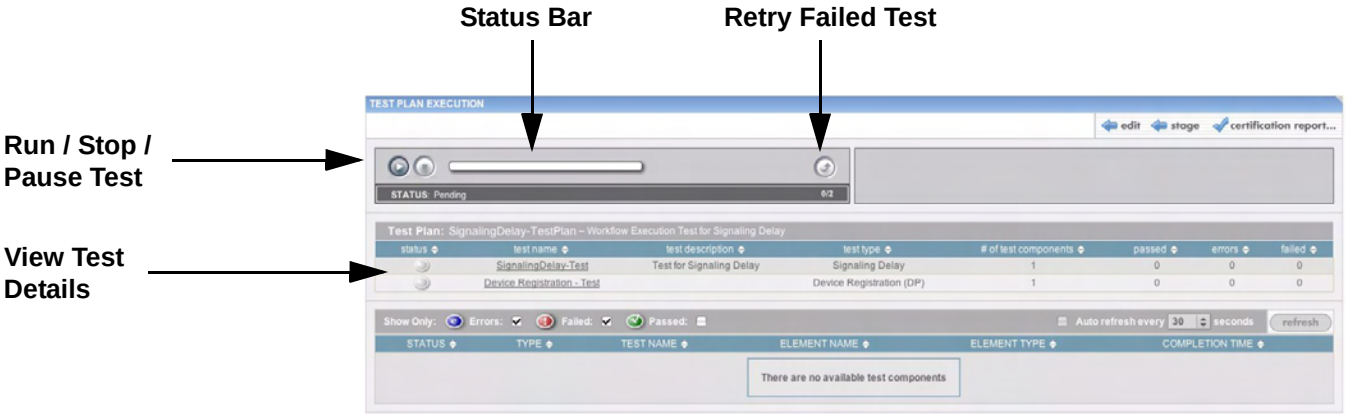


Figure 4-26 Test Plan Execution

2. The test is now in a *Pending* state.

Execution Control Panel

The Test Plan Execution window allows you to start, stop and retry tests.

Start Test Plan

Select **Run** by clicking the arrow to the left of the progress bar. If you stop the test, you can restart it by clicking the **Pause** that replaced the arrow button after stopping the test.

The status bar displays green unless a portion of the test fails, turning the bar red.

NOTE: When a Test Plan is executing, you will not be able to edit any of its Cluster or Site Definition pieces (Phone Groups, Phonebook entries, etc.).

Stop Test Plan

You can stop a running Test Plan by clicking the **Pause** button. The status of the test becomes *Halting* while the system stops the test, as shown below:

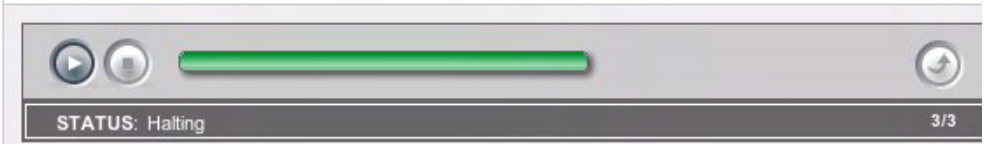


Figure 4-27 Stop Test Plan

Rerun Failed Test

You can rerun a test after failure if:

- The test failed or contained errors.
- The test or failure was not a result of changes to resources after the test began.
- You have not tried to rerun this test before.

To rerun a test, click the **Retry Failed Test** button shown above.

Viewing Test Results

To view details of the test components being tested, click on that test name, as shown in Figure 4-27. The default view for detailed test results will display *Errors* and *Failed* results. Add *Passed* to that display by selecting its checkbox. The following screen expansion occurs:

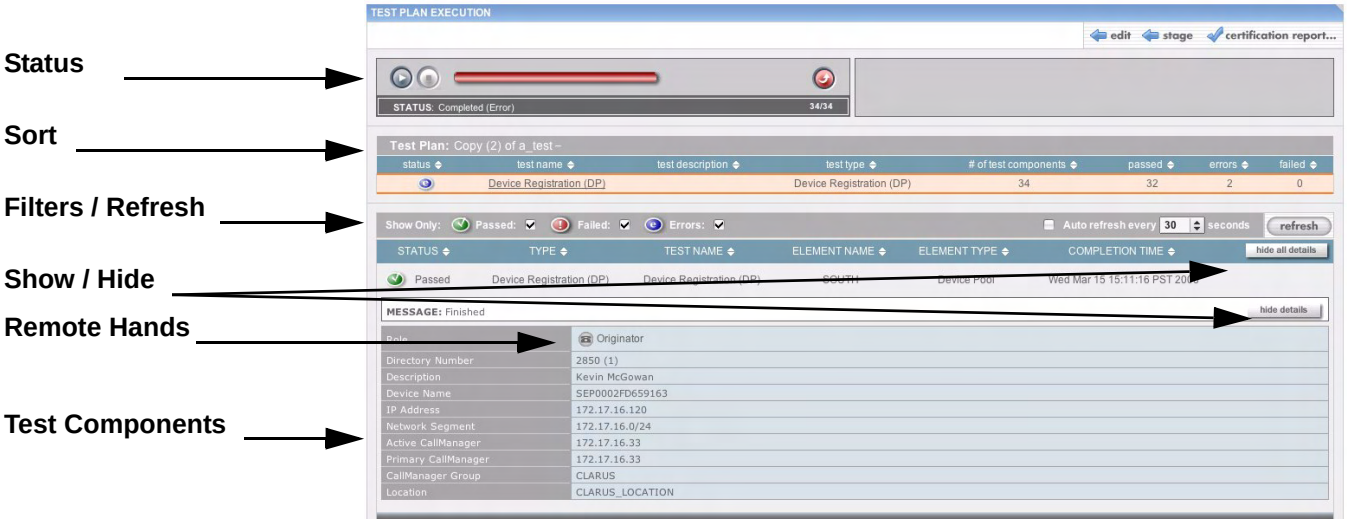


Figure 4-28 Test Plan Results

Each test that is part of the Test Plan is listed, along with its name, element type and element name.

Refresh the test details display by selecting the **Refresh** button. Check the **Auto Refresh** box and enter a number of seconds to refresh regularly.

Display or hide these tests' test components by selecting the **Show/Hide Details** buttons, as shown in Figure 4-29.

Errors are conditions where the test was not able to execute or complete. Failed tests did not receive the expected response based on user-defined parameters or established success criteria. For information about failed and error conditions, see Chapter 5, *Test Interpretation*.

Filtering Detailed Test Results

You can filter your display so that it shows only specific areas of interest to you. For example, if you select the **Passed** box and click **Refresh**, only the portions of your test that passed will be displayed.

Sorting Detailed Test Results

You may sort the items displayed under Test Plans currently running and under test details. Items may be displayed in ascending or descending alphabetic order. Columns which may be used as sorting items display two white arrows. Clicking a column name sorts the Test Plans by the column's contents in descending alphabetical order. For example, clicking *Test Name* under the currently running test plans section, lists all Test Plans in descending alphabetic order by Test Name. Clicking the column name again reverses the sort order.

Generating a Certification Report

Once your Test Plan completes, the **certification report** button becomes available.

Generate Report

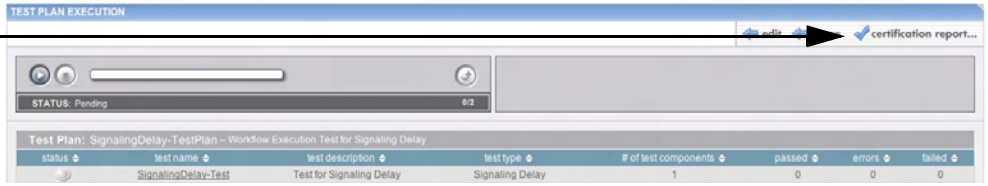


Figure 4-29 Generate Report

Certification reports allow you to print a compilation of all tests run for you records. For more information, see *Certification Summary* on page 6-14.

Launching Remote Hands

A small phone icon will display next to the Originator for each Test Component. Clicking on this icon starts the Remote Hands application, which allows you to remotely control the phone. In order to run Remote Hands, you must have a Java Runtime Environment installed. This download installer is available from:

```
http://<csipc-address>/clarusipc/jre-installer/jre-1_5_0_06-
windows-i586-p.exe
```

Where <*csipc-address*> is the hostname or IP address of the ClarusIPC server.

NOTE: For a list of Cisco phones supported for Remote Hands, please see Appendix D, *Phone Models / Test Type Matrix*.

To open the Remote Hands interface, click the phone icon:

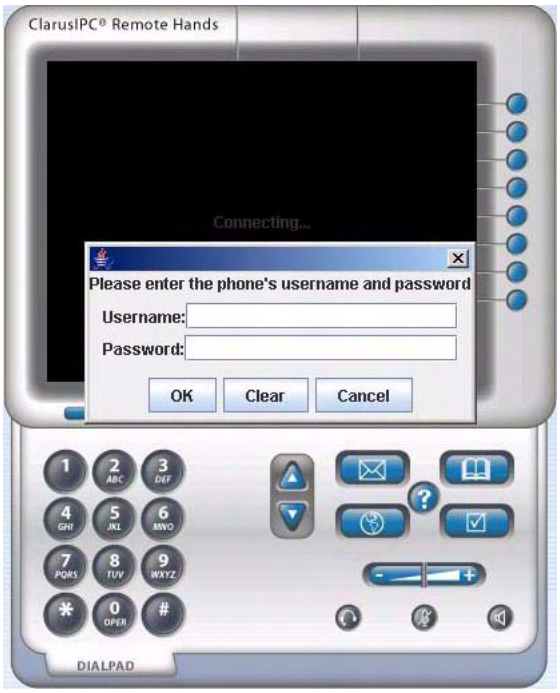


Figure 4-30 Remote Hands Login

Enter a CUCM LDAP user associated with the phone you are troubleshooting. The following screen displays:

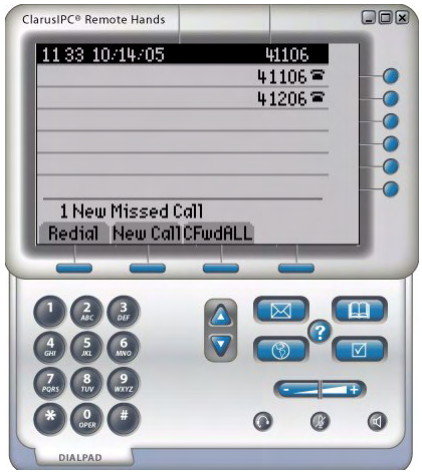


Figure 4-31 Remote Hands

Controlling the Phone

Control the phone using the mouse to click buttons and dial numbers. The phone's display will alter to match the display on the actual phone. You can also control the phone with your computer's keyboard using the following shortcuts.

Table 4-2 Shortcuts

Phone Option	Shortcut
Number Pad 0-9	0-9
# Pad	#
* Pad	*
VolUp	+
VolDwn	-
Headset	h
Speaker	s
Mute	m
Info	i
Messages	v
Services	l
Directory	d
Settings	t
NavUp	Up
NavDwn	Down

Test Descriptions

This section describes each test available for creating Test Plans. Each test description contains discussions of its field values, test elements and dependencies. (Dependencies are items that need to have been defined before you can use the test in a test plan. For example, the Voice Protocol OffNet test requires that you have at least one entry in the Phonebook with the call classification of VP OffNet.)

Class of Service

Class of Service tests focus on verification of calling privileges of users.

Call Permission

This test verifies whether a User Class is either allowed or blocked from calling a particular OffNet dialing string as defined in the Phonebook. The terminating device is not expected to be controllable, but rather answer automatically within a specified timeout. The expected outcome of the call (allow or block) is defined as part of the User Class intent properties. For each User Class selected, IP Phones representing that class will be randomly selected to dial one dialing string for each call classification (internal, local, long distance) selected. A Block outcome means that only if the call fails to connect will the test pass.

Dependencies

The Calling Permissions test requires that all call classifications selected to be tested for either **allow** or **block** results *MUST* have at least one entry in the Phonebook with the same call classification. (The third option, **ignore**, does not require matching entries, as these call classifications will not be tested.) If there are no entries for even one classification, the test will display zero selected phones for that User Class.

Table 4-3 Call Permissions Parameters

Field Name	Values	Description
Connection Timeout	• 10 minimum • 60 maximum • 30 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Test Elements	One or more User Classes	Phones are randomly chosen from selected User Classes.

Network

Network tests provide verification of the signaling and audio portion of your IPC system. ClarusIPC offers the following network test types:

- Device Registration (DP): By Device Pool
- Device Registration (Loc): By Location
- Device Registration (NS): By Network Segment
- Signaling Delay
- Voice Protocol OnNet (DP): By Device Pool
- Voice Protocol OnNet (Loc): By Location
- Voice Protocol OnNet (NS): By Network Segment
- Voice Protocol OffNet (DP): By Device Pool
- Voice Protocol OffNet (Loc): By Location
- Voice Protocol OffNet (NS): By Network Segment

Device Registration

This test verifies that an IP phone in a specific network segment, Device Pool, or location can register to the configured primary CUCM. If the primary CUCM is not reachable via SCCP, the IP phone will not be able to register and will either register to a backup CUCM/SRST or stay unregistered.

NOTE: This test is NOT designed to report on phone registration status. In fact, unregistered phones are automatically excluded from the test during the staging process. To view registration status, use the Reports module Phone Registration Report.

Table 4-4 Device Registration Parameters

Field Name	Values	Description
Test Elements	• Network Segments • Device Pools • Locations	Phones are chosen randomly from the OnNet Resource Pool belonging to the specified element.

Signaling Delay

This test verifies that an IP Phone in a specific Device Pool can receive a request for service acknowledgement (dial tone) from the configured primary CUCM within a predetermined time period.

Table 4-5 Signal Delay Parameters

Field Name	Values	Description
Max Delay	• 200 minimum • 5000 maximum • 1000 default	Use the **Default** value, (ms), unless you have more strict requirements on delay, or remote offices that cause longer, yet acceptable delays.
Test Elements	Device Pools	Phones are chosen randomly from the OnNet Resource Pool belonging to the specified Device Pool.

Voice Protocol OnNet

This test allows you to verify that there is no problem routing required voice protocols over various network paths in your deployment. These network paths are identified by two endpoints which can be either network segments, locations, or Device Pools. For example, if you plan to exercise this test between branch offices over WAN links, you might wish to use the location form of this test, assuming phones in each branch office have a unique location. On the other hand, for single-site campus deployments, either Device Pool or network segment forms can provide the granularity necessary to exercise inter-CUCM and inter-VLAN verification or protocol routing. For each path, an originating phone is randomly selected from one side and a terminating phone from the other side. Once the call is in progress, the voice stream flow will be verified.

By increasing the sampling rate, you obtain more data points and increased confidence in your network configuration.

Table 4-6 Voice Protocol OnNet Parameters

Field Name	Values	Description
Connection Timeout	• minimum: 5 • maximum: 30 • default: 15	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed). **NOTE:** Do not change this value unless you are getting failures due to the call setup time being too long.
Transform Mask	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* on page 4-6 for more information.)
Test Elements	Network path defined by: • Network Segments • Device Pools • Locations	For each element, two phones are randomly selected to represent each endpoint and make the call. Endpoints may be selected by pairs of Device Pools, locations, or network segments. All phones must be in the OnNet Resource Pool.

Voice Protocol OffNet

This test exercises the ability of a phone to place an OffNet call to a station on the PSTN. It is assumed the end station cannot be controlled by ClarusIPC and will, therefore, need to answer automatically after a predetermined number of ringbacks. This test also verifies audio path (RTP) communication between the gateway and the originating phone.

Each test component consists of a phone and a dialing string from the Phonebook that belongs to the Voice Protocol OffNet call classification. You can have several Phonebook entries with this classification. The more you have, the more components can be run simultaneously (fewer bottlenecks waiting for an available PSTN phone.)

Dependencies

The Voice Protocol OffNet test requires that you have at least one entry in the Phonebook with the call classification of VP OffNet; that is, at least one phone to test to. The more entries you have, the more tests may be run simultaneously, and, therefore, the less time required to complete the test.

Table 4-7 Voice Protocol OffNet Parameters

Field Name	Values	Description
Connection Timeout	• 10 minimum • 60 maximum • 30 default	The connection timeout (sec) to wait for the call to be connected (measured from the moment the last digit is dialed).
Test Elements	• Network Segments • Device Pools • Locations	Phones are randomly chosen from the OffNet Resource Pool based upon the chosen element.

Route Plan

Route Plan tests focus on exercising all aspects of call routing, from pattern matching, to route selection and path verification. ClarusIPC offers the Direct Inward Dial test.

Direct Inward Dial

Verifies that PSTN DID numbers can be dialed and ring on the correct internal phone's primary directory number. This test uses internal phones, found in the OnNet Resource Pool, to dial the PSTN DID number generated, by either applying a user-supplied transform mask to the directory number, or by looking up an alternate number from the Augmented Data information on the targeted phone. The call will traverse a gateway, hairpin at the local Central Office, and return back into the network, ringing the internal target phone. ClarusIPC will automatically answer this call to complete the test.

Alternate DID numbers are used when:

a. your PSTN DID numbers do not have any overlap with the internal primary directory numbers; or

b. additional numbers that route to user primary directory numbers must be tested, such as 1-800 numbers.

In this case, you must first import these numbers as augmented data to the desired phones. The Alternate DID1 field is recommended to use for case a above, whereas Alternate DID2 is recommended for the case b.

Table 4-8 Direct Inward Dial Parameters

Field Name	Values	Description
Alternate DID 2	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	If checked, the system will use the Alternate DID 2 added through augmented data. If unchecked, and an alternate DID 1 has been added, it will be used instead. (See *Augmenting Device Data* on page 2-14 for more information.)
Connection Timeout	• 5 minimum • 30 maximum • 15 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Transform Mask	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* on page 4-6 for more information.)
Test Elements	One or more Phone Groups	These Phone Groups must contain phones whose primary directory number is configured with a valid DID number.

Application

Application tests exercise the function of supporting communications applications. ClarusIPC offers the Directory Handler Lookup, and the Meet-me Conference tests.

Directory Handler Lookup

This test verifies that the Directory Handler (dial-by-extension) function of the Auto Attendant application allows users to select, dial, and connect to the primary Directory Number on a target set of phones. The Auto-Attendant number is dialed by a supporting resource, and the sampled phones from the Phone Group are accessed and called to ensure they are listed and reachable through the application.

Table 4-9 Directory Handler Lookup Parameters

Field Name	Values	Description
Connection Timeout	• 10 minimum • 60 maximum • 30 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Prefix Digits	0-9, *, #	Digits required to navigate to the Directory Handler portion of the application. Enter whichever string (if any) of digits allows you to hear a message similar to "Enter the extension of the person you are trying to reach."
Postfix Digits	0-9, *, #	Digits (if any) required to signify that the extension has been entered completely. Typically this value is either blank (no digit required) or #.
Transform Mask	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* for more information.)
Test Elements	One or more Phone Groups.	This test requires one supporting resource to originate the call to the target resource.

Meet-me Conference

This test requires one supporting resource to a Phone Group to originate the call to the target resource. Verifies that a user-supplied number of users can dial a specific Meet-me pattern and participate in a conference call. As the test begins, the first number in the Meet-me pattern is selected; supporting resources begin calling this number until the maximum load is attained.

Table 4-10 Meet-me Conference Bridge Parameters

Field Name	Values	Description
Connection Timeout	• 10 minimum • 60 maximum • 30 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Maximum Connections	Minimum of 1 and maximum of 8 numeric characters (0-9)	The number of phones taking part in the conference.
Test Elements	• Meet-Me Patterns	The conference bridge/meet-me pattern configuration. All resources must have appropriate calling permissions to dial the Meet-me pattern.

Phone Feature

Phone Feature tests exercise phone functionality controlled by device profiles and directory number properties. ClarusIPC offers the Softkey Functions, the Forward to Voice Mail, and the Rollover tests.

Forward to Voice Mail

This test verifies that a phone's primary directory number will forward *All* or *No* Answer to Voice Mail (specifically, to an endpoint that will auto-answer).

Table 4-11 Forward to Voice Mail Parameters

Field Name	Values	Description
Connection Timeout	• 5 minimum • 30 maximum • 15 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Transform Mask	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* on page 4-6 for more information.)
Test Elements	One or more Phone Groups.	This test requires one supporting resource to originate the call to the target resource.

Rollover

This test verifies that a call to a phone's primary directory number will be forwarded to the second line on the same phone when the first line is busy.

Table 4-12 Rollover Parameters

Field Name	Values	Description
Connection Timeout	• 5 minimum • 30 maximum • 15 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Transform Mask	Minimum of 1 and maximum of 15 alphanumeric characters (0-9, X)	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* on page 4-6 for more information.)
Test Elements	One or more Phone Groups.	This test requires two supporting resources, both originators, to generate separate calls to line one on the target resource. The target resource phone is randomly selected from the defined Phone Group; the supporting comes from the OnNet Resource Pool. When creating your Phone Group, select only phones equipped with rollover.

Softkey Functions

This test exercises the phone functions listed below to determine that they operate correctly by mimicking user button pushes on the phone control panel. Select which functions to test in the OPTIONS section. All selected functions will be tested against the sampled amount of each Phone Group chosen as a test element.

NOTE: This test requires that the phone support XML. For a list of Cisco phones supported by Softkey Functions, please see Appendix D, *Phone Models / Test Type Matrix*.

Select a function for testing by checkmarking it. Skip that function by removing the check. Default is **Test All.** Select a sampling rate and Phone Group test elements.

Table 4-13 Softkey Functions

Function	Description
Transform Mask	The mask used to translate the targeted phone's directory number into an external, OffNet number. (See *Abbreviated Dialing* on page 4-6 for more information.)
AdHoc Conference	Verifies that phones can establish a 3-way conference call with two auto-selected phones using the *Confirm* softkey.
Call Transfer	Verifies that phones can perform a blind transfer of an incoming call to another destination using the *Transfer* softkey.
Corporate Directory	Verifies that a phone can access the corporate directory to navigate, and dial-by-number to the destination as defined in the Phonebook.
Call Hold	Verifies that a phone can make a call to an autoselected phone and place the called party on hold using the *Hold* softkey.
Call Park	Verifies that a phone can park an outgoing call by using the *Park* softkey, and that this call can be retrieved by a third auto-selected phone.
Redial	Verifies that a phone can make a call, hang up, and redial the same auto-selected phone as before using the *Redial* softkey.
Use Abbreviated Dialing	If checked, verification of calling permissions will not be run as part of the Test's staging process.

Dependencies

The Corporate Directory function, if selected, requires that your Phonebook has at least one entry with the call classification *Corporate Directory Search Number.* The phone must also be included in the Phone Group as an OnNet Resource Constraint.

Capacity

Capacity tests are designed to load components of an IPC system that have maximum expected thresholds. ClarusIPC offers the Voice Mail Port Loading test.

Voice Mail Port Loading

Verifies that the CUCM is correctly configured with the appropriate number of voice mail ports, that they are set to forward to the next port in line, and that the last port forwards to a useful destination (typically, the receptionist).

Table 4-14 Voice Mail Port Loading Parameters

Field Name	Values	Description
ConnectionTimeout	• 5 minimum • 30 maximum • 15 default	The connection timeout (sec) to wait for the call to be connected (measured from after the last digit is dialed).
Maximum Connections	Minimum of 1 and maximum of 8 numeric characters (0-9)	The number of phones taking part in the conference.
Overload	• True • False	Whether or not to allow the phone to be forwarded in the case of overloaded calls.
Test Elements	Voice Mail Profiles	This test uses devices to call the Voice Mail port DN matching the VM pilot number that is referenced from the specified VM profile.

CHAPTER 5 TEST INTERPRETATION

ClarusIPC features enhanced test results, including relevant device information from the inventory and additional real time execution metrics. Using this information, you can expedite the process of troubleshooting errors and failures in your test results.

In the results, each test produces a specific set of test result values and messages. In this chapter, we offer next steps to investigate errors and failures, and provide a table outlining resource selection rules.

Viewing Test Results

From the **Test Plan Execution** screen, select **Certification Report** to open the Generate Report window.

Certification Report

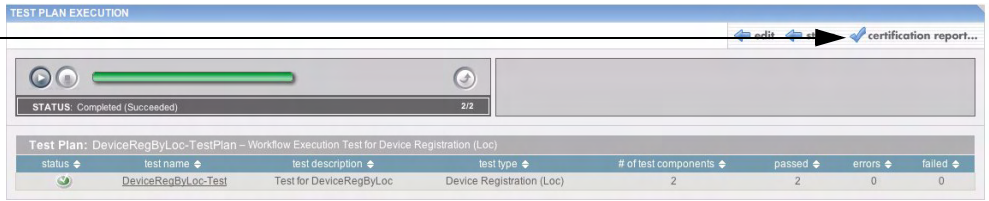


Figure 5-1 Select Certification Report

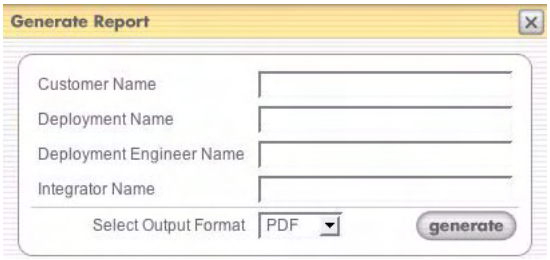


Figure 5-2 Generate Report

In the Generate Report window, enter the requested fields, select an output format (PDF, HTML, CSV, or XLS), and click **generate**. (You may leave the fields blank, if you wish, and simply click **generate**.)

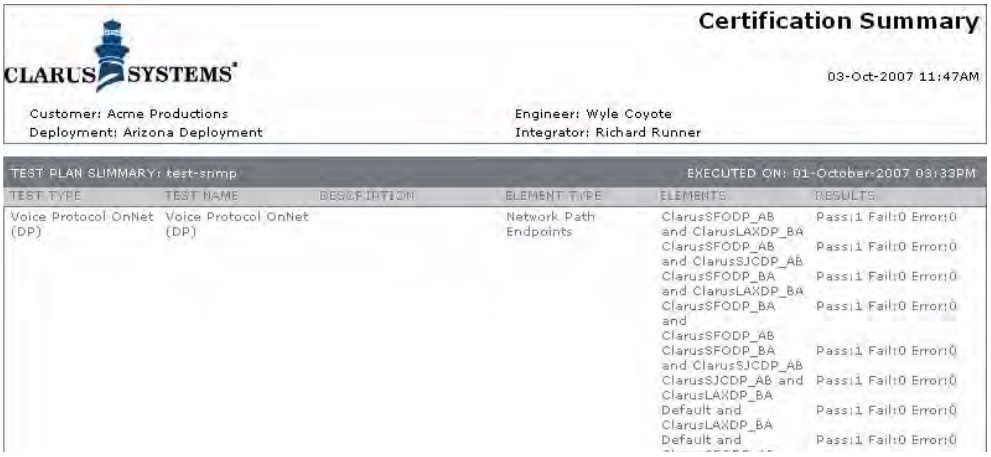


Figure 5-3 Certification Summary Report

The top portion provides a summary of the test results. The details portion displays individual results of each element tested. The bottom portion of the test provides a sign-off sheet for you and your customers. For information about printing this report, see *Printing Tips* on page 6-16.

Interpreting Test Errors

Test Message Classification

The following results can be returned:

- Pass
- Failure
- Error

Pass

The application was able to successfully perform the test using the specified resources & target devices.

AND

Any measured values were within acceptable limits and/or the functionality being tested was successfully verified.

Failure

The application was able to control and initialize devices to perform the test.

AND

Measured values that specifically relate to the functionality tested were not within acceptable limits, and/or the functionality tested could not be successfully verified.

Error

The application attempted to perform the test, but was not able to successfully complete it. The errors are divided into two types: Device Initialization, & Test Interruption.

Device Initialization

When the application begins the execution of a test, it first attempts to initialize the target devices and supporting resources to verify that they are ready to be used in the test. If there is a problem initializing the device, the test is stopped and an error is reported.

Sample errors of this type include:

- Previously registered devices (at time of synchronization) are currently unregistered.
- Devices are currently in use.
- Devices are unresponsive within specified timeout limits.
- Device profile has changed since last synchronization time.

Test Interruption

While the application is performing the test, it is monitoring for events and activities that would interfere with the outcome of the test. If such an event/activity is detected, the test is stopped and an error is reported.

Sample errors of this type include:

- User-Initiated Disconnect
- Device Interruption
- Inbound call interference

Test Result Message Formatting

Most error messages are provided with the following syntax:

`[41105] Step` *`[Step]`* `resulted in` *`[Result]`* `expected` *`[Return]`*

The *Step*, *Result*, and *Return* will vary:

- *Step* shows what the test was doing when the error or failure occurred.
- *Result* shows what actually happened when performing that action.
- *Return* shows what the test expected to happen as a result of that action.

For example:

```
Step [MakeCallImpl] resulted in [DeviceConnected] expected
[CallCannotConnect]
```

During this test, the application attempted to make a call and received a message back saying that the call was completed. `[MakeCallImpl]` was the step in the process that the test was executing when the failure `[DeviceConnected]` occurred, when it was expecting a `[CallCannotConnect]` response.

NOTE: When examining your results, keep in mind that the inventory data displayed here is accurate as of the last sync prior to test plan execution. If you have synchronized since executing the test plan, the inventory data you find in other areas of the application might not match up with the results on screen.

NOTE: Any synchronization performed subsequent to the execution will only update the current inventory data set for the Cluster. Synchronizing will not update any inventory data in your test plan results.

Test-Specific Result Interpretations

This section contains generic and specific interpretations of test results for some specific test types, including sample messages with explanations.

Generic Results

The following error and failure messages may be displayed across all test types. Some possible causes are listed below:

Table 5-1 Generic Test Results

Failure	Explanation
Runtime Exception occurred during execution.com.cisco.jtapi.PlatformExceptionImpl: or Unable to create provider -- bad login or password.	Bad CTI manager login or password.
`Step [UsageCheckImpl] resulted in [DeviceInUse] expect [DeviceNotInUse]`	A device in the test is already in Use and could not be initialized.
`Step [InitFeatureDeviceImpl] resulted in [DeviceTimeOut] expected [DeviceInitalized]`	• A device (or line) is in the test which does not exist in the CUCM. • The configured CUCM user is not enabled as a super provider • A device is not associated to the configured CUCM user

`Step [MakeCallImpl] resulted in [DeviceTimeOut] expected [DeviceConnected]`
or
`Step[CompleteAnswerCallImpl] resulted in [DeviceTimeOut] expected [DeviceConnected]`
	A call in the test was placed but not connected.

`Step [MakeCallImpl] resulted in [CallCanNotConnect] expected [DeviceConnected]`	Call permissions or some CUCM limitation prevents the call from being placed.

Class Of Service: Call Permissions

Sample Test Result Data:

Phonebook Entry	Call Classification	Allow/Block	Dialed Number
Dateline	Pay-per-call	Block	919006801120
MESSAGE: Finished			

Role	Target
Directory Number	2878 (1)
Description	John Smith
Device Name	SEP00137AAAFE91
IP Address	172.17.16.62
Dialed Number	915107773456
Remote Gateway	172.17.16.1:19084
Sender Codec	G.711u
Receiver Codec	G.711u
CSS DN	XYZCORP_LOCAL
CSS Phone	XYZCORP_911
Active CUCM	172.17.16.44
CUCM Group	XYZ
Connection Time (ms)	6344
Connection Timeout Limit (ms)	30000

Sample Messages:

Table 5-2 Call Permissions Results

Failure	Explanation

`Step [MakeCallImpl] resulted in [CallCannot-Connect] expected [DeviceConnected]`
or
`Step [MakeCallImpl] resulted in [DeviceCon-nected] expected [CallCannotConnect]`
	The resource dialed the digits but the outcome (allow/block) did not match the intended outcome as defined by the User Class. Examine the relevant route pattern defined in CUCM and its associated permission set-tings. All block reasons will be detected by this test (e.g. Call Reject, No Error, etc.).

Network: Device Registration by Device Pool / Network Segment / Location

Sample Test Result Data:

Role	Originator
Directory Number	2200 (1)
Description	North Conference Room
Device Name	SEP000AAAABB46E
IP Address	172.17.16.74
Network Segment	172.17.16.0/24
Active CUCM	172.17.16.44
Primary CUCM	172.17.16.44
CUCM Group	XYZ
Location	XYZ_LOCATION

Sample messages:

Table 5-3 Device Registration Results

Failure	Explanation
`Step [CheckRegistrationImpl] resulted in [NotRegisteredToPrimary] expected [DeviceRegisteredToPrimary]`	The device being tested was queried to determine its active CUCM value. If the device is not registered to its primary CUCM, we report a failure. In this case, the device was registered and upon querying the device we received a value that did not match the expected primary CUCM value.
`Step [CheckRegistrationImpl] resulted in [NotRegisteredToPrimary] expected [DeviceRegisteredToPrimary] ACTUAL [registered to secondary]`	If the active CUCM value returned was something other than the primary CUCM value, ClarusIPC reports a failure. Investigate the availability and reachability of the device's primary CUCM and TFTP server.

Network: Signal Delay

Sample Test Result Data:

Role	Originator
Directory Number	2875 (1)
Description	Bob Smith
Device Name	SEP000AAAAEF6C8
IP Address	172.17.16.60
Network Segment	172.17.16.0/24
Active CUCM	172.17.16.44
Primary CUCM	172.17.16.44
CUCM Group	XYZ
Device Pool	NORTH
Signaling Delay (ms)	266
Signaling Delay Limit (ms)	1000

Sample messages:

Table 5-4 Signal Delay Results

Failure	Explanation
delay exceeds threshold value set	ClarusIPC attempts to measure signal delay by first taking the device off-hook via a request to the CTI Manager. It then monitors the delay between acknowledgement of the off-hook request, and the service acknowledgement from the primary CUCM. If this delay exceeds the threshold defined in the test parameter, ClarusIPC reports a failure. Investigate the network bandwidth utilization and/or QOS settings.

Phone Features: Softkeys: Corporate Directory Lookup

Sample Test Result Data:

Role	Originator
Directory Number	2200 (1)
Description	Jerry Garcia-Conference Room
Device Name	SEP0002FD3BB46E
IP Address	172.17.16.74
Softkey Template	Enhanced User
Directory Lookup Number	
Connection Time (ms)	
Connection Timeout Limit (ms)	

Sample messages:

Table 5-5 Softkey Results

Failure	Explanation
Error: Unable to find Terminator	The system was unable to find a Corporate Directory Phonebook entry.

CHAPTER 6 REPORTS

ClarusIPC gives you the ability to generate reports about the configuration of integral components in your Communications Manager system. Reports are broken down by categories, and may either be summary in nature, for producing As-Built documentation, or detailed for troubleshooting purposes. Most reports may be generated as HTML, PDF, XLS, CSV, and DOC files.

Available Reports

Reports are organized by type.

- **Service Analysis** reports compile a high level list of failures and alerts generated during a specified time frame. These reports rely on CDR/CMR data collection. For more information on defining the CDR/CMR collection schedule, please see Chapter 2, *ClarusIPC Clusters*.
- **Change Tracking** reports describe changes in Cluster inventory and CUCM system components between two selected Snapshots. (A Snapshot is the data collected while performing a full Sync.)
- **Inventory Summary** reports provide a high-level overview of your Cluster layout; Feature objects, and Route, Service, and CUCM System components.
- **System** reports provide detailed lists of system elements, such as Device Pool components, Service Parameters, and Enterprise Parameters.
- **Route Plan** reports describe your network's route plans and directory number structures.
- **Media** reports provide lists of media resources, such as Conference Bridges and Media Termination Points.
- **Voice Mail** reports provide information on your Voice Mail system.
- **Device** reports provide summary and detailed device information.
- **Special** report provides a starting point for augmenting data.
- **Security** reports provide phones' security-related properties.
- **Test Results** reports provide a list of the reports run at the completion of test execution. This offers you a printed compilation of test results to be used as documentation at the end of the testing cycle.

(Service Analysis and Change Tracking reports are available only with certain licensing options. Please contact Clarus Systems for more information.)

The following is a list of available reports:

Table 6-1 Available Reports

Category	Report	Description
Service Analysis	Alert Details	A detailed listing of unacknowledged alerts [xls, csv] (ver. 001)
	Business Hour Call Failures	A raw, unformatted listing of failed call setup attempts during the last 12 hours [xls, csv] (ver. 002)
	Daily Alert Summary	A high level summary of Voice Monitor alerts generated over the last day [pdf, html, doc] (ver. 001)
	Daily Call Failures	A raw, unformatted listing of failed call setup attempts during the last 24 hours [xls, csv] (ver. 001)
	Daily Call Volume	A summary of inbound, outbound, and total inbound/outbound calls generated over the last day [pdf, html, doc] (ver. 001)
	Daily Most Impacted	A raw, unformatted listing of daily calls impacted by poor voice quality [xls, csv] (ver. 002)
	Hourly Call History	A raw, unformatted listing of all calls made during the last hours [xls, csv] (ver. 001)
	Weekly Call Volume	A summary of inbound, outbound, and total inbound/outbound calls generated over the last week [pdf, html, doc] (ver. 001)
	Hourly Voice and Network Quality	Hourly Voice quality MOS score (MLQKmn) and Network Performance Results [xls, csv] (ver. 002)
	Monthly Alert Summary	A high level summary of Voice Monitor alerts generated over the last month [pdf, html, doc] (ver. 001)
	Monthly Call Failures	A summary of call failures by release cause codes over the last month [pdf, html, doc] (ver. 001)
	Monthly Call Usage	A summary of call usage by user over the last month [pdf, html, doc] (ver. 001)
	Monthly Call Volume	A summary of inbound, outbound, and total inbound/outbound calls generated over the last month [pdf, html, doc] (ver. 001)
	Weekly Alert Summary	A high level summary of Voice Monitor alerts generated over the last week [pdf, html, doc] (ver. 001)
	Weekly Call Usage	A summary of call usage by user over the last 7 days [pdf, html, doc] (ver. 001)

Table 6-1 Available Reports

Category	Report	Description
Change Tracking	Change Summary	A graphical summary of configuration change counts (adds, removes, updates) between consecutive Snapshots grouped by configuration element categories [pdf, html, doc] (ver. 001) Calculates the percentage change between sync counts by dividing the number of changes by the original sync number. For example, after removing 80 devices from a 100 device cluster, the Change Summary report will calculate (removed 80) / (original 100), and show an 80% change.
	Device Defaults Changes	An audit report that highlights Device Defaults updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Directory Number Changes	An audit report that highlights Directory Number moves, adds, and changes between two points in time (based on Snapshots) [pdf, html, xls, doc] (ver. 002)
	Enterprise Parameter Changes	An audit report that highlights Enterprise Parameter updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Media Changes	An audit report that highlights MRG, MRGL updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Phone Changes	An audit report that highlights moves, adds, and changes that occur on devices between two points in time (based on Snapshots) [pdf, html, xls, doc] (ver. 002)
	Phone Accounting	An audit report that highlights adds and removals of phones between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Phone Firmware Changes	An audit report that highlights phone firmware changes (based on Snapshots) [xls, csv] (ver. 001)
	Phone Registration Changes	An audit report that highlights phone registration changes (based on Snapshots) [xls, csv] (ver. 001)
	Phone Relocation	An audit report that highlights relocation of phones to new switch or switchports. (based on Snapshots) [xls, csv] (ver. 001)
	Route Plan Changes	An audit report that highlights Route/Translation Pattern, CSS, Partition, Route Group/List updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)

Table 6-1 Available Reports

Category	Report	Description
(Change Tracking continued)	Routing Device Changes	An audit report that highlights Gateway, Trunk, and Gatekeeper updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Service Parameter Changes	An audit report that highlights Service Parameter updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	System Changes	An audit report that highlights CUCM Group, CUCM, Location and Device Pool updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Template Changes	An audit report that highlights Softkey Template and Phone Template updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Voice Mail Changes	An audit report that highlights Voice Mail Port, Pilot and Profile updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
	Unity Subscriber Changes	An audit report that highlights Unity subscriber updates, adds, and deletes between two points in time (based on Snapshots) [xls, csv] (ver. 001)
Inventory Summary	Cluster Summary	A high-level, executive view of your cluster layout [pdf, html, xls, doc] (ver. 001)
	Device Distribution	A high-level executive view of your devices [pdf, html, doc] (ver. 001)
	Device Pool Load	A summary of device counts by device pool, CMG, and CallManager [xls, csv] (ver. 001)
	Device Summary	A summary of device counts by type [xls, csv] (ver. 002)
	Feature Summary	A detailed listing of Feature objects including Client Matter & Forced Authorization Codes, Meet Me Patterns, and Voice Mail Ports/Profiles [pdf, html, xls, doc] (ver. 001)
	Monthly Inventory Trends	A summary of Inventory Trends for the last month [pdf, html, doc] (ver. 001)
	Route Plan Summary	A detailed list of route components including Calling Search Spaces, Partitions, Route/Translation Patterns, and Route Filters [pdf, html, xls, doc] (ver. 001)

Table 6-1 Available Reports

Category	Report	Description
(Inventory Summary continued)	Service Summary	A detailed listing of Service objects including Conference Bridges, Media Resource Groups, and Service Parameters [pdf, html, xls, doc] (ver. 001)
	System Summary	A high-level view of your CallManager System components including CallManager Servers, Groups, and Device Pools [pdf, html, xls, doc] (ver. 001)
System	Component Versions	A raw, unformatted, list of component versions for each server in the Cluster. [xls, csv] (ver. 001)
	Device Pools	A raw, unformatted list of device pool components [xls, csv] (ver. 001)
	Enterprise Parameters	A raw, unformatted list of Enterprise Parameters. [xls, csv] (ver. 001)
	Installed Applications	A raw, unformatted listing of all installed applications on each CUCM server [xls, csv] (ver. 001)
	Installed CUCM Components	A raw, unformatted listing of all installed CUCM component applications on each CUCM server [xls, csv] (ver. 001)
	Locations	A raw, unformatted list of locations [xls, csv] (ver. 001)
	Regions	A raw, unformatted list of regions [xls, csv] (ver. 001)
	Server Storage	A raw, unformatted listing of all storage volumes and their usage for each CUCM server [xls, csv] (ver. 001)
	Service Parameters	A raw, unformatted list of device defaults by Device Pool. [xls, csv] (ver. 001)
	Unity Installed Applications	A raw, unformatted listing of all installed applications on each Unity server [xls, csv] (ver. 001)
	Unity Storage	A raw, unformatted listing of all storage volumes and their usage for each Unity server [xls, csv] (ver. 001)
Route Plan	10-Digit DN Pattern Summary	A DN report summarizing NPA-NXX groupings used to help identify suspect (fat fingered) 10-digit directory numbers [xls, csv] (ver. 001)
	Directory Number	A breakdown of all directory numbers, their properties, and assigned phones [pdf, html, xls, doc] (ver. 001)
	Unassigned Directory Number	A breakdown of all unassigned directory numbers and their properties [pdf, html, xls, doc] (ver. 001)
	CTI Route Point	A raw, unformatted, detailed inventory of all CTI Route Points [xls, csv] (ver. 002)

Table 6-1 Available Reports

Category	Report	Description
(Route Plan continued)	Call Handling	A detailed, raw line listing displaying all call handling fields for lines and associated directory numbers. [xls, csv] (ver. 004)
	Call Park Numbers	A raw, unformatted list of Call Park numbers [xls, csv] (ver. 001)
	Call Permissions	A raw, unformatted list of Calling Search Spaces and associated Partitions [xls, csv] (ver. 001)
	Call Pickup Groups	A raw, unformatted, list of call pickup groups. [xls, csv] (ver. 001)
	Line Groups	A raw, unformatted list of devices used for line groups. [xls, csv] (ver. 001)
	Routing Devices	A raw, unformatted, list of devices used for call routing such as gateways and trunks. [xls, csv] (ver. 001)
	Routing Patterns	A raw, unformatted list of route and translation patterns. [xls, csv] (ver. 002)
	Time Schedules	A raw, unformatted list of Time Schedules [xls, csv] (ver. 001)
Media	Conference Bridges	A raw, unformatted list of conference bridges [xls, csv] (ver. 001)
	Media Resource Groups	A raw, unformatted list of Media Resource Groups [xls, csv] (ver. 001)
	Media Termination Points	A raw, unformatted list of media termination points [xls, csv] (ver. 001)
Voice Mail	Voice Mail Ports	A raw, unformatted, list of Voice Mail ports. [xls, csv] (ver. 001)
	Unity Subscribers	A detailed, raw line listing displaying all unity subscriber fields for associated directory numbers. [xls, csv] (ver. 001)
Device	Phone Configuration Summary	A summary of all phone configurations grouped by Device Pool [pdf, html, xls, doc] (ver. 002)
	Phone Inventory	An inventory listing of selected phones, their Serial Number, specific switchport locations and settings [pdf, html, csv, xls, doc] (ver. 001)
	Phone Profile	A breakdown of phone profiles including assigned Directory Numbers, Calling Search Space, Device Pool, and Softkey Template [pdf, html, csv, xls, doc] (ver. 001)

Table 6-1 Available Reports

Category	Report	Description
(Device continued)	Phone Version	An inventory listing of specified phones, their serial number and app load, boot load, hardware revision and version [pdf, html, xls, doc] (ver. 001)
	Registered Phone	A comprehensive listing of all registered phones [pdf, html, xls, doc] (ver. 001)
	Unregistered Phone Listing	A comprehensive summary and listing of all unregistered phones [pdf, html, xls, doc] (ver. 001)
	Detailed Phone Inventory	A raw, unformatted, detailed inventory of selected phones grouped by Device Pools including Model, Primary CallManager, App/Boot Loads, Version, Network Settings, CSS-DN [xls, csv] (ver. 009)
	Device Defaults	A raw, unformatted list of device defaults by Device Pool. [xls, csv] (ver. 001)
	Device Profiles	A raw, unformatted, detailed inventory of all Device Profiles [xls, csv] (ver. 001)
	Phone Load	A raw, unformatted, detailed inventory of selected phones grouped by Device Pools including Model, Primary CallManager, App/Boot Loads, Version [xls, csv] (ver. 010)
	Unregistered Phones	A raw, unformatted, detailed inventory of unregistered phones grouped by Device Pools including Model, Primary CallManager, CallManager Group [xls, csv] (ver. 001)
Special	Augment Data Input	A populated input report to be used to augment data. [xls, csv] (ver. 001)
Security	Phone Vulnerability Assessment	A listing of selected phones security-related properties that may affect their ability to be compromised [pdf, html, xls, doc] (ver. 001)
Test Results	Certification	A detailed report of test plan results. Generate as part of the As-Built documentation delivered upon completion of an IPT rollout [pdf, html, xls, doc] (ver. 001)
	Certification Summary	A summary report of test plan results. Generate as part of the As-Built documentation delivered upon completion of an IPT rollout [pdf, html, xls, doc] (ver. 001)
	Result Details	A detailed list of all test results used to help troubleshoot errors and failures. [xls, csv] (ver. 002)

Generating Reports

Click **reports** in the menu bar to open the **Reports** window:

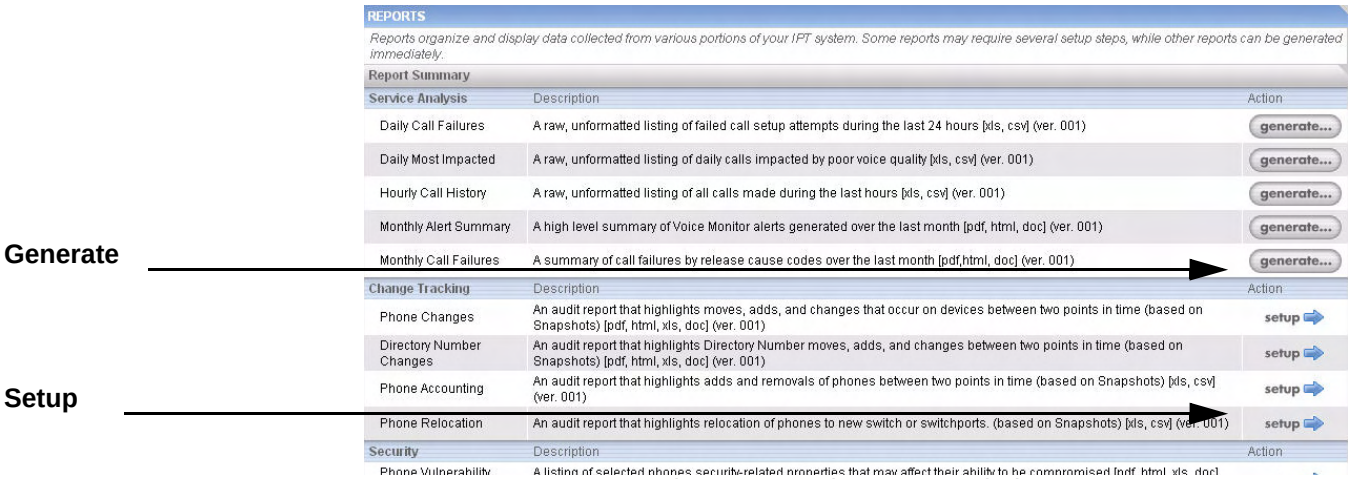


Figure 6-1 Main Reports Window

NOTE: For the majority of Reports, it is strongly recommended that you synchronize your Cluster immediately before generation to ensure that your data is valid and up to date. For the Test Results reports, you must not run a synchronization after running the tests on which you wish to report, or your Test Results data will be lost.

To generate most reports, simply click the **generate** button at the right of their row. To generate configurable reports, click the **setup** button at the right of the row, and follow the prompts.

All reports provide the Generate Report window, in which customized text may be entered which will be printed in the header of the report. (These fields may also be left blank.)

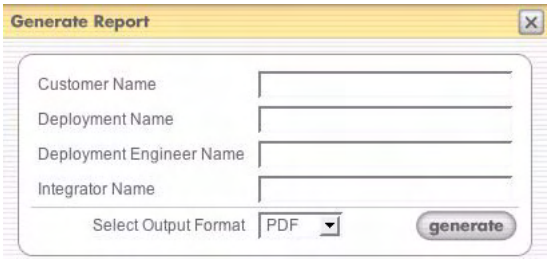


Figure 6-2 Generate Report Window

Most reports may be generated in one of five formats: PDF, HTML, XLS, CSV, or DOC. Some reports, as a result of the number of columns reported, are available only in CSV or XLS file output formats.

Some reports may occasionally return a message of **Unavailable** or **Unsupported** for some phones queried.

- **Unavailable** indicates that the data requested could not be collected during the last Sync.
- **Unsupported** indicates that the queried feature is not supported for the selected device.

Automatically Generated Reports

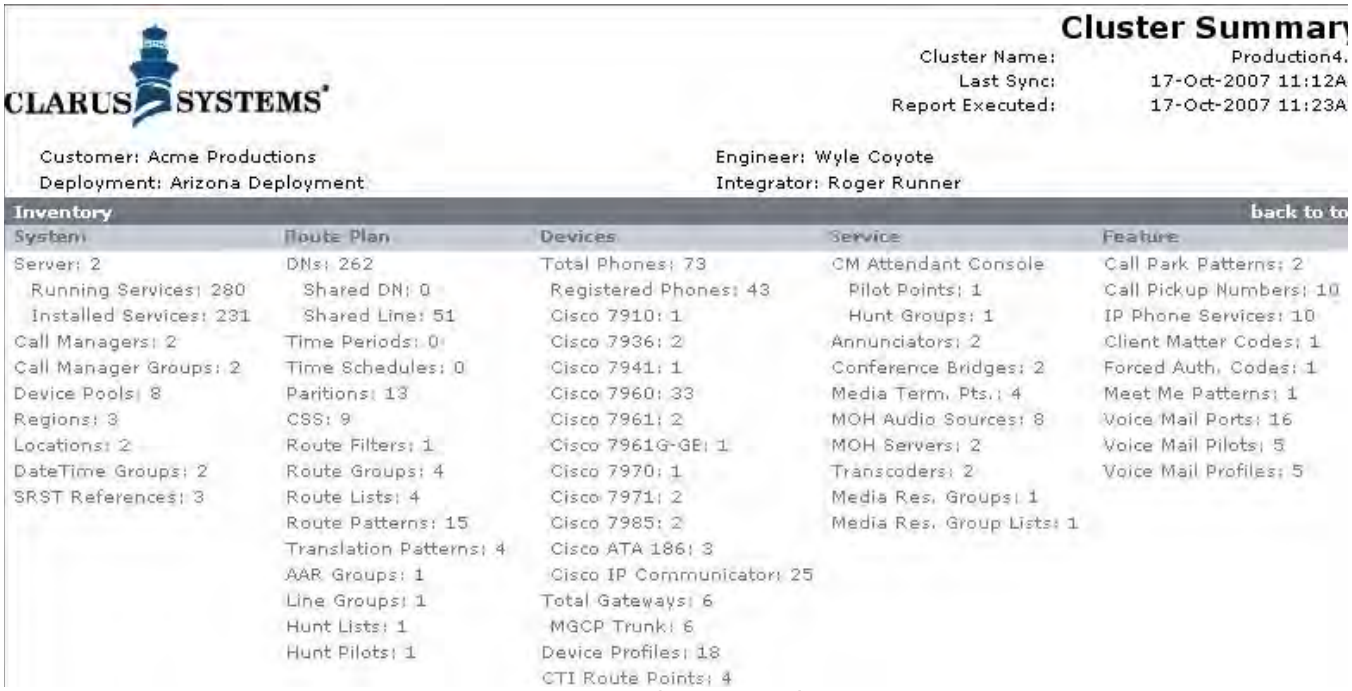
ClarusIPC provides several reports that require no customization. These reports document your telephony system as installed, and include such things as Service Analysis reports, Inventory Summary reports, and Device availability reports.

To generate these reports,

1. click the generate button beside the desired report name,
2. enter the desired company information,
3. select an output format, and
4. click **generate**.

Cluster Summary

The Cluster Summary report lists the Cluster's inventory as of the most recent synchronization. To generate this report, click **reports > Inventory Summary > Cluster Summary**. In the Generate Report window that opens, enter company information as desired, and click **generate**.



CLARUS SYSTEMS

Cluster Summar

Cluster Name: Production4.
Last Sync: 17-Oct-2007 11:12A
Report Executed: 17-Oct-2007 11:23A

Customer: Acme Productions
Deployment: Arizona Deployment
Engineer: Wyle Coyote
Integrator: Roger Runner

Inventory — back to to

System	Route Plan	Devices	Service	Feature
Server: 2	DNs: 262	Total Phones: 73	CM Attendant Console	Call Park Patterns: 2
Running Services: 280	Shared DN: 0	Registered Phones: 43	Pilot Points: 1	Call Pickup Numbers: 10
Installed Services: 231	Shared Line: 51	Cisco 7910: 1	Hunt Groups: 1	IP Phone Services: 10
Call Managers: 2	Time Periods: 0	Cisco 7936: 2	Annunciators: 2	Client Matter Codes: 1
Call Manager Groups: 2	Time Schedules: 0	Cisco 7941: 1	Conference Bridges: 2	Forced Auth. Codes: 1
Device Pools: 8	Paritions: 13	Cisco 7960: 33	Media Term. Pts.: 4	Meet Me Patterns: 1
Regions: 3	CSS: 9	Cisco 7961: 2	MOH Audio Sources: 8	Voice Mail Ports: 16
Locations: 2	Route Filters: 1	Cisco 7961G-GE: 1	MOH Servers: 2	Voice Mail Pilots: 5
DateTime Groups: 2	Route Groups: 4	Cisco 7970: 1	Transcoders: 2	Voice Mail Profiles: 5
SRST References: 3	Route Lists: 4	Cisco 7971: 2	Media Res. Groups: 1	
	Route Patterns: 15	Cisco 7985: 2	Media Res. Group Lists: 1	
	Translation Patterns: 4	Cisco ATA 186: 3		
	AAR Groups: 1	Cisco IP Communicator: 25		
	Line Groups: 1	Total Gateways: 6		
	Hunt Lists: 1	MGCP Trunk: 6		
	Hunt Pilots: 1	Device Profiles: 18		
		CTI Route Points: 4		

Figure 6-3 Cluster Summary Report

Configurable Reports

ClarusIPC also provides several reports which allow you to select parameters controlling the reports. To generate these reports, click the **setup** button to the right of the report name, and follow the prompts.

Directory Number Changes

Change Tracking reports describe changes in Cluster inventory and CUCM system components between two selected Snapshots (data collected during a full sync).

The Directory Number Changes report displays changes in devices between two Snapshots, including added, removed, and changed directory numbers.

1. To generate the report, click **reports > Change Tracking > Directory Number Changes**.

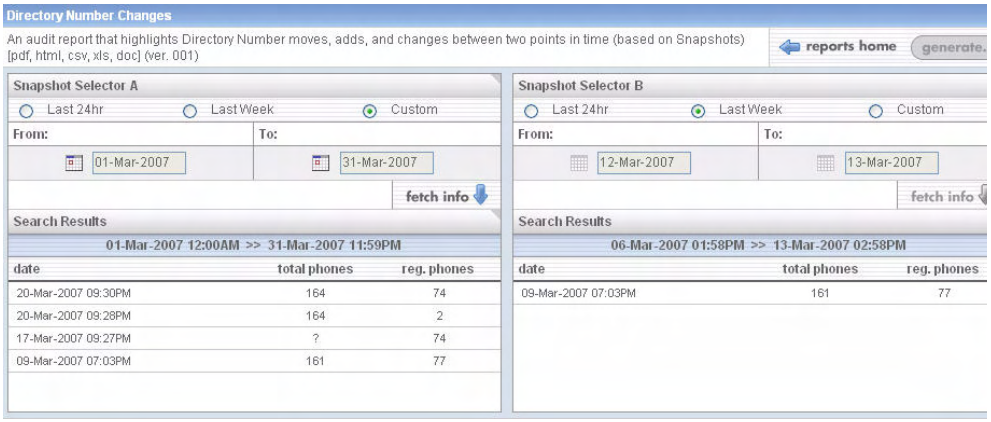


Figure 6-4 Snapshot Selector

2. For each Snapshot, select a date range and click **Fetch Info** to list the synchronizations performed within that range.
3. To generate the report, select one Snapshot from the Selector A pane, and one from Selector B, and click **generate**.

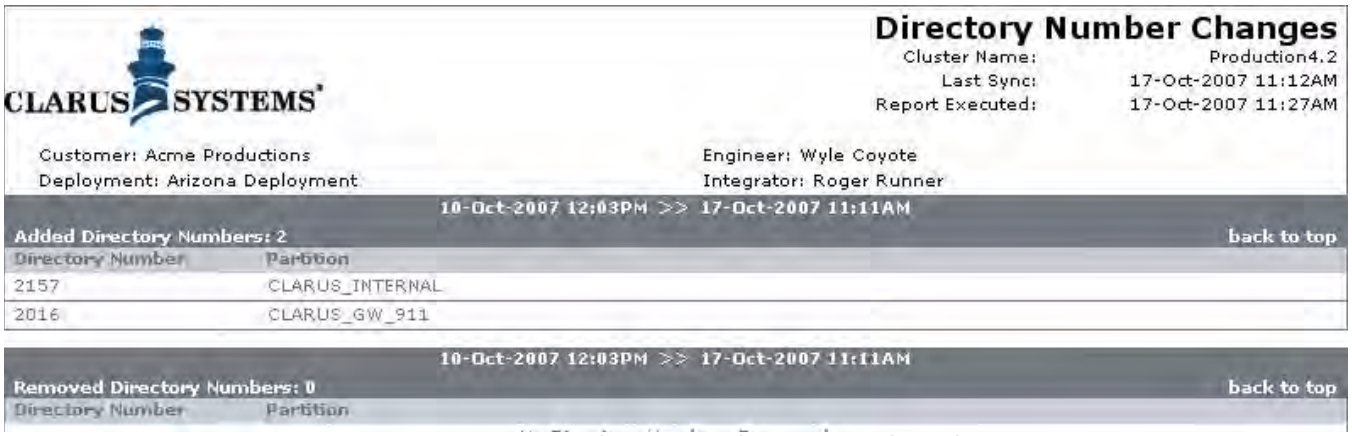


Figure 6-5 Directory Number Changes Report

NOTE: For more information on the Directory Numbers ClarusIPC includes in its counts, please see *Directory Number Counting*, later in this chapter.

Detailed Phone Inventory

Tabular Data Reports export raw data in a row and column format. These reports may be output as Excel spreadsheets, or as CSV files, allowing you to manipulate the generated data as desired.

The Detailed Phone Inventory report produces a CSV or Excel file listing a detailed inventory of all phones, grouped by Device Pools, including Model, Primary CUCM, App/Boot Loads, Version, Network Settings, and CSS-DN.

1. To generate the report, select **reports > Tabular Data Exports > Detailed Phone Inventory**.

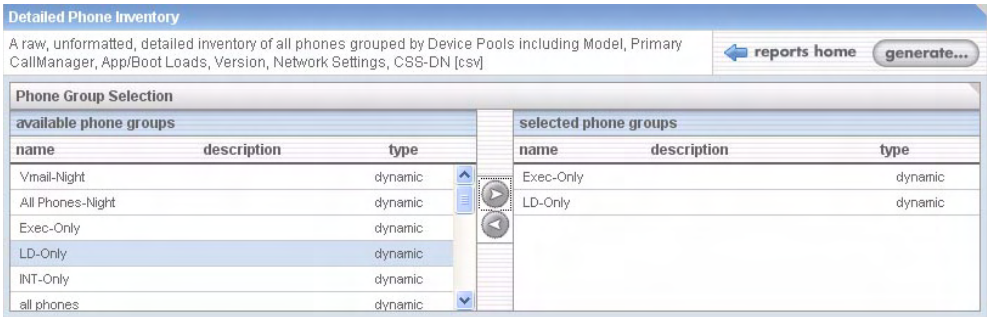
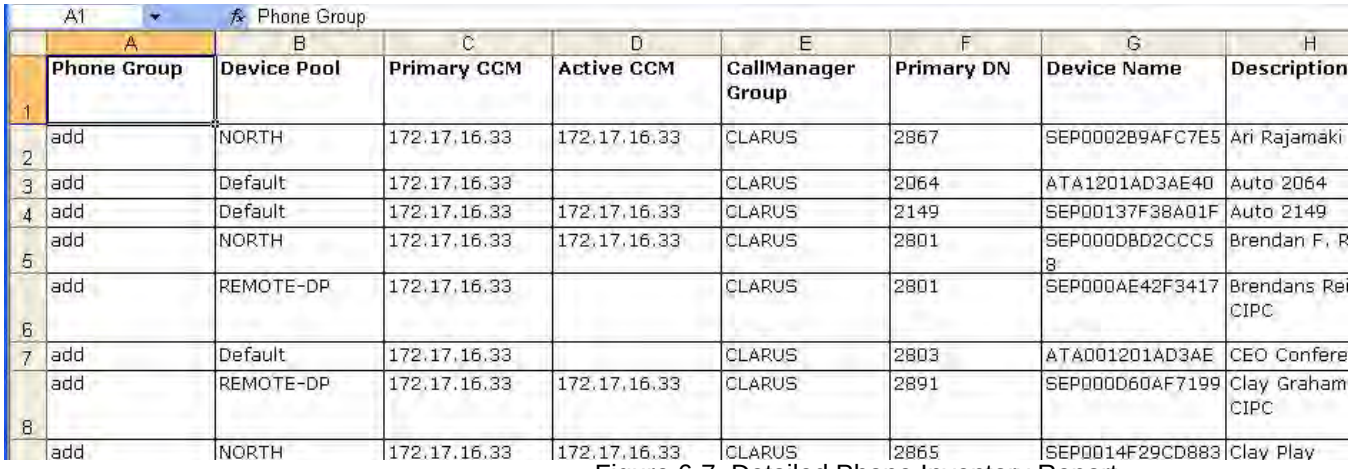


Figure 6-6 Detailed Phone Inventory Setup

2. Select the desired phone groups from the **available phone groups** window, and use the right arrow button to move them into the **selected phone groups** pane, and click generate.



A1 Phone Group

	A	B	C	D	E	F	G	H
1	Phone Group	Device Pool	Primary CCM	Active CCM	CallManager Group	Primary DN	Device Name	Description
2	add	NORTH	172.17.16.33	172.17.16.33	CLARUS	2867	SEP0002B9AFC7E5	Ari Rajamaki
3	add	Default	172.17.16.33		CLARUS	2064	ATA1201AD3AE40	Auto 2064
4	add	Default	172.17.16.33	172.17.16.33	CLARUS	2149	SEP00137F38A01F	Auto 2149
5	add	NORTH	172.17.16.33	172.17.16.33	CLARUS	2801	SEP000DBD2CCC58	Brendan F. R
6	add	REMOTE-DP	172.17.16.33		CLARUS	2801	SEP000AE42F3417	Brendans Rei CIPC
7	add	Default	172.17.16.33		CLARUS	2803	ATA001201AD3AE	CEO Confere
8	add	REMOTE-DP	172.17.16.33	172.17.16.33	CLARUS	2891	SEP000D60AF7199	Clay Graham CIPC
	add	NORTH	172.17.16.33	172.17.16.33	CLARUS	2865	SEP0014F29CD883	Clay Play

Figure 6-7 Detailed Phone Inventory Report

Service Analysis Reports

These reports rely on CDR/CMR data, the collection of which is controlled through the Cluster Details window. For more information please see Chapter 2, *ClarusIPC Clusters*.

Monthly Call Failures

Service Analysis reports compile a high level list of failures and alerts generated during a specified time frame.

The Monthly Call Failures report provides a summary of call failures by release cause codes over the last month.

To generate the report, simply click **reports > Service Analysis > Monthly Call Features,** enter company information, select an output format, and click **generate**.

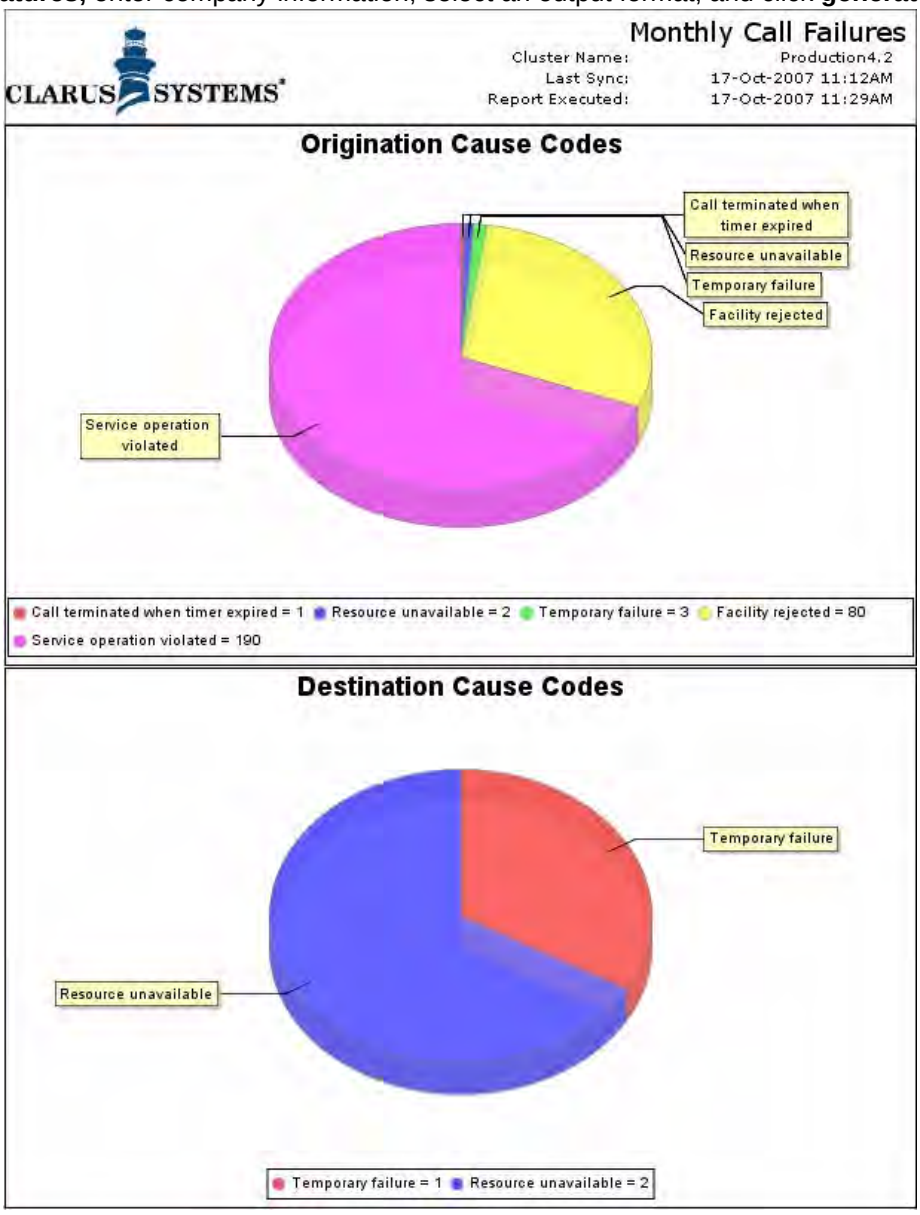


Figure 6-8 Monthly Call Failures Report

Test Results Reports

At the completion of test execution, Test Results reports provide a list of the tests run, and results achieved. This offers you a printed compilation of test results to be used as documentation at the end of the testing cycle.

Please note that Test Results reports may not be generated until after the tests involved have been successfully run. For more information, see Chapter 4, *Test Design*.

Certification Summary

The Certification Summary report provides a list of test plan results, and should be generated as part of the As-Built documentation delivered upon completion of an IPC rollout.

1. To generate a Certification Summary report, click **reports > Test Results > Certification Summary**. The following screen displays:

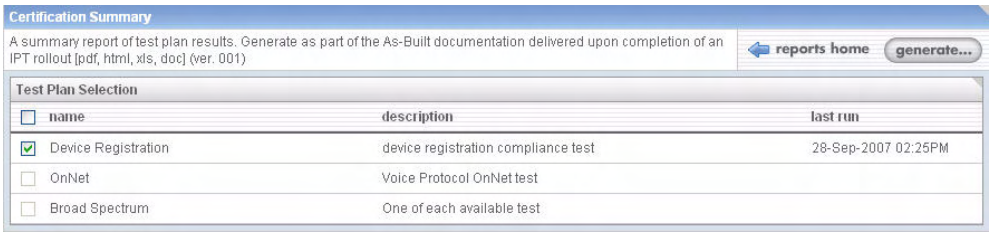


Figure 6-9 Certification Summary Report Setup

2. Check the boxes of the Test Plans you wish to include, and click **generate** to open the **Generate Report** window.

3. Complete the requested fields, select an output format from the pulldown menu, and click **generate** to view the report.

CLARUS SYSTEMS

Certification Summary

03-Oct-2007 11:47AM

Customer: Acme Productions
Deployment: Arizona Deployment

Engineer: Wyle Coyote
Integrator: Richard Runner

TEST PLAN SUMMARY: test-snmp — EXECUTED ON: 01-October-2007 03:33PM

TEST TYPE	TEST NAME	DESCRIPTION	ELEMENT TYPE	ELEMENTS	RESULTS
Voice Protocol OnNet (DP)	Voice Protocol OnNet (DP)		Network Path Endpoints	ClarusSFODP_AB and ClarusLAXDP_BA	Pass:1 Fail:0 Error:0
				ClarusSFODP_AB and ClarusSJCDP_AB	Pass:1 Fail:0 Error:0
				ClarusSFODP_BA and ClarusLAXDP_BA	Pass:1 Fail:0 Error:0
				ClarusSFODP_BA and ClarusSFODP_AB	Pass:1 Fail:0 Error:0
				ClarusSFODP_BA and ClarusSJCDP_AB	Pass:1 Fail:0 Error:0
				ClarusSJCDP_AB and ClarusLAXDP_BA	Pass:1 Fail:0 Error:0
				Default and ClarusLAXDP_BA	Pass:1 Fail:0 Error:0
				Default and ClarusSFODP_AB	Pass:1 Fail:0 Error:0
				Default and ClarusSFODP_BA	Pass:1 Fail:0 Error:0
				Default and ClarusSJCDP_AB	Pass:1 Fail:0 Error:0

SIGNATURE — CUSTOMER: Acme Productions — TEST PLAN NAME

Customer: Acme Productions — Integrator: Richard Runner

Representative Name: — Certifier Name:

Figure 6-10 Certification Summary Report

Directory Number Counting

ClarusIPC includes the following types of Directory Numbers when displaying counts within reports:

- Unassigned DNs
- DNs assigned to phones
- DNs assigned to Line Groups
- DNs assigned to CTI Route Points
- DNs assigned to Auto-Attendants
- DNs assigned to Personal Assistants
- DNs assigned to Hunt Groups

ClarusIPC does not include duplicate DNs, such as shared lines.

Printing Tips

For optimal results when printing your Reports, reset your IE print options:

1. Select **Tools > Internet Options** from the IE menu bar.
2. In the **Advanced** tab, scroll down to **Printing**, check **Print background colors and images,** and click **OK**.
3. Select **File > Page Setup**, and select **Orientation: Landscape**.
4. To remove the browser URL and page footers from your report, go to **File > Page Setup** and remove the text from the **Header** and **Footer** fields. (For your reference, the original settings were HEADER: '&w&bPage &p of &P', FOOTER: '&u&b&d'.)
5. When you have finished making changes in the Page Setup window, click **OK**.

CHAPTER 7 TASKS

ClarusIPC offers the ability to create Tasks, which contain groups of operations, scheduled to be performed at a predetermined time, on either a Unity system, or CUCM Cluster. Operations include tests, synchronizations, and reports for CUCM Clusters, and Syncs and reports for Unity systems.

Tasks may be set to run on a repeating schedule. For example, you may set up a series of test plans to execute during off hours or weekends when your users are not in the office. Tasks may be created to perform a scheduled set of test plans repeatedly over time, executing on a hourly, daily, weekly, or monthly basis.

Notification of operation status is available via SNMP or email before, during, and upon completion of a Task.

Tasks may include report production. Reports may be selected from your available list of customized reports, configured, and scheduled for production at any given interval. After they have been generated, reports are stored locally, and are accessible through a URL published in the task email.

Multiple Tasks may be run simultaneously, as long as there are no blocking mechanisms in place. Operations that will prevent Tasks from running simultaneously include a request for two Syncs of the same cluster at the same time, or the deletion of a Phone Group while a test is being staged for that Phone Group. For more information on running multiple tasks concurrently, please see *Concurrent Tasks* on page 7-10.

(If enabled in the Cluster Details, ClarusIPC lists KPI and CDR/CMR collection as system tasks, which may not be altered or deleted.)

Creating Tasks

ClarusIPC allows you to create Tasks, which may include the execution of Test Plans, or Reports, and which may be scheduled to occur on a one-time or recurring basis. ClarusIPC saves defined operations, including Syncs, tests, and reports, as "Tasks." (For more information about creating and executing Test Plans, see Chapter 4, *Test Design*. For more information about creating and executing Reports, see Chapter 6, *Reports*.)

To create a Task, click **tasks** in the menu bar to open the Tasks window.

Figure 7-1 Tasks Window

NOTE: If Cluster CDR/CMR or KPI collection has been enabled, the corresponding system Task is generated automatically. This task cannot be edited or removed from the Task page; the task may only be edited from the Cluster settings. (These Tasks represents the periodic collection of new CDR and KPI records from the CUCM into the ClarusIPC database.)

After Tasks are created, the Tasks window displays a summary list of each Task, the Test Plans and Reports contained within it, the results of the last execution, and the ongoing schedule for future executions.

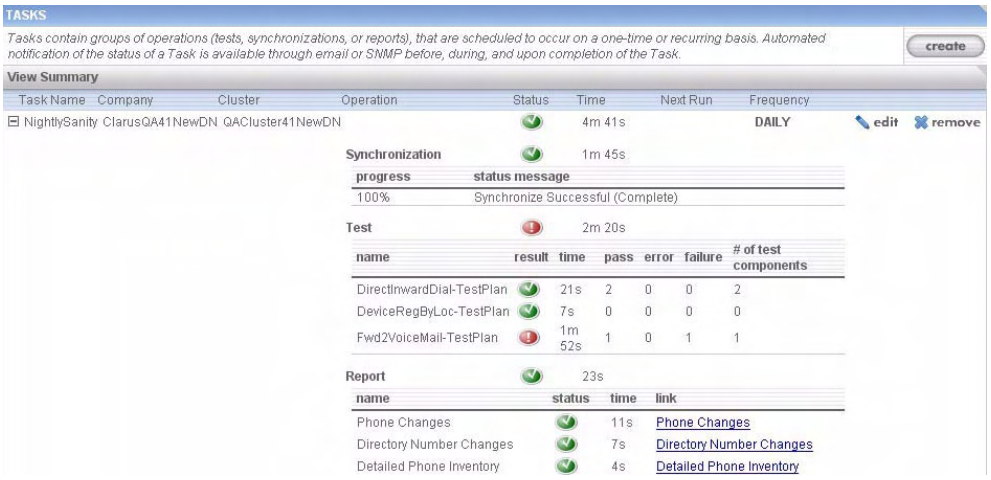


Figure 7-2 Tasks Window

To create a new Task, select **create** in the Tasks window to open the Task Details screen.

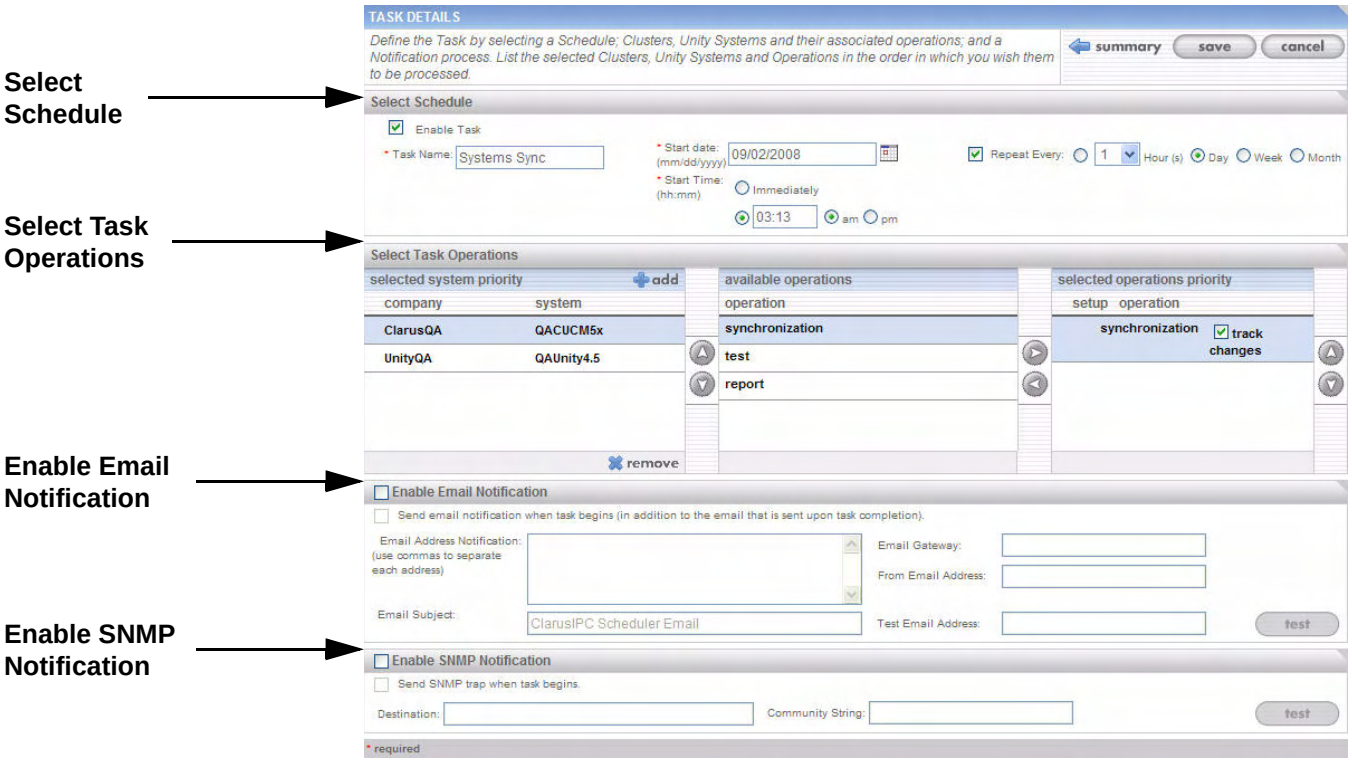


Figure 7-3 Task Details

Scheduling a Task

The Select Schedule section allows you to name, schedule, and enable Tasks.

To Select a Schedule for a Task:

1. Enter a name in the Task Name field.
2. Select a start date using the MM/DD/YYYY format
3. Select a start time, which may be **Immediately** if you wish the Task to execute upon completion of its definition.
4. Define whether you wish the Task to repeat, and, if so, at which frequency.
5. If you wish to run the Task as defined, select **Enable Task**. To save the Task, without having it run at its designated time, leave the **Enable Task** checkbox unchecked.

Enable a Task

An enabled Task is active, and will run at its next scheduled time. A disabled Task is visible on the **Tasks** screen with a disabled icon displayed in the **Status** column.

A Task must be enabled to run. Disabled Tasks are saved, but not run at their designated time.

Name a Task

Define your Task by naming it. Tasks must have unique names, which are most useful if they are descriptive. Use names like "Customer X Rollout, Phase 2," or "Nightly Health Check, 2nd floor."

Schedule a Task

Define starting dates and times as well as their frequency of execution.

Defining Task Operations

Define the Task(s) you would like to have executed.

To define a Task:

1. Select the Cluster(s) and/or Unity system(s) to be used for the Task.
2. For each element selected, choose from a list of available operations:
   - **synchronization** allows you to synchronize your systems before each Task Executes.
   - **test** allows you to include any available Test Plan(s) in your Task.
   - **report** allows you to include any available Report(s) in your Task.
3. Configure and arrange the selected operations in the desired fashion.

Operations may be ordered in any sequence, and multiple operations may be included in a single Task.

Selected System Priority

This window allows you to add and arrange Clusters and/or Unity systems to be used for the defined Tasks.

Add Systems

To add a system, click **add** in the top right corner of the **selected system priority** column, to open the select elements window.

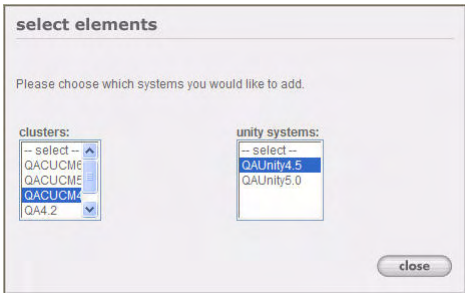


Figure 7-4 Add Element

Click on the system elements you wish to add, and click **close**.

The Task Details screen will list selected systems in the **selected system priority** column. Clicking on a system will populate the list in the **available operations** column.

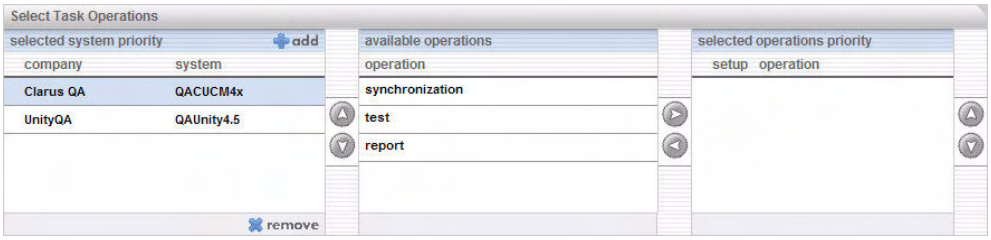


Figure 7-5 Add Element Results

NOTE: Available operations include synchronization, test, and report for Clusters, and synchronization and report for Unity systems.

Change System Execution Priority

Tasks process Clusters and Unity systems sequentially, based on their order in the **selected system priority** column. To change the order, click on a system, and use the up and down arrows immediately to the right to move it up or down in the list.

Remove System

To remove a system, simply click on the Cluster or Unity system to highlight it, and click the **remove** button in the lower right corner of the window. Please note that removing a system will remove all of its associated Test Plans and Reports from the available operations list as well.

Available Operations

The **available operations** column lists the operations associated with the selected system which are available for Tasks.

Synchronize

When using ClarusIPC, it is recommended that you synchronize regularly when working with a CUCM Cluster or Unity system. The synchronization process updates the locally stored database of information gathered from CUCM and the devices on the network. Creating a Task which includes this operation allows you to automatically synchronize each Cluster and Unity system prior to executing any associated operations. It is recommended that you select **synchronization** as the first operation in any scheduled Task, so that the system is always working with the most recent system data. (For more information on Synchronization, see *Synchronizing With CUCM* on page 2-9.)

Selecting **Track Changes** generates a *Snapshot* of this Sync operation for subsequent Change Tracking reports. Note that Snapshots include all aspects of the system's configuration. Snapshots are not selective, nor may they be customized.

Test

For each Cluster, include Test Plans in the Task by highlighting **test**, and clicking the right arrow to move it into the **selected operations priority** column.

To add and configure specific Test Plans, click **setup** to open the Test Configuration window.

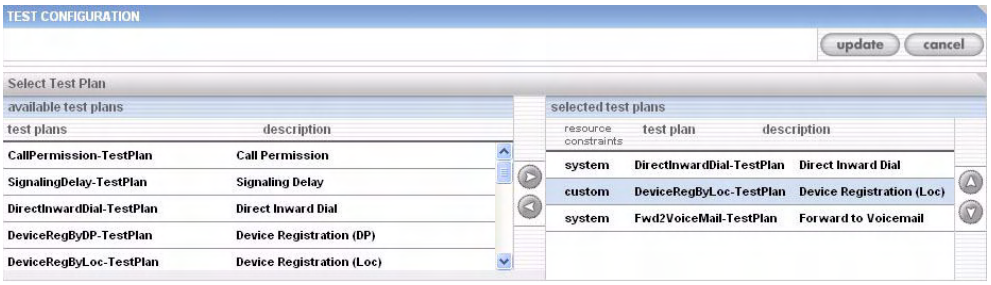


Figure 7-6 Test Configuration

Add a Test Plan to your Task by clicking it in the **available test plans** column, and using the arrow to move it into the **selected test plans** column. Each successive addition is added to the bottom of the list, putting the newly added Test Plan at the end of the queue. Adjust this order by clicking a plan to highlight it, then using the up and down arrows to the right of the **selected test plans** column to move it up or down the list. To remove a Test Plan from the Task, select it in the **selected test plans** column, and click the left arrow button to return it to the pool of **available test plans.**

To add reports to your Task, select **report**, and move it to the **selected operations priority** column.

A ClarusIPC User may schedule a Task to generate one or more reports from the set of available reports. Certain report templates may require additional information, such as a set of devices, time periods, etc.

After adding **report** to the **selected operations priority** column, and clicking the **setup** link, the **Report Configuration** window will open.

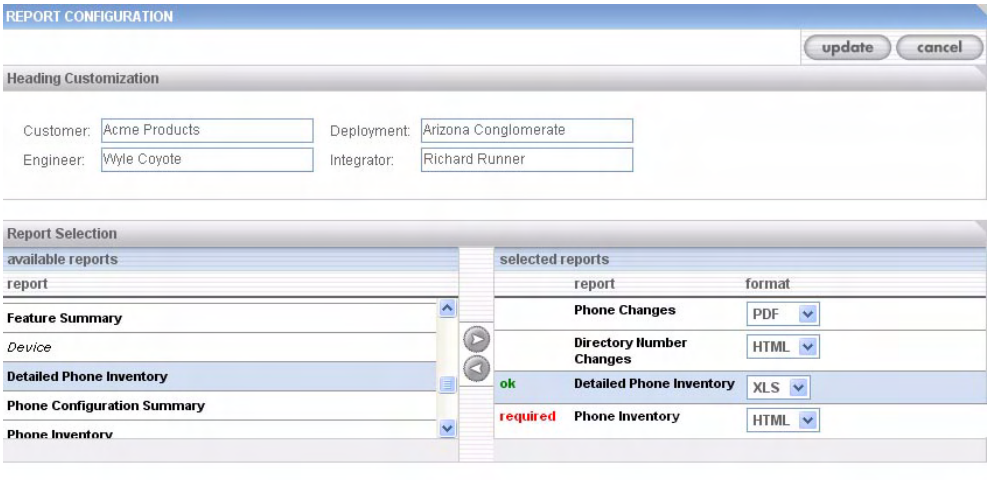


Figure 7-7 Report Configuration

The Report Configuration window lists all available report templates, and allows you to configure them based on standard report configuration rules. (For more information, see Chapter 6, *Reports*.)

Clicking on a report in the **selected reports** column which requires configuration will open an appropriate pane below, in which the required selections may be made. For instance, clicking on a report which requires the selection of Phone Groups, such as a Phone Inventory report, will open the **Phone Group Selection** pane, in which the desired groups may be selected.

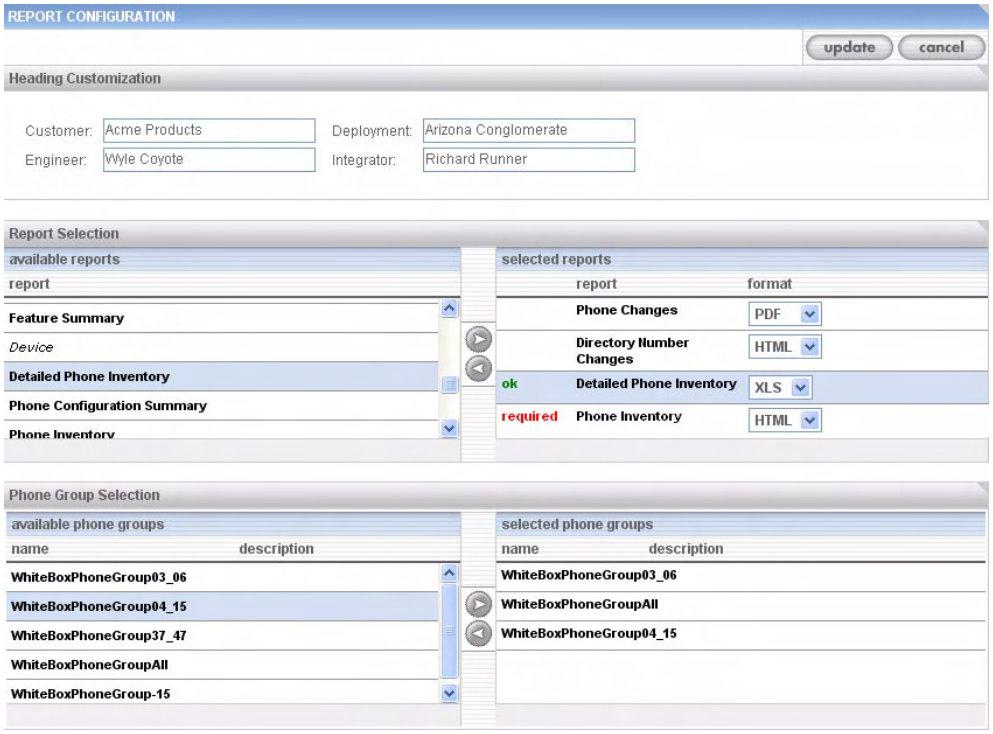


Figure 7-8 Report Configuration with Phone Group Selection Pane

Heading Customization

Enter information you wish to be included in the header of the report. These fields may be left blank.

Report Selection

Click on a report type in the **available reports** column, and use the left and right arrows to move it into the **selected reports** column.

Individual Report Customizations

The Report Configuration window changes to reflect the type of selected report: those that require no configuration; those that require Phone Group selection; and those that require Test Plan selection. The Configuration window indicates required configuration elements, and will not allow the report to be added or saved to the Task until all required information has been entered.

After generation, the reports will be stored in a local file path, the URL of which may be sent to the Inbox of a list of email recipients. Reports are stored in local folder:

```
Clarus/tomcat/webapps/webdav/publish;
```

and automatically named

```
year/month/day/<report name>-hh:mm:ss.<output type> (xls, html,
etc.).
```

(For example:

```
http://172.13.14.117/webdav/publish/2006/10/6/
System_SystemSummaryReport_1160175815432.HTML.)
```

When a Task is complete, email containing the URL reference to the stored report may be sent to a list of recipients defined by the user. Please note that access to these reports will not be password or license protected, enabling you to send reports to people who are not registered users of ClarusIPC.

Selected Operations Priority

This window lists all operations for the selected system, in the order in which they will be run, and indicates whether they are ready to run, or require configuration.

Click on the **setup** link to configure individual operations. Use the up and down arrows to rearrange the order in which operations will be performed during execution of the Task.

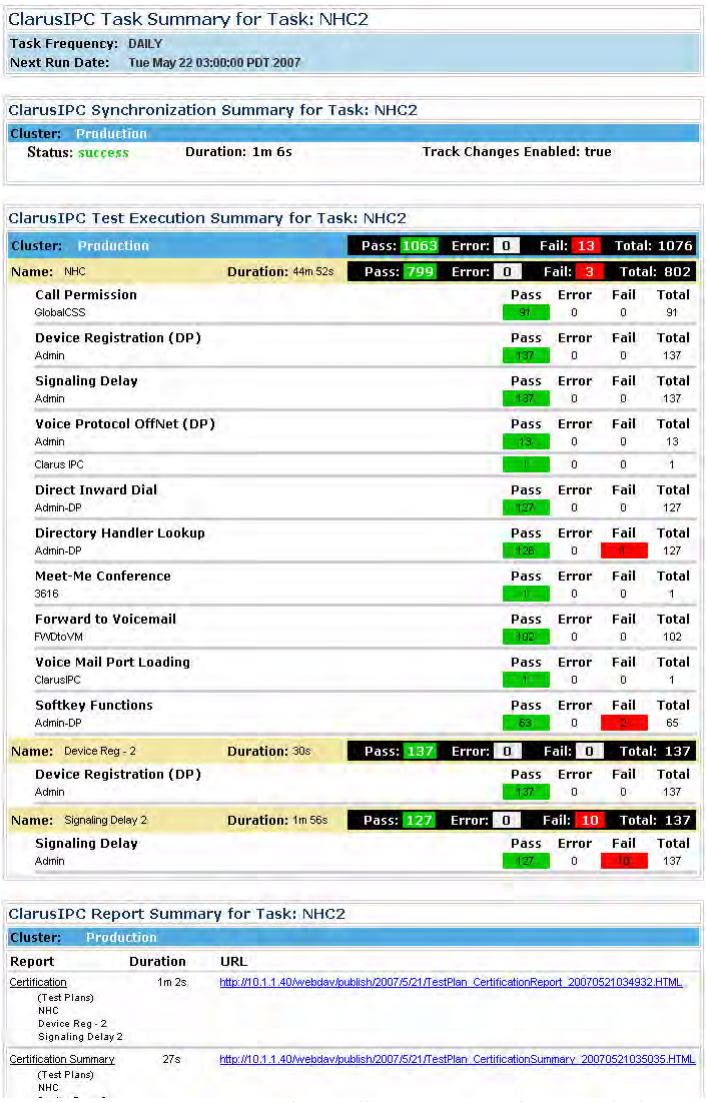
Enabling Email Notification

This pane allows you to automate email generation for the selected Task. To enable email notification for the completion of the Task, select the checkbox at the beginning of this field, and enter the required information. To send mail at the onset of the Task, check the "Send email notification when task begins" box as well. The notification email at the beginning of a Task execution informs you that the module tried to start the Task at the time you specified. The email sent upon Task completion is useful to quickly validate the completion of the Task's operations.

To generate email notification, select the **Enable Email Notification** checkbox, and complete the fields as required.

- **Send email notification when task begins:** generates a notification email on task onset.
- **Email Address Notification:** the email addresses to which you wish notification to be sent.
- **Email Subject:** the subject of the Notification sent.
- **Email Gateway:** the gateway through which Notification emails will be routed. Enter the Hostname or IP address for the desired gateway.
- **From Email Address:** the From address to be used for Notification.
- **Test Email Address:** the Address to which test Notification is to be sent.

- **Test Button:** clicking this button allows you to test Task notification email routing.



ClarusIPC Task Summary for Task: NHC2

Task Frequency: DAILY
Next Run Date: Tue May 22 03:00:00 PDT 2007

ClarusIPC Synchronization Summary for Task: NHC2

Cluster: Production
Status: success Duration: 1m 6s Track Changes Enabled: true

ClarusIPC Test Execution Summary for Task: NHC2

Cluster: Production Pass: 1063 Error: 0 Fail: 13 Total: 1076

Name: NHC Duration: 44m 52s Pass: 799 Error: 0 Fail: 3 Total: 802

		Pass	Error	Fail	Total
Call Permission	GlobalCSS	91	0	0	91
Device Registration (DP)	Admin	137	0	0	137
Signaling Delay	Admin	137	0	0	137
Voice Protocol OffNet (DP)	Admin	13	0	0	13
	Clarus IPC	1	0	0	1
Direct Inward Dial	Admin-DP	127	0	0	127
Directory Handler Lookup	Admin-DP	126	0	1	127
Meet-Me Conference	3616	1	0	0	1
Forward to Voicemail	FWDtoVM	102	0	0	102
Voice Mail Port Loading	ClarusIPC	1	0	0	1
Softkey Functions	Admin-DP	63	0	2	65

Name: Device Reg - 2 Duration: 30s Pass: 137 Error: 0 Fail: 0 Total: 137

		Pass	Error	Fail	Total
Device Registration (DP)	Admin	137	0	0	137

Name: Signaling Delay 2 Duration: 1m 56s Pass: 127 Error: 0 Fail: 10 Total: 137

		Pass	Error	Fail	Total
Signaling Delay	Admin	127	0	10	137

ClarusIPC Report Summary for Task: NHC2

Cluster: Production

Report	Duration	URL
Certification (Test Plans) NHC Device Reg - 2 Signaling Delay 2	1m 2s	http://10.1.1.40/webdav/publish/2007/5/21/TestPlan_CertificationReport_20070521034932.HTML
Certification Summary (Test Plans) NHC	27s	http://10.1.1.40/webdav/publish/2007/5/21/TestPlan_CertificationSummary_20070521035035.HTML

Figure 7-9 Automated Email Sent on Task Completion

Enabling SNMP Trap Notification

For each Task, the system can also send an SNMP v1.0 trap upon Test Plan completion.

For **Destination**, enter the IP address or hostname of your SNMP Trap Host.

For **Community String,** if you are not using *public*, enter the community string required by your Trap Host to receive traps.

To test the trap, click the **Test** button.

OID	Var-bin	Values	Example	Description
10	taskName	max 30 char	Nightly Run	*Name of scheduled Task*
13	nextRunTime	max 20 char	11/11/2011, 12:01 pm	*Next scheduled run time*
14	clusterName	max 30 char	cluster1	*Cluster name*
100	messageString	max 64 char	Passed	*General Information Message String*
15	testPlanName	max 30 char	Branch Availabilty	*Name of Test Plan*
16	numPassed	integer	50	*Number of passed activities*
17	numError	integer	0	*Number of activities reporting an error*
18	numFailed	integer	0	*Number of failed activities*
19	executeDuration	max 14 char	0h 46m 12s	*Duration of executed Test Plan*

Figure 7-10 Sample Trap

Concurrent Tasks

Tasks may be run concurrently, if they do not encounter any blocking operations. Blocking operations include such requests as the initiation of a second Sync on a system while one Sync is running; updating a resource constraint while a test plan using that resource constraint is being staged, or the initiation of a test execution on a cluster while a Sync of that cluster is running.

While a Task is in progress, it will proceed according to its defined sequence.

While there are no specific limits on how many tasks may be run simultaneously, the performance of each task may degrade due to limits of system resources.

The following table lists specific constraints.

Table 7-1 Activity Matrix for Single Cluster, Multiple Session Tasks

Concurrent Sessions	Sync	Stage a Test Plan	Execute a Test Plan
Sync the same Cluster	no	no	no
Sync a different Cluster	yes	yes	yes
Stage the same Test Plan	no	no	no
Stage a different Test Plan	no	yes	yes
Execute the same Test Plan	no	no	no
Execute a different Test Plan	no	yes	yes
Create/Import a new Test Plan	no	yes	yes
Export a Test Plan	no	yes	yes
Modify/Delete an existing Test Plan	no	yes, but not the same one	yes, but not the same one

Table 7-1 Activity Matrix for Single Cluster, Multiple Session Tasks

Concurrent Sessions	Sync	Stage a Test Plan	Execute a Test Plan
Create/Import a new Phone-book Entry	no	no	no
Export the Phonebook	yes	yes	yes
Modify/Delete an existing Phonebook Entry	no	no	no
Create a new Phone Group	no	yes	yes
Modify/Delete an existing Phone Group	no	no	yes
Create a new User Class	no	yes	yes
Modify/Delete an existing User Class	no	no	yes
Create a new Task	yes	yes	yes
Modify/Delete an existing Task	yes	yes	yes
Update a Resource Constraint	no	no	yes
Change Admin Settings	yes	yes	yes
Create/Change a Collector	yes	yes	yes
Generate a Report	no[1]	yes	yes

NOTE: [1]Generating a Report during a Sync is blocked only for those reports which use Phone Groups. Reports which do not use Phone Groups may be generated during a Sync.

APPENDIX A INTEGRATING WITH NMS

ClarusIPC offers integration to Network Management Systems (NMS) via a Simple Network Management (SNMP) V1 TRAP Protocol Data Unit (PDU) as defined in IETF RFC1215. This chapter covers the following:

- Interpret Notifications
- Tivoli Netview Integration
- HP OpenView Network Node Manager Integration

Interpreting Notifications

To help interpret the notifications (TRAPS) issued by ClarusIPC:

1. The *PDU Format* section of this appendix identifies the format of the generic SNMP TRAP fields as required in RFC1215. These are common for all ClarusIPC TRAPS.
2. Each individual notification, or Trap type, is identified by a unique Trap ID number. These TrapIDs are documented in the *Trap Type* section of this appendix. Each unique TRAP Type can carry a different *payload*, or list of parameters. These are also defined in this section.
3. The *Var-Bind-Defs* section defines each parameter in detail.

An NMS can be configured to interpret these TRAPS either manually, as per the manufacturers instructions, or to some extent, by importing a machine-readable (ASN.1 format) document (MIB File) prepared and provided by Clarus Systems, Inc.

PDU Format

Table A-1 PDU Formats

Field/Attribute	Value	Comments
Enterprise	1.3.6.1.4.1.12928.1.1	ISO(1).IdentifiedOrganization(3).dod(6).internet(1).private(4).enterprise(1).clarussystems(12928).clarusIPC(1).cstrapinfo(1)
Agent Address	User Configurable	Default to IP address of ClarusIPC System, possible enhancement to substitute IP Addr of Pub, or CTI Manager?)
Generic Trap Type	6	Enterprise
Specific Trap Code	Per "TRAP Types"	In the range of 1001 through 1007
Time Stamp	Local Time	Defined as the time in ticks since the "Agent" (scheduler) was restarted
Var-Bind List	Per "TRAP Types"	

Table A-2 Trap Types

TrapID	Name	Description	Var-bind List	Comments	Default Severity
1001	clarusipcTaskInitiation	Task Kickoff	1=taskName		Normal
1004	clarusipcTask SyncFailed	Sync failed for a Cluster	1=taskName, 2=nextRunTime, 3=clusterName, 4=messageString	One trap sent for each Cluster that failed.	Major
1005	clarusipcTPPass	Test Plan executed with no Failures or Errors	1=taskName, 2=nextRunTime, 3=clusterName, 4=messageString, 5=testPlanName, 6=numPassed, 7=numError, 8=numFailed, 9=executeDuration	One trap sent for each test plan, for each Cluster. Message could be as description.	Normal
1006	clarusipcTPFail	Test Plan executed with Failures (no errors)	1=taskName, 2=nextRunTime, 3=clusterName, 4=messageString, 5=testPlanName, 6=numPassed, 7=numError, 8=numFailed, 9=executeDuration	One trap sent for each test plan, for each Cluster, message could be as per description.	Critical
1007	clarusipcTPErr	Test Plan executed with at least one error (including staging, TP unavailable and other "Could not execute" errors) and no failures	1=taskName, 2=nextRunTime, 3=clusterName, 4=messageString, 5=testPlanName, 6=numPassed, 7=numError, 8=numFailed, 9=executeDuration	One trap sent for each test plan, for each Cluster. In the event of staging error, send this trap as well. Message should contain the nature of the error.	Major

Var-Bind-Defs

OID	Var-bin	Values	Example	Description
10	taskName	max 30 char	Nightly Run	*Name of scheduled Task*
13	nextRunTime	max 20 char	11/11/2011, 12:01 pm	*Next scheduled run time*
14	clusterName	max 30 char	cluster1	*Cluster name*
100	messageString	max 64 char	Passed	*General Information Message String*
15	testPlanName	max 30 char	Branch Availabilty	*Name of Test Plan*
16	numPassed	integer	50	*Number of passed activities*
17	numError	integer	0	*Number of activities reporting an error*
18	numFailed	integer	0	*Number of failed activities*
19	executeDuration	max 14 char	0h 46m 12s	*Duration of executed Test Plan*

NOTE: An asterix (*) indicates a high probability of truncation, as this is a theoretically infinite list of 30 char Cluster name strings, separated by commas.

Tivoli® NetView Integration Summary

This section describes how to perform basic integration of ClarusIPC, and Tivoli NetView for Windows.

Prerequisites

Tivoli NetView must be installed. Internet Explorer must be installed. You must be able to access the machine running ClarusIPC via HTTP, and the machine running ClarusIPC must be able to send SNMP traps to the NetView machine.

Manifest

The integration is comprised of ClarusIPC V2.0 or later, plus the following files:

- `csaddtrapnv.bat:` a DOS batch command, that will configure NetView to correctly interpret and display ClarusIPC traps.
- ClarusIPC: an Application Registration File containing the information required to add ClarusIPC Launch commands to the NetView "Tools" menu.
- clarusipcmib.mib: an SNMP V1 MIB file containing the OID definitions and Trap macro for the ClarusIPC application. Can be optionally loaded if the user wishes not to use our default configuration.

Event Configuration

1. Copy the supplied files to a location on your system, and unpack (if zipped).
2. Execute the `csaddtrapnv.bat` command within a DOS command window. The batch file assumes NetView commands are in your DOS search path.
3. Confirm the configuration has occurred correctly, using the NetView event configuration utility. (This can also be used to make manual configuration changes.) You may need to select the "Advanced Menu" option in order to make the menu selection options visible.

Options > Trap Settings

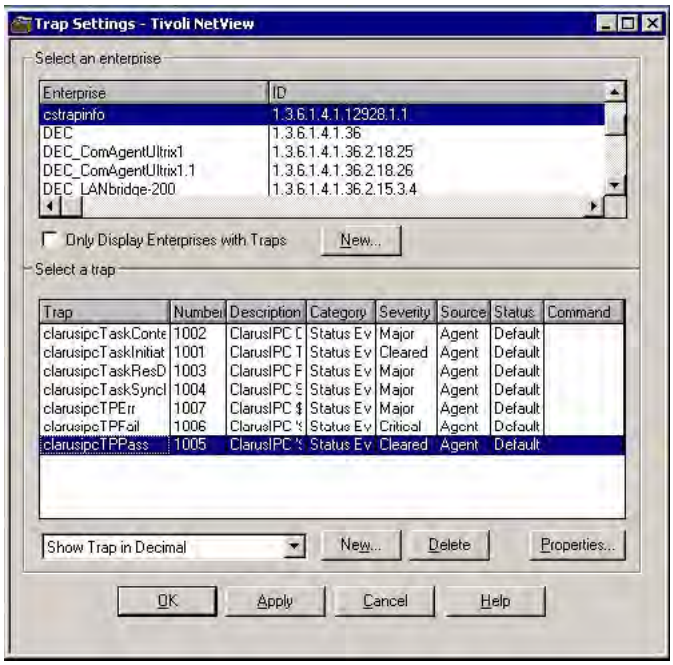


Figure A-1 Tivoli Trap Settings

When a trap is received, the event browser should display a received ClarusIPC trap something like this:

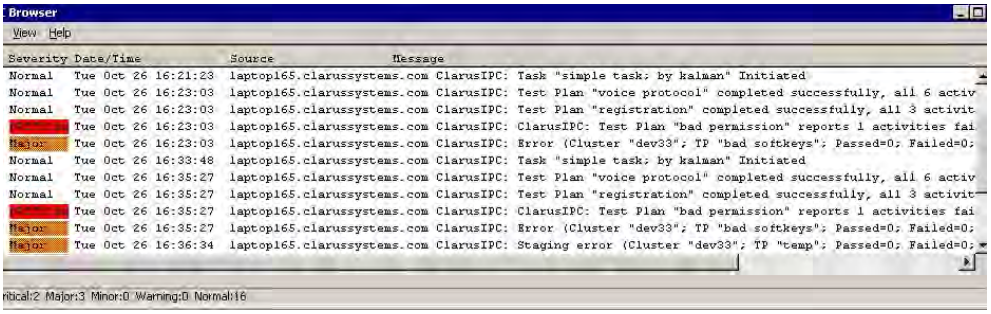


Figure A-2 Event Browser

If required, the MIB file can be loaded, using the MIB loader utility:

```
Tools -> Loader SNMP V1
```

Menu Configuration

1. Copy the "ClarusIPC" registration file to the appropriate location on your system. Typically this would be: "…ov\registration\c"
2. Create a system wide environmental variable "CLARUSIPC" with the value set to the hostname, or IP address of your ClarusIPC system.
3. Close the NetView console (if running) and log out of Windows.
4. Log back into Windows (to activate the environmental variable).
5. Restart the NetView console.The ClarusIPC tools should now be visible under the NetView Tools menu.

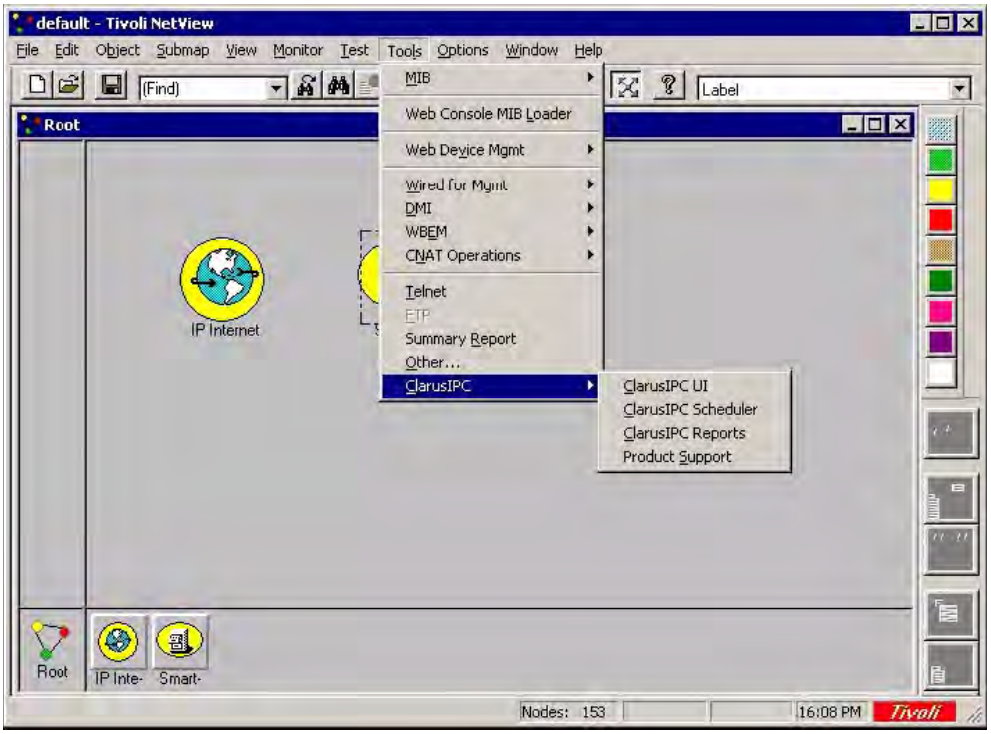


Figure A-3 ClarusIPC Tools

HP® NNM Integration Summary

This appendix describes how to perform basic integration of ClarusIPC and Hewlett Packard OpenView Network Node Manager (NNM) for Windows.

Prerequisites

NNM must be installed. Internet Explorer must be installed. You must be able to access the machine running ClarusIPC via HTTP, and the machine running ClarusIPC must be able to send SNMP traps to the NNM machine.

Manifest

The *integration* comprises ClarusIPC V2.0 or later, plus the following files:

- `csaddtrapnnm.bat:` a DOS batch command, that will configure NNM to correctly interpret and display ClarusIPC traps.
- cstrapd111.txt: a file, in trapd.conf format, containing the instructions used to configure NNM. Used by csaddtrapnnm.bat
- ClarusIPC: an Application Registration File containing the information required to add ClarusIPC Launch commands to the NNM “Tools” menu.
- clarusipcmib.mib: an SNMP V1 MIB file containing the OID definitions and Trap macro for the ClarusIPC application. Can be loaded if the user wishes not to use the default configuration.

Event Configuration

1. Copy the supplied files to a location on your system, and unpack (if zipped).
2. Execute the `csaddtrapnnm.bat` command within a DOS command window. The batch file assumes OpenView commands are in your DOS search path.
3. Confirm the configuration has occurred correctly, using the NNM event configuration utility. (This can also be used to make manual configuration changes.)

Options > Event Configuration

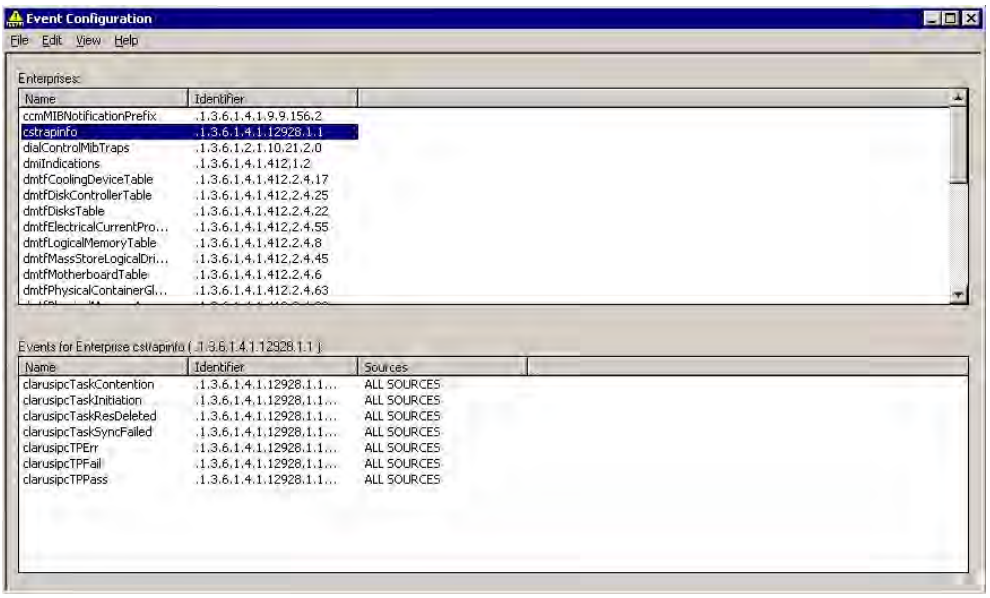


Figure A-4 Event Configuration

When a trap is received, the event browser will display a received ClarusIPC trap:

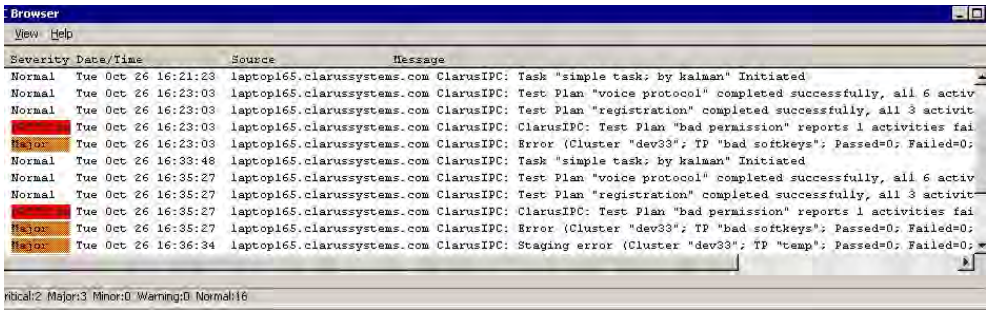


Figure A-5 EventBrowser

If required, the MIB file can be loaded, using the MIB loader utility:

```
Options -> Load/Unload MIBs: SNMP
```

Menu Configuration

1. Copy the “ClarusIPC” registration file to the appropriate location on your system. Typically this would be: “…Program Files\HP OpenView\NNM\registration\C.”
2. Create a system wide environmental variable “CLARUSIPC” with the value set to the hostname, or the IP address of your ClarusIPC system.
3. Close the NNM console (if running) and log out of Windows.
4. Log back into Windows (to activate the environmental variable).
5. Restart the NNM console.The ClarusIPC tools should now be visible under the NNM Tools menu.

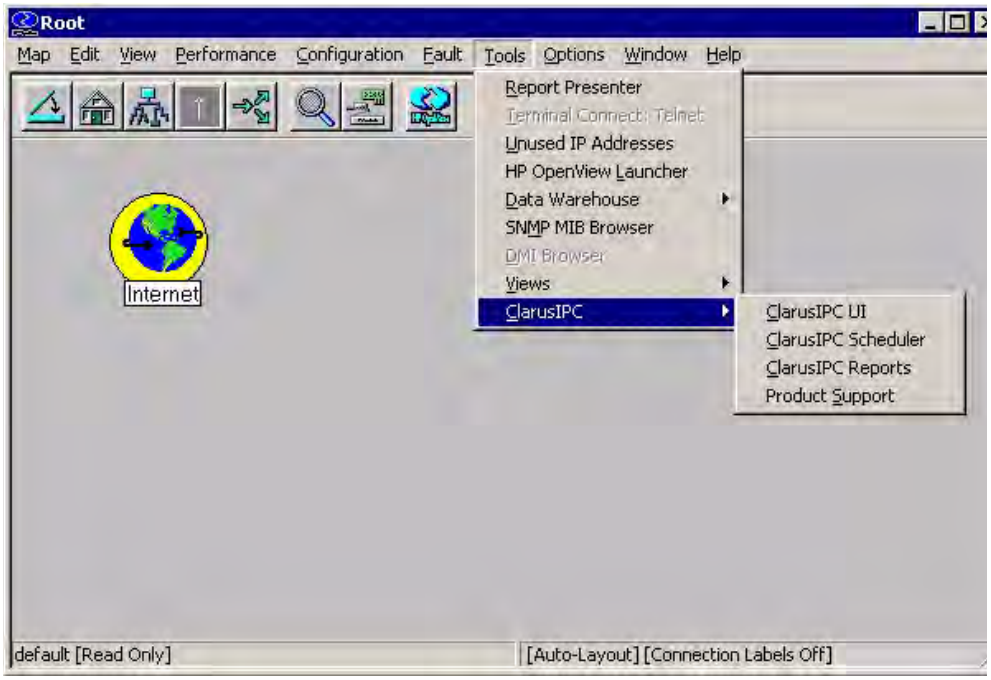


Figure A-6 ClarusIPC Tools

APPENDIX B TEST TYPES

This Appendix is provided as a quick reference list of all test categories and test types available for the Test Plan creation process, a description of the test, and a list of elements which are tested on execution.

Table B-1 Test Plan Categories and Types

Test Plan Category	Test Type	Purpose	Test Element
Class Of Service: Verifies a user's call permission based on the User Class defined intent.	Call Permissions	Verifies that a User Class is either allowed or blocked from calling a particular PSTN number as defined in the Phonebook. The PSTN number should be selected to automatically answer within the specified timeout.	User Class
Network: Verifies the signaling and audio portion of your IPC system.	Device Registration: • Device Registration (Loc) • Device Registration (NS) • Device Registration (DP)	Verifies that IP Phones in specified Device Pools, locations, or network segments are registered to their configured primary CUCM.	• Network Segments • Device Pools • Locations
	Signaling Delay	Verifies that an IP Phone in a specific Device Pool can receive a request for service acknowledgement from the configured primary CUCM within a predetermined time period.	Device Pools

Table B-1 Test Plan Categories and Types

Test Plan Category	Test Type	Purpose	Test Element
	• Voice Protocol OnNet (Loc) • Voice Protocol OnNet (NS) • Voice Protocol OnNet (DP)	Verifies Call Signaling to CUCM and Media Streaming between IP Phones across network paths marked by endpoints of two Device Pools, locations, or network segments.	• Network Segments • Device Pools • Locations
	• Voice Protocol OffNet (Loc) • Voice Protocol OffNet (NS) • Voice Protocol OffNet (DP)	Verifies Call Signaling to CUCM and Media Streaming between an IP Phone and a PSTN Gateway across network paths marked by endpoints of two Device Pools, locations, or network segments.	• Network Segments • Device Pools • Locations
Route Plan: Verifies the availability and performance of Direct Inward Dial.	Direct Inward Dial	Verifies that DNs configured for Direct Inward Dial (DID) are directly accessible from an external caller.	Phone Group
Application: Verifies Auto Attendant and Conference Bridge components.	Directory Handler Lookup	Verifies that DNs configured within the Auto Attendant application are accessible from internal and external callers.	Phone Group
	Meet-me Conference	Verifies that a user-defined number of IP Phones can dial a specific meet-me number and participate in a conference call.	Meet-Me Pattern
Phone Feature: Verifies features specific to the user environment.	Forward to Voice Mail	Verifies that DNs forward and connect to the voice mail application within the specified timeout.	Phone Group
	Rollover	Verifies a second call to a user's primary Directory Number (DN) rolls to a second line when the primary DN is busy.	Phone Group
	Softkey Functions	Verifies the selected set of Softkey functions are working correctly on selected IP Phones. These functions include the following: Call Hold, Redial, Call Park, Call Transfer, Corporate Directory, Ad-Hoc Conference.	Phone Group
Capacity: Verifies the availability and performance of the voice mail system.	Voice Mail Port Loading	Verifies the availability of the required number of voice mail ports for each selected voice mail profile.	Voice Mail Profile

APPENDIX C RESOURCE SELECTION RULES

In order to be eligible to participate in a test, phones must pass a set of resource selection rules as described below. Understanding these rules may help you solve the problem of a population count which is too low for a test.

Table C-1 Resource Selection Rules

Test Category	Test Type	Expected Input	Resource Selection Rules
Network	Voice Protocol OnNet: • Voice Protocol OnNet (Loc) • Voice Protocol OnNet (NS) • Voice Protocol OnNet (DP)	Network Path End-points represented by two: • Device Pools • Locations • Network segments	This test requires two roles: an originator and a terminator. The originator is chosen to be able to call the terminator. Each role must represent the specified test element (Device Pool, a location, or a network segment) for one end of the network path. **Originating Resource Requirements:** All phones to be considered for use as an originator must: be registered, support web access, not contain shared DNs, and belong to the OnNet Resource Pool. **Terminating Resources Requirements:** All phones to be considered for use as a terminator must: be registered, support web access, not contain shared DNs, not have CfwdAll or auto-answer set, and be a member of the OnNet Resource Pool
(Network)	Voice Protocol OffNet: • Voice Protocol OffNet (Loc) • Voice Protocol OffNet (NS) • Voice Protocol OffNet (DP)	Network origination identified by one: • Device Pool • Location • Network segment	This test requires a single originator role. The originator must represent the specified test element (Device Pool, a location, or a network segment). The destination number is selected from Phone Book entries in the VP OffNet call classification. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support web access, and belong to the OnNet Resource Pool.

Table C-1 Resource Selection Rules

Test Category	Test Type	Expected Input	Resource Selection Rules
(Network)	Signaling Delay	• A Device Pool element • Resource coverage by percentage	This test requires a single originator role. The originator must represent the specified test element (Device Pool). **Originator Requirements:** All phones to be considered for use as an originator must: be registered, not contain shared DNs, support XML phone-control, and belong to the OnNet Resource Pool.
(Network)	Device Registration: • Device Registration (Loc) • Device Registration (NS) • Device Registration (DP)	One and only one of the following elements: • Device Pool • Location • Network segment or • Resource coverage by percentage	Device Registration uses a percentage of devices characterized by the specified attribute (a Device Pool, a location, or a network segment). The subset is further restricted for phone models supporting HTTP access. The known phone models with such support will be derived from an inclusion list. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support web access, and belong to the OnNet Resource Pool.
Class Of Service	Call Permissions	• A User Class element • Resource coverage by percentage	Call Permissions makes direct use of a percentage of the resources grouped by a User Class. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support Device control, have a non-shared DN, and have a Phonebook entry with User Class-specified call classification.
Phone Feature	Softkey Functions	• A Phone Group element • Resource coverage by percentage	**Feature-phone requirements:** All phones to be considered for use must: be registered, support Device control, not contain shared DNs, not have CfwdAll or auto-answer set, have Available phone key(s), and support XML phone control. **Feature-phone-originator and Unpark requirements:** All phones to be considered for use must: be registered, support Device control, not contain shared DNs, and belong to the OnNet Resource Pool. **Feature-phone-terminator, Feature-phone-forwarded, and Directory-member requirements:** All phones to be considered for this use must: be registered, support Device control, not contain shared DNs, not have CfwdAll or auto-answer set, and belong to the OnNet Resource Pool.

Table C-1 Resource Selection Rules

Test Category	Test Type	Expected Input	Resource Selection Rules
(Phone Feature)	Rollover	• A Phone Group element • Resource coverage by percentage	This test has two roles: (two) originating resources and (one) rollover resource (per atomic test). The originating resources are chosen to be able to call the rollover resource. The rollover resources are a percentage of resources from the Phone Group. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support Device control, not contain shared DNs, and belong to the OnNet Resource Pool. **Rollover Requirements:** All phones to be considered for use as a rollover must: be registered, support Device control, not contain shared DNs, and not have auto-answer set.
(Phone Feature)	Forward To Voice Mail	• A Phone Group element • Resource coverage by percentage	This test has two roles: originating and forwarding. The originating resource is chosen to be able to call the forwarding resource. The forwarding resource is a percentage of resources from the Phone Group. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support Device control, support web access, not contain shared DNs, and belong to the OnNet Resource Pool. **Forwarding Requirements:** All phones to be considered for use as an forwarding resource must: be registered, support Device control, and not contain shared DNs.

Table C-1 Resource Selection Rules

Test Category	Test Type	Expected Input	Resource Selection Rules
Application	Directory Handler Lookup	• A Phone Group element (consisting of AA directory members) • Resource coverage by percentage • A Phone Group (with off-net dialing permissions)	This test has two roles: originating and terminating. The originating resource is derived from the global Phone Group with Off-Net dialing permissions. The terminating resource is a percentage of resources from the test-specific Phone Group. There are no direct dependencies among the roles. **Requirements:** Phonebook entry (with the "autoattendant number" call classification). **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support Device control, support web access, not contain shared DNs, and belong to the OffNet Resource Pool. **Terminator Requirements:** All phones to be considered for use as an terminator must: be registered, support Device control, support web access, not contain shared DNs, and not have CfwdAll or auto-answer set.
(Application)	Meet-me Conference	• A meet-me pattern element • Resource coverage by count (of total number of call participants)	This test has two roles: initiating and joining. All resources need calling permissions to the Meet-me pattern. Additionally, the initiating resource needs the proper softkeys for initiating a meet-me conference. The initiating resource is further restricted for phone models supporting XML phone-control. The known phone models with such support will be derived from an inclusion list. The specified total number of resources refers to one initiating resource and potentially many joining resources. There are no direct dependencies among the roles. **Conference-Initiator Requirements:** All phones to be considered for use as an initiator must: be registered, support Device control, not contain shared DNs, have available phone key(s), support XML phone-control, and belong to the OnNet Resource Pool. **Conference-Joiner Requirements:** All phones to be considered for use as a joiner must: be registered, support Device control, not contain shared DNs, and belong to the OnNet Resource Pool.

Table C-1 Resource Selection Rules

Test Category	Test Type	Expected Input	Resource Selection Rules
Route Plan	Direct Inward Dial	• A Phone Group element (consisting of DID resources) • Resource coverage by percentage • A Phone Group (with OffNet dialing permissions)	This test has two roles: originating and terminating. The originating resource is derived from the global Phone Group with OffNet dialing permissions. The terminating resource is a percentage of resources from the test-specific Phone Group. There are no direct dependencies among the roles. **Originator Requirements:** All phones to be considered for use as an originator must: be registered, support Device control, support web access, not contain shared DNs, and be a member of the OffNet Resource Pool. **Terminator Requirements:** All phones to be considered for use as a terminator must: be registered, support Device control, support web access, not contain shared DNs, and not have CfwdAll or auto-answer enabled.
Capacity	Voice Mail Port Loading	• A voice mail profile element • Resource coverage by count (of total number of call participants)	This test uses devices to call the V(oice) M(ail) port DN matching the VM pilot number that is referenced from the specified VM profile. Calling permission is established using the VM pilot's CSS. **Requirements:** All phones to be considered for use must: be registered, support Device control, not contain shared DNs, and belong to the OnNet Resource Pool.

APPENDIX D PHONE MODELS / TEST TYPE MATRIX

This appendix maps Test Types to supported phone models.

NOTE: ClarusIPC supports Analog and ATA devices for the Collectors and Test Execution. SIP phones are also included for all functionality listed, with the same parameters as the phones listed.

ClarusIPC 2.5.0 CUCM Versions - 4.X, 5.X, 6.X																
Listed Devices are supported for all ClarusIPC features, with the following exceptions:			Model 7902	Model 7905	Model 7906	Model 7910	Model 7911	Model 7912	Model 7920	Model 7921	Model 7935	Model 7936	Model 7985	ATA Phones	Analog	Communicator
Call Permission	User Class	Target														
Direct Inward Dial	Phone Group	Originator				I*			I*	I*	I*	I*		I*	I*	
		Target				I*			I*	I*	I*	I*		I*	I*	
Directory Handler Lookup	Phone Group	Originator														
		Dialed Member														
Forward to Voicemail	Phone Group	Originator				I*			I*	I*	I*	I*		I*	I*	
		Target														
Meet-me Conference Bridge		Chairperson	E	E	E	E	E	E	E	E	E	E		E	E	
		Participants														
Rollover	Phone Group	Originators														
		Target	E	E	E	E	E	E	E	E	E	E		E	E	
Signaling Delay	DP	Originator	E	E	E	E	E	E	E	E	E	E		E	E	
Voice Protocol OffNet	DP, NS, Loc	Target				E			E	E	E	E		E	E	E*
Softkey Functions: Park	Phone Group	Target	E	E	E	E	E	E	E	E	E	E		E	E	
		Terminator														
		Park Retriever														
Softkey Functions: Redial	Phone Group	Target	E	E	E	E	E	E	E	E	E	E		E	E	
		Terminator														
Softkey Functions: Ad-hoc Conference		Originator														
		Target	E	E	E	E	E	E	E	E	E	E		E	E	
		Terminator														
Softkey Functions: Transfer		Originator														
		Target	E	E	E	E	E	E	E	E	E	E		E	E	
		Terminator														
Softkey Functions: Hold		Originator														
		Target	E	E	E	E	E	E	E	E	E	E		E	E	
Softkey Functions: Corporate Directory		Target	E	E	E	E	E	E	E	E	E	E	X			
		Terminator														
Voice Protocol OnNet	DP, NS, Loc	Originator				E			E	E	E	E		E	E	E*
		Terminator				E			E	E	E	E		E	E	E*
Voice Mail Port Loading		Participants														
Help Desk																
Remote Hands			E	E	E	E	E	E	E	E	E	E		E	E	
Voice Monitor																
Data Collection																
CMR: VQMetrics															E	E
Device Registration	DP, NS, Loc	Originator								E	E				E	E
Phone Web Info Collection									E	E	E				E	E

Listed Devices are supported for all ClarusIPC features, with the following exceptions:

- E: excluded from the functionality listed.
- E*: the device does not support network segment tests.
- X: the test fails for the device.
- I*: included if the default settings are used; if not, the device is excluded.

The following devices are supported in their entirety:

- Models 7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, 7975, and 7914 Expansion Module.

APPENDIX E REDUNDANCY AND BACKUP STRATEGIES

There are several best practices that may be followed to ensure the ClarusIPC system is available in the event of an unplanned failure or outage.

Warm Standby

This strategy involves deploying two ClarusIPC servers: a *primary*, and a *failover*.

These two servers are configured to share a common file system, using RAID or SAN reliable storage systems. The primary ClarusIPC server is used to perform daily tasks. In the event of a failure of this primary server (hardware, OS, or data corruption), the secondary server may be started and used with minimal delay, as it will run the same ClarusIPC configuration as the primary.

Configuration Process

1. Set up two Windows servers with access to a remote RAID device (with the same drive letter or path).
2. Install ClarusIPC on common path from both servers (to ensure the registry keys are setup on both local Operating Systems), and license each. (Note that the second installation will ask to upgrade, as the software is already installed. Ignore this message., and continue with installation.)
3. Stop the ClarusIPC services on the standby server, and set the startup type to “Manual.”
4. Configure the ClarusIPC system by accessing the primary server, then begin daily use.

Recovery Process

1. As a test, shutdown the primary server to simulate a failure during sync, or test or task execution.
2. Prevent the server from automatically restarting either by setting the ClarusIPC services to manual, or by disconnecting the server from the network, removing power, or otherwise preventing it from rebooting.
3. Launch the ClarusIPC services on the secondary server.

4. Resume work by accessing ClarusIPC on the secondary server while repairs are made to the primary.
5. If a new server or new installation is required for the primary server, be sure to backup the ClarusIPC system prior to reinstallation of the ClarusIPC server.

NOTE: If you do not wish to dedicate a server as a secondary ClarusIPC server, you may decide to allocate a server only at the time of primary failure. The recovery time may be increased, but you should still be able to resume work from this new secondary server.

Backup / Recovery

A backup strategy should always be a part of ClarusIPC Best Practices to ensure that a system may be reconstructed in the event of data loss due to unforeseen circumstances. The key components that require backup are:

- Postgres databases. These house nearly all configuration and discovered information.
- Generated reports
- Custom report templates
- Configuration files

It is strongly recommended that you use the ClarusIPC dbutil.bat script to backup your data.

Contact Clarus Systems support for assistance setting up a database user.

Setup

1. Use the dbutil.bat script to schedule a backup of all databases managed by ClarusIPC on a regular basis, preferably when the system will not be heavily used.
2. Add the ClarusIPC server to the existing backup mechanism. Schedule regular backup of the following files:
   - ClarusIPC generated reports (<*clarus_home*>/tomcat/webapps/webdav/publish)
   - ClarusIPC custom report templates (if applicable) (<*clarus_home*>/tomcat/shared/classes/content/reports)
   - ClarusIPC config files (if publishing reports remotely) (<*clarus_home*>/tomcat/shared/classes/reports.properties and <*clarus_home*>/tomcat/conf/server.xml)
   - Database dump files

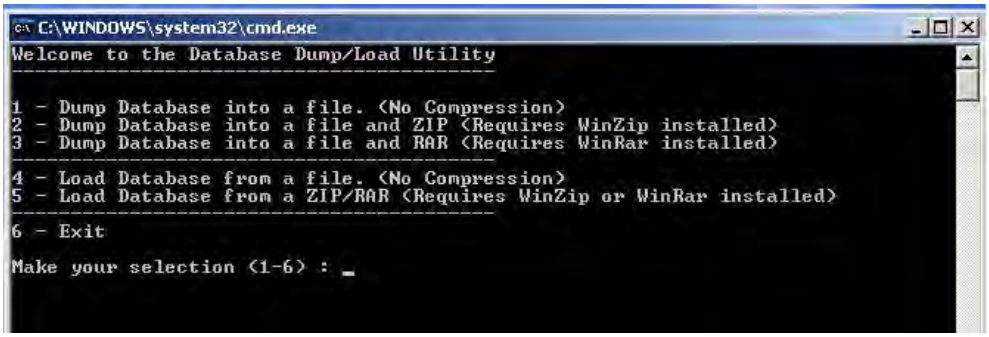
Automated Backup

Backups of the ClarusIPC database may be performed by using the db_backup.bat utility located in `<clarus_home>\postgres\bin`. This script requires no arguments, and will dump all databases into a single file, named by the current hour and minute, inside an automatically created directory, named by the current month, day, year (060108/_09_10). It is recommended that you invoke this script daily using the Windows Task service, or any other 3rd party backup software, and then back up these files to external storage.

To restore this archive, use the interactive dbutil.bat utility, as described below.

Manual Backup

1. To backup your system, go to <*clarus_home*>`\postgres\bin`, and run `dbutil.bat` from the command line.



2. Select Option 1, 2, or 3.
   - **Option 1:** Dumps the database into a file with no compression. The file name and extension must be entered.
   - **Option 2:** Dumps the database into a file with no compression. File name and extension must be entered. Checks C:/program files/winzip (default directory) for winzip installation.
     - If there, prompts the user to enter a file name. (.zip will be added to all file names). Compresses the dumped database in the .zip format.
     - If Winzip is not found in the default directory, allows the user to enter the appropriate directory.
   - **Option 3:** Same as #2 but for .RAR
3. Take the resulting file and copy it to <*clarus_home*>`\postgres\bin` on the new system.
4. Run `dbutil.bat` on the new system.

Recovery

To recover data to a ClarusIPC server (rebuild a server, or recover user deleted data, etc.):

1. Rebuild the server designated as the replacement, and install the operating system.
2. Reinstall ClarusIPC on the server
3. Restore all files to the server.
   - Run `dbutil.bat`, and select Option 4 or 5.
     - **Option 4:** Restores the database from the uncompressed file created using Option 1. Both DButil.bat and the uncompressed database file must be in <*clarus_home*>`\postgres\bin`.
     - **Option 5:** Restores the database from a compressed file (.zip or .rar). Winzip or Winrar must be installed, depending on the format for the compressed file. Then restores the database from the decompressed file.
     - When complete, exit the utility by selecting **Option 6: Exit.**
4. Verify ClarusIPC operation.