# CICM Configuration Management

This document provides the configuration management strategy and procedures for Centrex IP Client Manager (CICM) nodes (gateways) and their element managers (CICM-EMs). This document is part of the CICM customer documentation suite. The complete list of documents in the suite is identified in *CICM Basics*, NN0044-111.

The software releases that this document supports are indicated in the running footer of the document, for example, (I)SN08.

The topics of this document include:



## What's new for CICM configuration

The following changes have occurred for this version of the document:

- updated the entry data for commands NEW and QLEN in the procedures
  - On a PC connected to the CICM Administration LAN
  - CS2000 Line provisioning for CICM clients
- updated the section Network Profiles to remove the VMG-specific context, especially in Example of Network domain addressing and new section Media routing in a CS2000 environment with NAT
- added the procedure Updating auto-discovery networks
- updated the procedure Configuring PAM on the CICM-EMs
- updated the procedure Configuring the apache proxy server for the CICM-EM pair

- added the chapter Installing and initializing IP phones for CICM nodes
- deleted the procedure “Add a slave CICM-EM to the master CICM-EM” since this is now handled through initial installation
- changed all occurrences of Succession Element and Sub-element Manager (SESM) to CS2K Management Tools (CMT)

## Configuration management strategy

The CICM-EM and its CICM nodes are initially configured during initial installation by Nortel system installers.

After initial system configuration, configuration may be changed or additional configuration completed by the Service Provider.

For SN08 and later, all configuration is performed directly on the CICM-EM or CICM node using the preboot tool. The other configuration procedures are included in this document. The command button to access the former Configuration Wizard still appears in the menu, but has no capabilities.

The CICM-EM web page menus that are used to configure a CICM node and its clients are:

- profiles
  - audio
  - enterprise
  - language
  - network
  - user
  - feature
  - security
- users
- client terminals

## Configuration data

Configuration data, such as IP addresses and the maximum number of concurrent sessions, resides within the Windows NT system registry.

Element Managers can be configured to periodically back up the configuration data of all CICM nodes and CICM-EMs (for example, every night at a specified time).

The operating company may use standard tools to ensure that this critical configuration data is archived externally to the CICM node or CICM-EM.

Previously backed up configuration data can be restored to the Windows NT registry in the event of data loss or data corruption. Service can then be resumed on a replacement or repaired system with minimal loss of service.

## Tools and utilities

The tools and utilities include the procedure Provisioning CICM client lines, which involves datafilling through SERVORD.

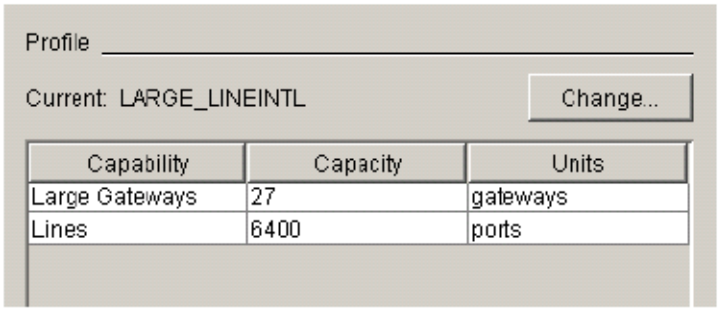
### Provisioning CICM client lines

The procedure to provision a CICM client (terminal) onto the CS2000 is similar to the method used to provision a line on other gateways.

***On a PC connected to the CICM Administration LAN***

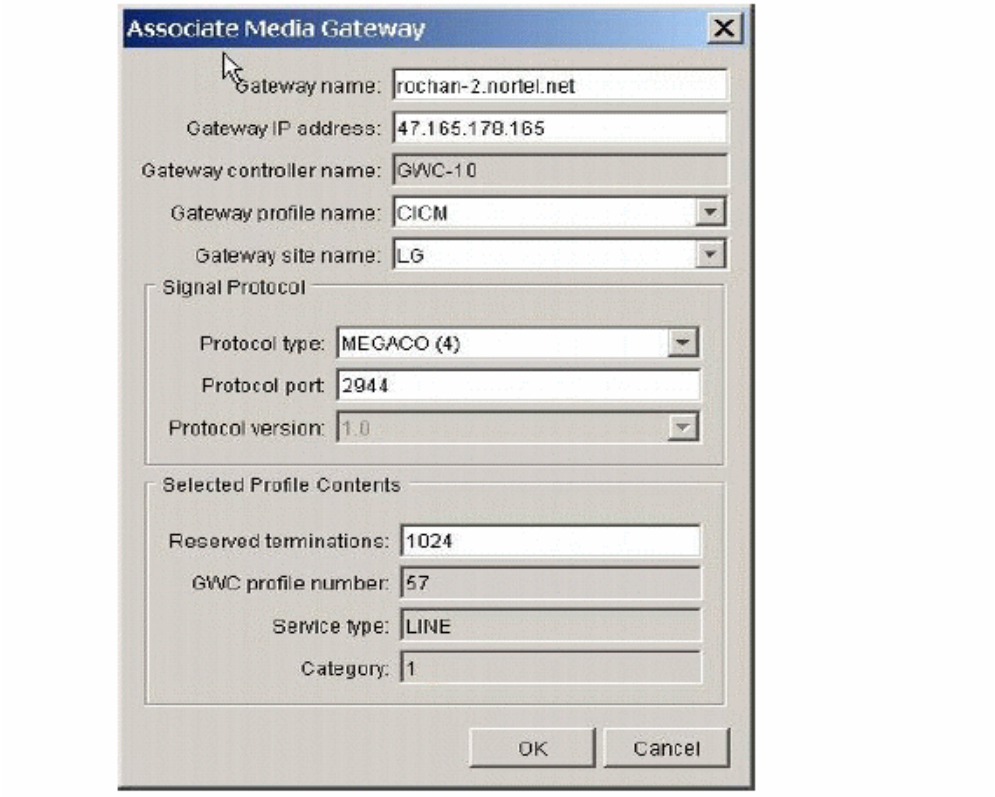
**1** Connect to the CS2000 Management Server for the selected CS2000.

**2** Ensure that the GWC is provisioned to support Large Lines Gateways.



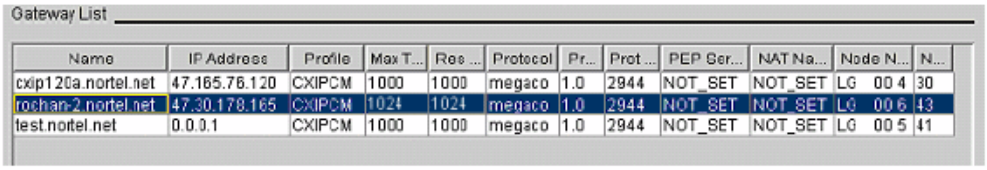

**3** Select **Associate Media Gateway** to associate a CICM node with the selected GWC.

The dialog *Associate Media Gateway* opens.




**4** Datafill the Associate Media Gateway window, then press **OK**.

The registration of the CICM gateway against the GWC is displayed.




**5** Create the logical group in table LGRPINV on the CS2000.

The table tuples may appear as shown in the following example.

```
TABLE: LGRPINV
>lis all
TOP
GRPNO SRVRNAME GRPTYPE LGRPOPTS
------------------------------
LG 00 0 GWC 6 C $
LG 00 1 GWC 13 C $
LG 00 2 GWC 14 C $
LG 00 3 GWC 15 C $
LG 00 4 GWC 9 C $
LG 00 5 GWC 9 C $
LG 00 6 GWC 9 C $ <------------ RESULTING ENTRY
BOTTOM
```

6 Log into OSSGATE and enter the command **NEW** to create new lines, for example:

```
NEW $ 8500001 m5216 SET IPLCLIENT OTHER PUBGRPA 0 0 1511 Y CICM 500 0 0 01 1 userid 000001 $ 1
passwd 1234 1 LNR 2 3WC IPCLIENT OTHER 3 MWT Y ALL N 4 CFU N 1 $ 5 INSPECT $
```

where

**8500001**
is the directory number (DN).

**m5216**
is the name of the line class code (LCC).

**IPCLIENT OTHER**
specifies the kind of phone service. OTHER indicates any of the Nortel IP phone sets.

**PUBGRPA**
is the customer group.

**151**
is the simplified numbering plan area (SNPA).

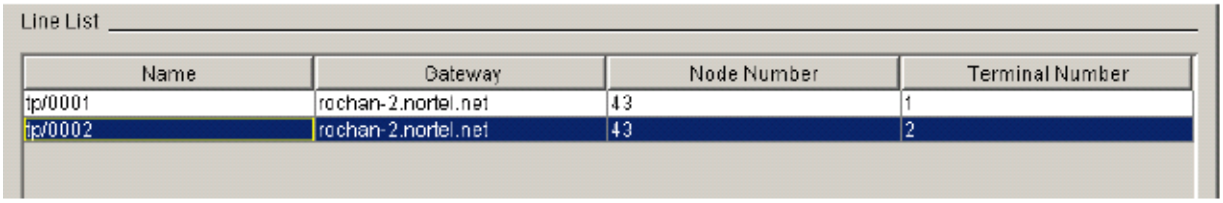
**CICM 500 0 00 01**
is the line equipment number (LEN)

**1 userid 000001 $**
is the user id of the CICM client (terminal).

**1 passwd 1234**
is the password of the user id.

**1 LNR 2 3WC IPCLIENT OTHER 3 MWT Y ALL N 4 CFU N 1 $ 5 INSPECT $**
is the list of features assigned to the line. Use OTHER to include any version of an IP phone for option IPCLIENT.

The CS2000 Management Server shows:




The response to the command QLEN on the CS2000 appears, for example:

```
>qlen 8500001
------------------------------------------------------------
LEN:   CICM 500 0 00 01
TYPE:  SINGLE LINE
SNPA:  151
DIRECTORY NUMBER:          8500001
LINE CLASS CODE:        M5216 SET
CUSTGRP:     PUBGRPA   SUBGRP: 0   NCOS: 0   RING:  Y
CARDCODE:   IPCLIENT   GND: N PADGRP: PKNIL BNV: NL MKO:  Y
PM NODE NUMBER       :    43
PM TERMINAL NUMBER :    2
OPTIONS:
  3WC  MWT  CFU

   KEY          DN
   -----        ----
     1          DN          2088500001

   KEY          FEATURE
   -----        -------------
```

**7** This procedure is complete.

# Configuration management procedures

This section provides the configuration procedures undertaken from the CICM-EM Web pages.

***Note:*** For all procedures provided in this document, it is required to use administrator userids and passwords to login to the CICM-EM.

The CICM products are configured during initial installation by Nortel system installers. After installation, the Service Provider must use the tool OSSGate to:

- create users or batch create users
- batch change the configuration of users
- configure or re-configure users
- delete a user

Using the OSSGate tool ensures that the gateway and the Succession Element and Sub-Element Manager (SESM) have synchronized configuration data. Refer to the *OSSGate User's Guide*, NE10004512.

## Viewing the users list and user configuration

Use the procedure View users list to identify the users of a CICM node and use the procedure View user configuration to view the configuration for a user on a CICM node.

### Procedure 1 View users list

***At the element manager home page***

**1** Select **users** from the left menu.

The page *user home page* opens.

**2** Select the CICM node identifier from the drop-down menu under **browse users** on the right menu, then click on the **browse users** text.

The page *users on CICM <cicm-nnn> (range <#-#> on vmg <name>)* opens with the list of current users on the CICM node.


**3** To view the user list for a different CICM node, a different VMG, or a different range, select from the drop-down menus of **browse users on** on the right menu.

The page *users on CICM <cicm-nnn> (range <#-#> on vmg <name>)* updates to display the selection.

**4** To view a list of active users with node and line number information, click on **list the active users** on the right menu.

The page *active users on <cicm-nnn>* opens.

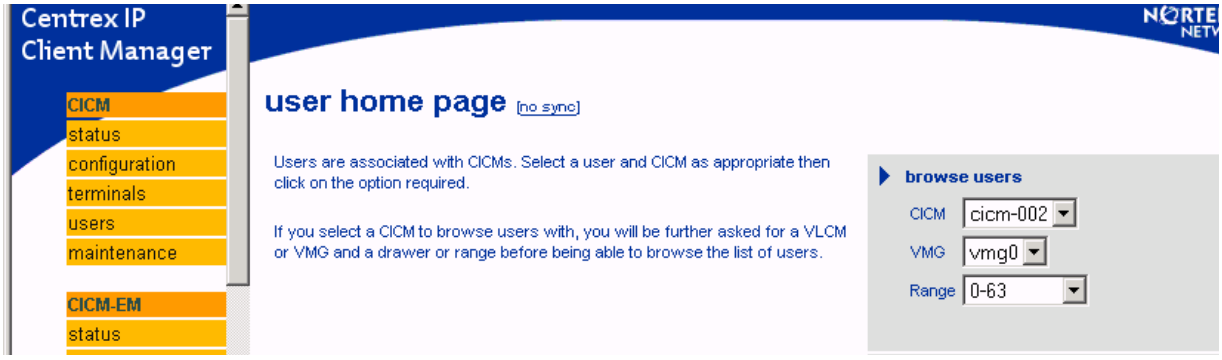

**5** This procedure is complete.

## Procedure 2 View user configuration

***At the users home page of the element manager Web pages***

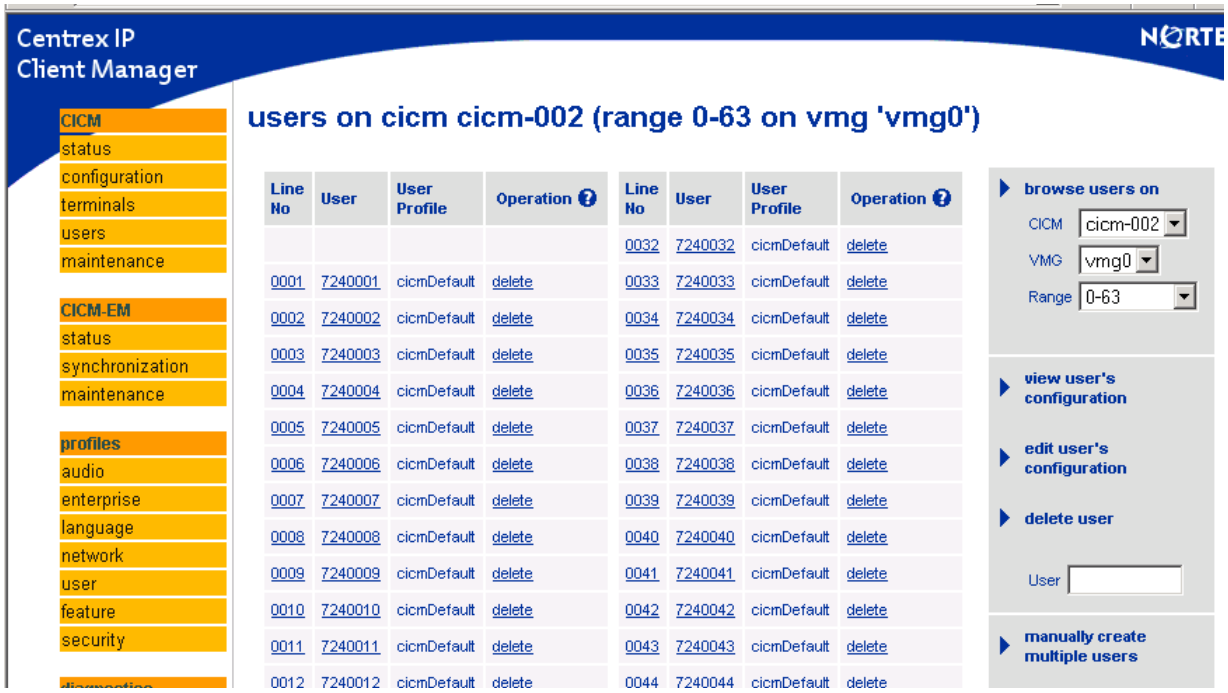
1 Select the CICM node identifier from the drop-down menu under **browse users** on the right menu, then click on **browse users**.

The VMG and Range fields are displayed under **browse users**.



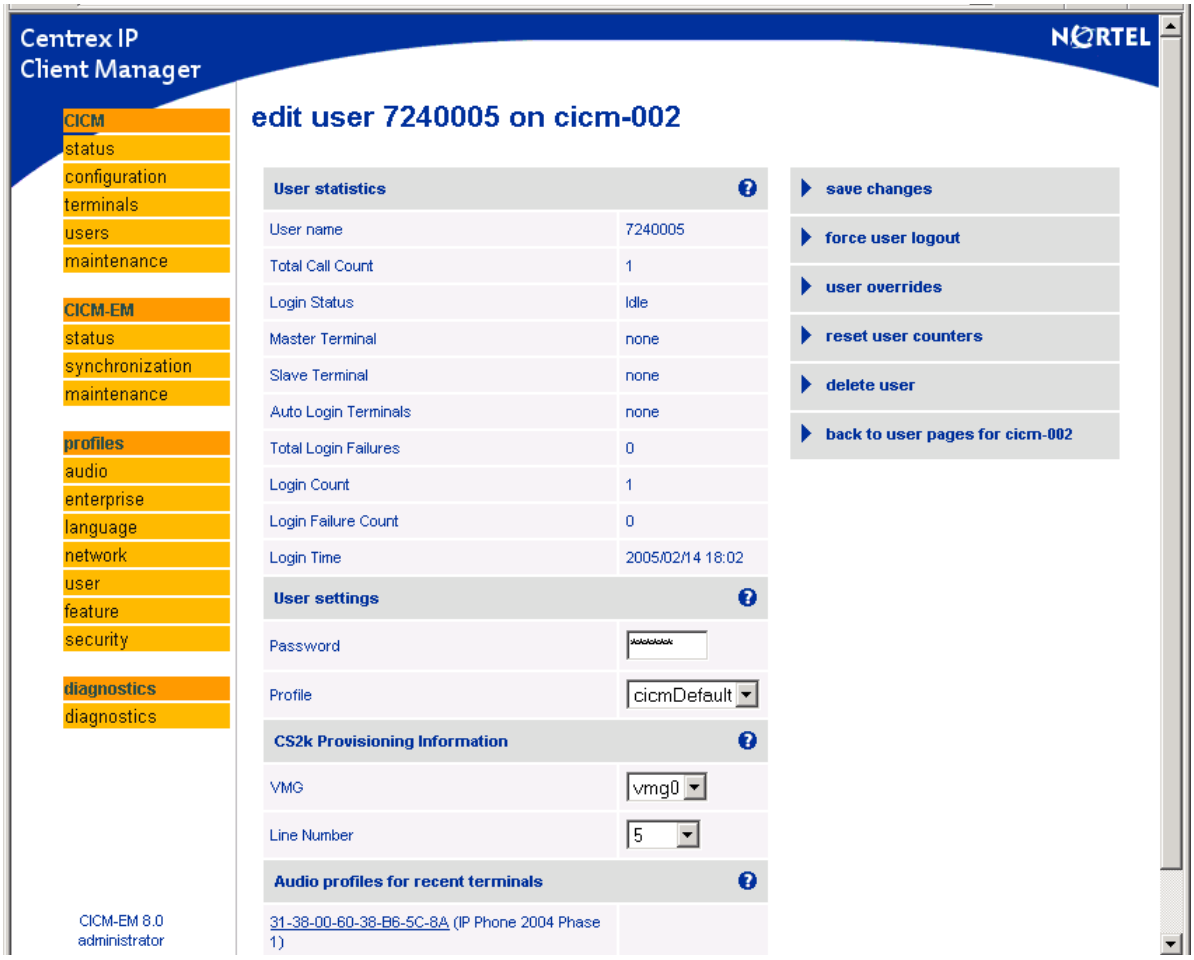

2 Click again on **browse users** on the right menu.

The page *users on CICM <cicm-nnn> (range <#-#> on vmg <vmg_name>)* opens.




3 To view a user configuration, click on the username on the list, or Enter a user name in the **User** field on the right menu, then click on the **view user's configuration** text.

The page *view user <username> on <cicm-nnn>* opens. Changes cannot be made from this page.




4 To configure or edit user configuration, refer to the *OSS Guide (ATM) Advance Feature Guide*, PLN-08AT-OSS.

5 This procedure is complete.

## Forcing a logout of a user on a CICM node

Force a user to log out of a CICM node.

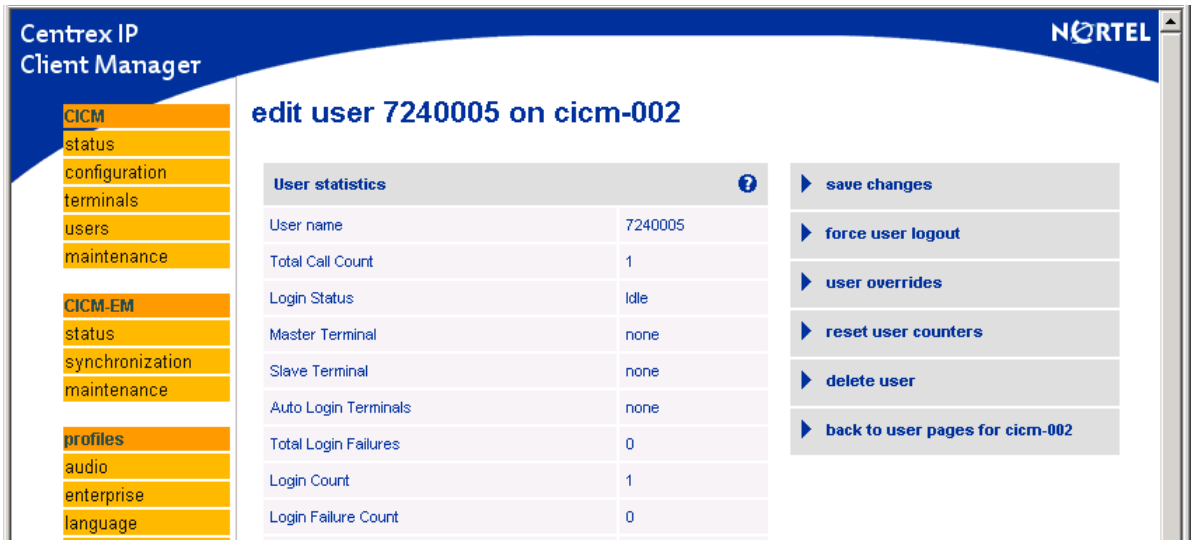
***At the users home page of the element manager Web pages***

1 Select the CICM node identifier from the drop-down menu in **browse users on**, then click on the **browse users on** text two times.

The page *users on CICM <name> (range <number> on vmg <name>)* opens.

2 Enter a user name under **delete users** on the right menu, then click on **edit a user's configuration**.

The page *edit user <name> on <cicm-nnn>* opens.




3 Click on **force user logout** on the right menu.

A status message appears with the result of the force logout action.

4 This procedure is complete.

## Resetting user counters

Reset thew following user counters to zero:

- Total login failures
- Login count
- Login failure count
- Total call count

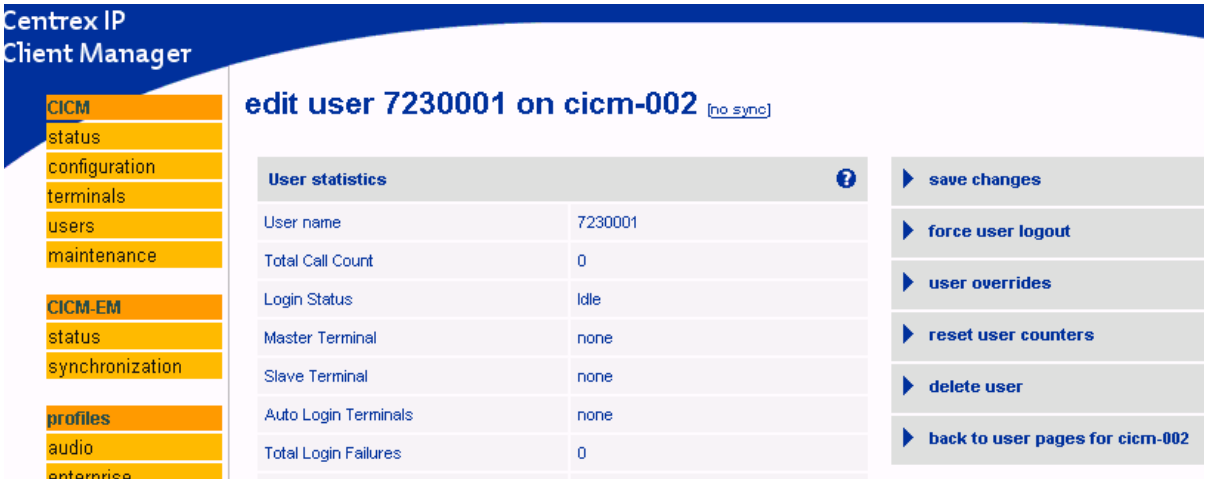
***At the user home page of the element manager Web pages***

1 Select the CICM node identifier from the drop-down menu in the **browse users on** box, then click on the **browse users on** text two times.

The page *users on CICM <cicm-nnn> (range <number> on vmg <name>)* opens.

2 Click on the user name to reset counters for.

The page *edit user <username> on <cicm-nnn>* opens.




3 Click on **reset user counters** on the right menu.

A status page displays the results of the reset command.

4 This procedure is complete.

### Creating and configuring profiles

Use the CICM-EM Web pages to configure the CICM nodes through creating, modifying, and applying different types of profiles. Profiles enable configuring many CICM nodes at one time. The profiles are maintained on the CICM-EM and include:

- Audio Profiles
- Audio Profiles
- Enterprise Profiles
- Language Profiles
- Network Profiles
- User Profiles
- Feature Profiles
- Security profiles

### Audio Profiles

An Audio Profile specifies audio parameters for making or receiving a call. Audio Profiles simplify the way in which users control the audio parameters that are used when making a call. The parameters which can be configured include voice coding type, voice activity detection and the voice packet size. These parameters are configured according to the specific network conditions that exist between the customer site and the CICM node. Having several profiles available to users means that they can select the most appropriate profile for each call.

Implementing the parameters in the Audio Profile can range from applying a specific codec to changing QoS marking in the headers of the IP packets, which in turn will affect how other devices in the network treat those packets.

Examples of audio parameters are:

- Which codec the client terminal should apply to an outgoing media stream
- Voice Activity Detection (VAD) capability with G.729A
- Packet size (that is, the number of voice frames per packet)
- Quality of Service (QoS) parameters to be applied to the IP packets originating from that terminal or destined for that terminal
- Jitter buffer setting on the terminal

The CICM administrator can adjust the parameters in an audio profile to compensate for different types of conditions in the network. For

example, a telecommuter's IP voice packets may encounter one set of network conditions when a call is placed from the home, and a different set of conditions when a call is placed from the office. In this case the telecommuter would need two different audio profiles, one for each terminal.

The CICM administrator controls the Audio Profiles and determines which ones will be available for end users to select for their terminals. When a user logs into a CICM node through a specific terminal, the CICM updates the items on the Audio Profile selection menu and applies the Audio Profile to that specific terminal.

When an end user or the CICM administrator selects an Audio Profile for a terminal, the following occurs:

- The terminal implements the parameters for all outgoing voice traffic
- The CICM node implements the parameters for all voice traffic destined for that terminal.

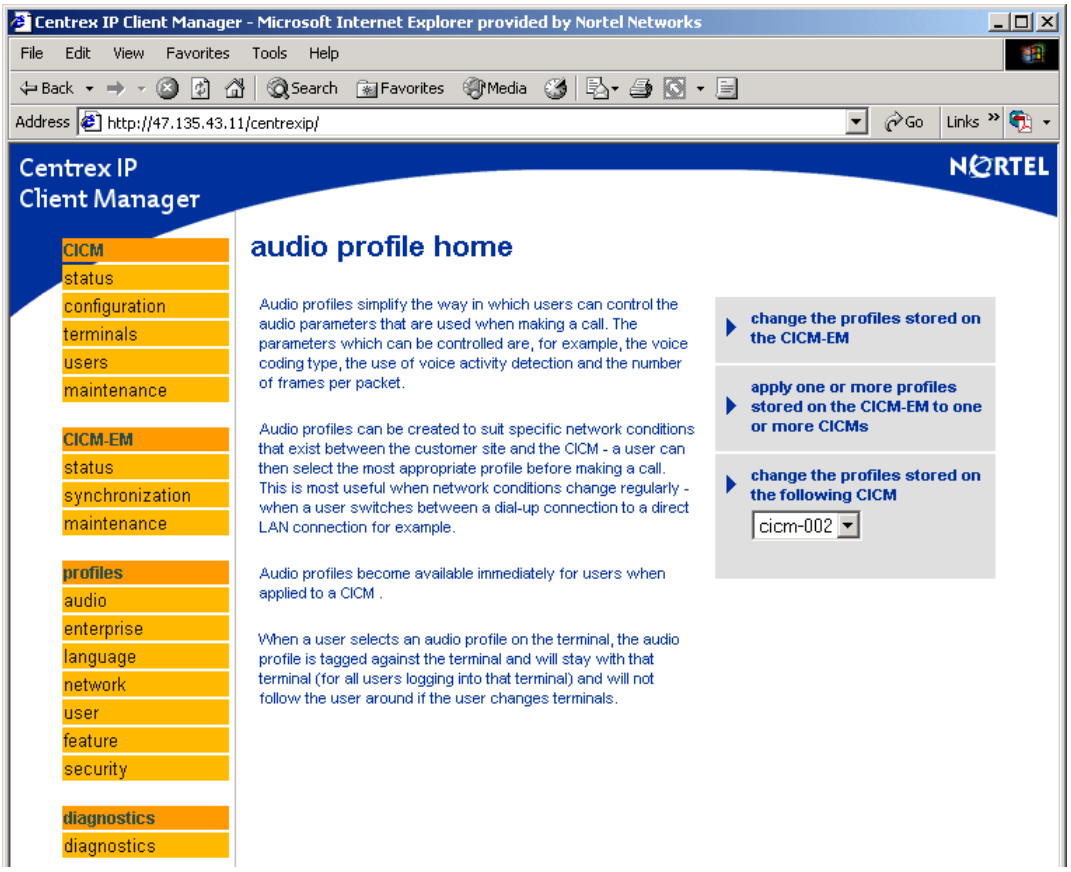
Audio profiles may be created, changed or deleted. Audio Profile changes take effect on the next call. They may be applied to a CICM node or to a terminal.

**Procedure 3 Creating an Audio Profile on a CICM-EM**

***At the Element Manager home page***

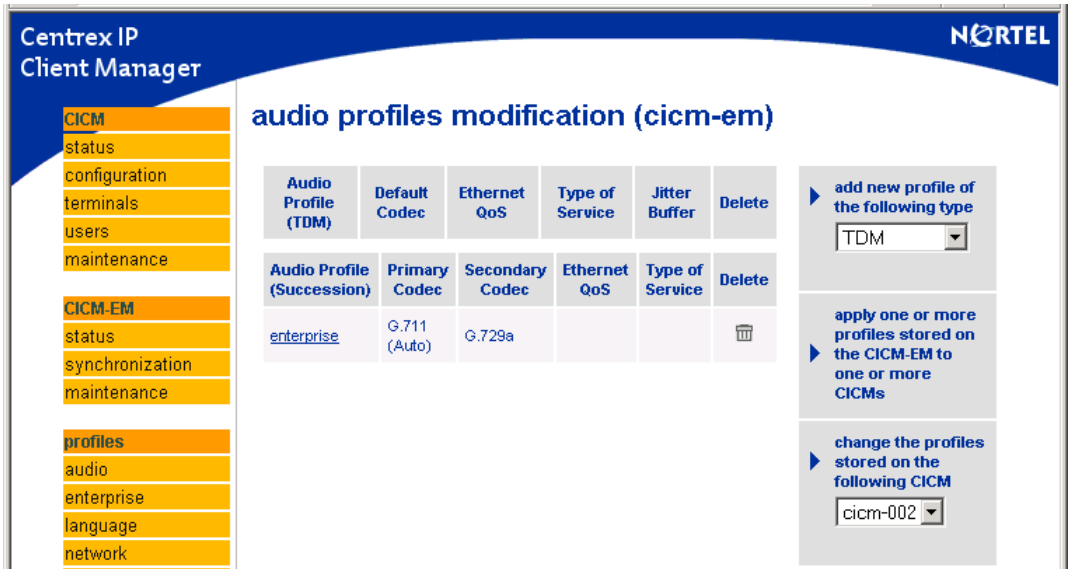
**1** Select **audio** from the **profiles** section of the left menu bar.

The page *audio profile home* opens.



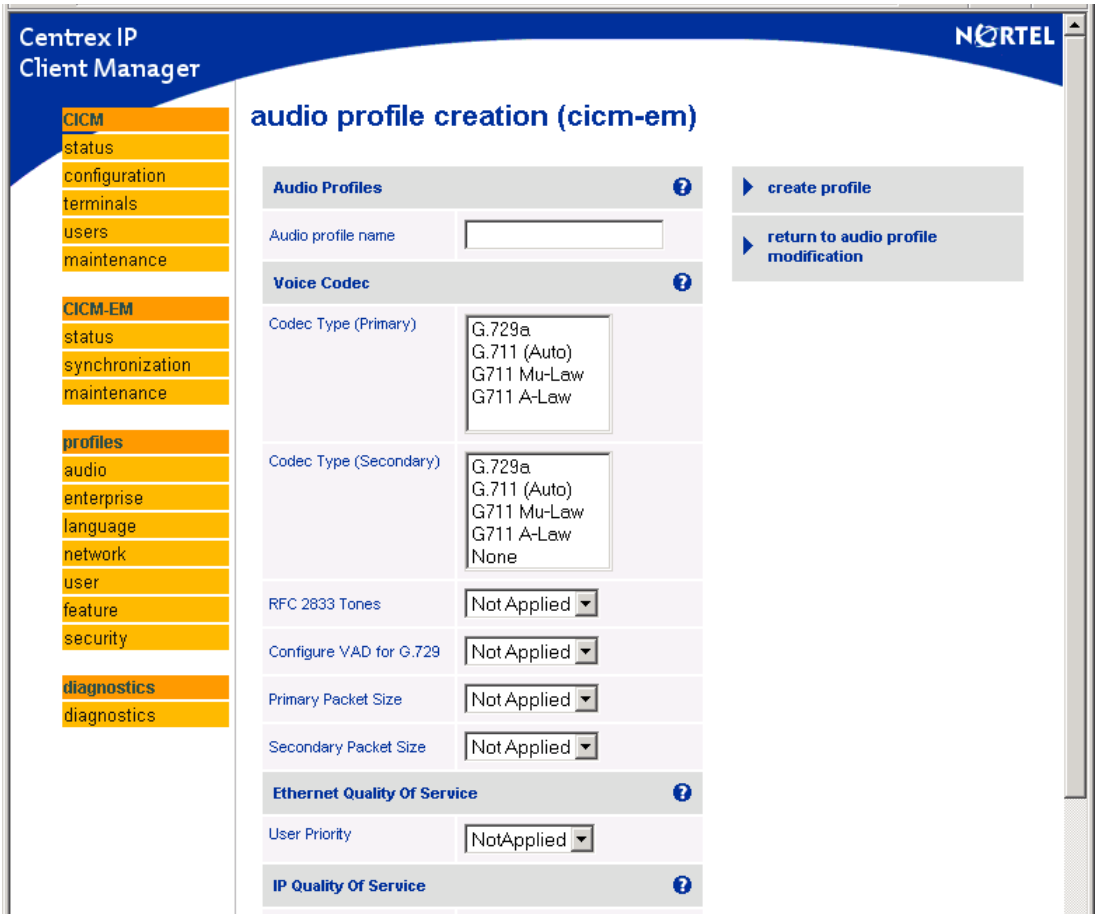

**2** To create a new Audio Profile, click on **change the profiles stored in the CICM-EM** on the right menu.

The page *audio profile modification* opens.




3 Choose **Succession** from the drop-down menu under **add new profile of the following type** on the right menu.

The page *audio profile creation* opens.




4 Type the new profile name in the **Audio Profile Name** field, then create the profile by datafilling each of the fields.

***Note:*** Click on the **?** icon in each field for detailed descriptions and decision criteria.

5 After the fields are datafilled, click on **create profile** on the right menu.

The display *profile creation results* shows the profile creation status and confirms completion.

***Note:*** The profile created is stored on the CICM-EM. To be activated, they must be applied to the CICM nodes by the procedure Applying an Audio Profile to a CICM node.

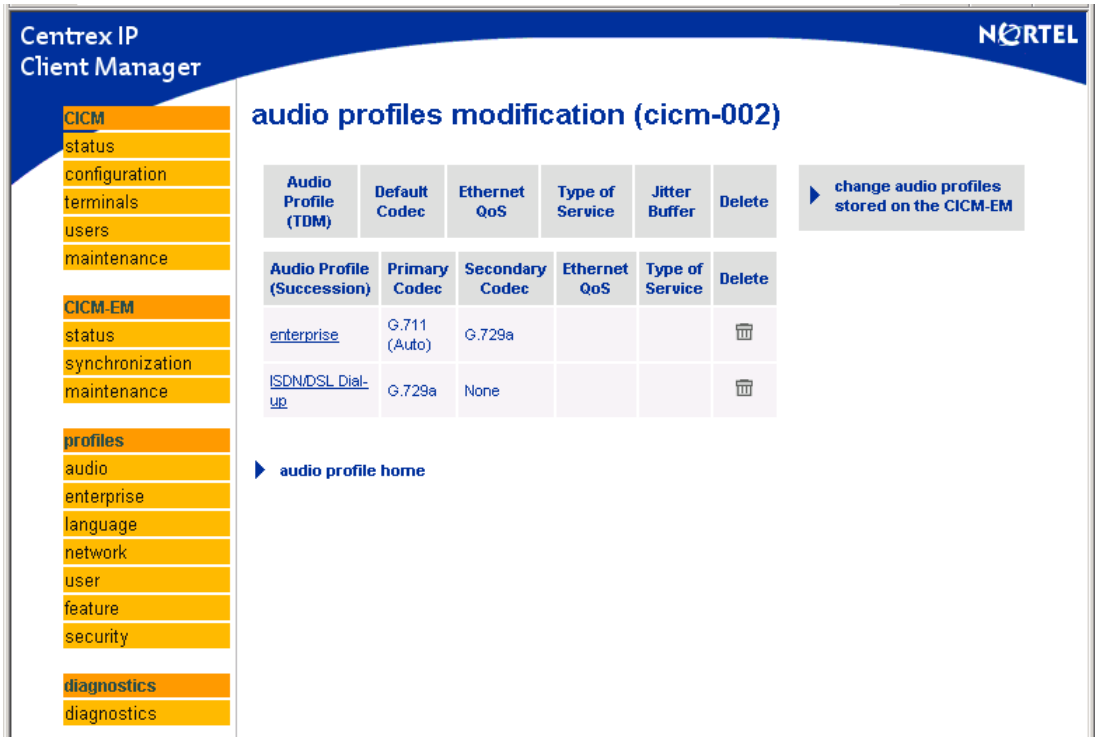
6 This procedure is complete.

## Procedure 4 Changing an Audio Profile on a CICM node

***At the Audio Profile home page of the Element Manager Web pages***

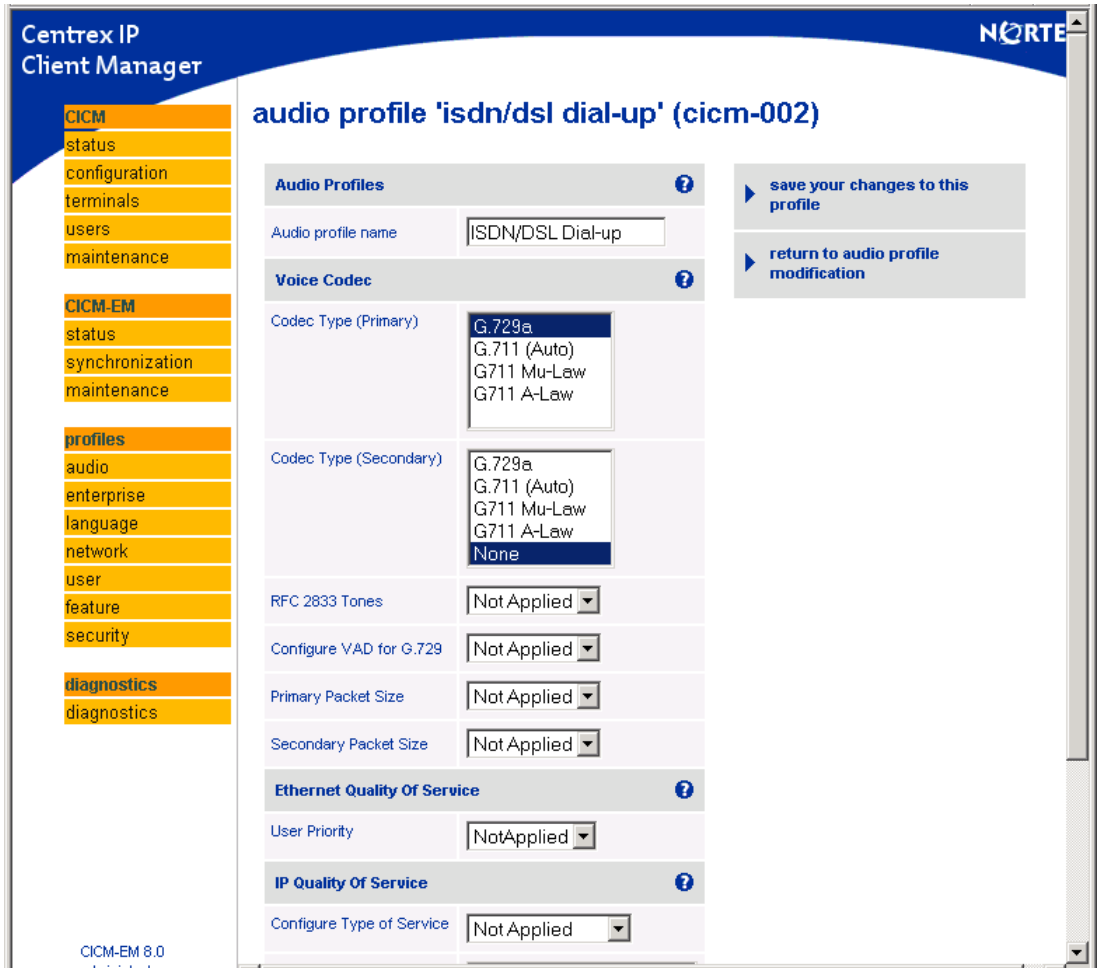
**1** Select the CICM node identifier from the drop-down menu under the **change the profiles stored on the following CICM** text on the right.

The page *audio profiles modification <cicm-nnn>* opens.




**2** Click on the audio profile to change.

The page *audio profile <profile_name> (<cicm-nnn>)* opens.




**3** Edit the audio profile by modifying the fields.

Click on the **?** icon in each field for detailed descriptions and decision criteria.

**4** Click on **save your changes to this profile** on the right menu to save the edited profile to the CICM-EM.

The display *profile save results* shows the results of the action.

**5** This procedure is complete.

## Procedure 5 Applying an Audio Profile to a CICM node

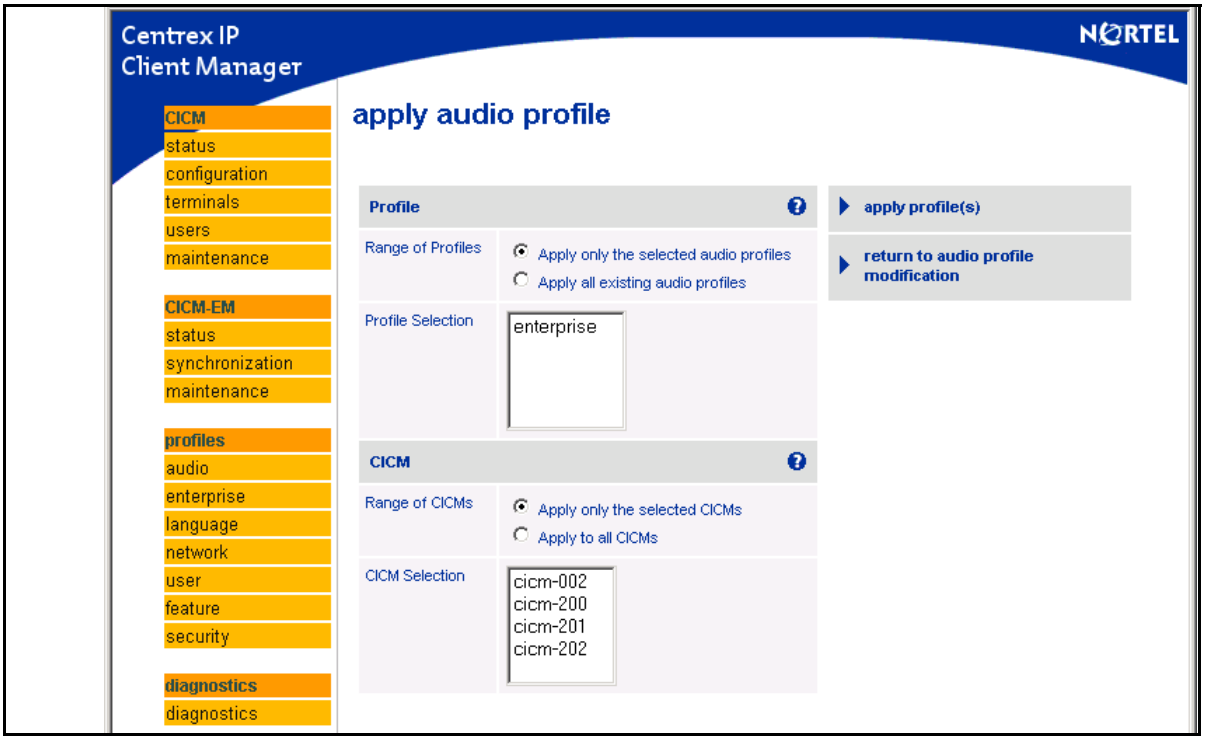
### *At the Element Manager home page*

1 Select **audio** from the **profiles** menu on the left.

The page *audio profile home* opens.

2 Click on **apply one or more profiles stored on the CICM-EM to one or more CICMs** on the right menu.

The page *apply audio profile* opens.




3 In the **Range of Profiles** box, click a radio button to either:

- apply only the selected audio profiles
- apply all existing audio profiles

4 In the **Profile Selection** box, choose the profiles to apply by clicking. Use **Shift +Click** to add a range, or **Control +Click** to add a nonconsecutive selection.

5 In the **Range of CICMs** box, click a radio button to either:

- apply the profiles only to the selected CICM node or nodes
- apply the profiles to all CICM nodes

6 In the **CICM Selection** box, click on the CICM identifiers to apply the profiles to. Use **Shift +Click** to add a range, or **Control +Click** to add a selection.

7 Click on **apply profile(s)** on the right menu.

A status page displays the results of the action and confirms completion.

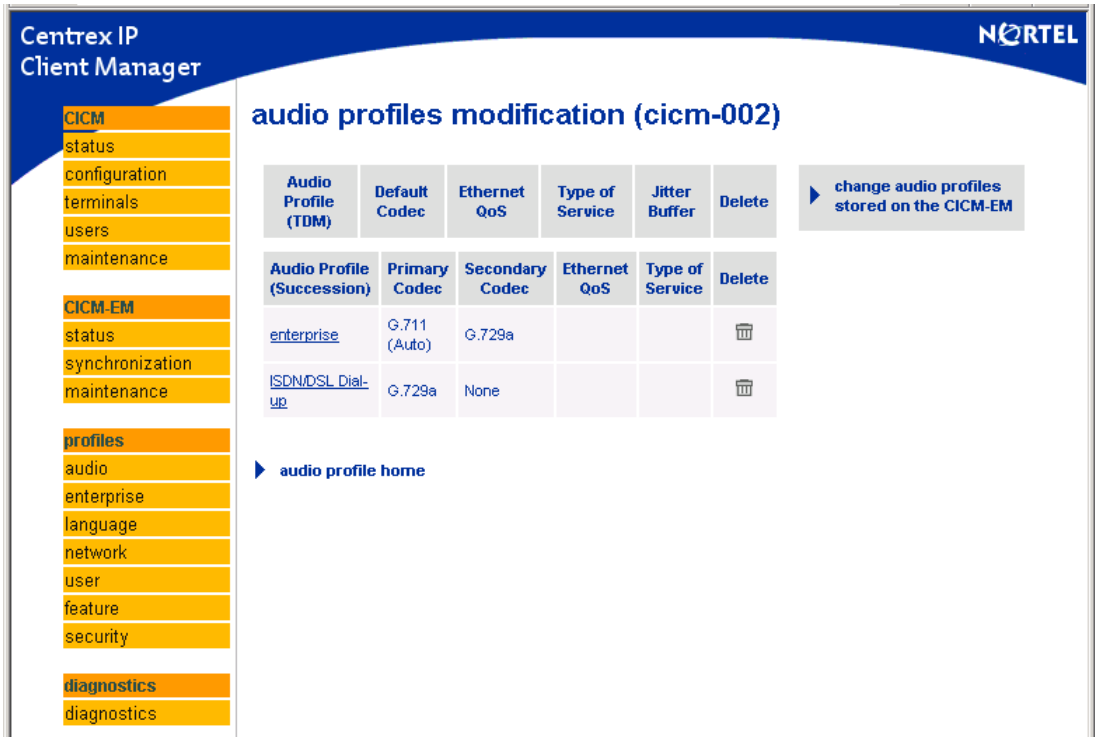
8 This procedure is complete.

## Procedure 6 Deleting an Audio Profile from a CICM node

***From the audio profile home page of the CICM-EM Web pages***

1 Choose the CICM node identifier from the drop-down menu on **change the profiles stored on the following CICM** on the right-hand menu.

The page *audio profiles modification on <cicm-nnn>* displays the list of audio profiles stored on the CICM node.




2 Click on the delete (trash can) icon for the audio profile to delete.

A status page opens to confirm the deletion.

3 This procedure is complete.

## Procedure 7 Applying an Audio Profile to a user

***At the User Home Page of the Element Manager home pages***

1 Select the CICM node identifier that the user is on from the drop-down menu of **browse users on**, then click on **browse users**.

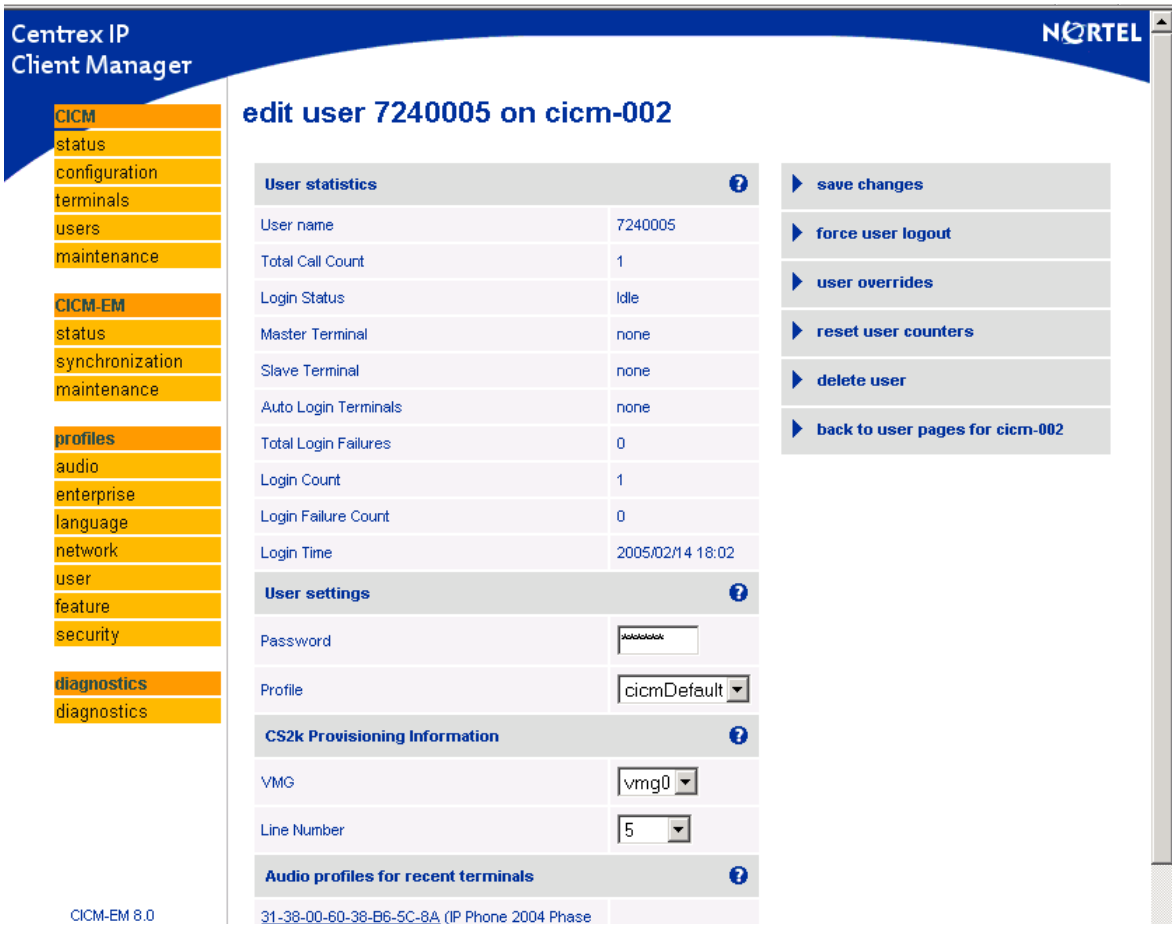
The **browse users** section expands to display the VMG and user ranges.

2 Select user range applicable from the drop-down menu of **browse users**, then click on **browse users** again.

The page *users on CICM <name> (range <#-#> on vmg <name>)* opens and displays a list of users.

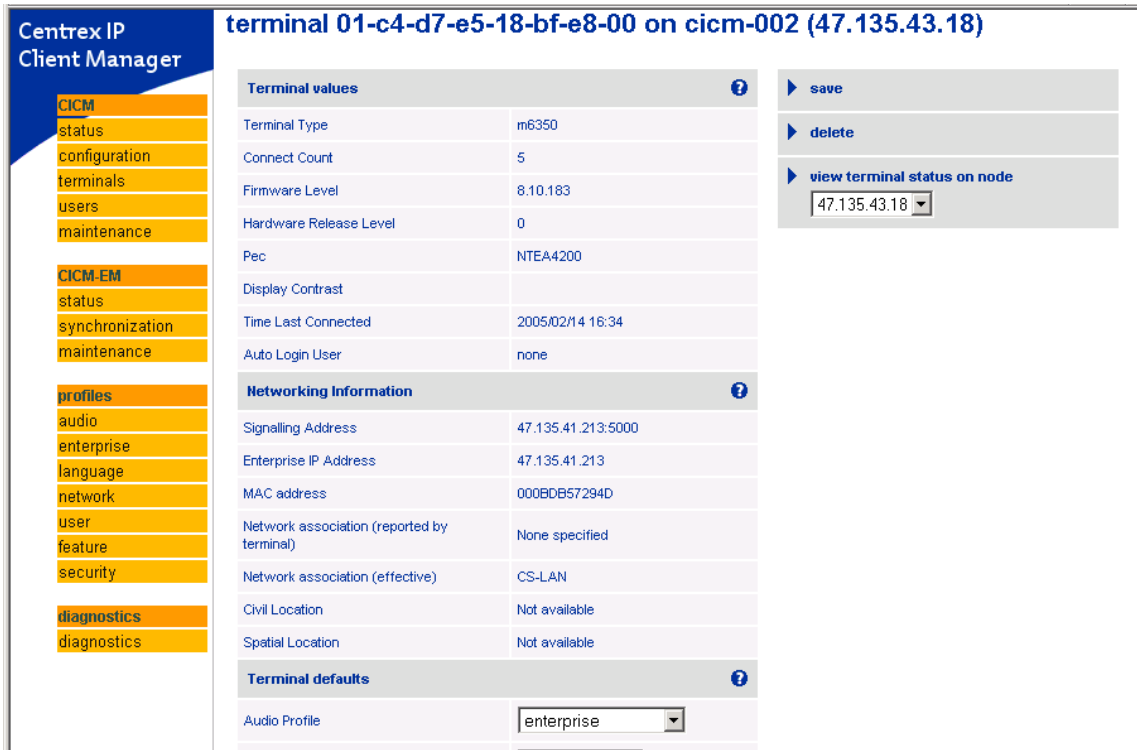

3 Click on the user name to apply an Audio Profile to.

The page *edit user <name> on <cicm-nnn>* opens.




4 In the **Audio profiles for recent terminals** section at the bottom, click on the user terminal to apply the Audio Profile to.

The page *terminal <MAC address> on <cicm-nnn>* opens.




5 In the **Audio Profiles** field of the **Terminal defaults** section, select the audio profile to apply from the drop-down menu, then click on **save** on the right menu.

6 This procedure is complete.

## Enterprise Profiles

Enterprise Profiles provide for groupings of Network Profiles and CICM nodes. The Enterprise Profile is created through the CICM-EM and stored on the CICM node, as is the Network Profile. An Enterprise Profile groups the Network Profile(s) of an enterprise with the CICM nodes that serve that enterprise.

The purpose of the Enterprise Profile is to support the Selective CICM Login feature (that is, Hot Desking capability). With this feature, users of an enterprise that is served by multiple CICM nodes will be provided with an option at the login prompt, to choose which CICM node to log into, from a list of nodes that serve this enterprise. The user can also log into any terminal connected to the selected CICM node.

A CICM node may be associated with many Enterprise Profiles if these enterprises are served by this CICM node. However, a Network Profile can only be associated with a single Enterprise Profile.

During the setup of a session when a client connects, the hosting CICM node checks the source IP address of the packet against the list of Network Profiles stored on the CICM node. If a Network Profile contains that source IP address and the Network Profile is also associated with an Enterprise Profile, the user is then presented with a list of all the CICM nodes associated with that Enterprise Profile, and will be able to redirect their terminal to any of these CICM nodes. Thus the Enterprise profile, in conjunction with the Network Profile, enhances security.

***Note:*** The source IP address may or may not be the client's IP address. If the client is behind an enterprise NAT, then the source IP address is the public IP address of the NAT.

The Enterprise Profile is created, edited and deleted on the Element Manager. The Enterprise Profile or its associated Networks Profiles cannot be edited on the CICM node they have been applied to.

The complete process for creation and configuration of Enterprise Profiles is summarized as follows:

- **Create an Enterprise Profile**. See the procedure Creating an Enterprise Profile.
- **Associate Network Profiles to the Enterprise Profile**. See the procedure Associating and applying an Enterprise Profile.

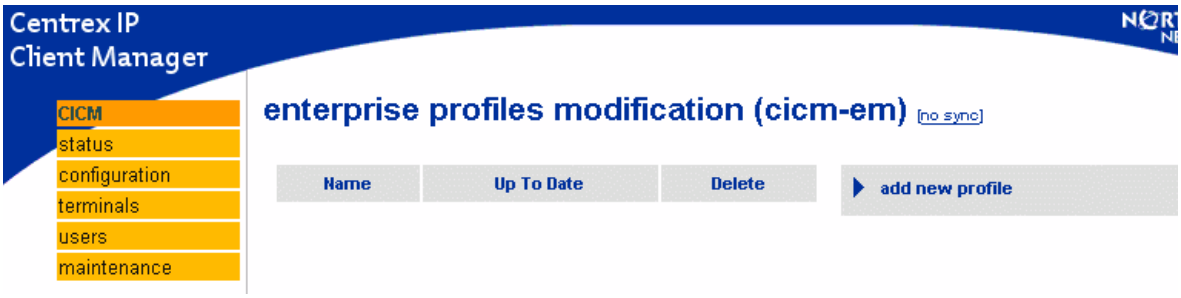
- **Associate CICM nodes to the Enterprise Profile**. See the procedure Associating and applying an Enterprise Profile.
- **Apply the Enterprise Profile to the CICM node**. This step downloads and saves the Enterprise Profile to the CICM node. See the procedure Associating and applying an Enterprise Profile.

### Procedure 8 Creating an Enterprise Profile

***At the CICM - Element Manager Home page***

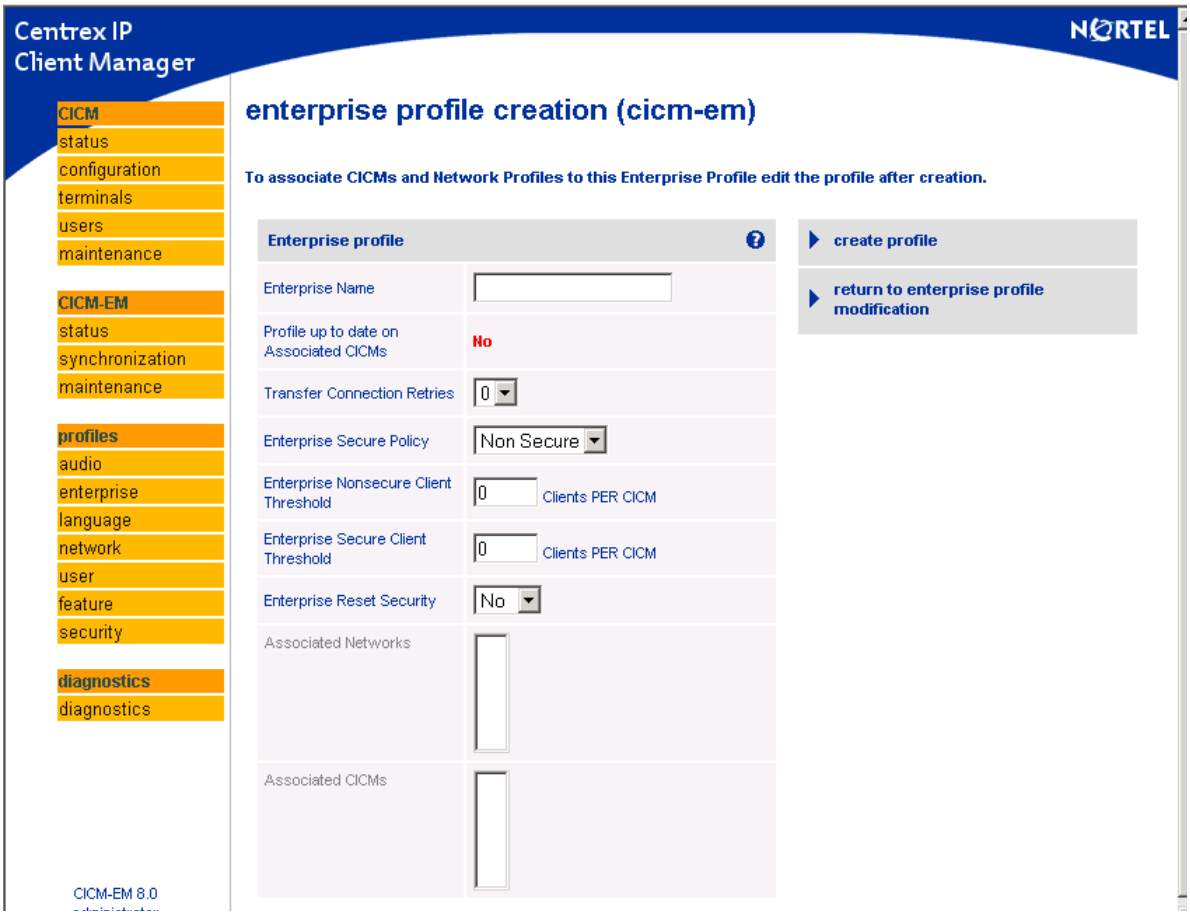
**1** Select **enterprise** from the **profiles** section of the left menu.

The page *enterprise profiles modification* opens.




**2** Click on **add new profile** on the right menu.

The page *enterprise profile creation (cicm-em)* opens.


Centrex IP
Client Manager
NORTEL
CICM
status
configuration
terminals
users
maintenance
CICM-EM
status
synchronization
maintenance
profiles
audio
enterprise
language
network
user
feature
security
diagnostics
diagnostics
CICM-EM 8.0
enterprise profile creation (cicm-em)
To associate CICMs and Network Profiles to this Enterprise Profile edit the profile after creation.
Enterprise profile
Enterprise Name
Profile up to date on Associated CICMs
No
Transfer Connection Retries
0
Enterprise Secure Policy
Non Secure
Enterprise Nonsecure Client Threshold
0
Clients PER CICM
Enterprise Secure Client Threshold
0
Clients PER CICM
Enterprise Reset Security
No
Associated Networks
Associated CICMs
create profile
return to enterprise profile modification

3 Datafill the **Enterprise Name** field, then datafill all other fields (refer to the table Enterprise Profile fields for field descriptions), then click on **create profile** on the right menu.

**Table 1 Enterprise Profile fields**

| Field | Entry | Description |
|---|---|---|
| Enterprise Name | User determined name no more than 20 alpha-numeric characters. | The Enterprise Name is chosen upon creation and cannot be edited thereafter. |
| Profile up to date on Associated CICM nodes | Read-only. Yes or No | Indicates whether the profile is up-to-date on all of its associated CICM nodes. The state changes to No when a change is made to the Enterprise Profile. The state changes to Yes when it is successfully applied to all of the CICM nodes in the Associated CICM nodes list. Refer to the procedure Associating and applying an Enterprise Profile.<br>***Note:*** If the Enterprise Profile is not kept up-to-date on the associated CICM(s), it will automatically deactivate upon its associated CICMs, and must be re-associated. |
| Transfer Connection Retries | 0 or 1<br>Default is 0 | Recommended setting: 0<br>This is the number of times a terminal redirecting to another CICM node will retry connecting to each node of the target CICM. The value should be set to zero (the default) for most applications. |
| Enterprise secure policy | Secure or Nonsecure | Indicates whether the communications between the CICM node servers within the enterprise, and their clients are secure or nonsecure. |
| Enterprise Nonsecure Client Threshold | 0 to 9999 | Indicates the number of clients permitted to connect in nonsecure mode to their secure CICM node servers within the enterprise (enterprise has security policy of Secure). |
| Enterprise Secure Client Threshold | 0 to 9999 | Indicates the number of clients permitted to connect in secure mode to their nonsecure CICM node servers within the enterprise (enterprise has a security policy of Nonsecure). |
| Enterprise Reset Security | Yes or No | Indicates whether all clients under the enterprise will have their security object cleared (yes). Clearing the security object from a client facilitates moving the client from one CICM node server to another. |

(Sheet 1 of 2)

**Table 1 Enterprise Profile fields (Continued)**

| Field | Entry | Description |
|---|---|---|
| Associated Networks (Network Profile) | Read-only | Terminals are associated with an enterprise based on their network location. Some terminals can automatically discover their location (for example, from a DHCP server) and provide it to the CICM node. For terminals that do not or cannot report an automatically discovered network location to the CICM node, a mapping, called a Network Profile, can be created to assign a network location based on the terminal's IP address. This is the list of network locations that are associated with the enterprise defined by this profile.<br><br>A non-editable list of Network Profiles that are associated with this Enterprise Profile. When a CICM node is disassociated from the Enterprise Profile, it will remain in this list with the postfix "disassociated" until the updated information is successfully applied to the CICM nodes in the list, whereupon it will be removed from the list. It will be blank for a new profile with no associations defined. |
| Associated CICM nodes | Read-only | A non-editable list of CICM nodes that are associated with this Enterprise Profile.<br>It will be blank for a new profile with no associations defined. |
| (Sheet 2 of 2) | | |

***Note:*** The **Associated Networks** and **Associated CICMs** fields are non-editable. The Network Profiles and CICM nodes are not associated on this **Enterprise Profile Creation** Web page. You must create the Enterprise Profile name first.

The page *profile creation results* opens and displays the result of the creation.

**4** Do the procedure Associating and applying an Enterprise Profile to associate Enterprise Profiles with Network Profiles and CICM nodes.

**5** This procedure is complete.

**Associate and apply an Enterprise Profile**
Use this procedure to associate an Enterprise Profile to Network Profiles and to CICM nodes, and to apply an Enterprise Profile to a CICM.

Also use this procedure to change the associations of an Enterprise Profile, and to apply the Enterprise Profile changes to a CICM node.

The complete process for creation and configuration of Enterprise Profiles is summarized as follows:

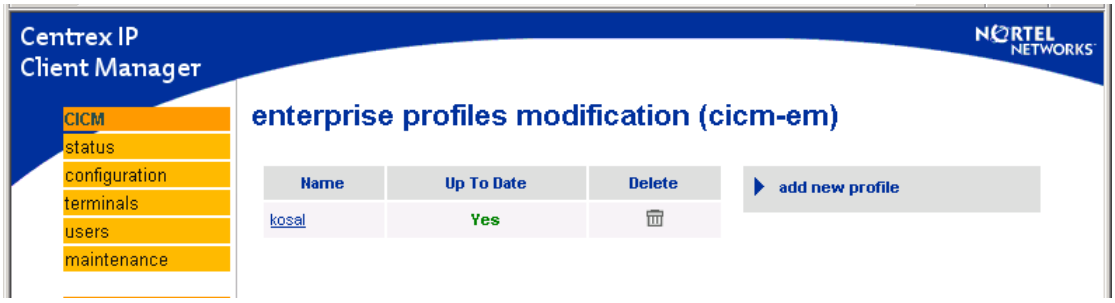
- **Create an Enterprise Profile**. See the procedure Creating an Enterprise Profile.
- **Associate Network Profiles to the Enterprise Profile**. See the procedure Associating and applying an Enterprise Profile.
- **Associate CICM nodes to the Enterprise Profile**. See the procedure Associating and applying an Enterprise Profile.
- **Apply the Enterprise Profile to the CICM node**. This step downloads and saves the Enterprise Profile to the CICM node. See the procedure Associating and applying an Enterprise Profile.

**Procedure 9 Associating and applying an Enterprise Profile**

***At the CICM - Element Manager home page***

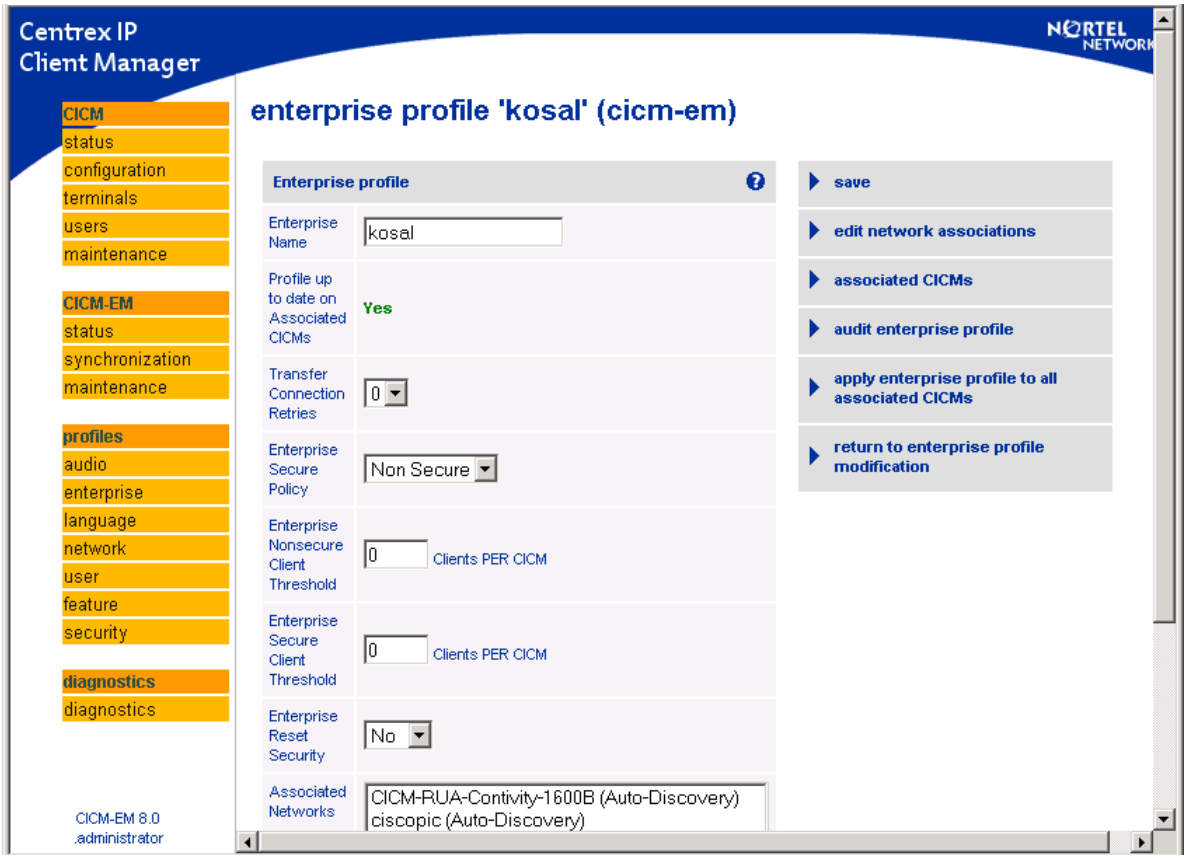
1 Select **enterprise profiles** from the left menu.

The page *enterprise profiles modification* opens.




2 Select the Enterprise Profile to associate from the list of profiles by clicking on the profile name.

The page *enterprise profile edit* opens and displays the Network Profiles and CICMs that are currently associated to this Enterprise Profile. The field *Profile up to date on the Associated CICMs* indicates whether or not the Enterprise Profile has been downloaded to its associated CICM nodes.



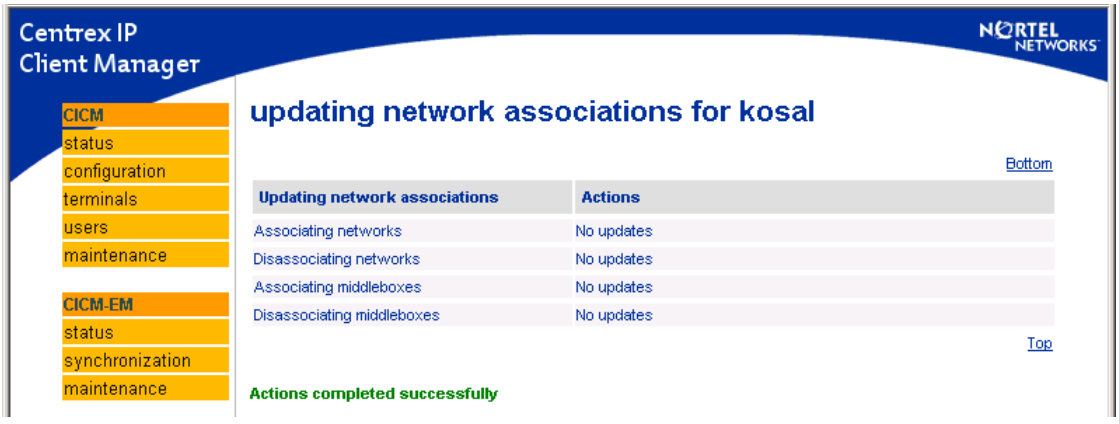

**3** To associate Network Profiles to the selected Enterprise Profile:

**a** Click on **edit network associations** on the right menu.

The page enterprise <name> - edit network associations opens and displays the current associations under the Associated column.


**b** Click the check box under Associated to choose network profiles that you want selected, then click on **update associated network locations** on the right menu.

The system updates the network associations.




***Note:*** Any modified profiles must be re-applied to the CICM node (step 8 of this procedure) to be effective.

**4** Click on the link to return to the enterprise profile <name> page.

**5** To disassociate Network Profiles from the Enterprise Profile, from the **enterprise profile edit** page:

**a** Click on **edit network associations** on the right menu.

The page *enterprise <name>* - edit network associations opens and displays the current associations under the Associated column.

**b** Uncheck the box under Associated to choose network profiles that you want deselected, then click on **update associated network locations** on the right menu.

The system updates the network associations.

**6** To associate CICM nodes to the Enterprise Profile: from the **enterprise profile edit** page:

**a** Click on **associated CICMs** on the right menu.

The page *cicms associated with enterprise profile <name>* opens to display the current CICM node associations.

**b** Click on **associate one or more cicms** on the right menu.

The page *cicm association with enterprise profile <name>* opens to display a list of available CICM nodes to associate.

**c** Select the CICM nodes to associate, then click on the **associate selected CICMs** text bar on the right menu.

The page *associating cicm(s)* opens to display the results of the action.

**7** To dissociate CICM nodes to the Enterprise Profile, from the page *enterprise profile edit*:

**a** Click on **associated CICMs** on the right menu.

The page cicms associated with enterprise profile <name> opens to display the current CICM node associations.

**b** Select the CICM nodes to disassociate by clicking in the **Disassociate** field check box, then click on **disassociate selected CICMs** on the right menu.

The display *disassociating cicms* shows the results of the action.

**8**

> **ATTENTION**
> This step is required to apply all profile association or disassociation changes to the CICM nodes.

Upon completion of the Network Profile and CICM node associations and disassociations, on the **enterprise profile edit** page, click on **apply enterprise profile to all associated CICMs** on the right menu.

The page *enterprise profile application results* opens to display the results of the action, and confirms the successful completion.

**9** This procedure is complete.

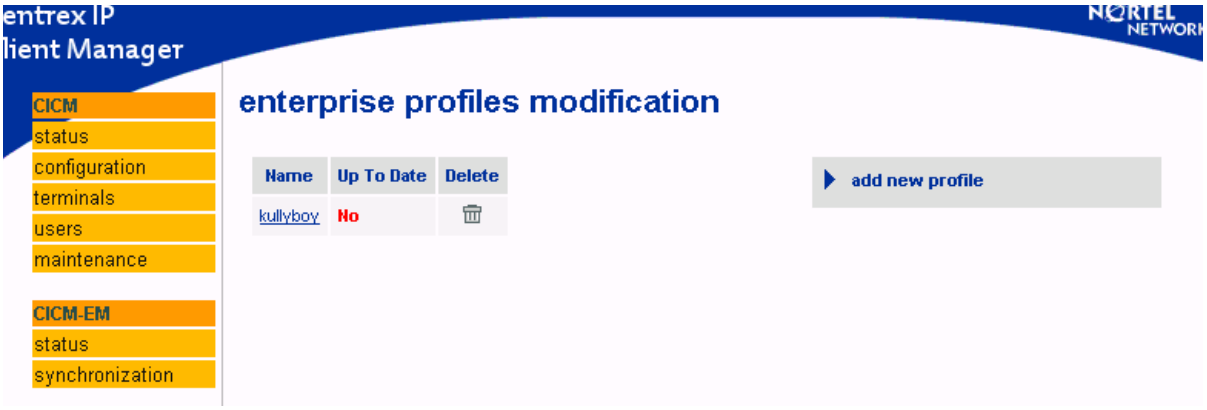
## Procedure 10 Deleting an Enterprise Profile

| | |
|---|---|
| | **CAUTION**<br>**Risk of service loss**<br>All CICM nodes and Network Profiles must be disassociated from the Enterprise Profile before it can be deleted. Use the *Edit an Enterprise Profile* procedure above first to disassociate all CICM nodes and Network Profiles from the Enterprise Profile to be deleted. |

***At the CICM - Element Manager home page***

**1** Select **enterprise profiles** from the left menu.

The page *enterprise profiles modification* opens to display the current list of Enterprise Profiles.




**2**

| |
|---|
| **ATTENTION**<br>The state of the Enterprise Profile (indicated in the Up To Date field on the enterprise profiles modification page) must be set to Yes before the Enterprise Profile can be deleted.<br><br>Refer to the table Enterprise Profile fields for a definition of the filed *Profile Up To Date on Associated CICMs*. Apply the Enterprise Profiles to the associated CICMs to change this Up to Date field to Yes, then proceed to delete the Enterprise Profile. |

In the field **Delete**, click on the delete (trash can) icon corresponding to the Enterprise Profile to be deleted.

The results of the action are displayed, and the deletion is confirmed.

3 This procedure is complete.

## Audit an Enterprise Profile

Use the following procedure to audit an Enterprise Profile on its associated Network Profiles and CICM nodes. The resulting audit report facilitates correct profile associations.

### Procedure 11 Auditing an Enterprise Profile

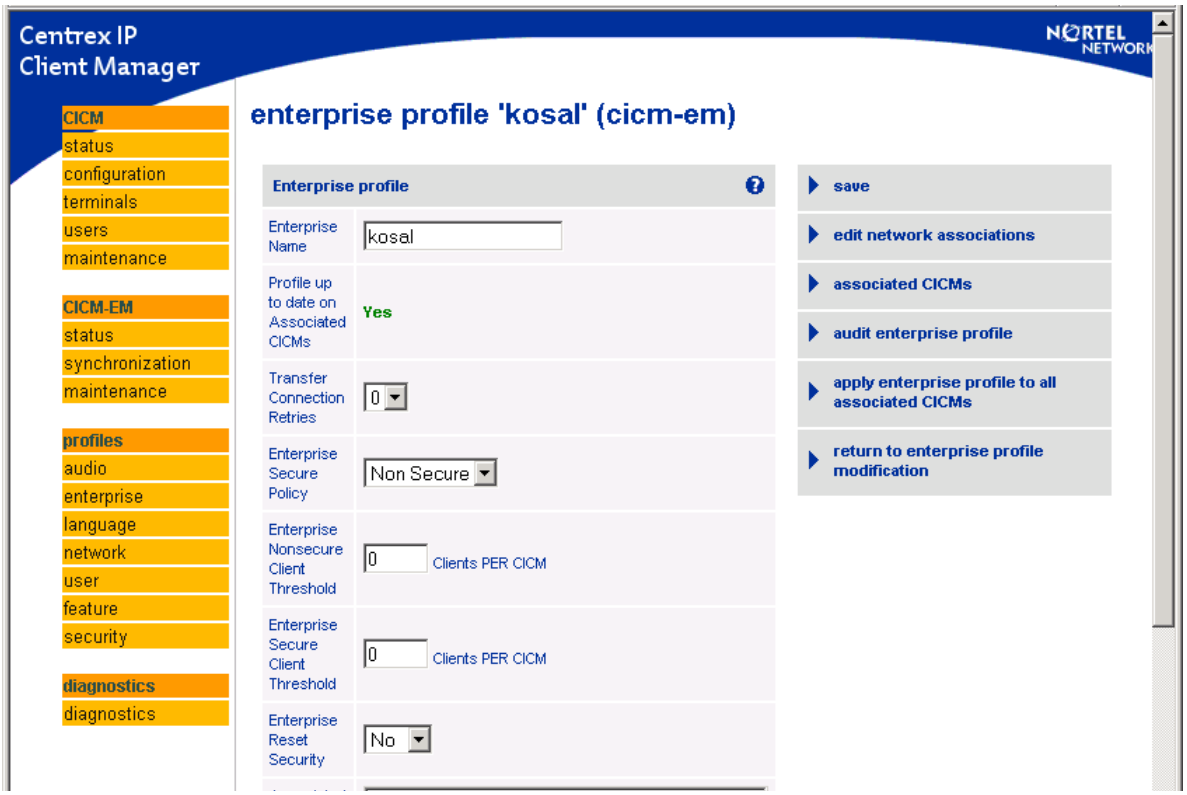
***At the CICM - Element Manager home page***

1 Select **enterprise** from the **profiles** section of the left menu.

The page *enterprise profiles modification* opens to display the current list of Enterprise Profiles.

2 Click on the Enterprise Profile to audit from the list of current profiles.

The page *enterprise profile edit* opens.




3 Click on **audit enterprise profile** on the right menu.

Datafill related to the Enterprise Profile and its associated CICM nodes is checked, and the **Audit of Enterprise Profile < name> upon associated CICMs** report is displayed.

4 This procedure is complete.

## Language Profiles

A Language Profile is a language file which support language selection for the IP Phones. Multiple languages are supported for the IP Phones and CICM SoftClients. A Language Profile must be enabled or disabled for the specific CICM for the IP Phones to access a particular language.

***Note:*** Although multiple languages are available on the m6350 SoftClient, the Language Profile does not apply to it. For information on language selection on the CICM SoftClient, refer to the *m6350 SoftClient Installation Guide*, NN10182-113.

Language profiles available are English, German, Spanish, Italian and French. Language profiles may be viewed from the Element Manager Web pages, but they cannot be created or changed. New languages will be added through new software releases or language patches.

### Procedure 12 Viewing Language Profiles

***At the Element Manager home page***

**1** Select **language** from the **profiles** section of the left menu.

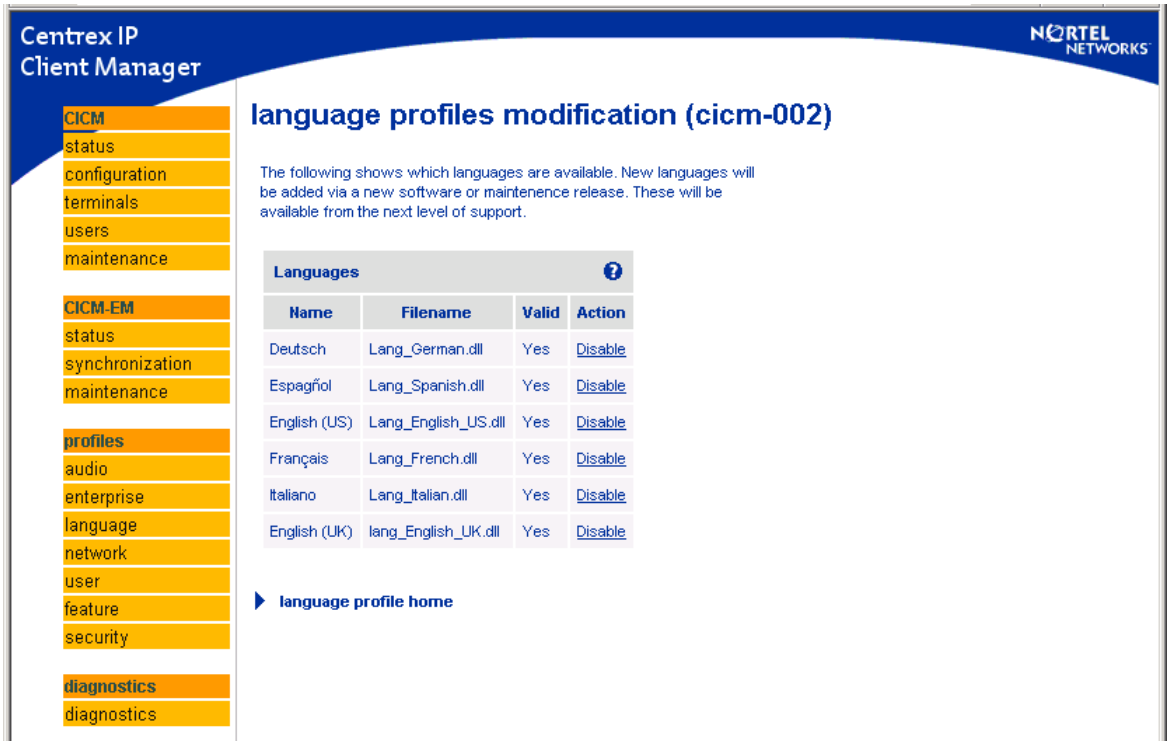
The page *language profile home* opens.


***Note:*** Standard language profiles of English, French, German, Italian, and Spanish are currently provided.

**2** Select the CICM node identifier from the drop-down menu on the **view the profiles stored on the following CICM** on the right

menu, then click on **view the profiles stored on the following CICM**.

The page *language profiles modification (cicm_name)* opens.




**3** If desired, enable or disable the language on the selected CICM node under the **Action** column.

After disabling, you will be notified if the language is in use by global settings, user profiles, or user overrides and given the choice to replace the references to the language being disabled with a language which is currently enabled.

**4** After enabling or disabling a language, reboot both CICM nodes.

**5** This procedure is complete.

## Network Profiles

Network Profiles define the IP address domains that are supported by the CICM node. Only terminals from within a valid IP address domain can be connected to the CICM node. An IP address domain is identified by the network device that connects it to the public IP address space that contains the CICM node. Typically, this is a Network Address Translation (NAT) device. Refer to the section “NAT and firewalls” in *CICM Security and Administration*, NN10252-611.

Centrex by definition is a carrier-hosted featured voice service offer to enterprises. Centrex IP maintains feature transparency to CS2K Centrex. One key difference between Centrex and Centrex IP is that with Centrex IP, enterprises are served over a converged IP network instead of a CS2K network. Each enterprise has its own enterprise IP network. It normally uses private IP addresses for communication within the enterprise, and public IP addresses for communication outside the enterprise through a Network Address Translator (NAT) associated with its gateway router.

Each enterprise IP network is uniquely represented by a network profile on the CICM node that serves this enterprise. A Network Profile identifies the IP address domain of the enterprise, represented by the public IP address of the enterprise NAT, along with an associated network location for this enterprise.

Network Profiles provide an effective means for authentication and control of Centrex IP traffic. Centrex IP traffic is only allowed to flow between the CICM node and the IP address domains that are specified by the Network Profiles on the node.

Network Profiles can only be created, changed and deleted by an administrator. They are stored on the CICM-EM and applied to a CICM node.

Network Profile configuration changes are immediately effective for new terminal connections. You do not need to restart the CICM node to implement the changes; they are immediate. However, you must restart terminals if they are assigned a new network domain.

### Enterprise IP address domain representation

For terminals behind a NAT, this NAT presence must be defined in the network profile. The network profile specifies the public IP address and the subnet of the NAT.

For an enterprise that uses public IP addresses (that is, no NAT is needed), the administrator can still create a Network Profile for it, either by using the network domain “0.0.0.0, 0.0.0.0” or by specifying the

subnet from which those customers originate (for example, 47.165.169.0, 255.255.255.0). It is recommended to lock down the allowed range of valid terminal IP addresses in this way as a means of preventing denial of service attacks from unknown subnets.

**Example of Network domain addressing**

Assume that two enterprise nodes are configured through the CICM-EM's Network Profile web page as follows:

- Enterprise 1 with 47.165.168.100 and 255.255.255.255
- Enterprise 2 with 47.165.168.200 and 255.255.255.255

The mask 255.255.255.255 informs the CICM node to consider only clients originating from the single IP address 47.165.168.100 to be in Enterprise 1.

NATs often only have a single IP address into which they multiplex the active connections by mapping them to unique ports. A NAT with four interfaces, for example, would be datafilled with the two least significant missing bits. Thus for 47.165.168.100, the mask 255.255.255.255 would permit addresses 47.165.168.100, 101,102, and 103 to be considered part of the network domain.

If Network Domain Licensing is enabled, a terminal could only log in if its IP address fell within one of the Network Profiles datafilled on the CICM node to which it was connected.

The procedures for handling a Network Profile include:

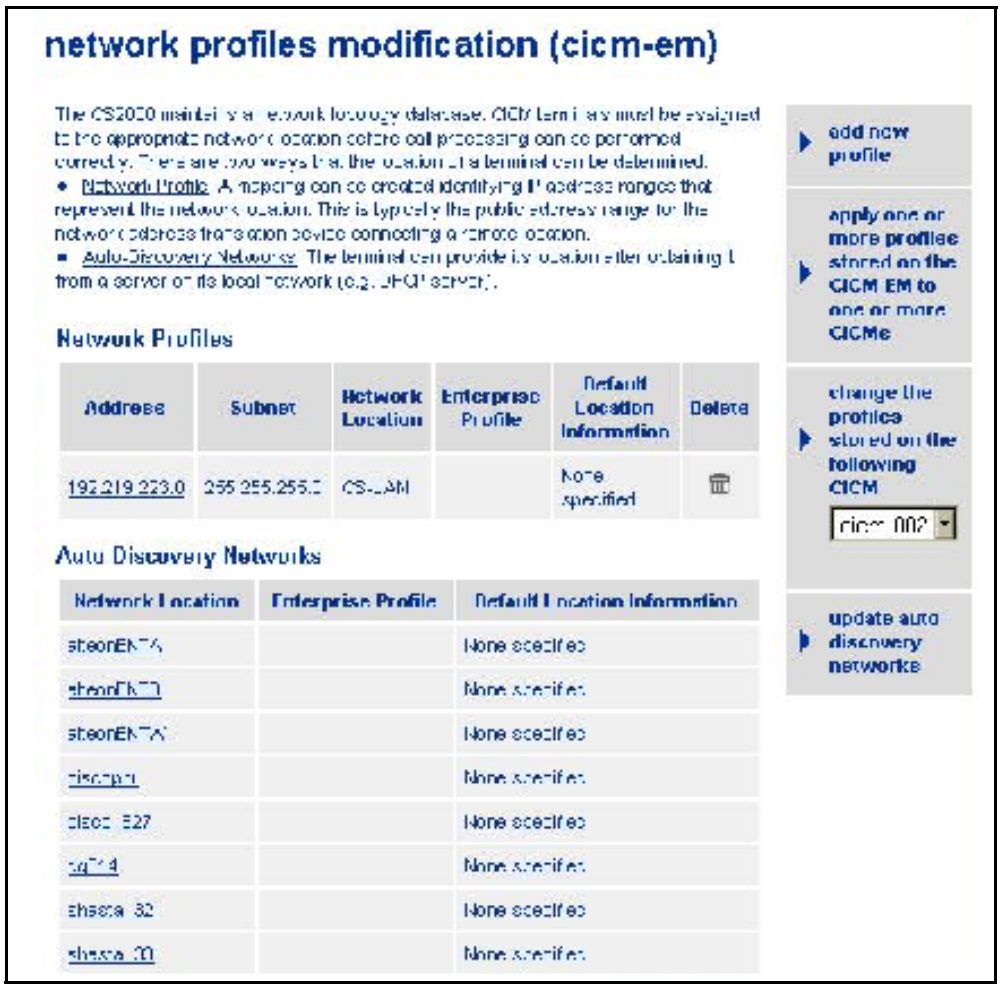
- Updating auto-discovery networks, to be used whenever the NAT list is changed for the CS2K Management Tools (CMT)
- Creating a Network Profile
- Changing a Network Profile
- Deleting a Network Profile
- Applying a Network Profile stored on the CICM-EM to a CICM node
- Enabling or disabling network domain address licensing

## Procedure 13 Updating auto-discovery networks

### *At the CICM - element manager home page*

1 Click on **network** in the *Profiles* menu.

The page *network profiles modification (cicm-em)* opens.




2 Click on **update auto-discovery networks** on the right menu.

The page *update global middlebox ids* opens.

3 Enter the details for the CS2K Management Tools (CMT). CMT was formerly known as the SESM.

4 Click on **Update middlebox ids**.

5 Confirm the update.

6 Return to Network Profiles to complete handling the profiles.

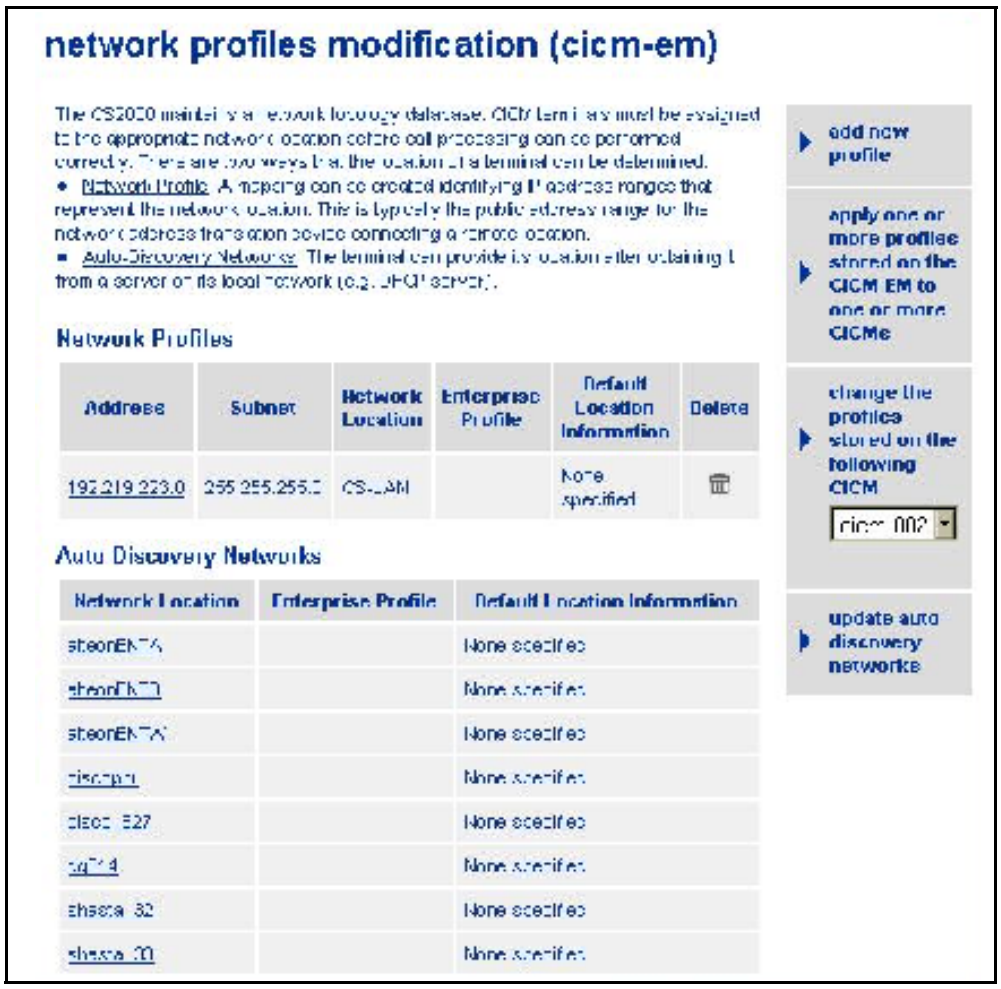
7 This procedure is complete.

## Procedure 14 Creating a Network Profile

### *At the CICM - element manager home page*

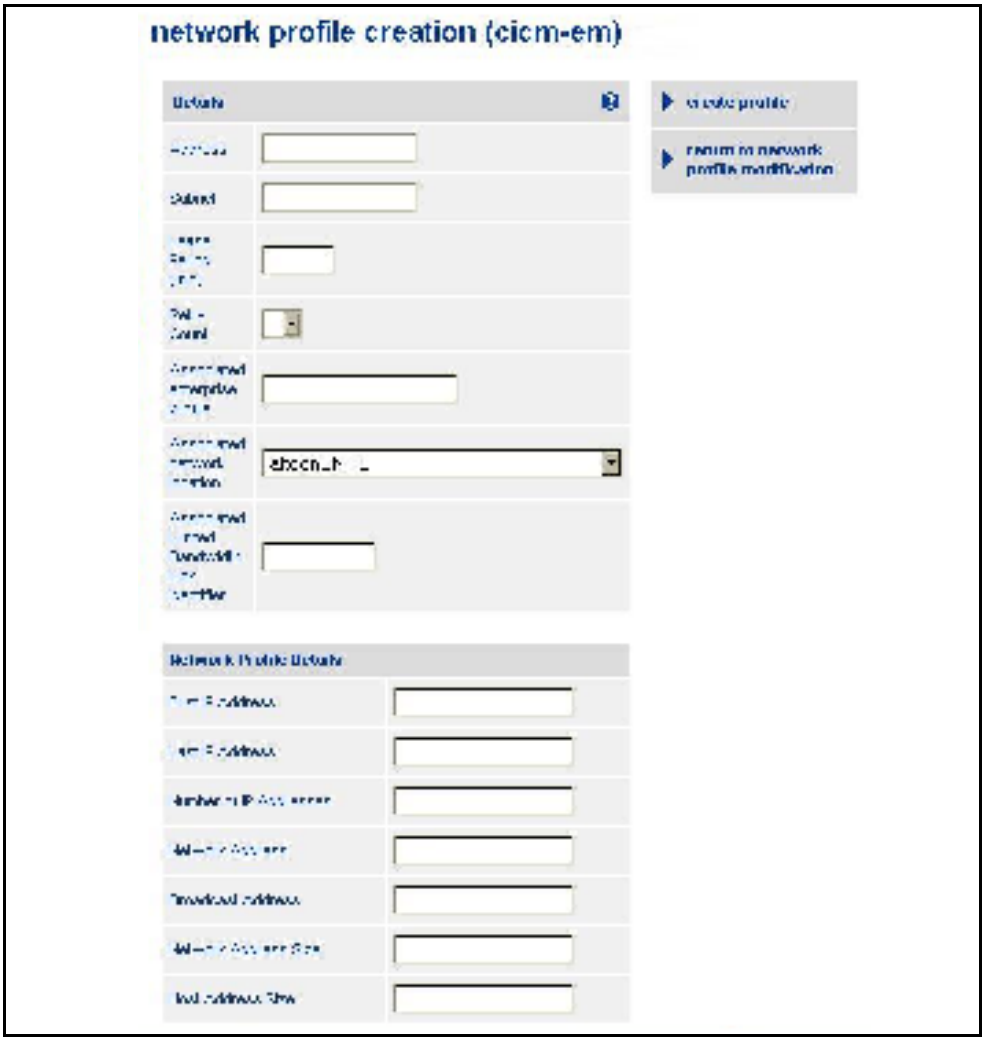
**1** Click on **network** under **Profiles** of the left menu.

The page *network profiles modification (cicm-em)* opens.




**2** Click on **add new profile** on the right menu.

The page *network profile creation (cicm-em)* opens.




3 Datafill the network profile fields.

***Note:*** Click on the **?** icon for detailed definitions of these fields.

**a** In the **Address** field, specify the network address of the subnet that contains the range of public addresses available to a NAT device.

**b** In the **Subnet** field, specify the subnet mask for the subnet that contains the range of public addresses available to a NAT device.

**c** In the **Lease period (min)** field, enter the period for which any UDP port mapping is maintained.

***Note:*** For SN08 CICM-EMs and gateways, the lease period is variable and the field can be datafilled.

**d** In the **Retry count** field, specify the number of times a terminal will attempt to connect to a CICM node before it fails over and attempts to connect to the other node. A terminal connecting to a CICM node with an IP address described by this Network Profile will have this retry connection count. This Network Profile needs to have been applied to the CICM or be associated with an Enterprise Profile which has been applied to the CICM for this to take effect. Leaving the field blank will result in the retry count taken from the Terminals Settings for that CICM.

**e** In the **Associated Enterprise Profiles** field, you do not need to enter anything as it is a read-only field. If this field is not blank, the Network Profile is associated with an Enterprise Profile and cannot be edited. The field must be dissociated from the Enterprise Profile before being edited.

**f** Set the field **Associated network location** to CS-LAN (no NAT), Manually defined (when the Associated Limited Bandwidth Link Identifier is also to be set) or to one of the Auto-Discovery Networks that have been downloaded to the CICM-EM in the procedure Updating auto-discovery networks.

**g** In the **Associated Limited Bandwidth Link Identifier** field, enter the global middlebox identifier of the Limited Bandwidth Link if you selected “Manually defined Limited Bandwidth Link” in the field Associated Network Location. If you selected CS-LAN or Auto-Discovery Network Location as the Associated Network Location, this field is ignored.

Derive the value of this field from the Succession Element and Sub-Element Manager (SESM).

**4** After completing the field datafill, click on **create profile**.

The page *profile creation results* displays the results of the action.

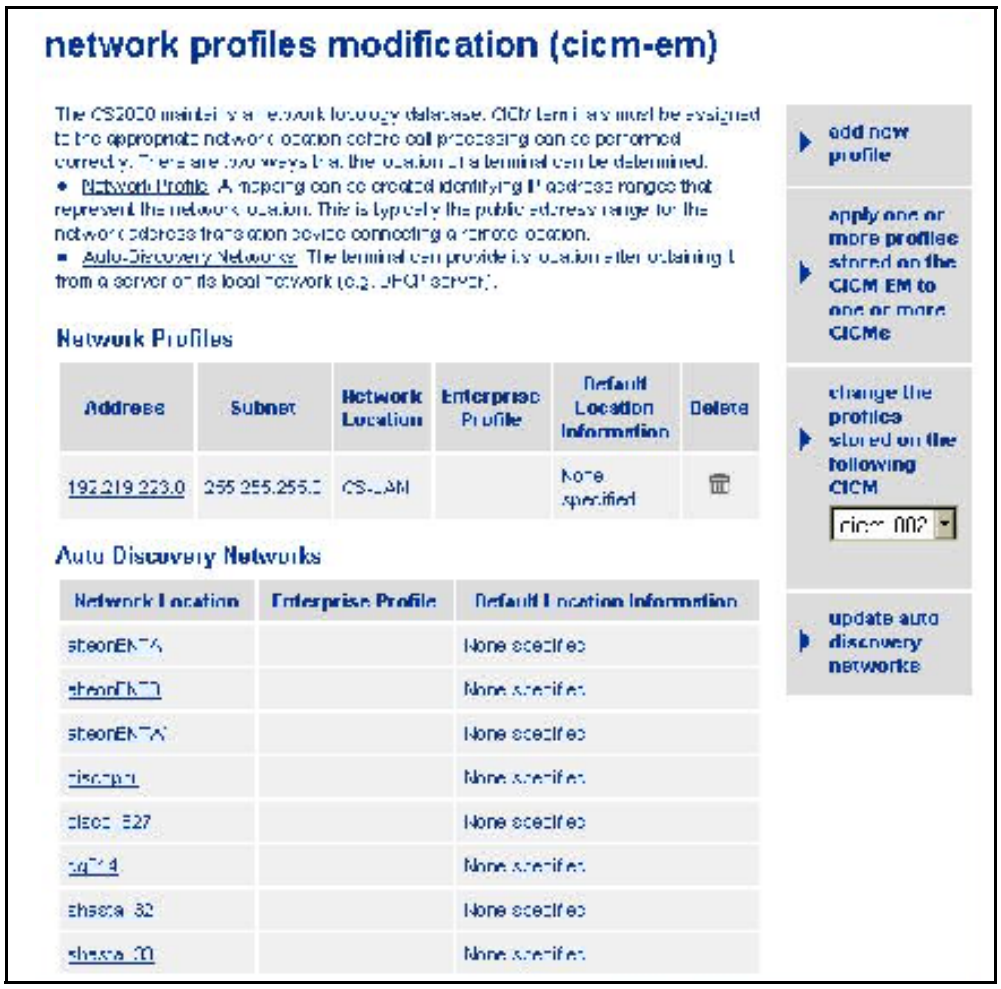
**5** This procedure is complete.

## Procedure 15 Changing a Network Profile

### *At the CICM -EM home page*

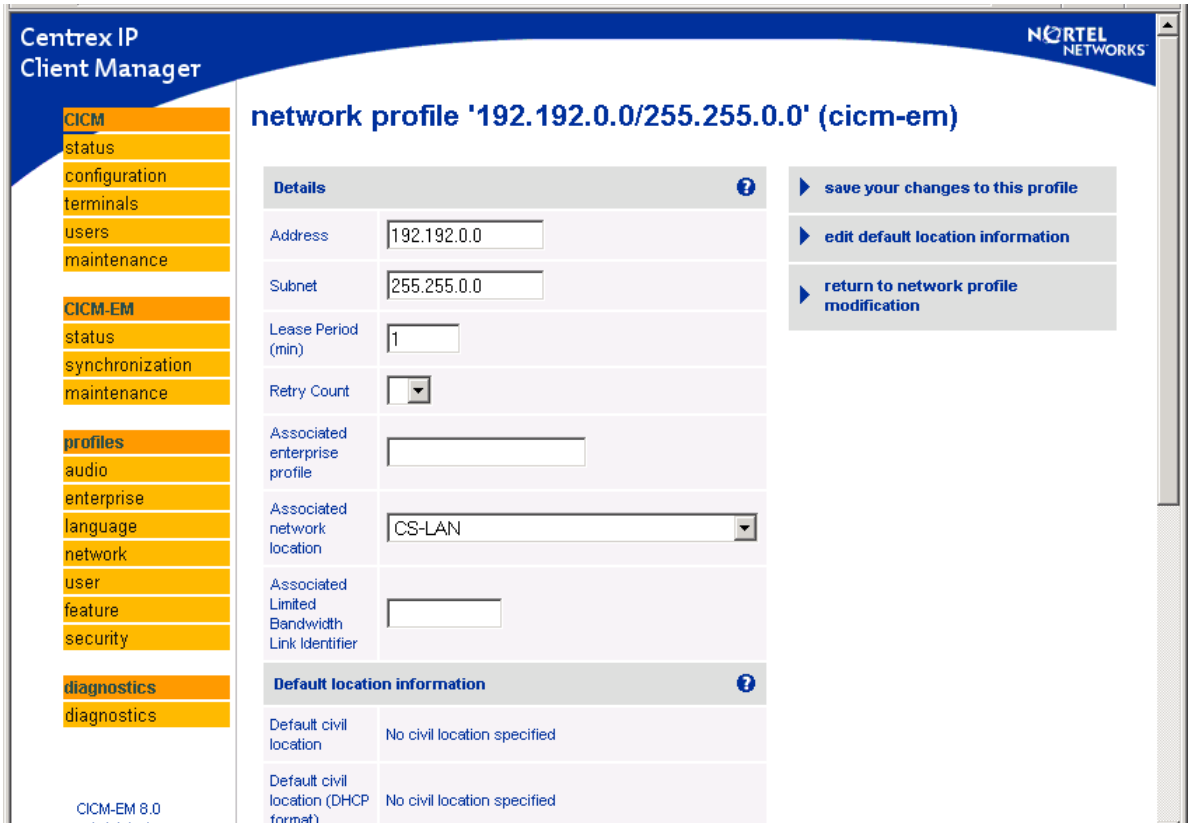
**1** Select **Network** from the **Profiles** section of the left menu.

The page *network profiles modification (cicm-em)* opens.




**2** Click on the IP address of the network profile to edit.

The page *network profile <IP_address/subnet> (cicm-em)* opens.




3 Edit the network profile fields in the **Details** section as required, then click on **save your changes to this profile** on the right menu.

Click on the **?** icon for definitions of these fields.

The page *profile save results* confirms the update completion.

4 To edit default location information:

**a** Click on **edit default location** on the right menu.

The page *edit default location information: <IP_address/subnet* opens.

**b** Datafill the fields in the **Type of Location**, **Civil Location**, and **Spatial Location** sections, then click on **save changes**.

Click on the **?** icon for definitions of these fields.

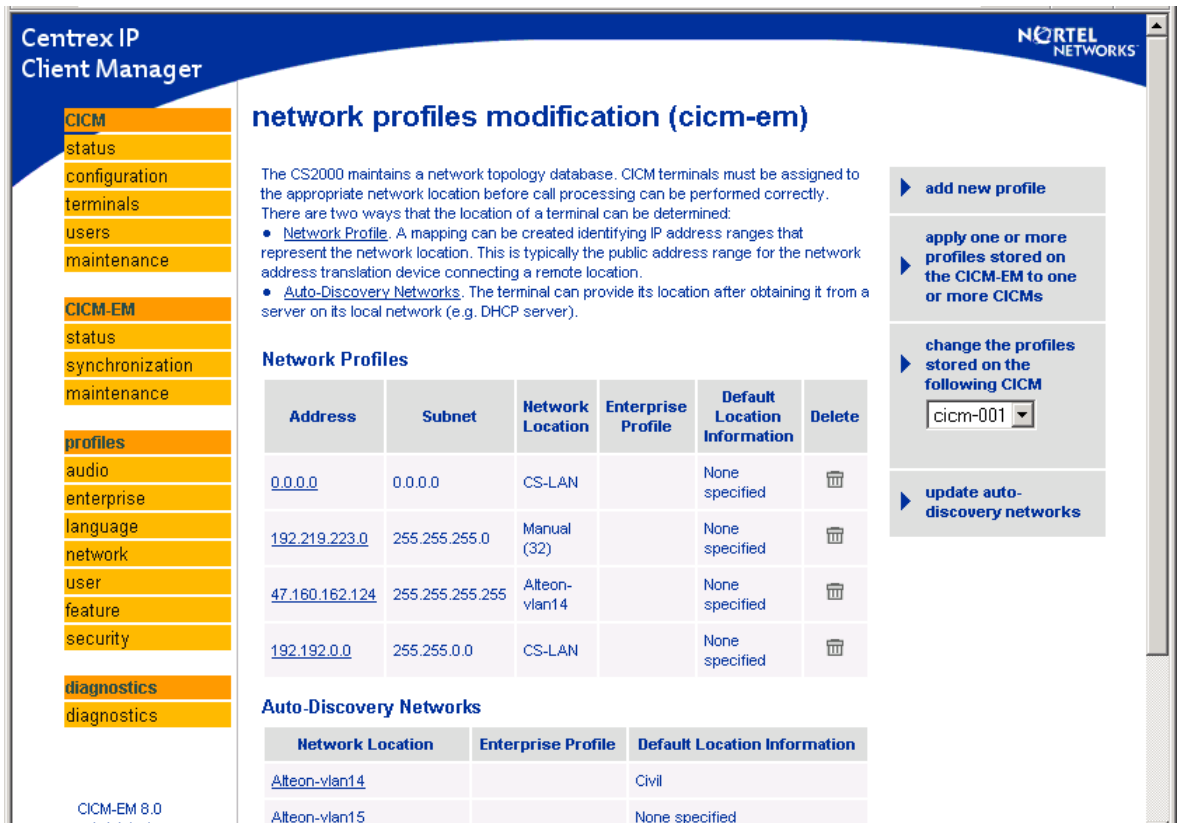
5 This procedure is complete.

## Procedure 16 Deleting a Network Profile

### *At the CICM-EM home page*

1 Select **Network** from the **Profiles** of the left menu.

The page *network profiles modification (cicm-em)* opens.




2 Click on the **Delete** (trash can) icon for the Network Profile to delete.

The deletion action is confirmed.

3 Click on the **delete** (trash can) icon for the network IP address to be deleted.

The status page shows confirmation of the deletion.

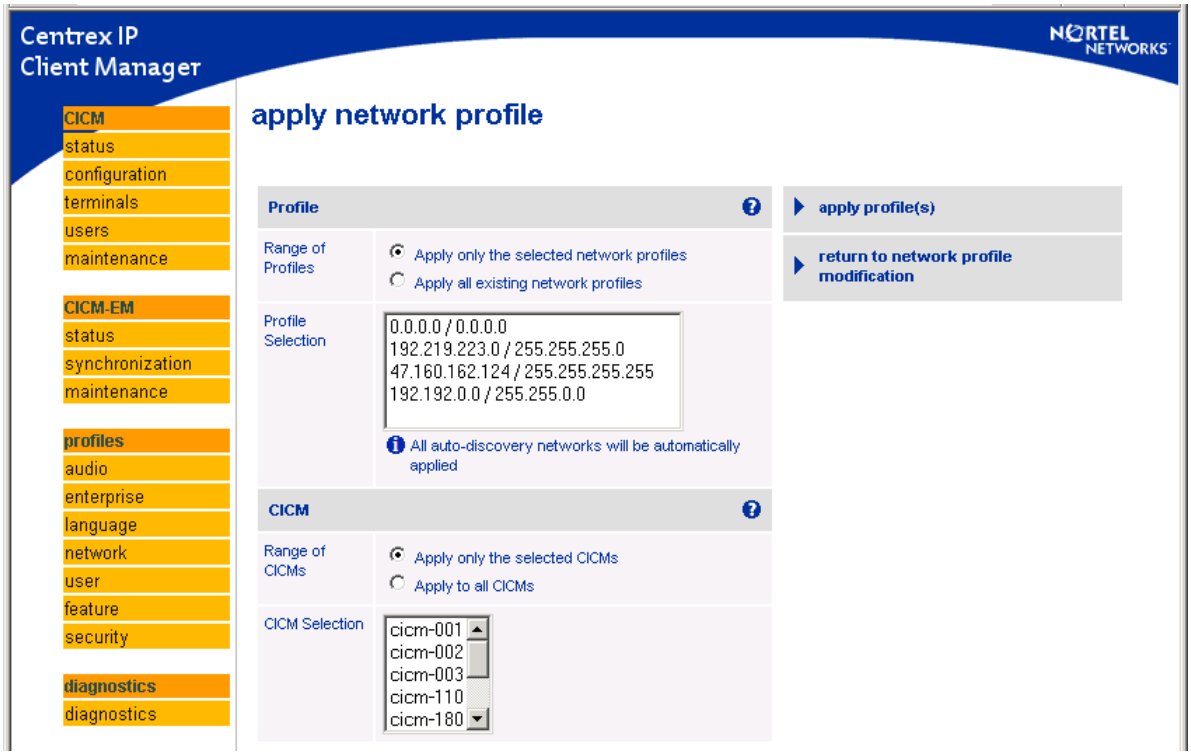
4 This procedure is complete.

## Procedure 17 Applying a Network Profile stored on the CICM-EM to a CICM node

***At the network profiles modification (cicm-em) page of the element manager Web pages***

1 Click on **apply one or more profiles stored on the CICM-EM to one or more CICMs** on the menu on the right.

The page *apply network profile* opens.




2 Datafill the **Profile** and **CICM** fields.

Click on the **?** icon for definitions of these fields.

3 Click **apply profile(s)** on the right menu.

The page *profile apply results* status opens and confirms completion.

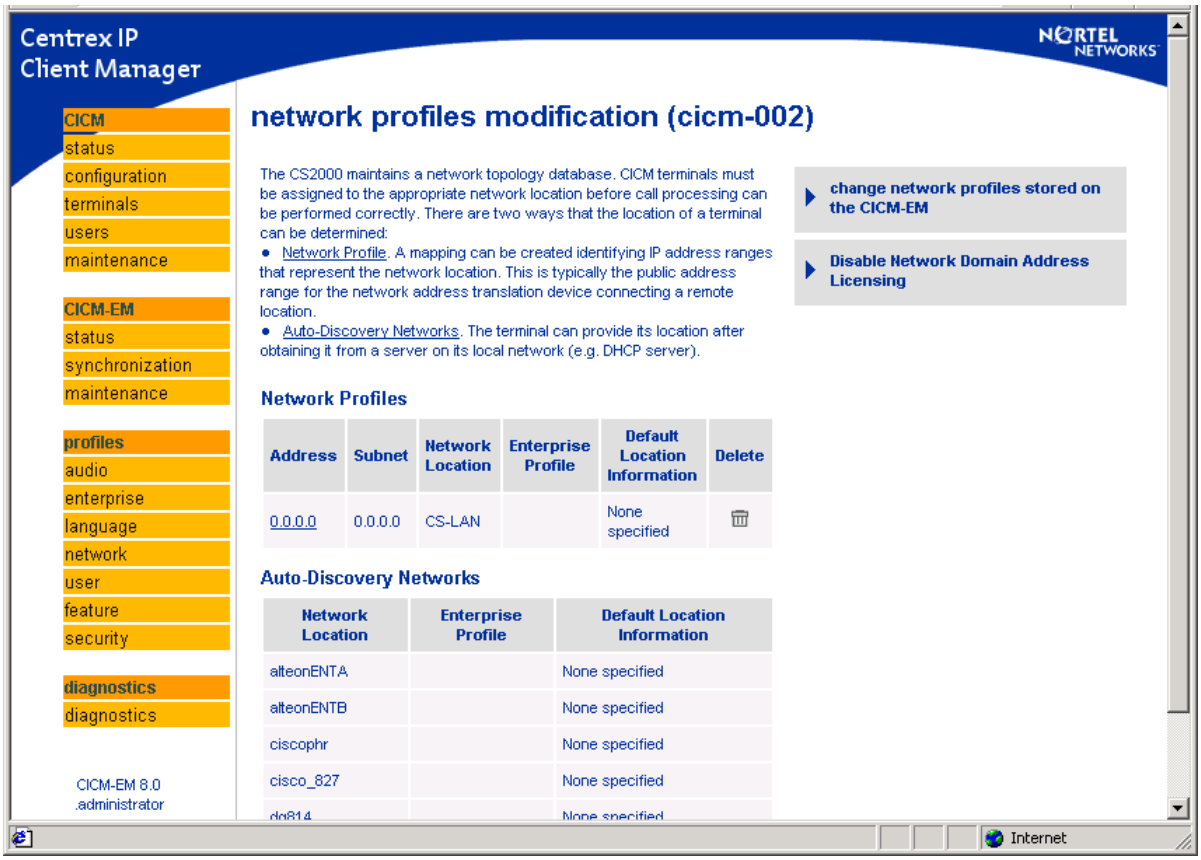
4 This procedure is complete.

## Procedure 18 Enabling or disabling network domain address licensing

### *At the network profiles modification (cicm-em) page of the element manager Web pages*

1 Select the CICM node identifier from the drop-down menu in the **change the profiles stored on the following CICM** menu on the right, then click on **change the profiles stored on the following CICM**.

The page *network profiles modification (<cicm-nnn>)* opens.




2 On the right menu bar, click on the **Enable/Disable Network Domain Address Licensing** text bar to toggle between **enable** and **disable,** as required.

A status page opens and confirms the results of the action.

3 This procedure is complete.

**Media routing in a CS2000 environment with NAT**

The routing of media between the CICM node phones will try to stay within the enterprise network when possible. This results in:

- improved voice quality
- increased CICM node capacity
- reduced bandwidth requirements from the enterprise to the carrier

However, intraswitched calls cannot traverse the boundaries of a Network Address Translator (NAT), for example, a call between a user in enterprise 1 and a user in enterprise 2, because:

- routing will likely be blocked by a security setup (for example, firewall rules)
- RTP packets use non-routable private IP addresses that are either overlapped between two enterprises or viewed as unreachable

It is the associated network location fields that is part of the network profiles that determines if calls can be routed directly between each other or if they have to go through a proxy.

## User Profiles

A User Profile is a set of default settings for a group of users. A User Profile can contain feature key settings, language, timezones, and permissions.

User profiles may be created, changed and deleted. They are stored on the CICM-EM and applied to a selected CICM node.

A user will inherit settings from the user profile configured, unless overridden locally. Overrides to user profiles may be applied or deleted by the administrator.

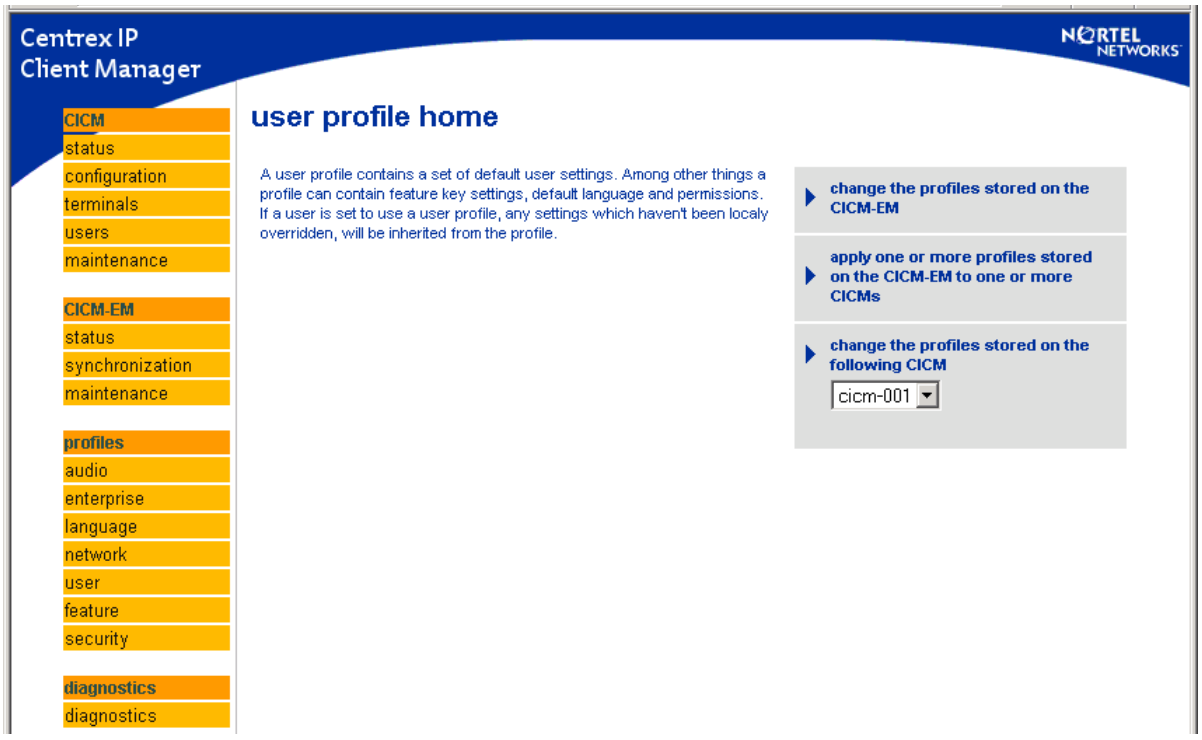
To create users (user ID, password, etc.), refer to *CICM Security and Administration*, NN10252-611.

### Procedure 19 Creating a User Profile

***At the CICM - Element Manager home page***

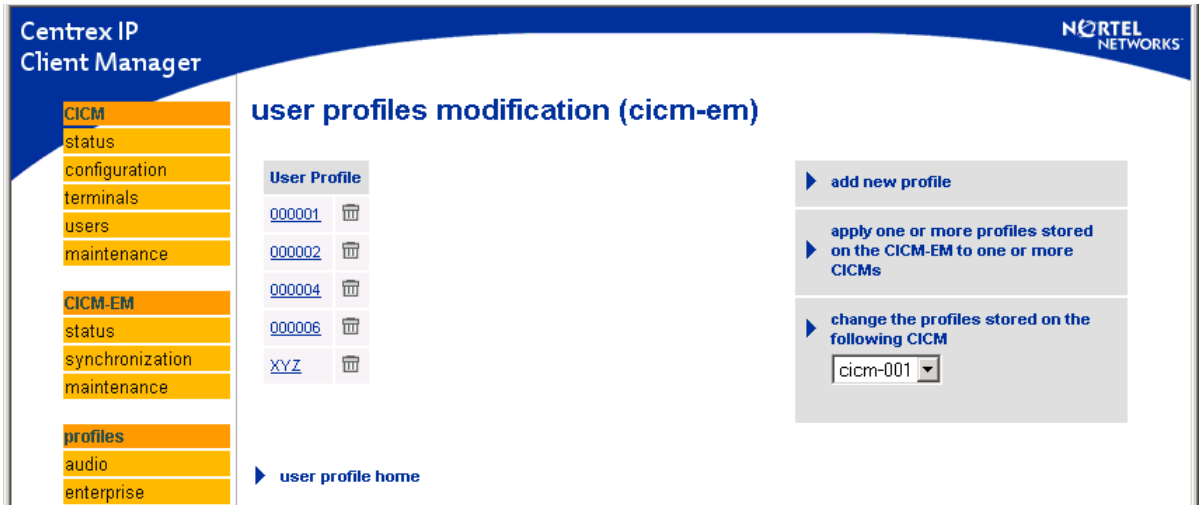
1 Select **user** from the **Profiles** section of the left menu bar.

The page *user profile home* opens.



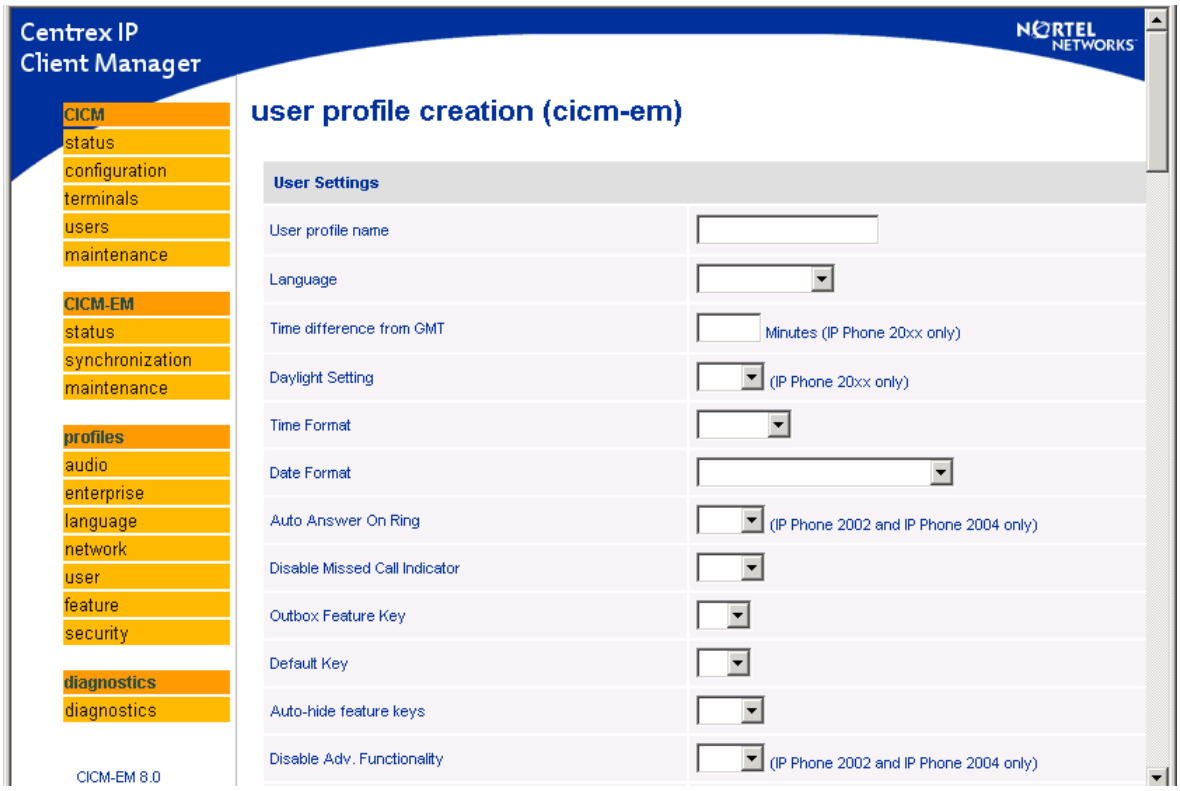

2 Click on **change the profiles stored on the following CICM-EM** on the right menu.

The page *user profiles modification (cicm-em)* opens.




**3** Click on **add new profile** on the right menu.

The page *user profile creation (cicm-em)* opens.




**4** Datafill the fields, then click on **create profile** on the right menu.

For definitions of these fields, click on the **?** icon for each field.

The display *user creation results* shows confirmation of file creation. The user profile is stored on the CICM-EM.

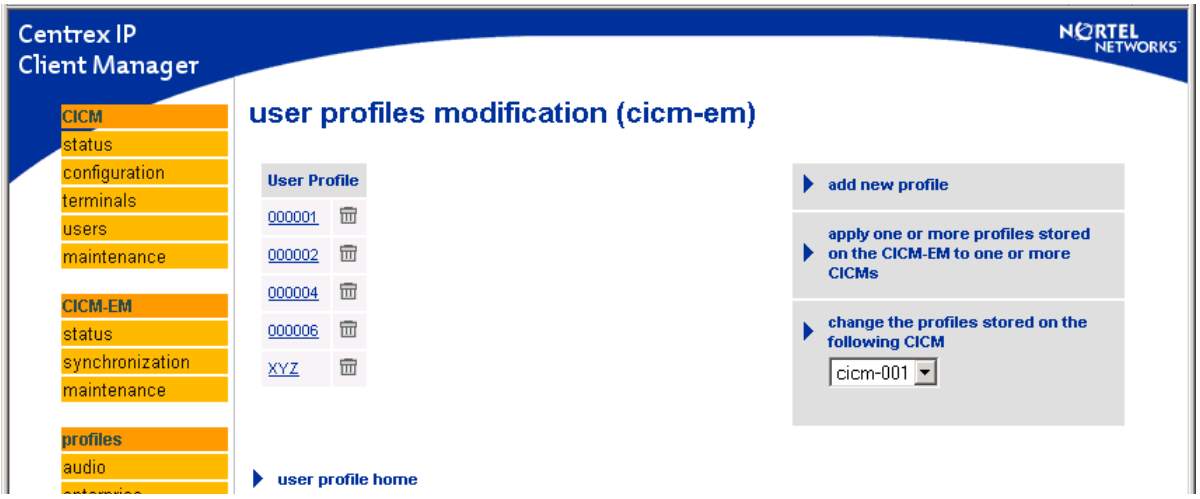
**5** This procedure is complete.

## Procedure 20 Changing a User Profile

***At the user profile home page on the Element Manager Web pages***

1 Select **change the profiles stored on the CICM-EM** menu on the right menu.

The page *user profiles modification (cicm-em)* opens.




2 Click on the user profile name that you want to modify.

The page *user profile edit* opens.

3 Revise the user profile fields as required, then click on **save your changes to this profile** on the right menu.

For definitions of these fields, click on the **?** icon for each field.

The status page opens and confirms completion of the edit.

4 This procedure is complete.

### Procedure 21 Deleting a User Profile

***At the user profile home page on the Element Manager Web page***

1 Click on **change the profiles stored on the CICM-EM** on the right menu.

The page *user profiles modification (cicm-em)* opens.

2 Click on **delete** (trash can) icon for the profile you want to delete.

The page *user profile deletion <cicm-em>* opens.

3 Click on **delete this profile on the element manager and ALL CICMs**.

The page *profile deletion results* opens and prompts for confirmed deletion.

4 Click on **Yes**.

A status page opens and confirms the deletion.

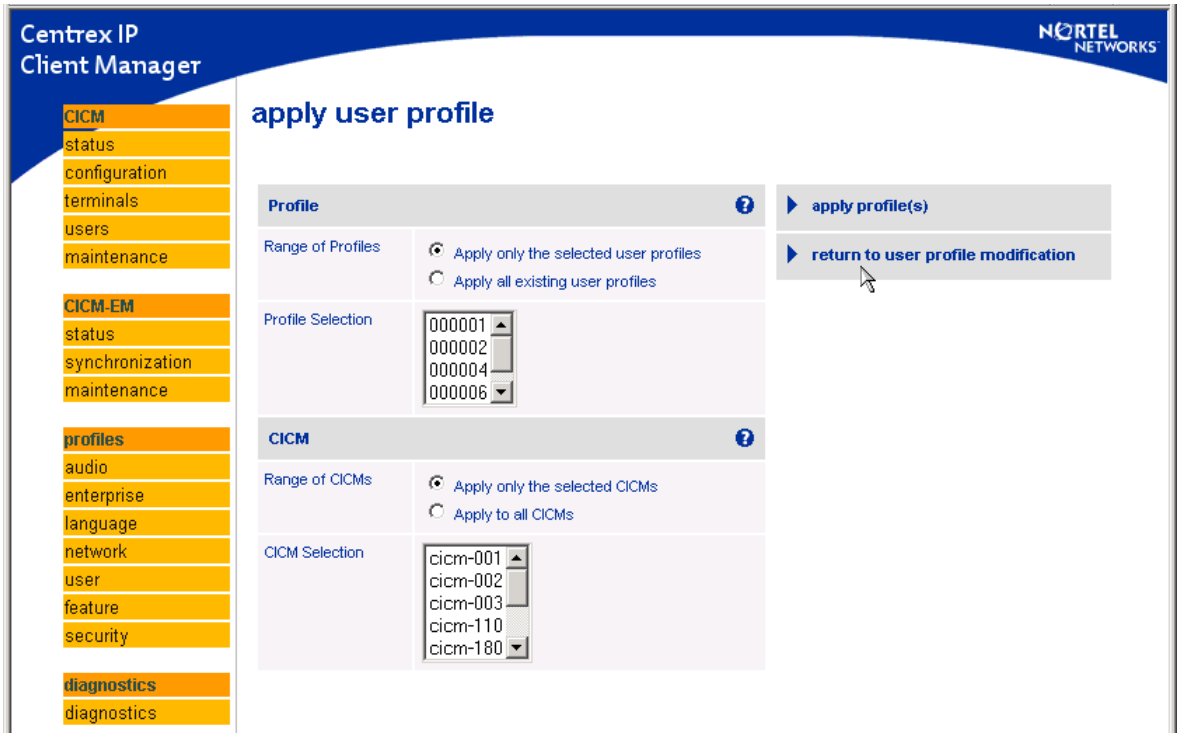
5 This procedure is complete.

## Procedure 22 Applying a User Profile to a CICM node

***At the user profile home page of the element manager Web pages***

1 Click on **apply one or more profiles stored on the CICM-EM to one or more CICMs** on the right menu.

The page *apply user profile* opens.




2 Select the profiles to apply and the CICM nodes to apply them to, by datafilling the fields on the **apply user profile** page.

Click on the **?** icon for definitions of each field.

Use the **CTRL** key to select more than one CICM node.

3 Click on **apply profile(s)** on the right menu.

The page *profile apply results* opens.

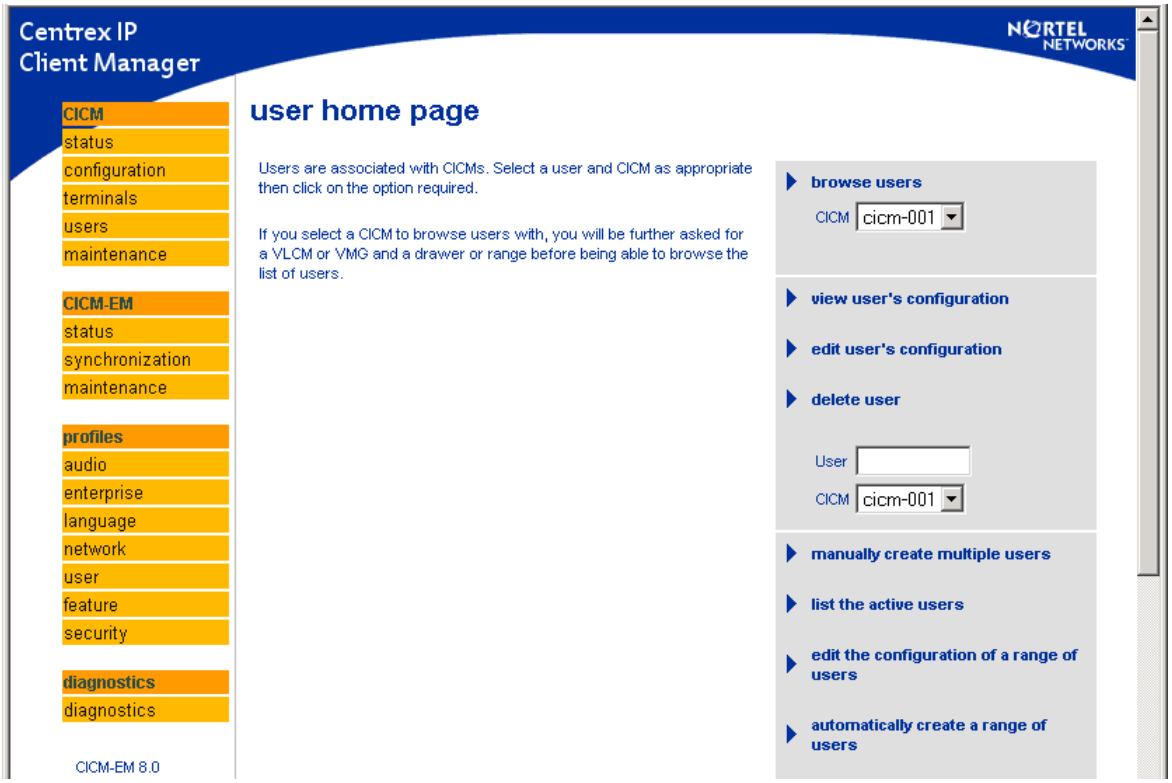
4 This procedure is complete.

## Procedure 23 Applying or removing User Profile overrides

### *At the element manager home page*

**1** Click on **users** from the *CICM* menu on the left.

The page *user home page* opens.

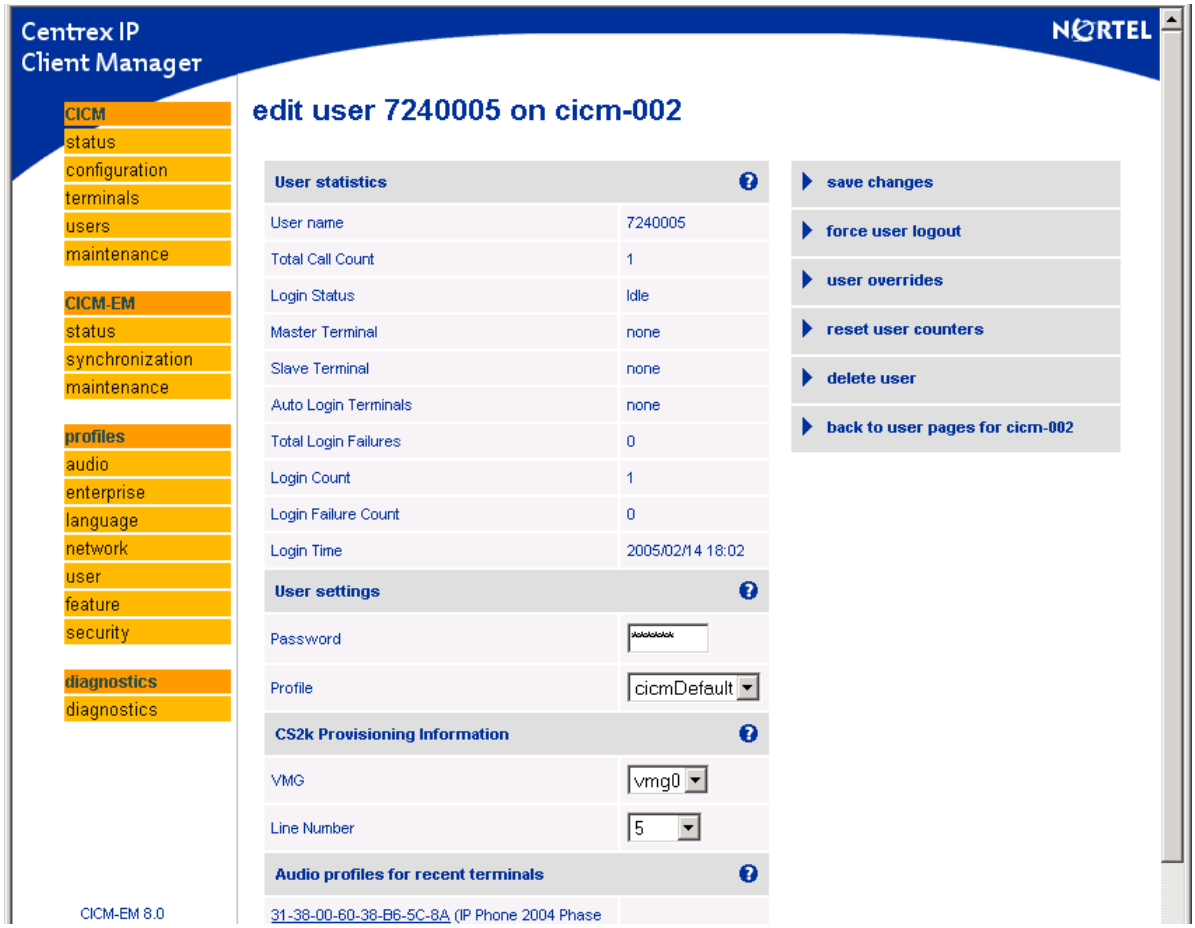



### *At the user home page*

**2** In the User input box on the right-hand menu, enter the user ID that you want to apply or remove overrides to, and select the correct CICM node in the drop-down menu immediately under the User input box.

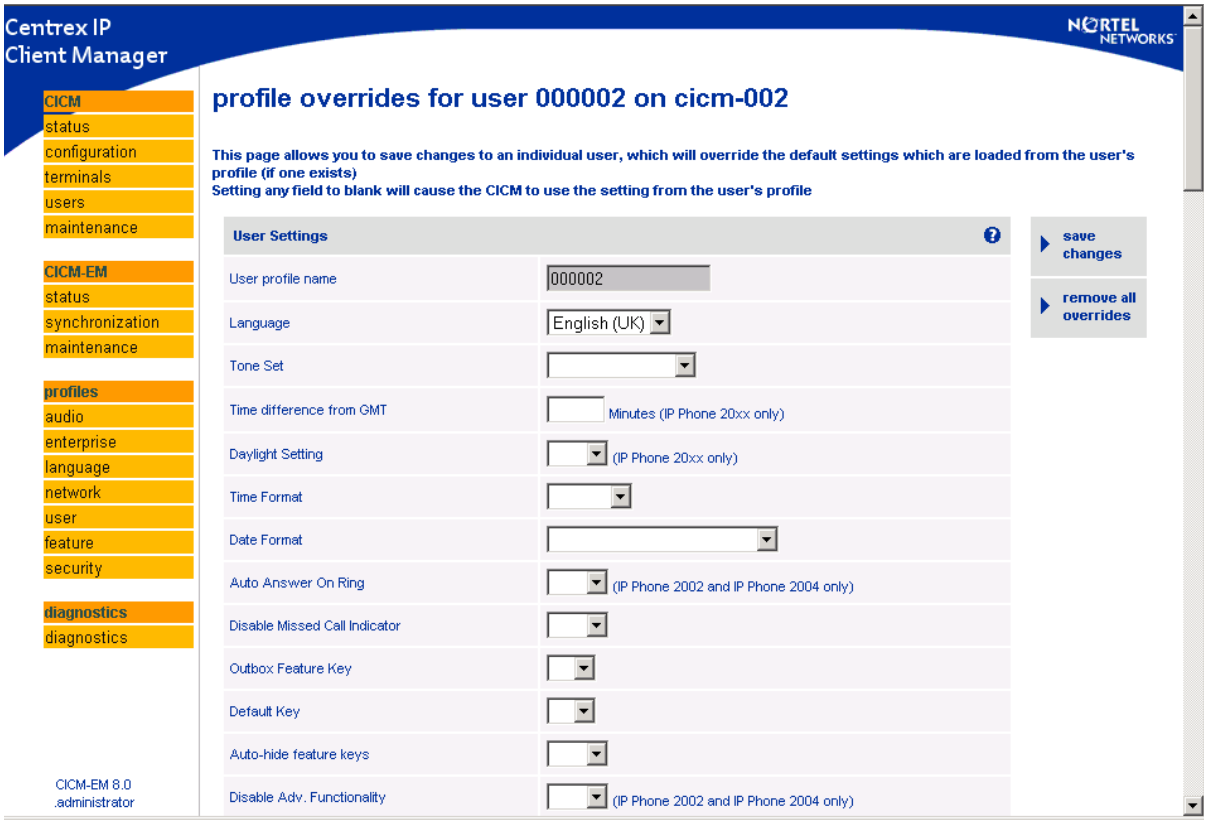
**3** Click on **edit user's**.

The page *edit user <username> on <cicm-nnn>* opens.




4 Click on **user overrides** on the right menu.

The page *profile overrides for user <name> on <cicm-nnn>* opens. The default settings are loaded from the user's profile (if one exists).




**5** Datafill the fields that you want to override for this user, then click on **save changes** on the right menu.

For field definitions, click on the **?** icon for each field.

Fields datafilled will override the default settings on the user's profile.

Fields left blank will default to the user profile.

To remove an override in a particular field, set the field to blank.

The status page opens to confirm the action taken.

**6** To remove all overrides, click on **remove all overrides** on the right menu.

The status page opens to confirm the action taken.

**7** This procedure is complete.

## Feature Profiles

The Feature Profile governs how features behave on the terminals supported by a CICM node. The attributes of each feature can cause the feature to be hidden or shown, based on the state of other features on the terminal. This allows maximum use to be made of the limited number of feature keys available on some terminals.

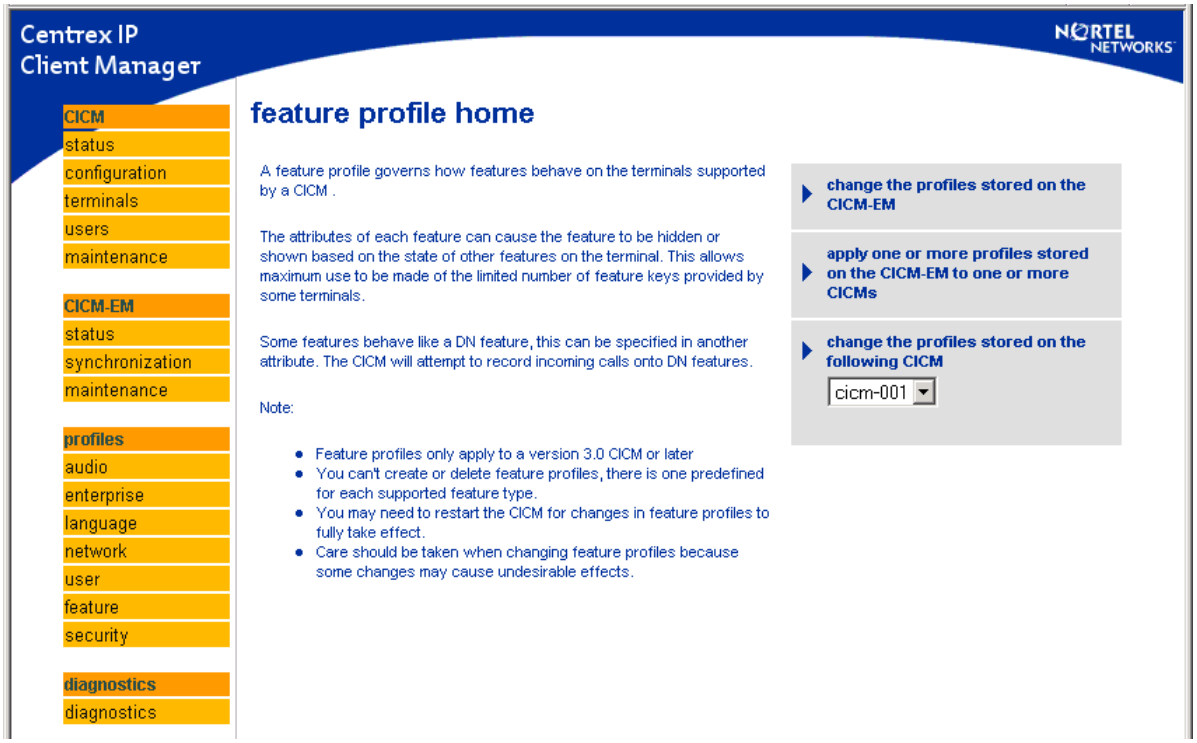
Use the following procedure to configure Feature Profiles.

### Procedure 24 Configuring the Feature Profile

***At the CICM - Element Manager home page***

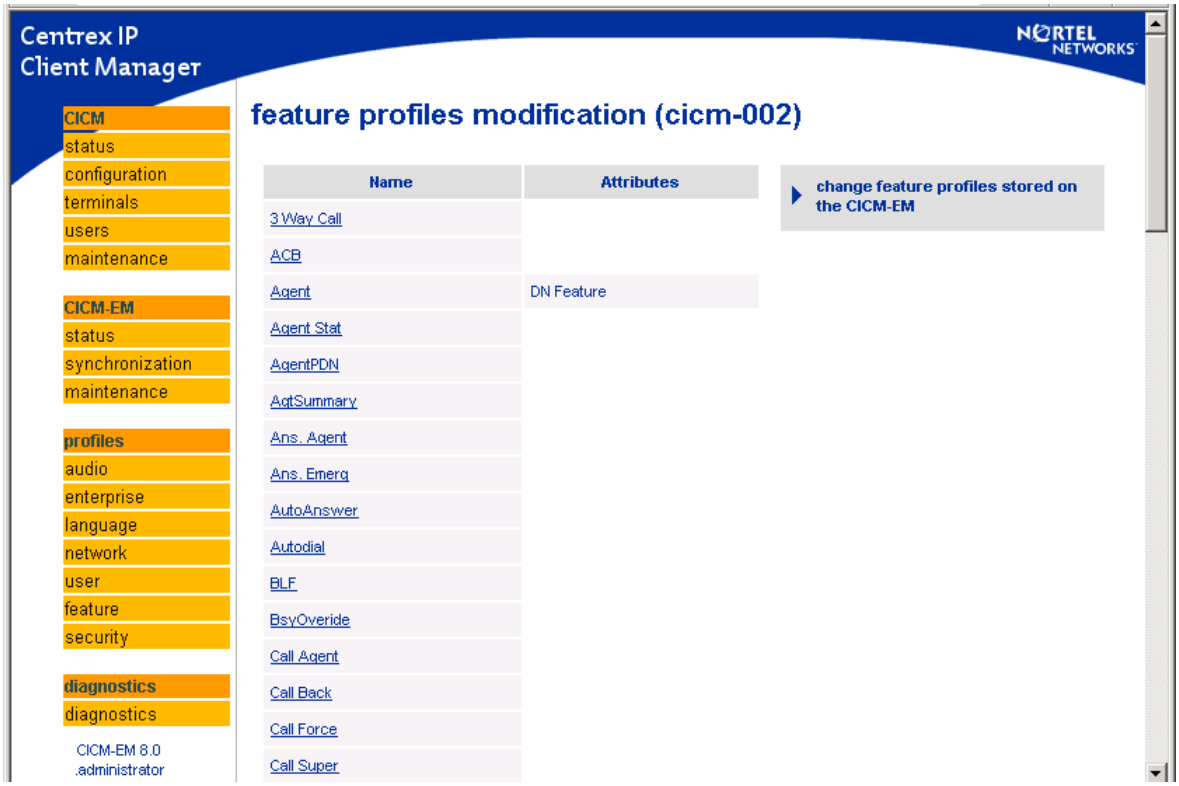
**1** Select **feature** from the **profiles** section of the left menu.

The page *feature profile home* opens.



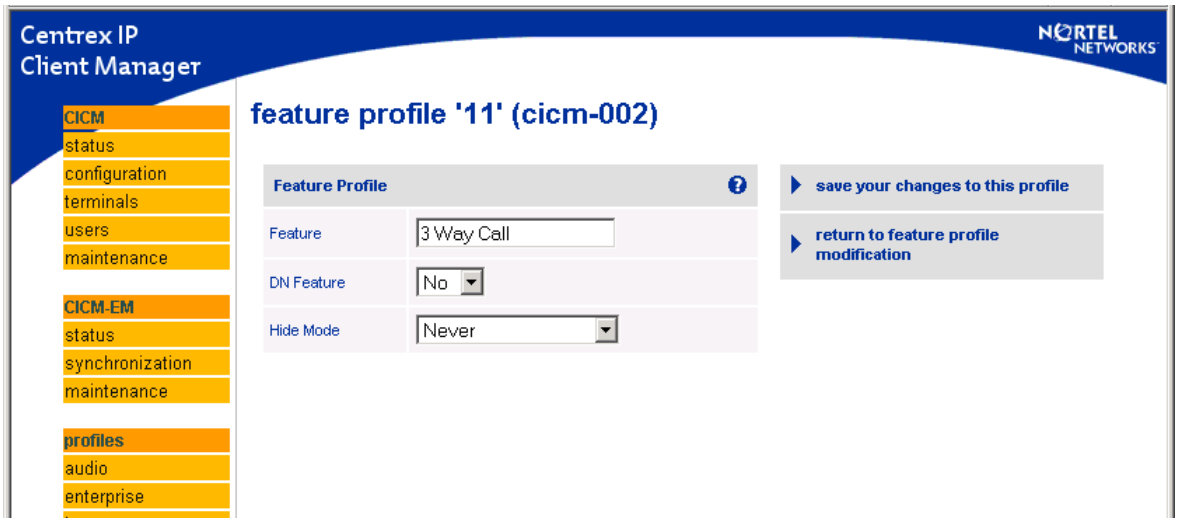

**2** Select the CICM node identifier from the drop-down menu on the right menu, then click on **change the profiles stored on the following CICM**.

The page *feature profiles modification (<cicm-nnn>)* opens. This provides the feature profile for the selected CICM node. The feature profile consists of a list of features; each feature has a set of attributes which can be configured.




**3** On the **feature profiles modification (<cicm-nnn>)** page, click on the name of each feature you want to configure.

The page *feature profile <#> (<cicm-nnn>)* opens for each feature chosen. The following figure shows the **3 Way Call** feature.

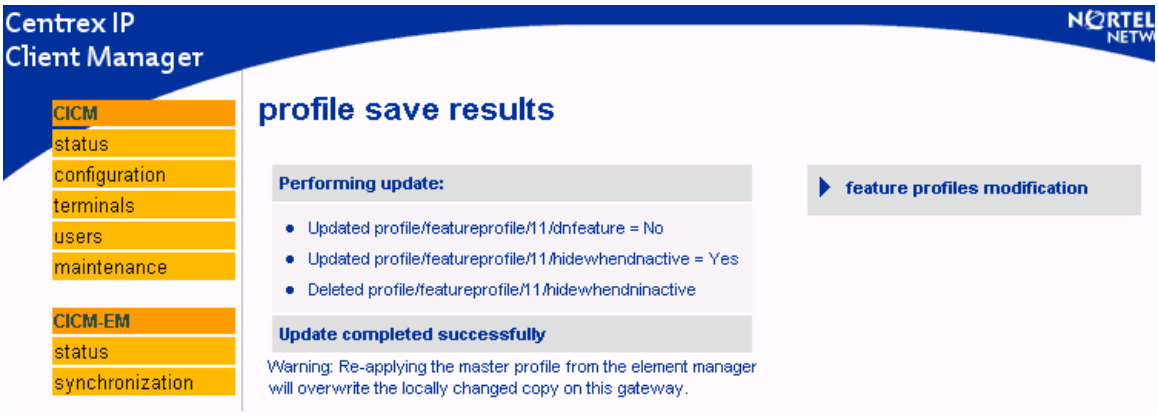



**4** Configure the feature as follows:

Click on the ? icon for a definition of the fields.

- To configure this feature as a DN (dynamic) feature, choose **Yes** from the drop-down menu on the **DN Feature** line, or choose **NO** to not designate it as a **DN Feature**.
- To configure the **Hide Mode**, choose from the drop-down menu on the **Hide Mode** line:
  - Never
  - When DN is active
  - when DN is inactive
- Click on **save your changes to this profile**.

The page *profile save results* displays configuration results.




5 To configure other features, repeat step 3 and 4 for each feature.

6 This procedure is complete.

### Enabling or Disabling the Dynamic Feature Key

Use the procedure Enabling or Disabling the Dynamic Feature key (terminal type) at the CICM-EM Terminal Configuration Web pages. This setting cannot be overridden by any other setting (that is, if the Dynamic feature key functionality is disabled on a terminal type basis the feature cannot be activated in any other way for that specific terminal type).

> ***Note:*** Users logged into the CICM node when the functionality is enabled/disabled will not pick up the changes until they log out and back into the CICM node.

Use the procedure to enable or disable the Dynamic Feature Key functionality by user overrides. These setting changes will take effect immediately.

The user may also disable the functionality from the terminal itself in the **Menu\Feature\Options** menu. These setting changes take effect immediately.

### Procedure 25 Enabling or Disabling the Dynamic Feature key (terminal type)

***At the CICM - Element Manager home page***

**1** Click on **terminals** in the *CICM* menu on the left.

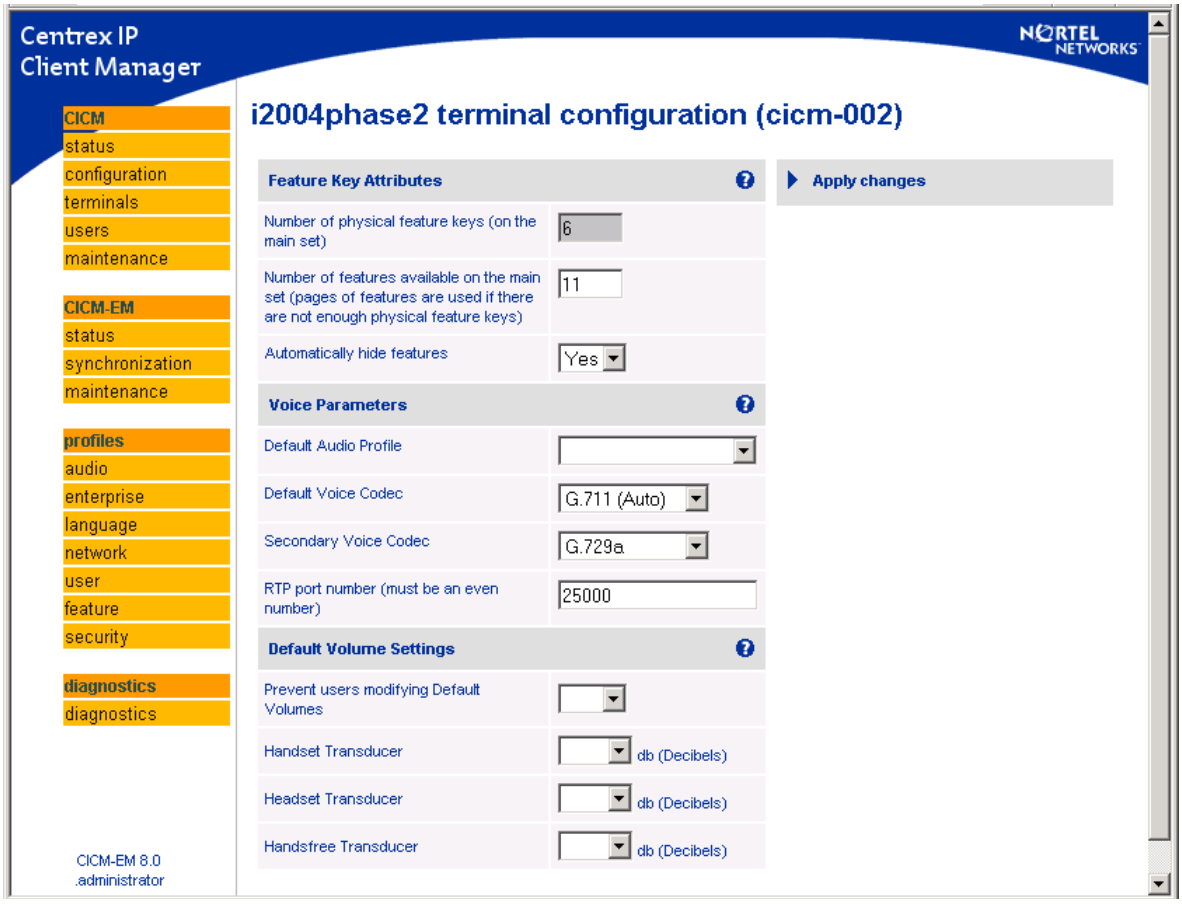
The page *terminal configuration* opens.


**2** Select the CICM node identifier from the drop-down menu, then click on **go to terminal configuration on CICM**.

The page *terminals on <cicm-nnn>* opens.


**3** On the **terminals on <cicm-nnn>** page, select the terminal type (m6350, IP Phone 2001, IP Phone 2002, IP Phone 2004, or IP Phone 2033) you want to configure from the drop-down menu of **configuration**, then click on **configuration**.

The page *<type> terminal configuration <cicm-nnn>* opens. The following figure shows the *IP Phone 200x* type of terminal.




4 To configure this terminal type as a DN (dynamic) feature, choose **Yes** from the drop-down menu on the **Automatically hide features** key attribute, then click on the **Apply changes** text on the right.

***Note:*** Users logged into the CICM when the functionality is enabled or disabled will not pick up the changes until they log out of and back into the CICM node.

The page *updating terminal configuration* opens to confirm the changes.

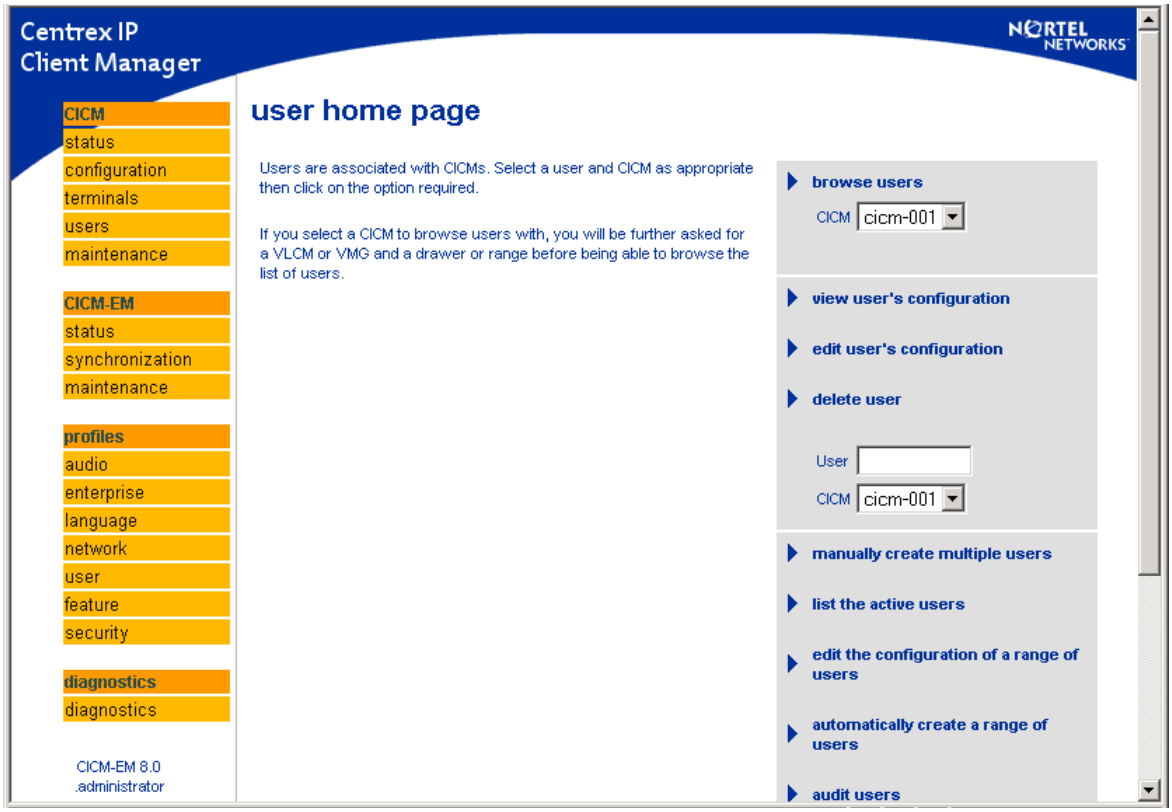
5 This procedure is complete.

## Procedure 26 Enabling or Disabling the Dynamic Feature key (user overrides)

### *At the CICM - Element Manager home page*

1 Click on **users** in *CICM* menu on the left.

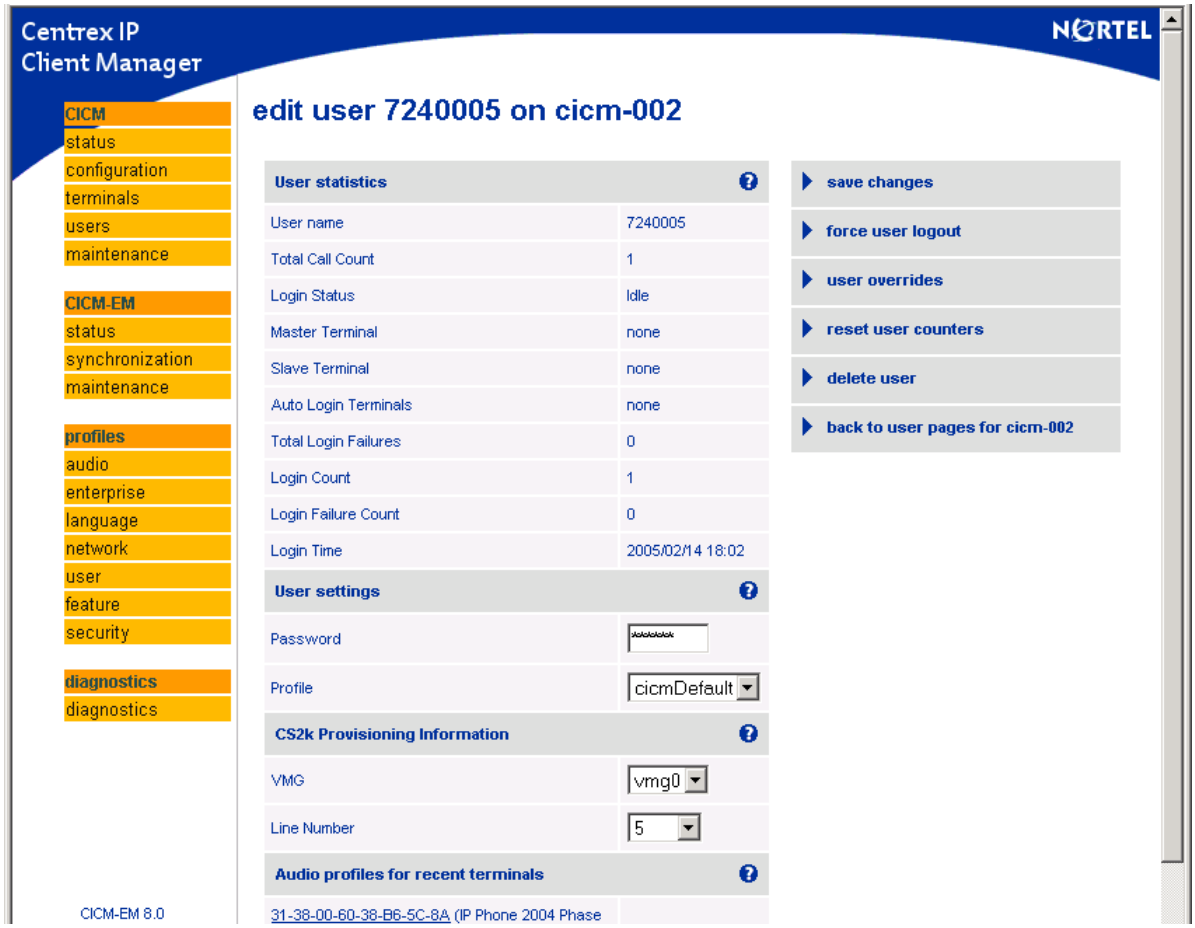
The page *user home page* opens.




2 In the **User** input box on the right-hand menu, enter the user ID that you want to apply or remove overrides to, and select the correct CICM in the drop-down menu immediately under the User input box.

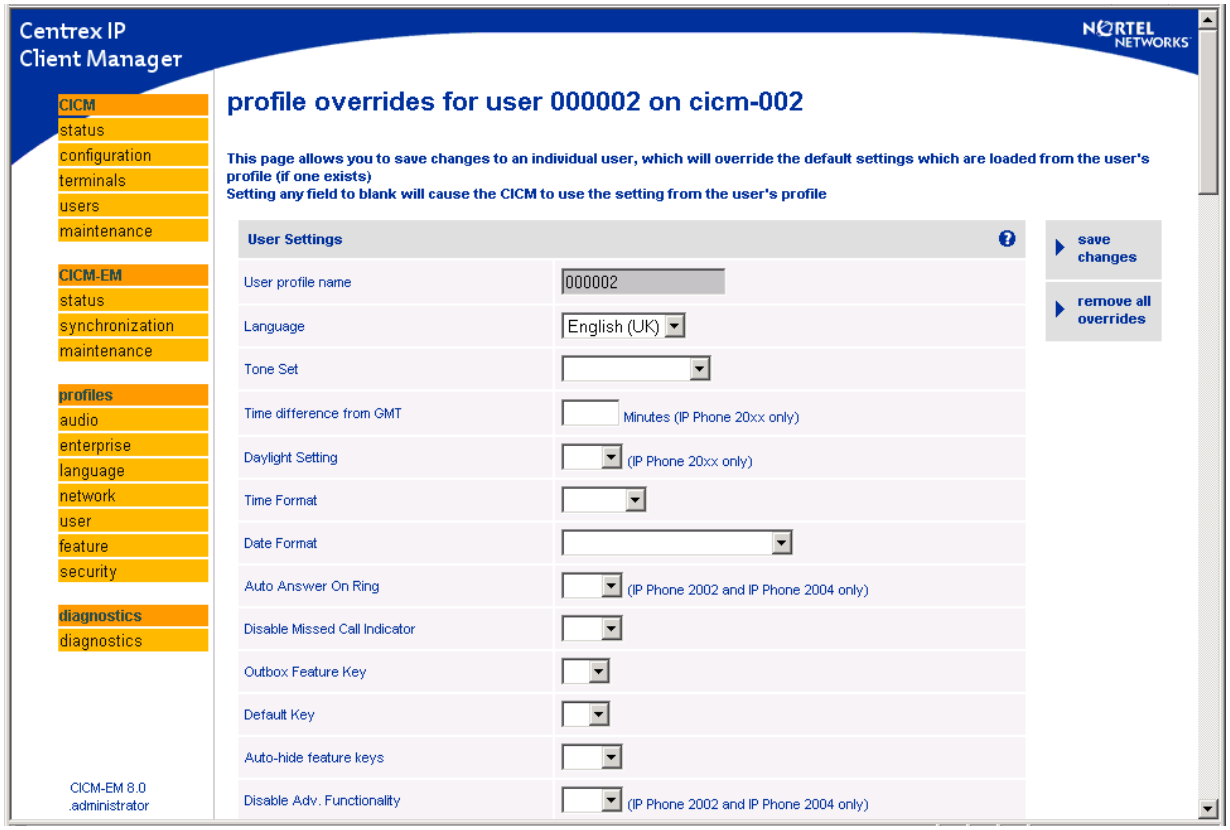
3 Click on **edit user's**.

The page *edit user <username> on <cicm-nnn>* opens.




4 Click on **User overrides** on the right menu.

The page *profile overrides for user <name> on <cicm-nnn>* opens.




5 To enable dynamic feature key functionality, choose **Yes** from the drop-down menu in the **Auto-hide feature keys User Setting** field,
OR
To disable dynamic feature key functionality, choose **No** from the drop-down menu in the **Auto-hide feature keys User Setting** field.
Then click on **save changes** on the right menu.

A confirmation of the override change is displayed.

6 This procedure is complete.

### Security profiles

Security configuration is available through the security function under profiles, and allows administrators to

- manage RSA keys for the CICM-EM and its associated CICM nodes
- view the security policies of associated CICM nodes
- view the security policies of associated enterprises on a CICM-EM

Security configuration consists of setting the following security parameters:

- security policy - indicates whether the communications between a CICM node server and its clients are secure or nonsecure
- nonsecure client threshold - indicates the number of clients permitted to connect in non-secure mode to a CICM node server that has a security policy of secure
- secure client threshold - indicates the number of clients permitted to connect in secure mode to a CICM node server that has a security policy of nonsecure
- reset security (new in this release) - clears the security objects that ties clients to a particular CICM node server, and therefore facilitates moving multiple secure clients (terminals) from one CICM node server to another

For details and procedures, refer to the section “UNIStim security” in *CICM Security and Administration*, NN10252-611.

## Line provisioning for CICM clients

The procedure used to provision a CICM client on the CS2000 is very similar to the method used to provision a line on other line gateways.

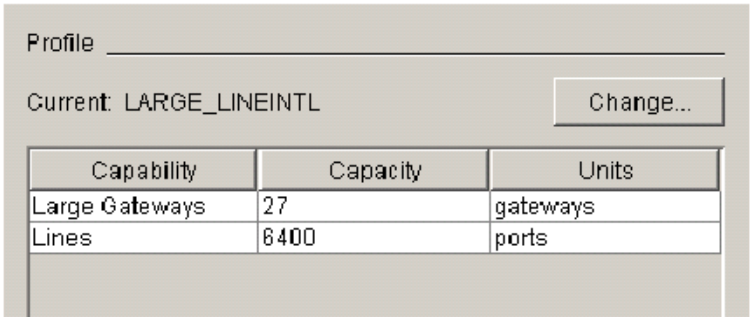
### Procedure 27 CS2000 Line provisioning for CICM clients

***At the Element Manager desktop***

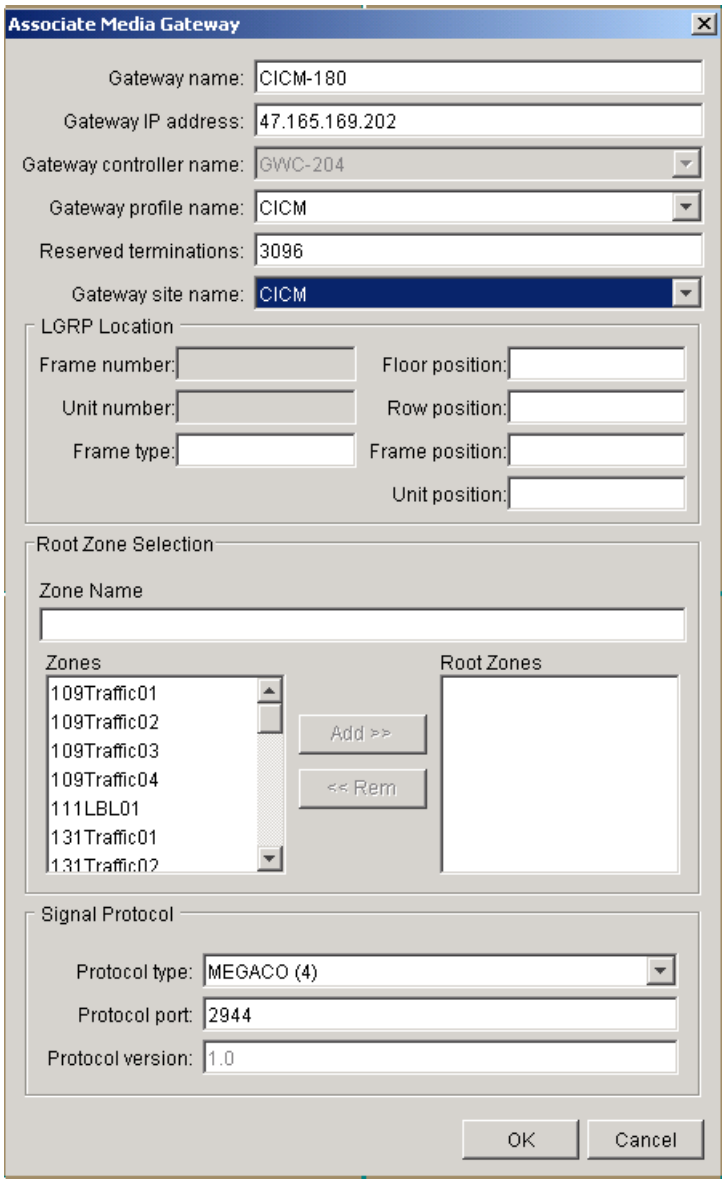
1 Connect to the CS2000 Management Server for the chosen CS2000.

2 Ensure that the gateway controller (GWC) is provisioned to support Large Lines Gateways.

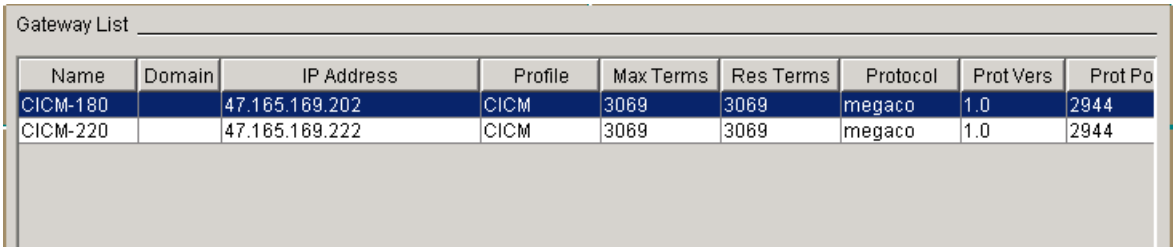
**Example:**




3 Use the dialog box *Associate Media Gateway* to associate a CICM gateway with the chosen GWC. Fill in the *Reserved terminations* with up to 1023 for SAM 16 or 3069 for SAM 21.




Response 1: The Gateway List displays a registration of the CICM gateway against the GWC.



Response 2: A logical group is automatically created in table LGRPINV on the CS2000.

With SAM 21, three tuples are created in table LGRPINV to accommodate the 3069 terminations it supports. With SAM 16, only one tuple is created for the 1023 terminations it supports.

```
TABLE LGRPINV
lis all
TOP
    GRPNO       SRVRNAME   GRPTYPE              LGRPOPTS
-------------------------------------------------------------------------
CICM 180 0      GWC 204      M                  $ <-
CICM 180 1      GWC 204      M                  $   |------ Resulting entries (for SAM 21)
CICM 180 2      GWC 204      M                  $ <-
CICM 200 0      GWC 210      M                  $
CICM 220 0      GWC 204      M                  $
CICM 220 1      GWC 204      M                  $
CICM 220 2      GWC 204      M                  $
CICM 260 0      GWC 200      M                  $
BOTTOM
>
```

**4** Log into OSSGATE and enter the command **NEW** to create new lines, for example:

```
NEW $ 8500001 m5216 SET IPLCLIENT OTHER PUBGRPA 0 0 1511 Y CICM 500 0 0 01 1 userid 000001 $ 1
passwd 1234 1 LNR 2 3WC IPCLIENT OTHER 3 MWT Y ALL N 4 CFU N 1 $ 5 INSPECT $
```

where

**8500001**
is the directory number (DN).

**m5216**
is the name of the line class code (LCC).

**IPCLIENT OTHER**
specifies the kind of phone service. OTHER indicates any of the Nortel IP phone sets.

**PUBGRPA**
is the customer group.

**151**
is the simplified numbering plan area (SNPA).

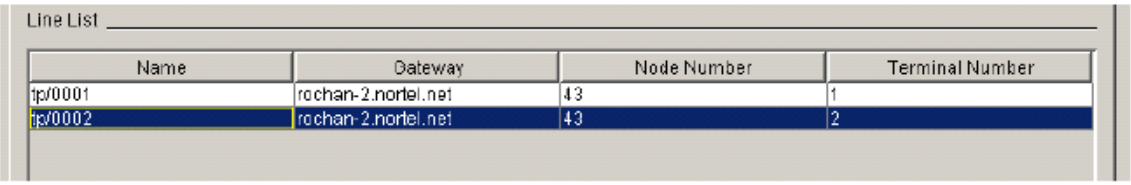
**CICM 500 0 00 01**
is the line equipment number (LEN)

**1 userid 000001 $**
is the user id of the CICM client (terminal).

**1 passwd 1234**
is the password of the user id.

**1 LNR 2 3WC IPCLIENT OTHER 3 MWT Y ALL N 4 CFU N 1 $ 5 INSPECT $**
is the list of features assigned to the line. Use OTHER to include any version of an IP phone for option IPCLIENT.

Response 1:
On the CS2000 Management Server:




The response to the command QLEN on the CS2000 appears, as in this example:

```
>qlen 8500001
------------------------------------------------------------
LEN:   CICM 500 0 00 01
TYPE:  SINGLE LINE
SNPA:  151
DIRECTORY NUMBER:        8500001
LINE CLASS CODE:       M5216 SET
CUSTGRP:    PUBGRPA  SUBGRP: 0  NCOS: 0  RING: Y
CARDCODE:   IPCLIENT  GND: N PADGRP: PKNIL BNV: NL MKO: Y
PM NODE NUMBER       :   43
PM TERMINAL NUMBER :   2
OPTIONS:
  3WC  MWT  CFU

   KEY          DN
   -----        ---
     1          DN          2088500001

   KEY          FEATURE
   -----        -------------
```

**5** This procedure is complete.

## Configuring PAM on the CICM-EMs

Configure the Pluggable Authentication Module (PAM) on a pair of redundant CICM-EMs to enable centralized security of the CICM-EMs and their subtending CICM node pairs through IEMS.

### Prerequisites to configuring PAM on a CICM-EM

Address the prerequisites before starting the procedure.

- The IEMS must already be running and you must already have a certificate on the IEMS before deploying one for both CICM-EMs.
- You must have a working knowledge of UNIX.
- There is no configuration of PAM for a CICM node.

### Procedure steps to configuring PAM on a CICM-EM

***At the CICM-EM***

**1** Telnet into the PAM server and gain root access.

**2** Go to the directory where the keystore file is by entering:

**cd /opt/jakarta/dist/tomcat/conf**

**3** Create an appropriately formatted certificate to import into the CICM-EM by entering:

**keytool -export -v -alias sesmkey -file sesmkey.cer -keystore ./keystore**

**4** For the keytool password prompt, enter:

**sesmkey**

**5** Transfer the newly-created file *sesmkey.cer* to the CICM-EM.

**6** Telnet or connect to the CICM-EM node A and open a command line interface (CLI).

**7** Run the command:

**preboot pamauth /interactive**

```
Will this Element Manager use the PAM on the
SSPFS to authenticate users? [T/N, default=N]
```

**8** Enter **Y** (yes).

```
Will this EM connect the PAM server via HTTPS?
[Y/N, default=N]]
```

**9** Enter **Y**.

```
Please enter the IP address of the PAM server.
```

**10** Enter the IP address of the SSPFS PAM server.

**Example**
47.135.42.226

The CLI prompts to enter the FQDN of PAM server.

**11** Enter the FQDN of the SSPFS PAM server:

**Example**
pamserver.nortel.com

```
Do you want to import a certificate? [Y/N,
default = N]
```

***Note 1:*** A Security Certificate is required for communicating through HTTPS to the PAM server. If you are using a certificate purchased from a valid signing authority (for example, Verisign, Thawte, etc.) then enter **N** to the prompt as the certificate will be automatically trusted. If you are using a self-signed or unsigned certificate, then answer **Y**, as it is required to import this type of certificate.

***Note 2:*** Ensure that the unsigned certificate is placed on the EM before proceeding. If the certificate is not in the current directory, then the path must be provided as part of the file name, for example, *C:\data\myCert.cer*

**12** Enter **Y** to import.

```
Filename of certificate to import ...
```

**13** Enter the full qualified name of the certificate to use to validate the PAM server:

**d:\data\cablab.cer**

The response would be similar to the following example:

```
Connection to PAM through HTTPS
Primary SSPFS PAM Proxy FQDN:
ucars0033c.ca.nortel.com
Primary SSPFS PAM Proxy IP Address:
47.135.42.226
Security Certificate
d:\data\cablab.cer

Is this correct? [Y/N, default=Y]
```

**14** Enter **Y** to save.

The CLI prompts to confirm the command summary, for example:

```
You have entered the name of the primary SSPFS
```

```
PAM proxy as: 47.135.42.226 Is this correct?
[Y/N, default=Y]:
```

**15** Enter **Y** to confirm the input.

Enter **N** to make a correction, then **Y** when it is correct.

**16** For the second CICM-EM of the redundant pair, repeat from step 5.

**17** For authentication to take effect, you must stop and start the PAM service, as follows:

**a** At the CLI, enter the command:

**net stop pamauthservice**

**b** At the CLI, enter the command:

**net start pamautheservice**

**18** Repeat from step 1 for node B of the redundant pair.

**19** Test PAM by logging into the CICM-EM by **central database** username and password as well as **.administrator**.

**20** This procedure is complete.

## Configuring the apache proxy server for the CICM-EM pair

As a proxy server, the integrated element management system (IEMS) on a Succession Server Platform Foundation Software (SSPFS)-based server can provide secure access to either node of a CICM-EM redundant pair. Use the procedure to configure the proxy (HTTPS connection) between the IEMS and the CICM-EMs.

### Prerequisites to configuring the apache proxy server for the CICM-EM pair

Address the prerequisites before starting the procedure.

- You need to know the floating hypertext transfer protocol secure (HTTPS) IP address of the master and slave CICM-EMs.
- You need the root userid and password for accessing the IEMS.
- Up to 6 IP addresses can be configured on the HTTPS proxy. This maximum includes CICM nodes and any other components in the network.

### Procedure steps to configuring the apache proxy server for the CICM-EM pair

***At the PC to access IEMS server***

**1** Log into the IEMS server by entering:

**telnet <ip_address_server>**

where <ip_address_server> is the IP address or host name of the SSPFS-based server on which the proxy is being configured.

**2** When prompted, enter your userid and password.

**3** Change to the root user by entering:

**su - root**

**4** When prompted, enter the root password.

***At the IEMS server to have the proxy connection***

**5** Enter **cli** to start the command line interface (CLI).

**6** At the prompt, enter the number to select **Configuration**.

**7** At the prompt, enter the number to select **Apache Proxy Configuration**.

**8** At the prompt, enter the number to select **add_proxy_conf**.

**9** At the prompt *Enter proxy IP address*, enter the floating HTTPS address of the master CICM-EM.

10 At the prompt for *hostname/tag associated with*, enter the same floating HTTPS address for the slave CICM-EM.

11 At the prompt *Optional, enter remote hostname*..., press enter to omit the entry.

12 At the prompt for the port field, enter the IEMS IP port number **443** for the public side of the IEMS.

13 Enter **Y** (yes) to accept the values and continue.

```
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped
Starting WEBSERVER through servstart
Found valid security certificate, starting
Web Services with SSL support...
Apache Web Service Starting
WEBSERVER Started
=== "add_proxy_conf" completed successfully
```

14 At the prompt, enter the number to select **add_proxy_conf** again.

15 At the prompt *Enter proxy IP address*, enter the same floating HTTPS address of the CICM-EM.

16 At the prompt *hostname/tag associated with*, enter the remote tag **centrexip**.

17 At the prompt *Optional, enter remote hostname*, enter the remote tag **centrexip** again.

18 At the prompt for the port field, enter the IEMS IP port number **443** for the public side of the IEMS.

19 Enter **Y** (yes) to accept the values and continue.

```
Stopping group using servstop
...
=== "add_proxy_conf" completed successfully
```

20 Exit each menu level until you exit the CLI by entering:

**x**

21 This procedure is complete.

## Setting the global m5216 emulation mode

The m5216 emulation mode is automatically used for any terminal with GIC or GIAC features assigned to it. If the global m5216 emulation mode flag is set, the m5216 emulation mode is used for all terminals, regardless of whether they have GIC or GIAC assigned. This ensures that all terminals will behave in a consistent manner.

### Procedure 28 Set global m5216 emulation mode

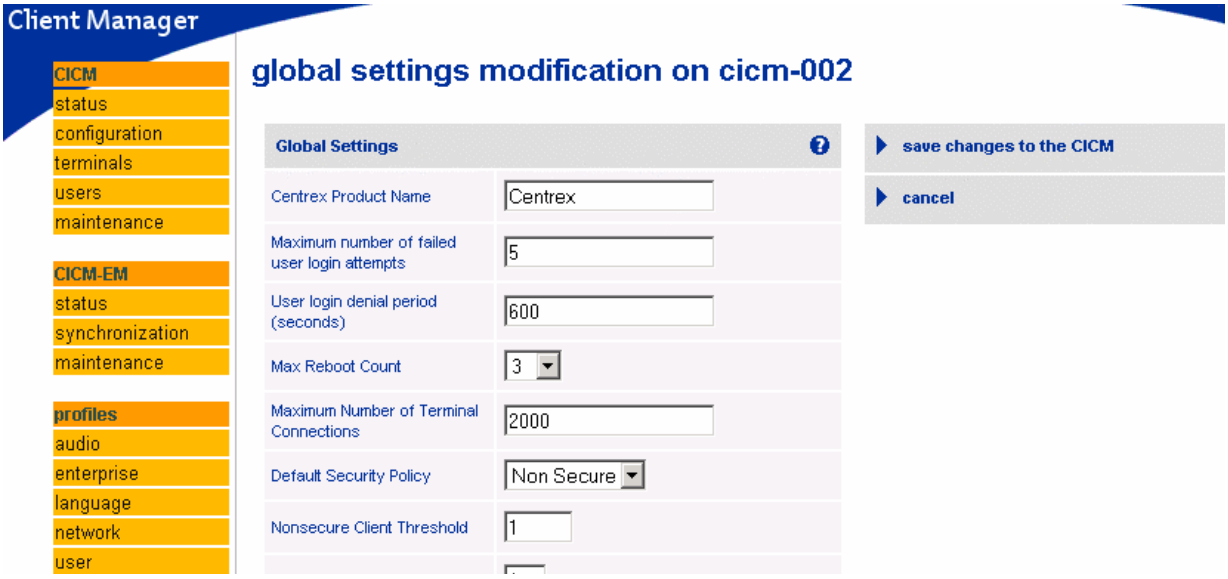
***At the CICM-EM web interface***

1 Select **Status** from the *CICM* menu at the left.

The page *cicm home* opens


2 Click on **change the global setting for the following CICM**.

The page *global settings modification on <cicm-nnn>* opens.




**3** Scroll down the **global settings modification on <cicm-nnn>** page to the **Terminal settings** section, and select **yes** in the **M5216 Emulation Mode** field.


**4** This procedure is complete.

# Installing and initializing IP phones for CICM nodes

Installing and initializing Internet Protocol (IP) phone set is the same for the following models:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Conference Phone 2033

Getting an IP phone to operate is divided into:

- Installing an IP phone
- Initializing an IP phone

## Installing an IP phone

Install an IP phone to become a client of a CICM node.

### Prerequisites to installing an IP phone

You must address the following before starting the installation.

- An IP phone set can be configured in different ways depending whether a full or partial Dynamic Host Configuration Protocol (DHCP) server is available in your network. DHCP can be used to provide the IP phone with an IP address and other information required to initialize the set. Determine from your network administrator whether DHCP is being used, and if so whether it is full or partial.
- Whether or not you are using DHCP, ensure that you know the information that is identified in table IP phone configuration parameters before you begin the installation.
- You need CAT-5 cable with an RJ45 connector at each end.
- You need an AC power outlet for the phone set. The outlet must provide up to 240 V.

### Procedure steps to installing an IP phone

#### *At the location for the phone*

**1** Place the phone where it is to be used.

**2** Measure the path from the phone to where it is to connect to the IP network.

**3** Make a CAT-5 cable with an RJ45 connector at each end long enough to follow the path.

4

**CAUTION**
**Risk of equipment damage**
Severe damage occurs to an IP phone set that is plugged into an ISDN connection. Ensure that you are plugging your set into a 10 or 100 BaseT Ethernet jack.

Connect one end of the CAT-5 cable to the line jack on the telephone base and the other end to an Ethernet jack into the IP voice network.

5 Connect one end of the handset cord to the handset jack on the telephone base. Connect the other end of the cord to the handset.

6 Plug the AC Power adapter into the telephone base and the other end into an AC outlet.

All hardkey indicator lights and softkey icons flash to indicate the phone is powered but not initialized. Continue the installation at Initializing an IP phone.

## Initializing an IP phone

Initialize an IP phone to complete its initial installation and enable its operation with a CICM node.

### Prerequisites to initializing an IP phone

You must address the following before starting the initializing.

- The initial installation must have been started as described in Installing an IP phone.

### Procedure steps to initializing an IP phone

#### *At the IP phone set*

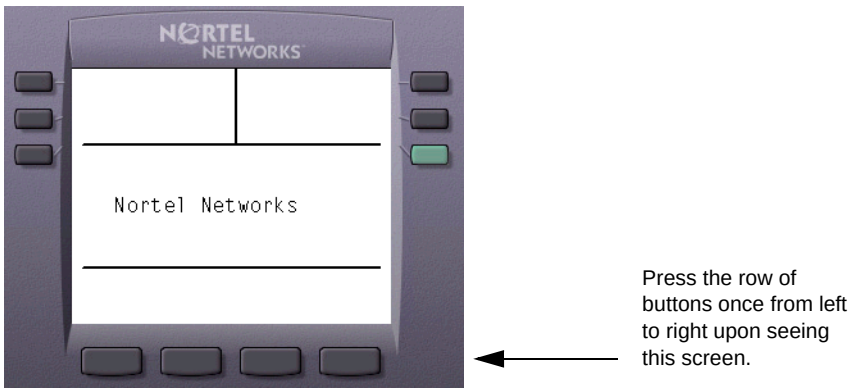
**1** Ensure that the IP phone set is powered. Power is indicated by flashing indicator lights and softkey icons.

If nothing is flashing, ensure that:

- the AC outlet has power
- the AC Power adapter has a good connection at both ends
- you unplug and plug in the AC adapter at the telephone base

Once the phone set is powered, it automatically begins initializing.

**2** As soon as the following screen appears on the phone set, press each of the softkeys once from left to right. Pressing the keys enables you to configure the phone.




***Note 1:*** If this screen does not appear, you must contact your system administrator to get the phone set upgraded.

***Note 2:*** If the next screen appears before you press all of the softkeys, you must unplug the power cord to restart the initializing and repeat this step.

3 As the prompts for configuration data appear, you must enter the appropriate information. The table IP phone configuration parameters identifies the prompts and what to enter for each.

When inputting data to answer the prompts, the softkeys become labelled as follows.

**OK**
is to record the entry and continue to the next prompt.

**Bkspace**
is to edit the current prompt by deleting an entry one character at a time.

**Clear**
is to erase the current entry for the prompt so that other data can be entered.

**Cancel**
is to abort the configuration process and return to step 1.

To input numbers for the data, use the number keys on the dial pad. When entering IP addresses, press the asterisk (*) to represent a period (.).

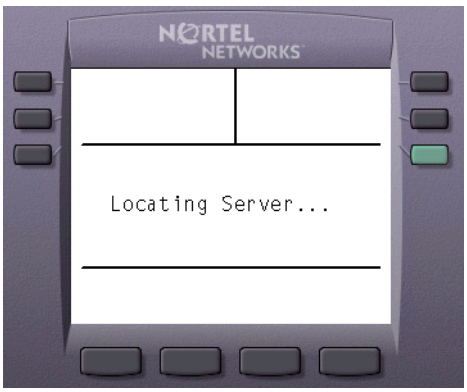
**Table 2 IP phone configuration parameters**

| Prompt | Entry data |
|---|---|
| 1. DHCP? (0 - No, 1 - Yes) | Enter 1 to use full or partial DHCP.<br>Enter 0 (zero) to manually configure the set. |
| 2. DHCP: 0 - Full, 1 - Partial | The prompt appears only when full or partial DHCP is selected. For full DHCP, all remaining prompts are automatically configured by the DHCP server.<br>For partial DHCP, prompts 3, 4, and 5 are automatically configured by a DHCP server. |
| 3. SET IP | Enter the IP address for the phone. |
| 4. NETMSK | Enter the network submask. |
| 5. DEF GW | Enter the IP network address of the default gateway. |
| 6. S1 IP | Enter the IP address of the primary server. |
| 7. S1 PORT | Enter **5000** for the port number of the primary server. |
| 8. S1 ACTION | Enter **1** for the primary action code. |
| (Sheet 1 of 2) | |

**Table 2 IP phone configuration parameters (Continued)**

| Prompt | Entry data |
|---|---|
| 9. S1 RETRY COUNT | Enter **6** for the primary retry count. |
| 10. S2 IP | Enter the IP address of the secondary server. |
| 11. S2 PORT | Enter **5000** for the port number of the secondary server. |
| 12. S2 ACTION | Enter **1** for the secondary action code. |
| 13. S2 RETRY COUNT | Enter **6** for the secondary retry count. |
| (Sheet 2 of 2) | |

**4** When all configuration data has been entered, the IP phone saves the entries and attempts to connect to the server. The attempt is shown by the following figure.

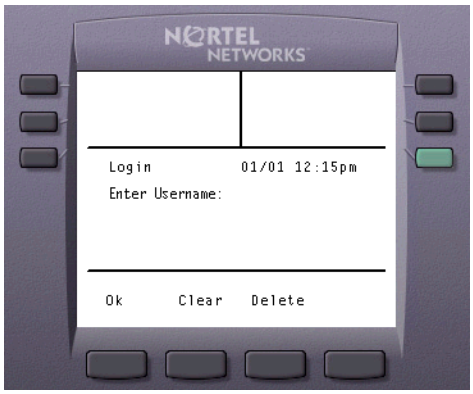



**5** Depending on the configuration of your gateway, you may be offered to upgrade the firmware for the IP phone. When there is a new firmware release, this message appears:

```
New firmware available. Perform upgrade now?
```

Select **Yes** by pressing the nearest key. Downloading takes less than two minutes.

**6** When the IP phone has successfully connected to the server, this screen appears:




Begin using the IP phone.

When the IP phone does not connect successfully to the server, it re-attempts connection.

When the IP phone cannot connect to the gateway, it may indicate that an invalid parameter was entered during the initialization. In this case:

**a** verify your entry data for the table IP phone configuration parameters is correct

**b** unplug the power to the phone to clear the initialization data and repeat the procedure from step 2

**7** If you still cannot connect to the network through the gateway, contact your next level of technical support for assistance.

**8** This procedure is complete.