CICM Security and Administration

This document provides the security and administration tools, utilities, 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 in CICM security and administration

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

- changed the term “terminal handover” to “terminal transfer” throughout the document, especially in the section Terminal transfers, and removed the procedure “Perform a terminal handover” which no longer applies
- updated the introduction to Terminal transfers
- changed the field “Service Status” to “Status” in the procedure Starting or stopping the CICM service, and updated the purpose statement of the procedure

Administration for CICM

Administering Centrex IP Client Manager (CICM) consists of CS2000 administration and CICM administration.

The topics in this section are:

- CS2000 administration
- CICM administration
- Device administration
- Terminal transfers

CS2000 administration

CS2K administration is undertaken upon installation, with the datafill of hardware data tables to specify connections. Once datafilled, there should be no reason to alter the datafill. Refer to the CS2000 documentation.

CICM administration

Administration for the CICM can be done from either its CICM-EM hosted web pages or from the Administration PC that allows access to the CICM. The CICM does not come equipped with a display or keyboard.

An Administration PC is attached to the service provider's Administration LAN. An Administration PC accesses the CICM-EM through a web interface.

The functions of the Centrex IP Client Manager administration interface are to:

- Display the status of the CentrexIP service
- Start or stop the CentrexIP service
- Configure the CICM and clients
- Collect event logs from the CICM
- Backup and restore the CICM configuration

Device administration

A CentrexIP line can be made busy (BSY), installation busy (INB) or returned to service (RTS) in the same manner as a conventional line. Refer to the CS2K documentation suite for complete procedures.

For information regarding configuration and administration of the IP Phones and the m6350 SoftClient, refer to “Related Documents” in *CICM Basics*, NN10044-111.

Terminal transfers

For SN08, all terminals (clients) connect to the master CICM node. When upgrading CICM node software with a product release from SN07 or rolling back from an upgrade to SN07, the terminals on the master node must be manually transferred over to the slave node. This ensures that the terminals can be returned to service when immediately followed by a switch of activity (SWACT) between the master and the slave nodes.

Terminal transfers are handled automatically by active call failover (ACF) for an upgrade from SN08 to SN08 or later.

Terminal transfer overview

When software or hardware maintenance or upgrades are being performed on a CICM node, the node is taken out of service. Terminals on the node to be shut down must be moved to the mate node prior to node shutdown. The mate node is still available to provide service during the node outage (although at a reduced capacity).

The terminal transfer enables the CICM node to shut down in a controlled manner, as follows:

- The administrator selects a shutdown timeout interval (between 5 and 60 minutes, in 5 minute intervals) and initiates the terminal transfer.
- Terminals attempting to register new sessions with the CICM node will be automatically redirected to the mate node.
- Terminals with no active user login session are transferred to the mate node immediately when the terminal transfer is initiated.
- For terminals with an active user login session:
  - Users are presented with a dialog screen informing them that maintenance is being performed, and requesting permission to perform a terminal reboot.
  - Users have the choice to defer the terminal reboot. If they defer the terminal reboot, after several minutes they will again be

presented with a dialog screen requesting permission to perform a terminal reboot.

- Users that repetitively defer the terminal reboot until the end of the shutdown timeout interval will be forced out. The active call is dropped and transferred to the mate node.
- When a terminal is transferred, the terminal loses service for a few seconds.
- The user login session is automatically restored when connectivity is restored on the mate node.

- If all terminals have been moved to the mate node before the timeout occurs, the shutdown will complete at that time instead of waiting for the timeout expiration.

Terminal transfer -- client terminals

This feature applies to the IP Phones 200x and 2033, and the m6350 clients. The transfer process differs for the IP Phones and m6350 primarily in the user interface.

For detailed information on the user interface for IP Phones and the m6350 SoftClient, refer to “Related Documents” in *CICM Basics*, NN10044-111.

Limitations and restrictions of terminal transfers

This section provides the limitations and restrictions of transferring terminals from one CICM node to another.

Cross-hosted call processing Cross-hosted calls that have terminals with active user sessions on the mate node and are using call processing resources on the node that is shut down, will lose active calls without notice when the node hosting the call processing resources is taken out of service.

Network addressing To move the terminal from one node to the other, the UNIStim SwitchServer command is used.

When a terminal connects to the CICM, the CICM queries the terminal’s server configuration (which is configured manually on the terminal or through DHCP). The CICM identifies which of the server entries corresponds to its own host address (the client LAN address on the CICM node).

The CICM then identifies which is the failover server. If the failover server is not configured correctly to be the mate node, the terminal transfer will fail. The terminal will eventually reconnect to the node being taken out of service when that node is brought back into service. The CICM does not reprogram the terminal's server configuration.

> **Example**
> **Failover terminal**: If a terminal connected to node B has node A configured for server S0, and node B configured for server S1, then node A is the failover server.

> ***Note:*** If a static NAT bind is being used to publish private CICM client LAN addresses on a public network, the CICM will be unable to match its own address to either of the addresses configured on the terminal. This will cause unpredictable results when transferring terminals.

Terminal server configuration Terminals with S1 and S2 configured as the same server (for example, both configured with the address of node A) are not candidates for transfer to the mate node. In this case, when a terminal transfer is being performed, a log is generated for these terminals and the terminal is left connected to the node until the node shuts down completely, at which point it loses service.

Security for CICM

The security model for the Centrex IP Client Manager (CICM) mandates two separate networks: the Administration network (Admin LAN) and the Client network. The topics in this section are:

- Admin and Client LAN security
- Access privileges and restrictions
- Element Manager security
- IIS filter access
- Read-only shared resources
- Authenticated web access
- Secure web access
- Firewall and NAT traversal
- UNIStim security

Admin and Client LAN security

The Admin LAN is a secure environment owned and managed by the telco. It is used for carrying operation and administration data and does not carry call control data or media streams. No voice services are available from the Admin LAN.

The Client network also belongs to the telco customer. The Client LAN is a non-secure network not under the control and management of the telco. It carries call control and bearer traffic.

For security purposes, the Admin LAN and Client LAN are physically isolated from each other within each CICM cabinet. Routing directly between the Admin and Client LAN is disabled in the CICM. Only the basic services needed for call control are available from the Client LAN connections to the CICM.

Because of the separation between Admin LAN and Client LAN, an administrator would have to do the following to test whether a client PC or IP Phones200x is visible on the client LAN:

- Use **Telnet** to log into the CICM on which the user is registered, or
- Use **ping** or **tracert** command from the Telnet command line to try the reach of the IP address of the client.

> ***Note:*** **Ping** and **Tracert** commands may not be used for deployment where the CICM and its clients are separated by firewalls and NATs because **Ping** and **Tracert** messages are not able to traverse firewall/NAT.

Access privileges and restrictions

The following access privileges are protected by user names and/or passwords:

- access to the CICM nodes and CICM-M through the Admin LAN
- access to the administration web pages on the Element Manager
- login to terminals on the Client LAN

To access the CICM-EM web pages, a user must be a member of the CentrexIP administrators group, which is configured as part of the installation process. As a member of the administrators group, the administrator password can be used for access to the Administration PC, the Element Manager web pages, and for Telnet access.

Refer to the *User Administration Procedures* section of this document for detailed instruction on setting up user and administrator groups and setting privileges.

Element Manager security

Access to the Element Manager is controlled by the Internet Information Server (IIS). For security purposes, authentication is required to obtain access to the EM (by IIS default configuration).

The following options may also be configured for extra security:

- Secure Sockets Layer (SSL) encryption may be configured to provide privacy of sensitive information
- Certificates may be configured for additional authentication
- Auditing may be configured to monitor security activities to prevent unauthorized access

IIS filter access

Internet Information Services (IIS) can filter access to web services based on selected IP addresses or domain names. Having only a small set of client addresses in the filter minimizes the chance of infraction.

Read-only shared resources

The Element Manager is initially configured with three shared directories, one for firmware, one for backup, and one for patching. All of these should be read-only. If directories are created for other purposes, ensure these are made writable for the minimum required period of time.

Authenticated web access

The web server can be configured to only permit access to authenticated NT users within the CICM domain or other domains where trust relationships have been established.

Secure web access

The web server supports secure web access using Secure Sockets Layer (SSL) when provided with a signed Certificate. This requires the administrator to obtain a Certificate from a provider. IIS supports client certificates that are manually distributed to trusted clients and entered into the browser. SSL can be configured using the Internet Service Manager.

Firewall and NAT traversal

Firewalls and Network Address Translation (NAT) devices are widely used by enterprises to maintain their network security and integrity.

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware or software, or a combination of both. All messages entering or leaving the private network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

A NAT needs to be deployed to translate from a private IP address to a public IP address and vice versa (if an enterprise uses private IP addresses internally and public IP addresses externally). A NAT is a software capability residing on a firewall. A NAT essentially hides an enterprise internal private IP address domain and makes it non-reachable from external points of origin, hence providing an additional layer of security.

In a typical deployment where the carrier provides IP Centrex as a carrier-hosted Centrex solution to its various enterprise customers, the CICM is normally located in the carrier Central Office LAN (CO-LAN), in the carrier's managed IP network and the carrier's IP address space. The IP phones reside on the enterprise LAN in the enterprise private IP address space behind the enterprise firewall and NAT. The IP phones communicate with the CICM over the carrier's managed IP network. The firewalling and NAT functions may be provided through software residing on an enterprise edge router, or a separate device linked to the edge router.

To enable CS2K to provide Centrex IP as the Carrier Voice over IP (VoIP)-hosted Centrex solution to its various enterprise customers, it is critical that the CS2K Centrex IP services are able to traverse enterprise firewalls and NAT devices.

Nortel has developed a comprehensive firewall and NAT traversal solution for CS2K-based Centrex IP Solution utilizing the CICM release 6.12 and later.

NAT traversal

Nortel's Centrex IP supports all types of NATs regardless if it is a full cone NAT, restricted cone NAT, port-restricted NAT or symmetric NAT. There is no change needed on existing NAT functions or NAT devices of enterprises.

UNIStim signaling NAT traversal Centrex IP UNIStim signaling messages can traverse any type of NAT as UNIStim messages are always initiated by Centrex IP clients from the private side of the enterprise NAT. That initial UNIStim message creates a binding on the NAT to allow UNIStim message traversal from the CICM from the public side of the NAT.

Keep NAT binding alive for UNIStim signaling Each IP Phones 200x is configured with the IP address of its hosting CICM. When the IP Phones 200x powers on, it sends a Resume Connection message to the CICM. A path through the NAT device is set up for UNIStim signaling.

Once the initial connection has been made, the IP Phones 200x starts the Watch Dog timer, with a default value of 2.5 minutes.

To keep the firewall pinhole open for the UNIStim signaling path throughout the user's logon session, the CICM has a built-in global terminal Watch Dog timer that has a default value of 2 minutes.

Every one minute, the CICM sends a UNIStim Reset Watchdog message to the client (that is, terminal) to reset the Watch Dog timer on the client, and the client responds with an ACK message. This ACK message goes through the firewall and resets the firewall (NAT) timer, hence keeping the firewall pinhole open and the NAT binding alive.

The configurable NAT binding (firewall) timer value is recommended to be 3 minutes. The guideline is to set the Watch Dog timer about 30 seconds smaller than the firewall timer.

RTP media NAT traversal Two uni-directional RTP media streams are needed to set up a VoIP call. The outgoing RTP media stream from Centrex IP clients to the CICM can traverse the NAT since it is initiated from the private side of the NAT. However, the incoming RTP media stream initiated at the CICM (on the public side of the NAT) and destined to the clients can not traverse the NAT since there is no address binding established at the NAT. Therefore, the call fails.

The real challenge of a NAT on any VoIP application, therefore, is how the incoming RTP media stream traverses the NAT.

Nortel NAT traversal solution

The Nortel Network NAT traversal solution is summarized by the following four factors, which are discussed below.

- CS2K-routed calls
- Intraswitched calls behind a single NAT
- Calls between two enterprises
- Keeping NAT open for RTP media

UNIStim security

CICM clients communicate with a CICM server using the Nortel proprietary UNIStim (Unified Networks IP Stimulus) protocol. The UNIStim security feature, introduced in the CICM 2.5 MR6 release, provides the infrastructure required for secure communications between the CICM server and its clients. Security configuration is available through the security function on the CICM element manager web page, and allows administrators to

- manage RSA keys for the CICM element manager and its associated CICM servers
- view security policies of associated CICM servers
- view security policies of enterprises

Security configuration consists of setting the following security parameters:

- security policy - indicates whether the communications between a CICM 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 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 server that has a security policy of nonsecure
- reset security - clears the security objects that ties clients to a particular CICM server, and therefore facilitates moving multiple secure clients (terminals) from one CICM server to another

The security parameters for CICM servers associated with an enterprise are specified as part of the enterprise's profile.

To set up secure communications between CICM servers and their clients, refer to procedure Setting up secure communications between a CICM server and its clients on page 62.

To clear security objects, refer to Clearing security objects on page 45.

Tools and utilities for CICM

The web interface is the primary user interface to the Centrex IP Client Manager. The CS2K Line Maintenance Manager (LMM) Interface may be used to perform administration and maintenance of the CS2K components that relate to the CICM.

A number of standard administration tools, such as SNMP and WMI, can be used on the Administration PC, in addition to the web Interface, for remote management of the CICMs.

Web interface

The CICM-EM web interface is designed for use with Microsoft Internet Explorer 5.0 or higher and uses standard Microsoft navigation techniques.

> ***Note:*** For the web Interface to be correctly displayed, a PC with a resolution of at least 800x600 and a color depth of at least 256 colors should be used.

The web interface allows you to configure and monitor CICMs through a set of web pages. Web pages are hosted on the CICM-EM. They offer configuration and status options to the administrator. These web pages are password protected and can also be accessed from a remote web enabled terminal.

The web interface is made up of two basic components: the left menu of commands and the context panel with dynamic displays and more commands.

The left menu is arranged upon installation to offer full administration of the CICM. For example, configuration and status web pages that are applicable to a particular CICM can be selected from the CICM menu.

LMM Interface

The Line Maintenance Manager (LMM) Interface on the CS2K is the primary interface between administration personnel and the CS2K. The LMM Interface is used to perform administrative and maintenance tasks on the CS2K, including:

- General maintenance
- Network management
- Operational measurements
- Service analysis
- Trunk tests

- Data modification
- Line tests

Refer to the CS2K documentation suite for detailed procedures on the LMM Interface.

CICM SNMP agent

Simple Network Management Protocol (SNMP) is an industry standard management interface. An SNMP agent provides a standard interface for status monitoring and fault reporting.

The CICM provides an SNMP interface for remote status monitoring. Each CICM node will send SNMP traps to a set of management systems when specific events occur.

An SNMP browser can be used to view the standard MIB-2 mibs as well as the Nortel specific CICM mib.

CICM WMI agent

WMI is a management interface from Microsoft, and is a standard component of the NT-embedded operating system. The WMI management system provides the capability to monitor the status of the CICMs. The WMI Agent does not need configuration.

WMI management systems are available from companies such as Hewlett Packard.

Security and administration procedures

Security and administration procedures are performed by means of the Element Manager web interface, a Telnet connection to the Administration LAN, and the Microsoft desktop. The procedures are divided into:

- User administration procedures
- CICM-EM web pages procedures

User administration procedures

This section provides procedures for the administration of user accounts on the CICM-EM, including the administration of user and administrator privileges. It does not address CICMs.

Since the standard operating system on CICM-EMs is Windows 2000, these procedures are written for a Windows 2000 CICM-EM. However, Windows NT is also supported on legacy EMs.

Assign/Remove administrator privileges

There are two privilege levels for users: user privileges and administrator privileges.

User privileges applies by default to all new users, who are put into the Users group automatically upon creation.

A user is assigned administrator privileges by adding them to the Administrator group. Administrator privileges are removed by removing the user from the Administrator group.

The user account “Administrator” that is automatically created upon EM configuration is set up as a member of the Administrator’s group.

The table User and administrator privileges on page 13 compares the two privilege levels.

Table 1 User and administrator privileges

Operation	User Privileges	Administrator Privileges
Logon locally	Given by default. This privilege can be removed by using the User Rights Assignment in the Local Security Settings program.	Given by default. Can be removed using the User Rights Assignment in the Local Security Settings program.
Telnet	Yes	Yes
FTP	Yes	Yes
CICM web page access	Yes	Yes
Certain operations such as installing some types of software, changing network settings, etc.	Restricted	Yes
Running **preboot** or **swupgrade** on the EM	No	Yes
Change other user’s passwords	No	Yes

Only a user with administrator privileges can perform this procedure to assign or remove administrator privileges.

Procedure 1 Assign/Remove administrator privileges

At the EM MS2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

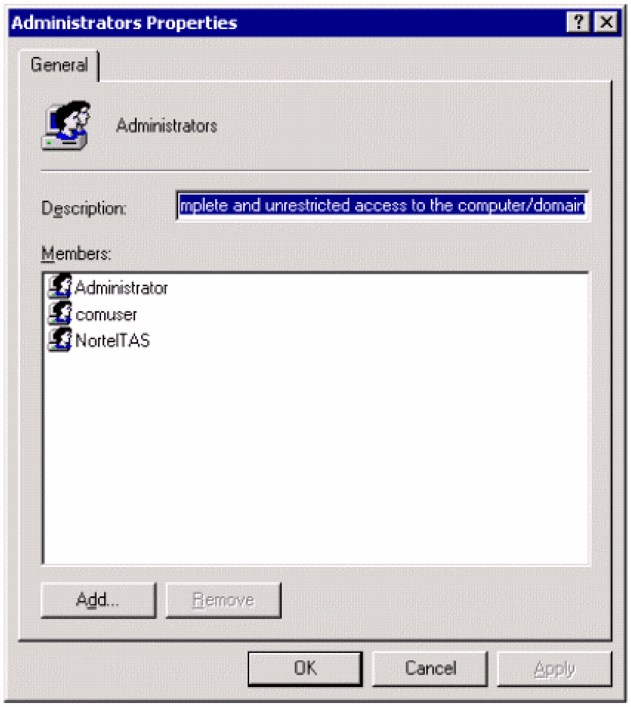
2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 Expand the **Local Users and Groups** file, and then the **Groups** file.

4 Double-click on **Administrators** from the list of groups in the right window.

Response: The Administrator's Properties dialog box opens with a list of the Administrator's group members.



Administrators Properties

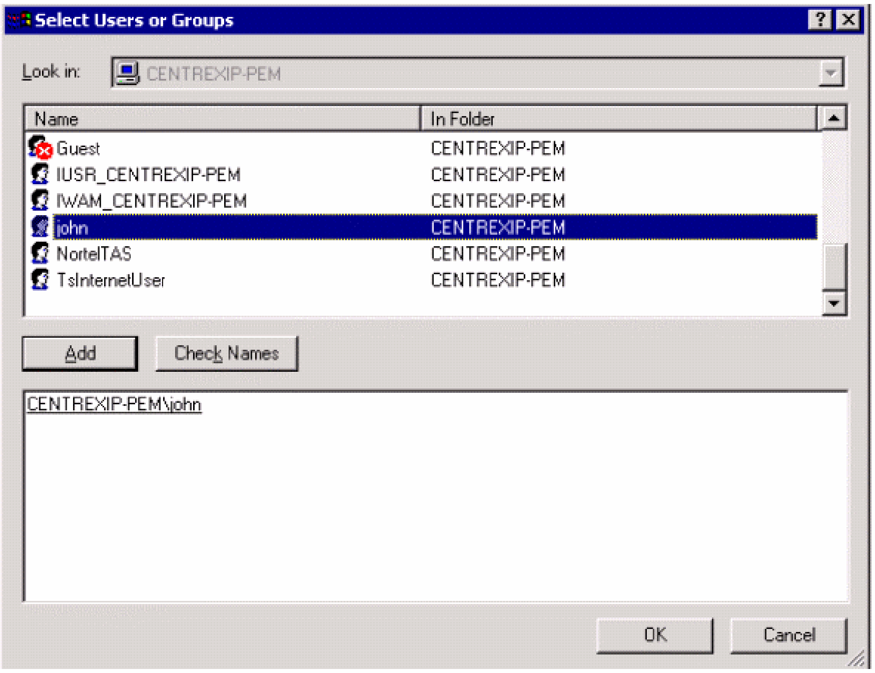
Description: mplete and unrestricted access to the computer/domain

Members:
Administrator
comuser
NortelTAS

5 To add a user to the Administrator group and assign them administrator privileges:

a In the Administrator's Properties window, click on the **Add** button

Response: The Select Users or Groups dialog box opens.



Look in: CENTREXIP-PEM

Name	In Folder
Guest	CENTREXIP-PEM
IUSR_CENTREXIP-PEM	CENTREXIP-PEM
IWAM_CENTREXIP-PEM	CENTREXIP-PEM
john	CENTREXIP-PEM
NortelTAS	CENTREXIP-PEM
TsInternetUser	CENTREXIP-PEM

CENTREXIP-PEM\john

b Search for and select the user to add from the list in the top half of the dialog box, or type the username into the bottom window of the dialog box,

c Then click on the **Add** button.

Response: The name added moves to the bottom half of the dialog box.

d Continue to select and add until you have completed your list,

e Then click **OK** to save your changes.

6 To remove a user's administrator's privileges:

a From the **Administrator's Properties** window's list of administrators, click on the user name to remove,

b Then click on the **Remove** button.

c Continue to remove user names until complete,

d Then click on **OK** to save your changes.

7 This procedure is complete.

Create new users

Use this procedure to create new users on the CICM EM. Only a user with administrator privileges can perform this procedure.

All new users are automatically assigned user privileges. To assign administrator privileges, first create the user, then perform the *Assign Administrator Privileges* procedure below.

Procedure 2 Create new users

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > **Programs** > **Administrative Tools** > **Computer Management**

3 In the Computer Management window, expand the **Local Users and Groups** file by double-clicking on this file.

Response: The Users and Groups sub-folders are displayed in the left window.

4 Click on the **Users** folder.

Response: The right window displays the contents of the Users folder.

5 Click on **Action**, then **New User**.

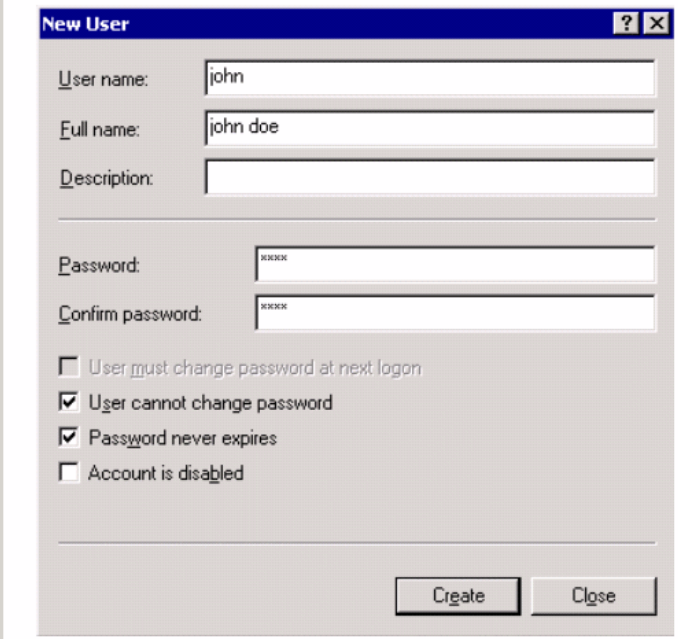
Response: A New User dialog box opens.

6 Datafill the New User dialog box:

a Enter the username and password for the new user.

b Check the boxes as shown in the following figure.

Note: The check boxes normally should be set as shown in the following figure. To set password expiration, see the procedure Set password expiry.



User name: john

Full name: john doe

Description:

Password: ****

Confirm password: ****

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

7 Click the **Create** button.

Response: The New User dialog box closes and the new user account appears in the Computer Management window's list of users.

8 This procedure is complete.

Delete or rename a user

Use this procedure to delete or rename a user account. Only a user with administrator privileges can perform this procedure.

Procedure 3 Delete or rename a user

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

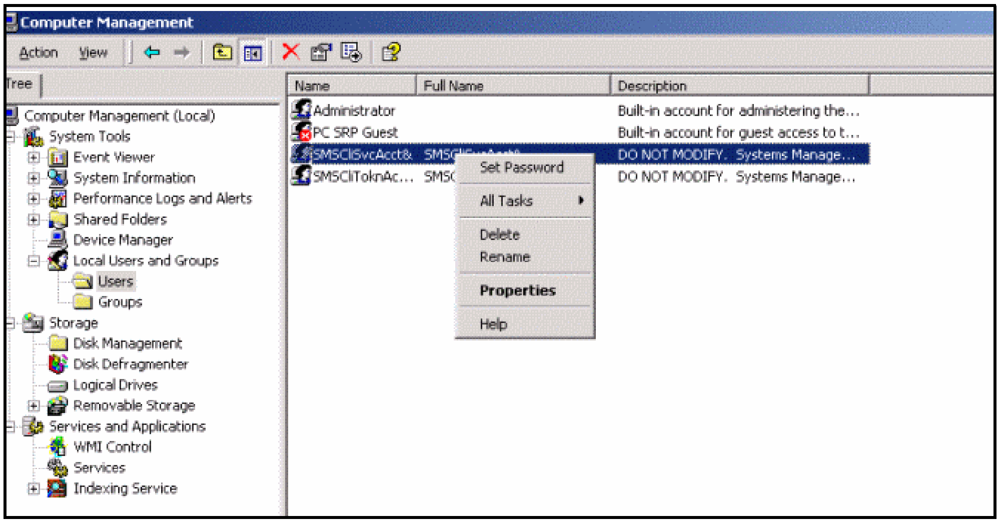
3 In the Computer Management window, expand the **Local Users and Groups** file by double-clicking on this file.

4 Click on the **Users** folder.

Response: The right window displays the contents of the Users folder.

5 From the list of users in the right window, right-click on the user to delete or rename, then

- **a** To delete the user, choose **Delete** from the pop-up menu.
- **b** To rename the user, choose **Rename** from the pop-up menu, then enter the new name and press **Enter**.



Name	Full Name	Description
Administrator		Built-in account for administering the...
PC SRP Guest		Built-in account for guest access to t...
SMSCliSvcAcct&	SMSC	DO NOT MODIFY. Systems Manage...
SMSCliToknAc...	SMSC	DO NOT MODIFY. Systems Manage...

6 This procedure is complete.

Disable the Telnet service

Use this procedure to disable the Telnet service. This will stop all users from using it. Only a user with administrator privileges can perform this procedure.

Procedure 4 Disable the Telnet service

On the EM MS 2000 desktop

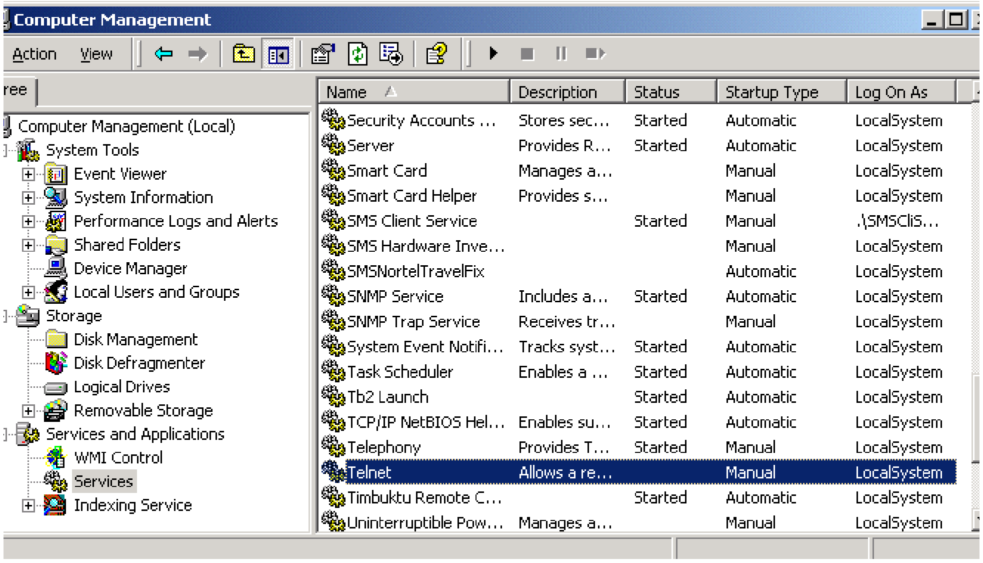
1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Computer Management window by selecting:

Start > Programs > Administrative Tools > Computer Management

3 Expand the **Services and Applications** file.

4 Click on **Services**.

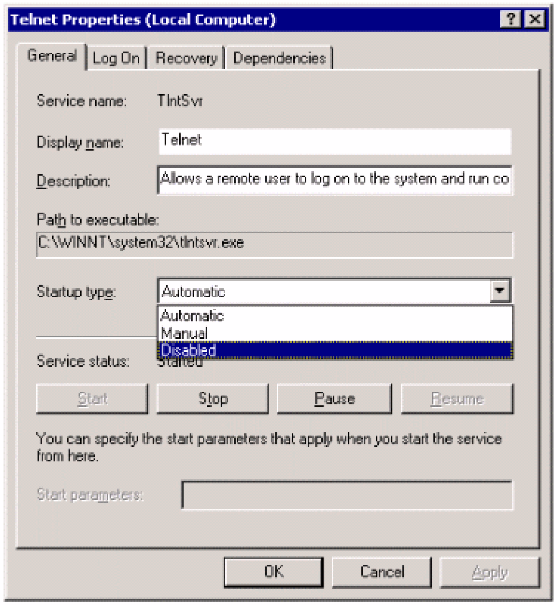


Computer Management (Local)
- System Tools
  - Event Viewer
  - System Information
  - Performance Logs and Alerts
  - Shared Folders
  - Device Manager
  - Local Users and Groups
- Storage
  - Disk Management
  - Disk Defragmenter
  - Logical Drives
  - Removable Storage
- Services and Applications
  - WMI Control
  - Services
  - Indexing Service

Name	Description	Status	Startup Type	Log On As
Security Accounts ...	Stores sec...	Started	Automatic	LocalSystem
Server	Provides R...	Started	Automatic	LocalSystem
Smart Card	Manages a...		Manual	LocalSystem
Smart Card Helper	Provides s...		Manual	LocalSystem
SMS Client Service		Started	Manual	.\SMSCliS...
SMS Hardware Inve...			Manual	LocalSystem
SMSNortelTravelFix			Automatic	LocalSystem
SNMP Service	Includes a...	Started	Automatic	LocalSystem
SNMP Trap Service	Receives tr...		Manual	LocalSystem
System Event Notifi...	Tracks syst...	Started	Automatic	LocalSystem
Task Scheduler	Enables a ...	Started	Automatic	LocalSystem
Tb2 Launch		Started	Automatic	LocalSystem
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	LocalSystem
Telephony	Provides T...	Started	Manual	LocalSystem
Telnet	Allows a re...		Manual	LocalSystem
Timbuktu Remote C...		Started	Automatic	LocalSystem
Uninterruptible Pow...	Manages a...		Manual	LocalSystem

5 In the list in the right window, double-click on the **Telnet** service.

The Telnet Properties dialog box opens.



Service name: TlntSvr

Display name: Telnet

Description: Allows a remote user to log on to the system and run co

Path to executable:
C:\WINNT\system32\tlntsvr.exe

Startup type: Automatic
Automatic
Manual
Disabled

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Change the **Startup type** to disabled, then click the **Stop** button, then click **OK** to save the changes.

7 This procedure is complete.

Open the Computer Management tool

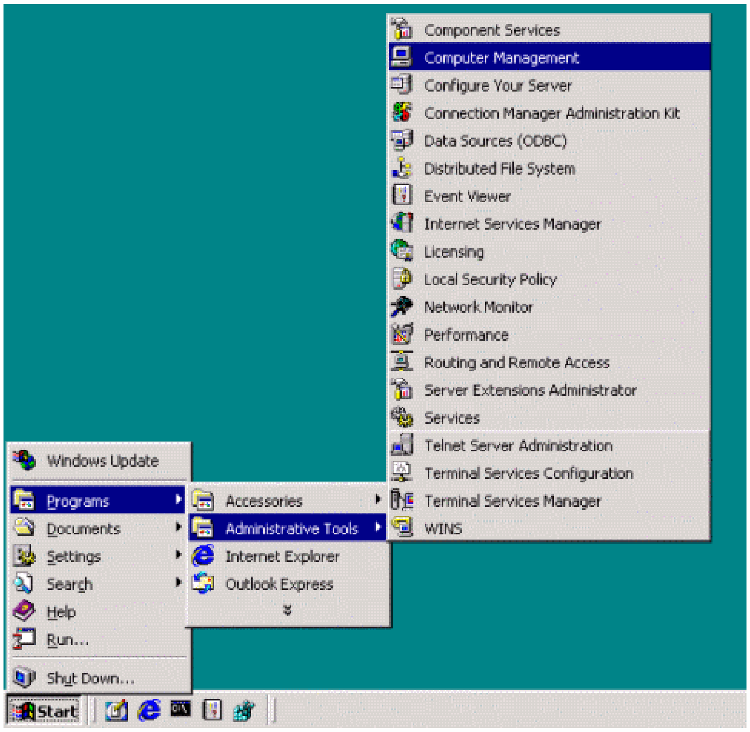
The User Administration procedures use the Computer Management tool, which is a program on Windows 2000 that allows various tasks to be performed, including the management of users. The following procedure demonstrates how to access this tool.

Procedure 5 Open the Computer Management tool

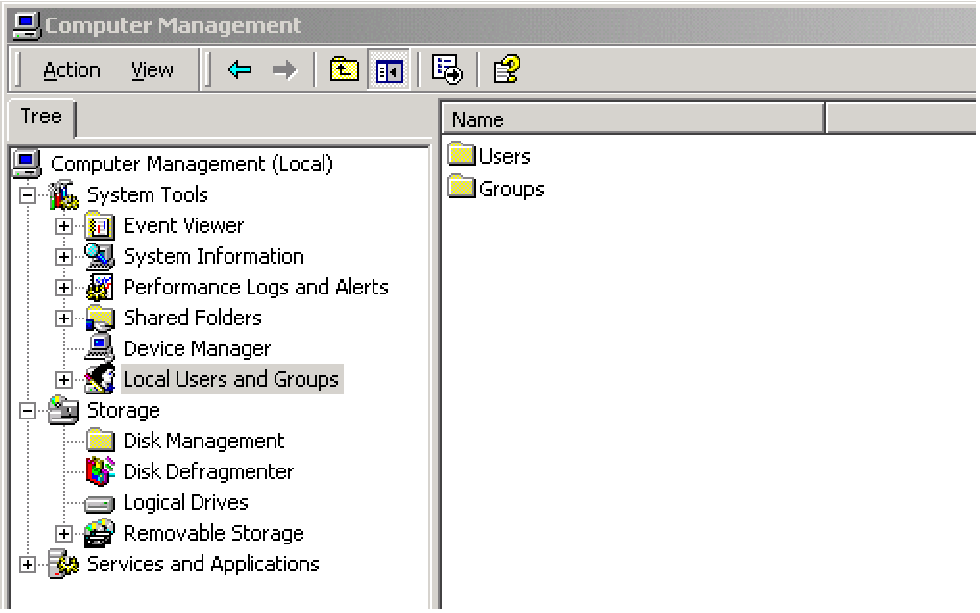
At the EM MS 2000 desktop

1 From the Microsoft Windows Start menu, select **Programs**, then **Administrative Tools**, then **Computer Management**:

Start > Programs > Administrative Tools > Computer Management



Response: The Computer Management window opens.



2 This procedure is complete.

Prevent user logon to local EM

Use this procedure to prevent a particular user from logging on locally to the EM. Users with or without administrator privileges can both be denied logon privileges. Only a user with administrator privileges can perform this procedure.

Procedure 6 Prevent user logon to local EM

On the EM MS 2000 desktop

1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Local Security Settings window by selecting:

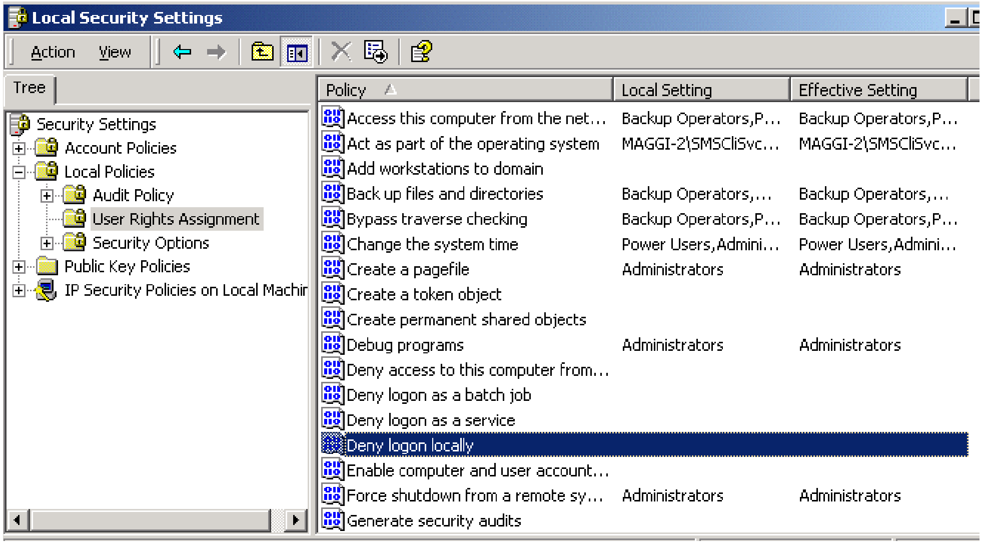
Start > Programs > Administrative Tools > Local Security Policy

Response: The Local Security Settings window opens.

3 In the left window of the Local Security Settings window, expand the **Local Policies** file.

4 Click on **User Rights Assignment**

Response: The right window displays the list of User Rights policies.



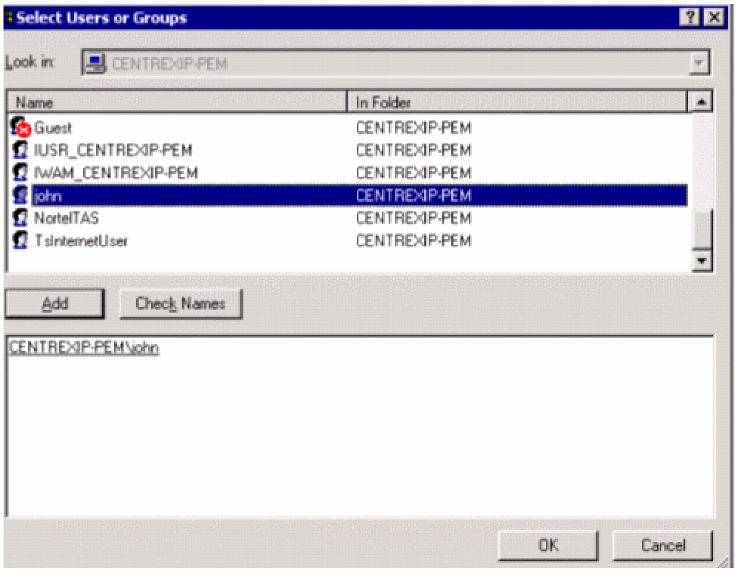
Policy	Local Setting	Effective Setting
Access this computer from the net…	Backup Operators,P…	Backup Operators,P…
Act as part of the operating system	MAGGI-2\SMSCliSvc…	MAGGI-2\SMSCliSvc…
Add workstations to domain		
Back up files and directories	Backup Operators,…	Backup Operators,…
Bypass traverse checking	Backup Operators,P…	Backup Operators,P…
Change the system time	Power Users,Admini…	Power Users,Admini…
Create a pagefile	Administrators	Administrators
Create a token object		
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from…		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account…		
Force shutdown from a remote sy…	Administrators	Administrators
Generate security audits		

5 In the right window, double-click on **Deny logon locally**.

Response: The Local Security Policy Settings dialog box opens to display the current list of users denied logon.

6 Click the Add button in the Local Security Policy Setting dialog box.

*Response: The **Select Users or Groups** dialog box opens.*



Look in: CENTREXIP-PEM

Name	In Folder
Guest	CENTREXIP-PEM
IUSR_CENTREXIP-PEM	CENTREXIP-PEM
IWAM_CENTREXIP-PEM	CENTREXIP-PEM
john	CENTREXIP-PEM
NortelTAS	CENTREXIP-PEM
TsInternetUser	CENTREXIP-PEM

CENTREXIP-PEM\john

7 Search and select from the top window, or type in the bottom window the username to deny access to, then click **OK**.

8 This procedure is complete.

Set password expiry

Microsoft Windows has a build-in method to manage password expiry. This is turned off on the EM to stop certain accounts from expiring, which could affect the running of the CICM. Before turning on password expiration, you must make sure the CICM account is set to never expire.

Only a user with administrator privileges can perform this procedure.

Procedure 7 Set password expiry

On the EM MS 2000 desktop

1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Computer Management tool by selecting:

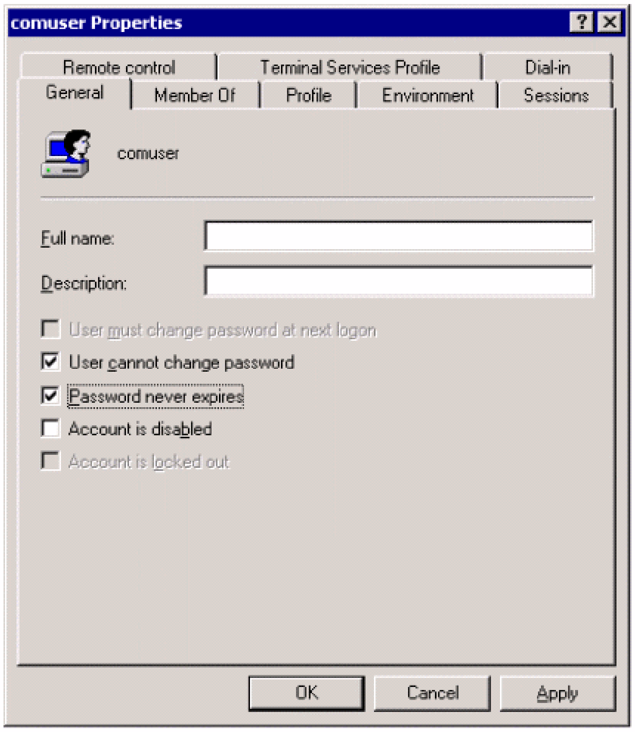
Start > Programs > Administrative Tools > Computer Management

3 In the Computer Management window, expand the **Local Users and Groups** file, then the **User** file.

4 Double-click on the CICM user account from the list of Users.

Note: The CICM user account is site-specific, but it is usually named **comuser**.

*Response: The **<CICM user account> Properties** dialog box opens.*



comuser

Full name:

Description:

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

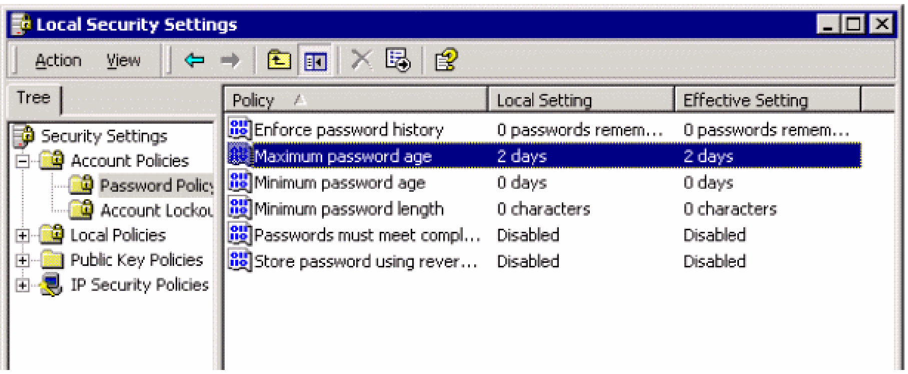
□ Account is locked out

5 In the **user Properties** dialog box, check the **User cannot change password** and **Password never expires** options, then click **OK**.

6 To turn on password expiry, it is necessary to first change a system setting. From the Microsoft Windows Start menu, open the Local Security Settings dialog box by selecting:

Start > Programs > Administrative Tools > Local Security Policy

Response: The Local Security Settings dialog box opens.



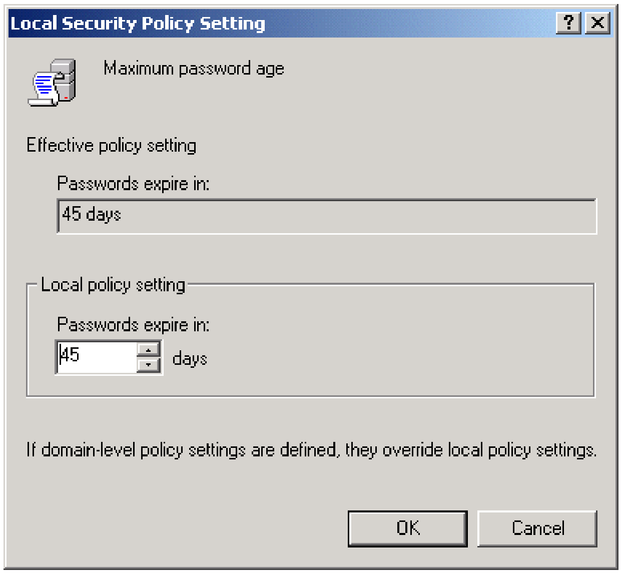
Policy	Local Setting	Effective Setting
Enforce password history	0 passwords remem...	0 passwords remem...
Maximum password age	2 days	2 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet compl...	Disabled	Disabled
Store password using rever...	Disabled	Disabled

7 From the **Local Security Settings** window, expand the **Account Policies** file, then expand the **Password Policy** file.

Response: The right window displays a list of settings that affect passwords.

8 It is recommended to only change the Maximum Password Age setting. To change this setting, double-click on **Maximum Password Age** from the list of settings in the right window of the **Local Security Settings** window.

*Response: The **Local Security Policy Setting** dialog box opens.*



Local Security Policy Setting

Maximum password age

Effective policy setting

Passwords expire in:

45 days

Local policy setting

Passwords expire in:

45 days

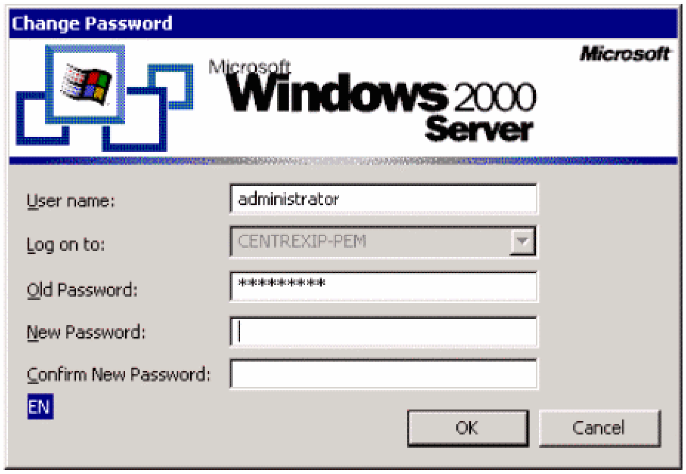
If domain-level policy settings are defined, they override local policy settings.

9 To change the expiry setting:

a To disable expiry, set the Maximum Password Age in the **Passwords expire in:** field to 0, then click **OK**.

b To enable expiry, set the Maximum Password Age in the **Passwords expire in:** field to the number of days you want passwords to be valid, then click **OK**.

10 *(OPTIONAL: FOR EXPIRED PASSWORDS)*
Once a user password is close to the expiry time, when the user logs into the EM the user will receive a warning message telling them to change their password. If their password is not changed and expires, they will not be able to login or use the EM web pages. Upon attempting to login, a **Change Password** dialog box opens, which must be completed before they can proceed.



User name: administrator

Log on to: CENTREXIP-PEM

Old Password: *********

New Password:

Confirm New Password:

11 This procedure is complete.

Set user password

Use either of the following procedures to set or change a user password, or to reset an expired password.

The procedure below changes passwords from the Computer Management tool, and the following procedure changes passwords from the CICM-EM web Interface.

Only a user with administrator privileges can perform these procedures.

Some user account passwords are controlled by IIS and shall not be modified. Refer to Table 3, *Standard User Accounts*, for information on these accounts.

Procedure 8 Set user password (Computer Management tool)

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

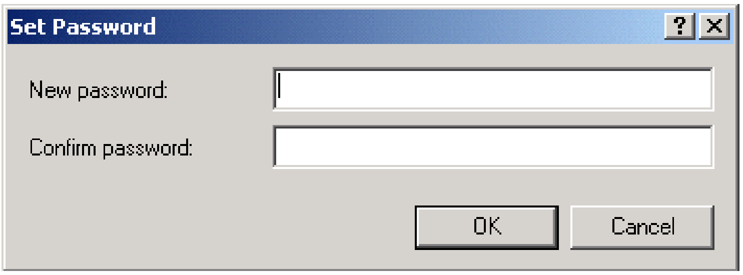
2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 Expand the **Local Users and Groups** file, then the **Users** file.

4 From the list of users in the right window, right-click the user, then select **Set Password** from the pop-up menu.

Response: The Set Password dialog box opens.



5 Enter the new password, confirm it, then press **OK**.

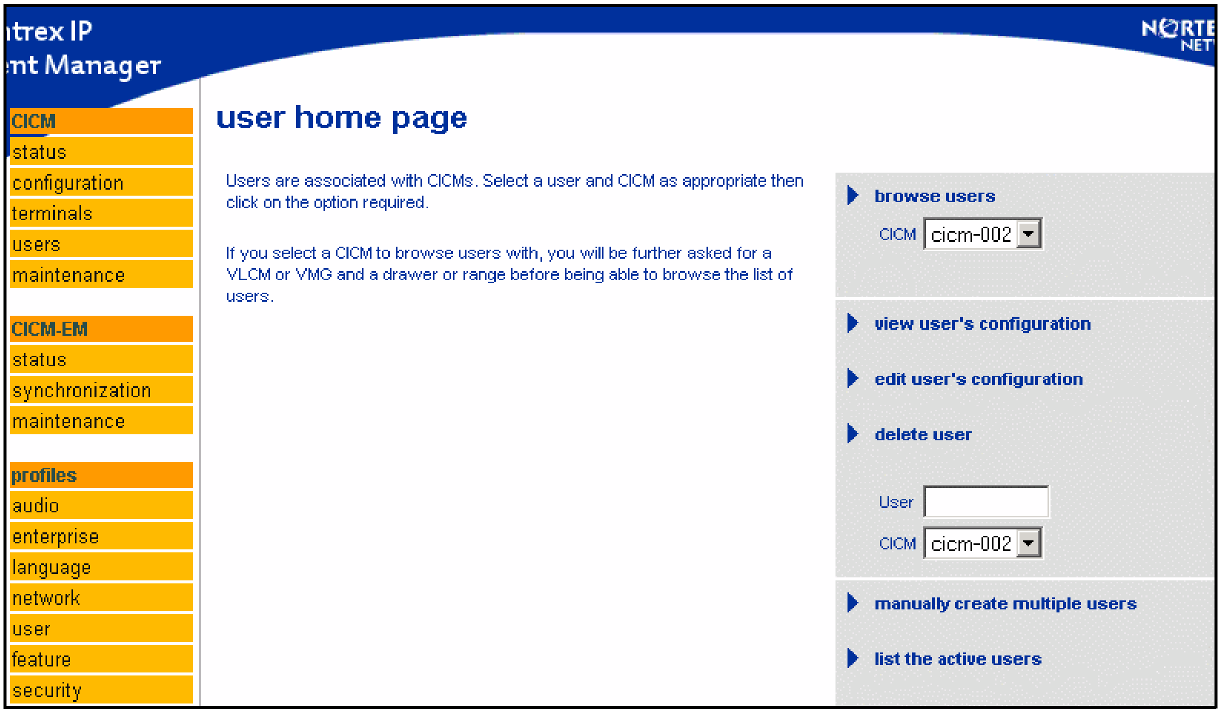
6 This procedure is complete.

Procedure 9 Set user password (CICM-EM web interface)

At the CICM - Element Manager home page

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

Response: The ***user home page*** *opens.*



user home page

Users are associated with CICMs. Select a user and CICM as appropriate then click on the option required.

If you select a CICM to browse users with, you will be further asked for a VLCM or VMG and a drawer or range before being able to browse the list of users.

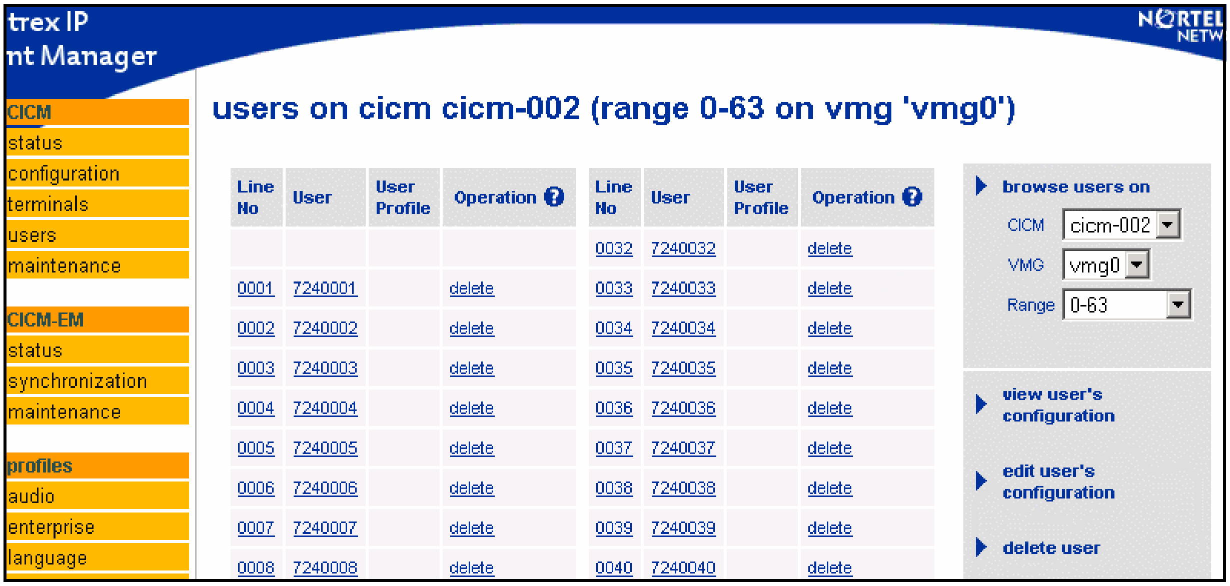
CICM cicm-002

User

CICM cicm-002

2 Select the CICM node identifier from the drop-down menu of **browse users**, then click on **browse users** twice.

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



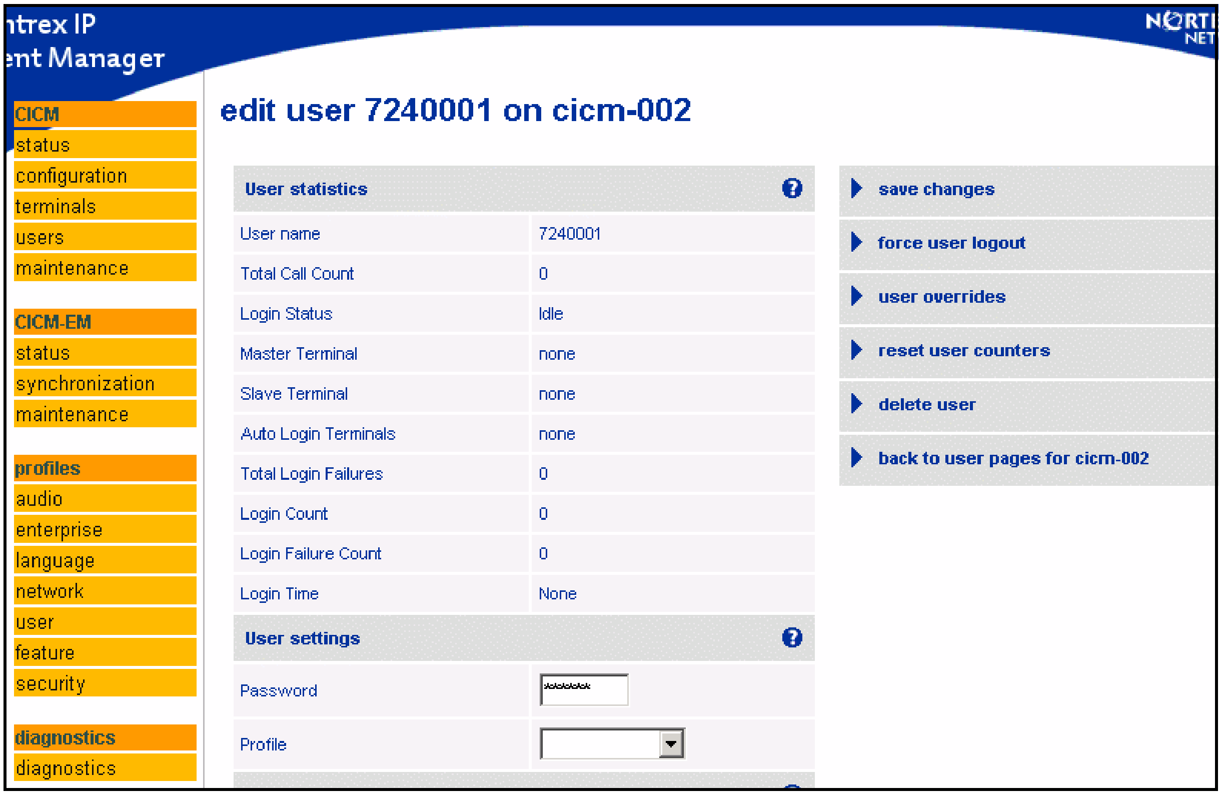
users on cicm cicm-002 (range 0-63 on vmg 'vmg0')

Line No	User	User Profile	Operation	Line No	User	User Profile	Operation
				0032	7240032		delete
0001	7240001		delete	0033	7240033		delete
0002	7240002		delete	0034	7240034		delete
0003	7240003		delete	0035	7240035		delete
0004	7240004		delete	0036	7240036		delete
0005	7240005		delete	0037	7240037		delete
0006	7240006		delete	0038	7240038		delete
0007	7240007		delete	0039	7240039		delete
0008	7240008		delete	0040	7240040		delete

CICM cicm-002
VMG vmg0
Range 0-63

3 From the list of users, click on the user name/ID to change the password for.

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



edit user 7240001 on cicm-002

User statistics	
User name	7240001
Total Call Count	0
Login Status	Idle
Master Terminal	none
Slave Terminal	none
Auto Login Terminals	none
Total Login Failures	0
Login Count	0
Login Failure Count	0
Login Time	None

User settings	
Password	******
Profile	

4 Enter the password in the **Password** field, then click on **save changes**.

> ***Note:*** The user password must be greater than 3 numbers and less than 16 (4-15), numeric characters only. Any more than fifteen numbers entered will be ignored.

Response: A status page opens to confirm the change.

5 This procedure is complete.

View users on a CICM-EM

When the release SN08 CICM software is installed on a CICM-EM, a standard set of user accounts is automatically created. The following table provides a description of these automatically created user accounts.

Table 2 Standard User Accounts

User Name	Purpose
IUSR_CENTREXIP-PEM	A built-in account for anonymous access to Internet Information Services (IIS). This user name and password is created and managed by IIS and as such should not be deleted or modified.
IWAM_CENTREXIP-PEM	A built-in account for Internet Information Services to start out of process applications. This user name and password is created and managed by IIS and as such should not be deleted or modified.
Guest	A built-in account for guest access to the computer. This account is not used by CICM and can be disabled if not needed.
Administrator	A built-in account for administering the computer with full access permissions. It is used for most operations on the CICM-EM. This user password is initially set to “centrexip” but can be changed at any time (see the procedure Set user password (Computer Management tool) or Set user password (CICM-EM web interface)). It is recommended to rename this user name to a less obvious name to enhance security. It is necessary to have an account on the CICM-EM with full privileges so all maintenance can be performed.
(Sheet 1 of 2)	

Table 2 Standard User Accounts (Continued)

User Name	Purpose
NortelTAS	This user account allows Nortel Support access to the CICM-EM. TAS is the Nortel Technical Assistance Service.
CICM account (site specific, but usually called comuser)	This is an important account that the majority of CICM software runs under. It is created on the CICM-EM installation by the preboot command (the install command in 2.4). It should have the same name and password on all CICMs and CICM-EMs that interface with each other. It is not possible to change this account’s password. This account should not be used for general administration.
(Sheet 2 of 2)	

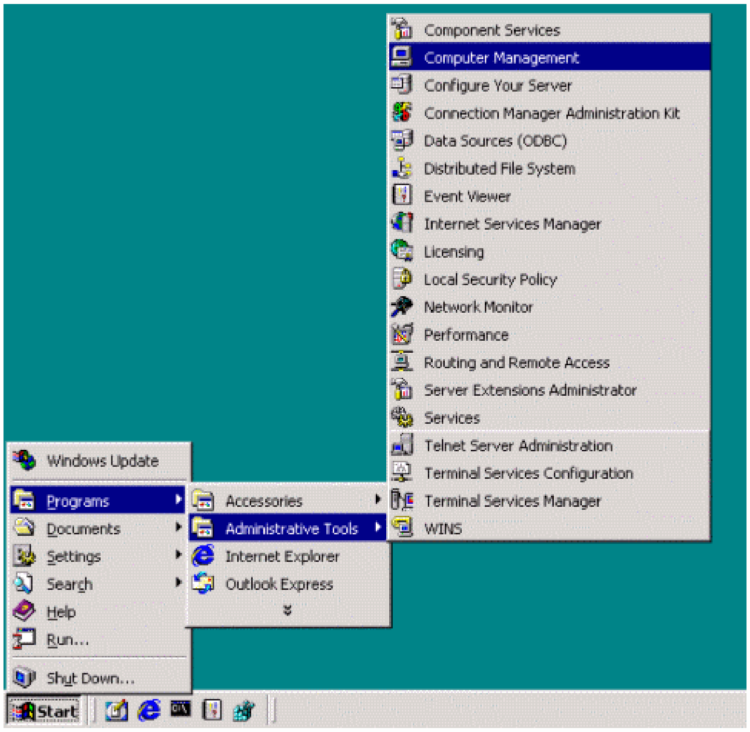
Use the procedure View users on a CICM-EM.

Procedure 10 View users on a CICM-EM

At the EM MS 2000 desktop

1 Open the Computer Management tool from the Microsoft Windows Start menu:

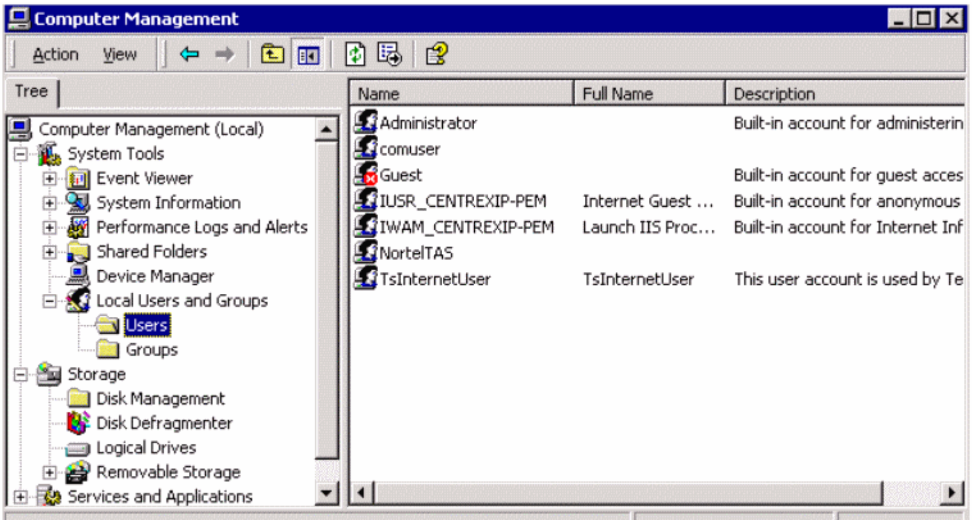
Start > Programs > Administrative Tools > Computer Management



2 In the Computer Management window, expand the **Local Users and Groups** file, then click on the **Users** folder.

Response: On the right of the Computer Management window is displayed a list of all users on the system.

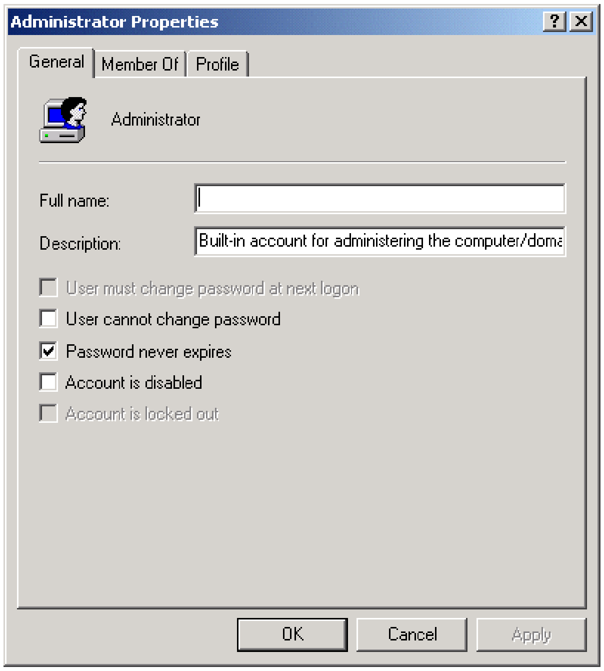
> ***Note:*** *The following figure shows the user accounts that are automatically created. Refer to Table 3 above, Standard User Accounts, for a description of these user accounts.*



Name	Full Name	Description
Administrator		Built-in account for administerin
comuser		
Guest		Built-in account for guest acces
IUSR_CENTREXIP-PEM	Internet Guest ...	Built-in account for anonymous
IWAM_CENTREXIP-PEM	Launch IIS Proc...	Built-in account for Internet Inf
NortelTAS		
TsInternetUser	TsInternetUser	This user account is used by Te

3 To view the properties of a user, double-click on the user name from the list in the right window.

*Response: The **<Username> Properties** window opens.*



Administrator

Full name:

Description: Built-in account for administering the computer/dom

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out

4 This procedure is complete.

CICM-EM web pages procedures

This section provides procedures based on the CICM-EM web pages. For all procedures provided in this document, it is required to use administrator userids and passwords to login to the EM. The procedures are listed alphabetically as follows:

- Accessing the CICM-EM home page
- Adding a CICM
- Backup and restore process
- Clearing security objects
- Deleting a CICM
- Editing CICM nodes
- Monitoring the status of a CICM node
- Performing a sanity check on a CICM
- Setting up secure communications between a CICM server and its clients
- Starting or stopping the CICM service
- Viewing CICM-EM synchronization
- Viewing Language Profiles on a CICM
- Viewing terminal status
- Viewing CICM information at the node level
- Viewing the record of backup sets for a CICM

Accessing the CICM-EM home page

The Element Manager Home page consolidates access to all of the user administration procedures. It is accessed from a PC running Internet Explorer 5.0 or above. From this home page, the following administrative web pages may be accessed:

- CICM home
- CICM - element manager home
- Configuration (described in *CICM Configuration Management*, NN10240-511)
- Terminals (described in *CICM Configuration Management*, NN10240-511)
- Users (described in *CICM Configuration Management*, NN10240-511)
- Maintenance

- Audio Profiles (described in *CICM Configuration Management*, NN10240-511)
- Language Profiles (described in *CICM Configuration Management*, NN10240-511)
- Network Profiles (described in *CICM Configuration Management*, NN10240-511)
- User Profiles (described in *CICM Configuration Management*, NN10240-511)
- CICM upgrades (described in *Upgrading CICM*, NN10230-461)
- synchronization
- diagnostics

Procedure 11 Access CICM home page

At the Internet Explorer address line

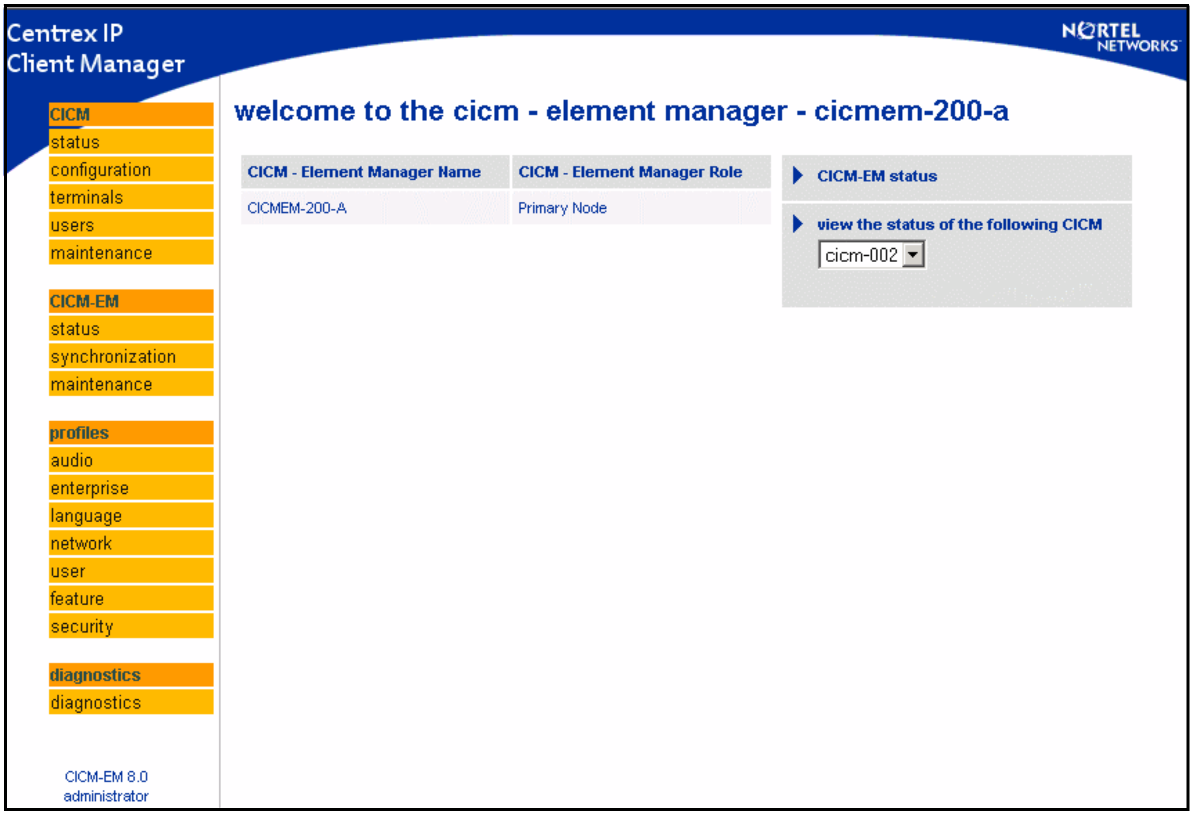
1 Type the IP address of the Element Manager, followed by **/centrexip/**, then press Enter.

Example
http://47.73.240.176/centrexip/

Response: A prompt for the user name and password opens.

2 Type your Administrator user name and password, then press Enter.

Response: The ***welcome to the cicm - element manager - <cicmname>*** *page opens.*



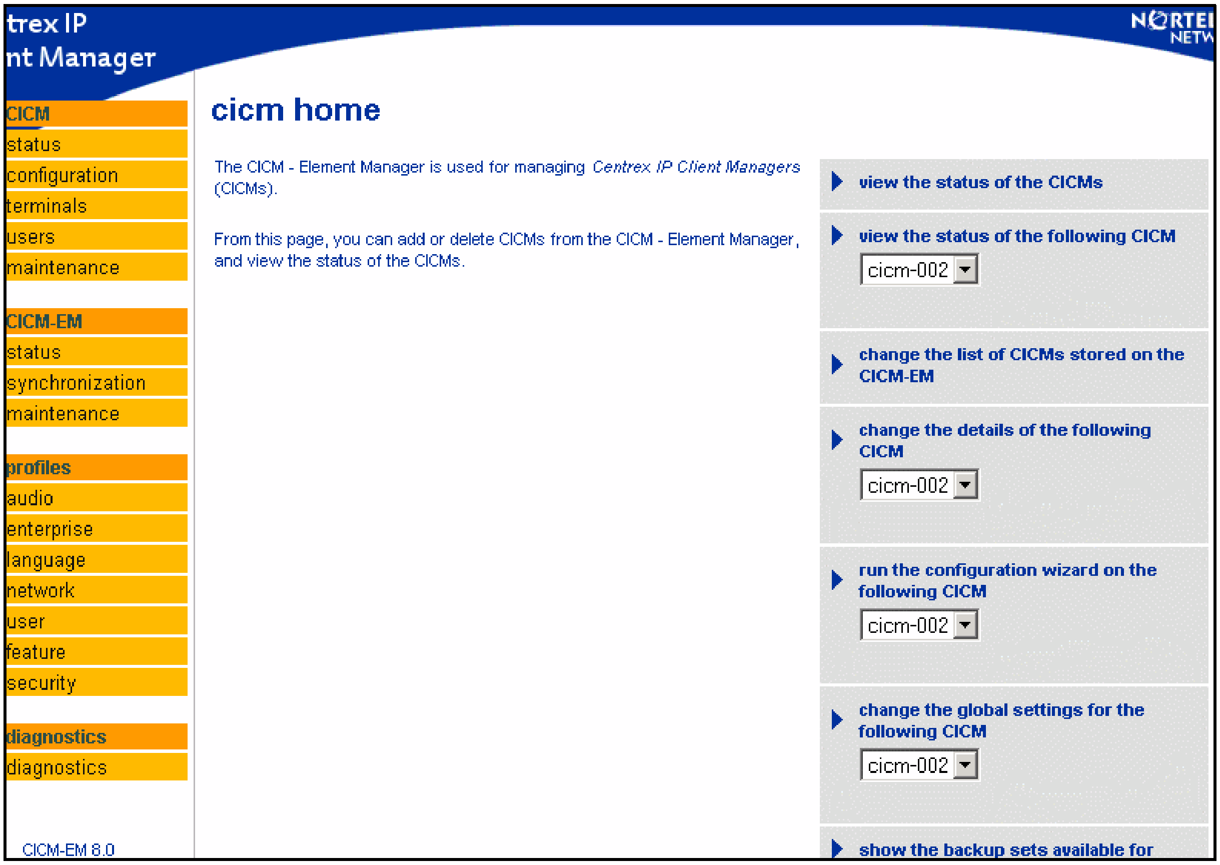
welcome to the cicm - element manager - cicmem-200-a

CICM - Element Manager Name	CICM - Element Manager Role
CICMEM-200-A	Primary Node

view the status of the following CICM: cicm-002

3 Click on **status** in the **CICM** section of the left menu.

Response: The ***cicm home*** *page opens.*



trex IP
nt Manager
NORTEL NETW
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

cicm home

The CICM - Element Manager is used for managing *Centrex IP Client Managers* (CICMs).

From this page, you can add or delete CICMs from the CICM - Element Manager, and view the status of the CICMs.

view the status of the CICMs
view the status of the following CICM
cicm-002
change the list of CICMs stored on the CICM-EM
change the details of the following CICM
cicm-002
run the configuration wizard on the following CICM
cicm-002
change the global settings for the following CICM
cicm-002
show the backup sets available for

4 This procedure is complete.

Adding a CICM

Use this procedure to add a CICM to an Element Manager.

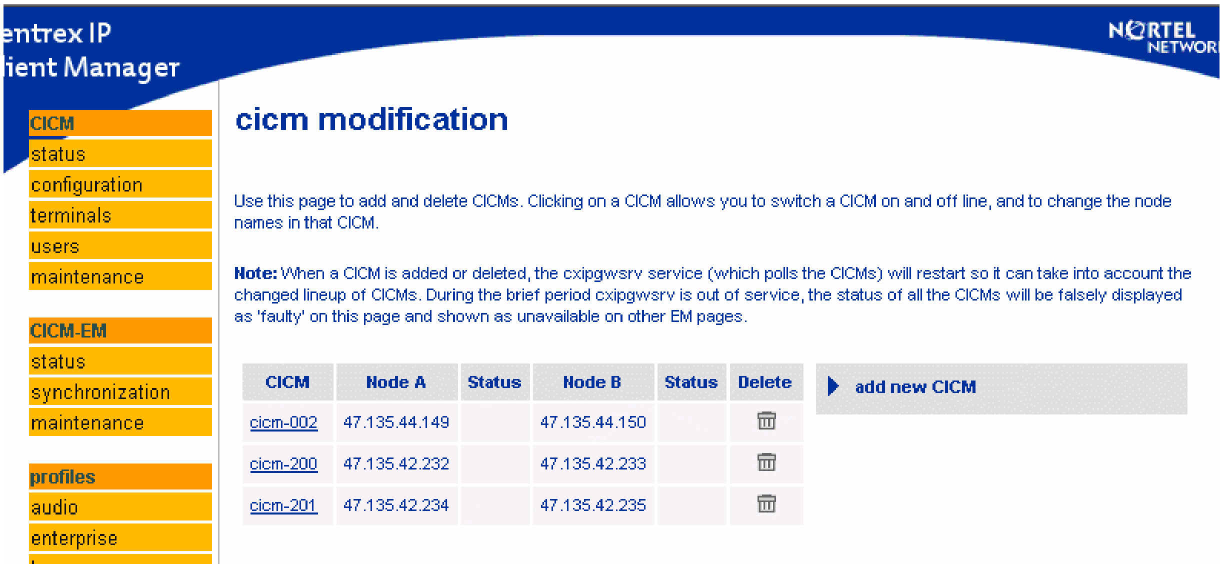
> ***Note:*** When a CICM server is added, it has a default security policy of nonsecure. If you want secure communications between the CICM server and its clients, refer to Setting up secure communications between a CICM server and its clients on page 62.

Procedure 12 Add a CICM

At the cicm home page

1 Click on the **Change the list of CICMs stored on the CICM-EM** text bar on the right menu.

*Response: The **cicm modification** page opens.*



cicm modification

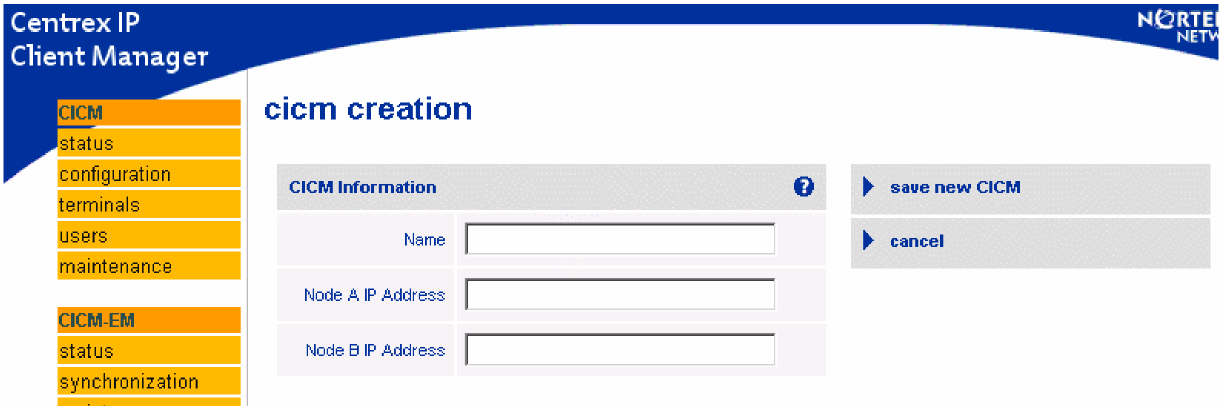
Use this page to add and delete CICMs. Clicking on a CICM allows you to switch a CICM on and off line, and to change the node names in that CICM.

Note: When a CICM is added or deleted, the cxipgwsrv service (which polls the CICMs) will restart so it can take into account the changed lineup of CICMs. During the brief period cxipgwsrv is out of service, the status of all the CICMs will be falsely displayed as 'faulty' on this page and shown as unavailable on other EM pages.

CICM	Node A	Status	Node B	Status	Delete
cicm-002	47.135.44.149		47.135.44.150		🗑
cicm-200	47.135.42.232		47.135.42.233		🗑
cicm-201	47.135.42.234		47.135.42.235		🗑

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

*Response: The **CICM creation** page opens.*



3 Type the CICM identifier in the **Name** field,

Where

CICM name
refers to both sides of the CICM.

Then enter the IP addresses in the **node A IP address** and **node B IP address** fields,

Where

nodes
are the names of each side of a CICM.

Then click on **save new CICM**.

*Response: The **CICM creation** page displays the status of the creation, and confirms completion.*

4 This procedure is complete.

Backup and restore process

With release (I)SN08, the CICM and CICM-EM provide a Backup & Restore functionality for the CICM, by means of scheduled and on-demand backups. This backup feature makes it possible to restore a CICM configuration that was backed up earlier.

This feature is useful in the following types of circumstances:

- When an unexpected system failure of one or both nodes occurs and it is necessary to re-image the CICM node(s) with a fresh load.
- When some parts of the CICM configuration are lost or accidentally deleted, the backup/restore feature makes it possible to avoid manually re-running all the configuration steps.

This feature provides the ability to perform a backup of the CICM data periodically or on demand. This functionality is provided under an individual application on the CICM, controlled by a scheduler and the CICM-EM.

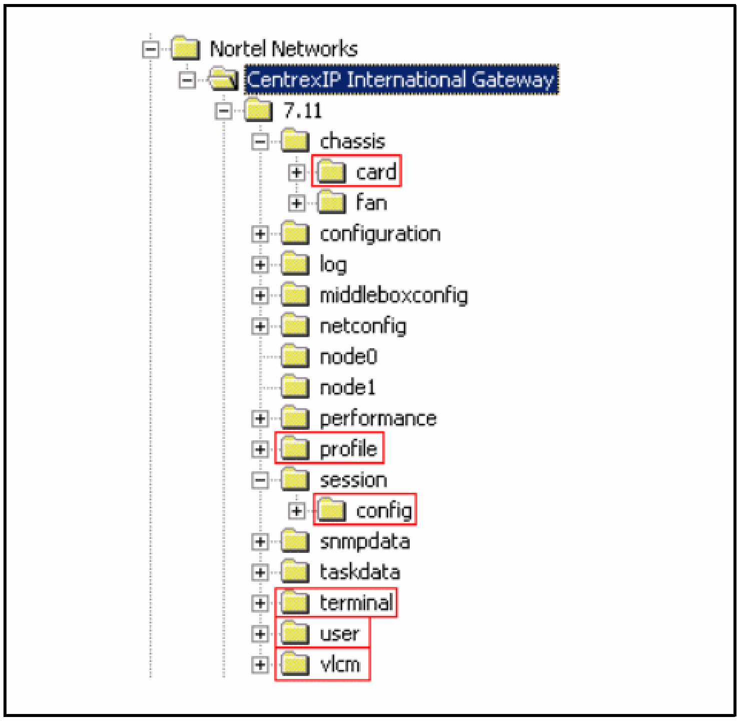
The backup process stores all elements of the MIB Registry that are considered to be static data, and that are directly relevant to the configuration of the CICM.

Although there is no specific restriction on the time when backups can be executed, they can only be restored on CICM nodes mounting the exact same version of the CICM software.

The configuration data to be copied falls into the following categories:

- virtual media gateways
- user configurations, including passwords, locality preferences, and contacts
- terminals, including locality preferences and the auto-login preference
- lines, including their features
- profiles of end-point equipment, including the global profile overrides stored on the CICM

The MIB branches copied during the backup process are highlighted in the MIB hierarchy shown in the following figure.



Backups can be created at a regularly scheduled time, or on demand by an operator (for example, prior to a CICM installation). On-demand backups are triggered through the CICM-EM, while scheduled backups will require no manual intervention once configured.

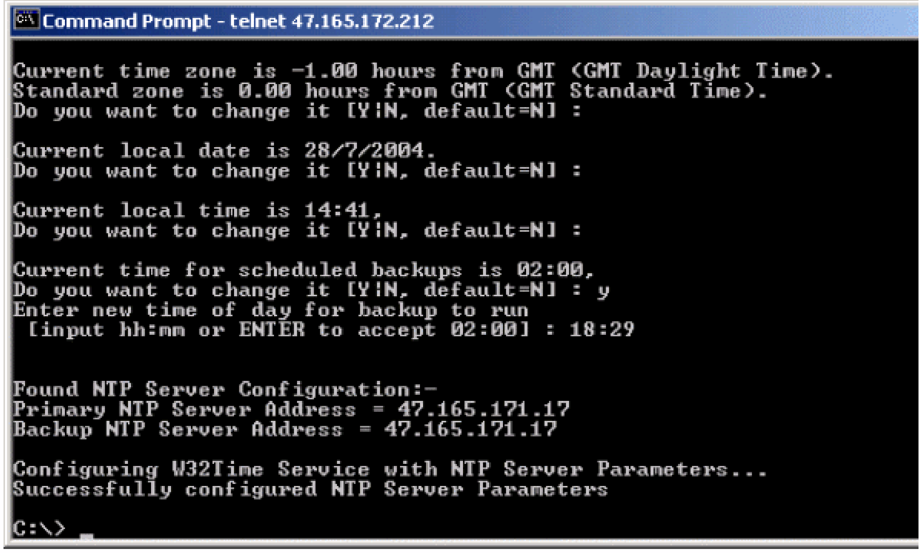
In both scheduled and on-demand backups, the result is an XML file, which is sent to the CICM-EM through anonymous FTP and stored locally in the following folder:
D:\CentrexIP\support\backups\<cicm_node>,
where **<cicm_node>** is the full name of the node.

The node-specific folder is automatically created the first time a backup (of either kind) is run for that node. Although both backups are designed to occupy a limited amount of disk space on the CICM-EM, it is entirely up to the administrator to actually manage the files, for example by moving them periodically to a separate secure location.

Scheduled Backups

Scheduled backups are automatically run daily by each CICM node and require no further intervention by the operator once they have been successfully set up during the initial installation of software.

The **time** portion of **preboot** (also accessible by typing **preboot time /interactive**) has been expanded to prompt for a base time for scheduled backups, expressed in hours and minutes. The default value for the base time is 2AM. The command line interface is illustrated in the following figure:



```
Current time zone is -1.00 hours from GMT (GMT Daylight Time).
Standard zone is 0.00 hours from GMT (GMT Standard Time).
Do you want to change it [Y|N, default=N] :

Current local date is 28/7/2004.
Do you want to change it [Y|N, default=N] :

Current local time is 14:41.
Do you want to change it [Y|N, default=N] :

Current time for scheduled backups is 02:00.
Do you want to change it [Y|N, default=N] : y
Enter new time of day for backup to run
 [input hh:mm or ENTER to accept 02:00] : 18:29


Found NTP Server Configuration:-
Primary NTP Server Address = 47.165.171.17
Backup NTP Server Address = 47.165.171.17

Configuring W32Time Service with NTP Server Parameters...
Successfully configured NTP Server Parameters

C:\> _
```

Once the base time has been chosen or the default value confirmed, a new scheduled job is allocated on the CICM to perform the actual backup and then FTP the result to the CICM-EM at the specified time, as can be seen in the figure above. The backup job is designed to send the XML file to the IP address of the master and slave CICM-EMs, alternating between them on a daily basis to ensure a balanced usage of their disk space.

The fixed name for the backup file is

backupconfig_<day>.xml

where **<day>** is the day of the month (for example, **backupconfig_25.xml**). As backup files are automatically overwritten, this naming convention ensures that the master or slave has to store only a limited set of automatic backup files (up to a maximum of 31) for any CICM node it manages.

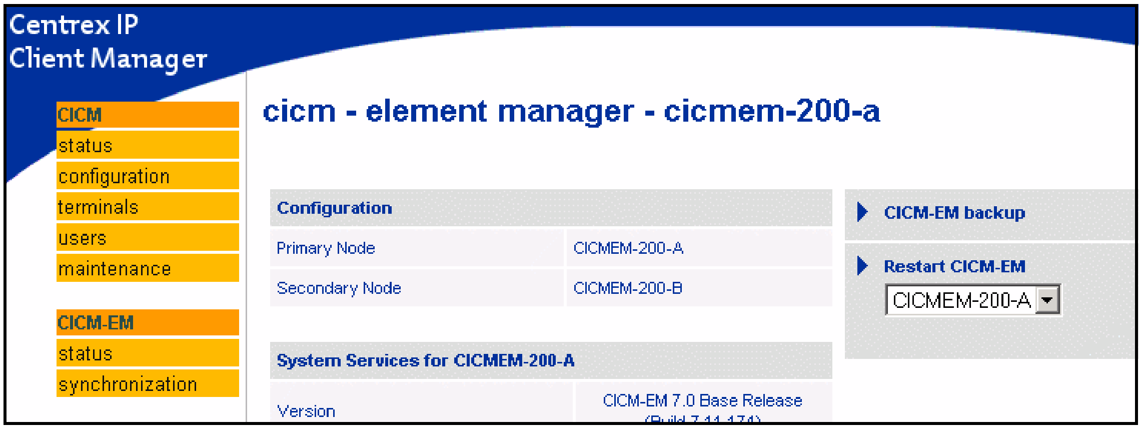
Scheduled backups can be turned off, if necessary. By running the **at** command on the CICM command line, the ID associated with the scheduled job will be output, just as it is automatically done by preboot. Then the following command is entered:

At <task_id> /delete

where **<task_id>** is the ID previously identified.

<u>On demand backups</u>

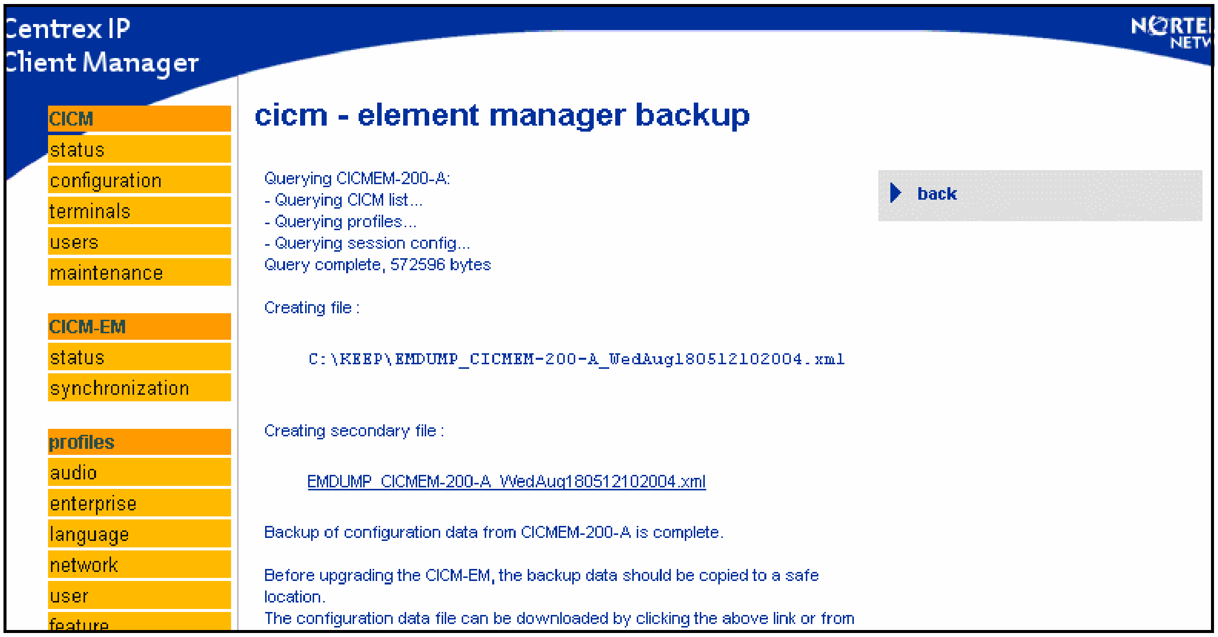
On-demand backups can be initiated at any time from any CICM-EM that manages the given CICM node. It is not necessary that the CICM-EM be the master or slave, just as for scheduled backups. The backup/restore functionality is accessed through the **CICM-EM backup** button, accessed from the CICM-EM home page **cicm - element manager - <cicmem-nnn-x>**, as shown in the following figure.



cicm - element manager - cicmem-200-a

Configuration	
Primary Node	CICMEM-200-A
Secondary Node	CICMEM-200-B
System Services for CICMEM-200-A	
Version	CICM-EM 7.0 Base Release (Build 7.11.174)

This backup action results in he backup page shown in the following figure.



cicm - element manager backup

Querying CICMEM-200-A:
- Querying CICM list...
- Querying profiles...
- Querying session config...
Query complete, 572596 bytes

Creating file :

```
C:\KEEP\EMDUMP_CICMEM-200-A_WedAug180512102004.xml
```

Creating secondary file :

EMDUMP_CICMEM-200-A_WedAug180512102004.xml

Backup of configuration data from CICMEM-200-A is complete.

Before upgrading the CICM-EM, the backup data should be copied to a safe location.
The configuration data file can be downloaded by clicking the above link or from

Once either node has been chosen, a task is run on that CICM node to carry out the backup and FTP the resulting XML file to the CICM-EM, which normally takes a few seconds, depending on the size of the MIB itself. The fixed name for the backup file is:
backupconfig_<day>_em.xml
where **<day>** is the day of the month (for example, **backupconfig_25_em.xml5**). As backup files are automatically

overwritten, this naming convention ensures that the CICM-EM has to store only a limited set of automatic backup files (up to a maximum of 31) for any CICM node it manages, despite the fact that on-demand backups can be triggered an unlimited number of times each day.

Although the backup files are stored in the same directory as the scheduled backups, the naming convention ensures there is no overlap between them. However, it is up to the administrator to make sure that the backup file for a given day is saved to a different location before it is automatically replaced, which happens in the event of another backup being triggered on the same day, or on the same day of a later month.

Restore

Although there is no specific restriction on the time when backups can be executed (whether they are scheduled or on demand), they can only be restored on CICM nodes mounting the exact same version of the CICM software, and specifically only in the two following scenarios:

- Upon accidental loss or deletion of portions of the MIB (on a pair of fully configured CICM nodes)
- Upon fresh re-image of both CICM nodes, after having fully run preboot on one node.

This means that the use of the restore functionality is NOT supported and hence strongly discouraged in the following scenarios:

- Across software upgrades within the same product release (for example, 8.11 to 8.12)
- Software upgrades across two different product releases (for example, 7.11 to release 8.0)

A version check is built into the restore facility purposely to prevent accidental usage of a backup file outside the scope intended by this feature (and specifically across any kind of software upgrade).

Moreover, this functionality does not provide direct support for automated restores of CICM backups. This means that, in order to apply any previously saved configuration, the operator must connect directly to both the CICM-EM and the CICM, as the CICM-EM itself will not include a restore interface.

Specifically, the following two steps must be performed:

- Locate the applicable XML file on the CICM-EM and copy or FTP it to the CICM node
- Telnet to the CICM and run the following command: **cxiprestore <xml_backup_file> /norestart <xml_backup_file>**

or
cxiprestore <xml_backup_file> /restart <xml_backup_file>
where **<xml_backup_file>** is the configuration file,
/norestart is specified to restore on fully configured CICM nodes, and **/restart** is used for freshly re-imaged CICM nodes (following completion of preboot).

In the case the **/restart** option is chosen, the main CICM services will be stopped prior to re-applying the actual data, to be restarted upon completion of the restore operation. Conversely, the **/norestart** option has no impact on the services running at the time the restore is performed.

> ***Note 1:*** For the restore procedure to succeed on freshly re-imaged CICM nodes (that is, when using the **/restart** option), the node being restored must be the only one currently running, which means it must be the Master node of the pair, with no Slave presently connected to the network or switched on. This is essential to ensure that the newly restored MIB content will not be accidentally deleted by a premature synchronization with the mate node, and that it will be properly replicated across following the re-imaging of the Slave at a later stage.
>
> ***Note 2:*** When using the **/restart** option, the restart of the main CICM services will mean that all networks adapters for the node will be re-initialized, and as a result the Telnet connection will be dropped.
>
> ***Note 3:*** Although there are other command line options available for the **cxiprestore** tool, they are not documented here as they are not relevant to this activity, and as such their usage should be avoided.
>
> ***Note 4:*** A version check is built into the restore facility, purposely to prevent accidental usage of a backup file outside the scope intended by this feature (and specifically across any kind of software upgrade).

Clearing security objects

Once a client is connected to a secure CICM server, it has a security object that associates it to that particular CICM server. To move a secure client from one CICM server to another, the first step is to clear the associated security object from the client. This is done through the Reset Security parameter at any one of the following three levels:

- enterprise level
- CICM server level
- client level

The following table shows the impact of setting the Reset Security parameter:

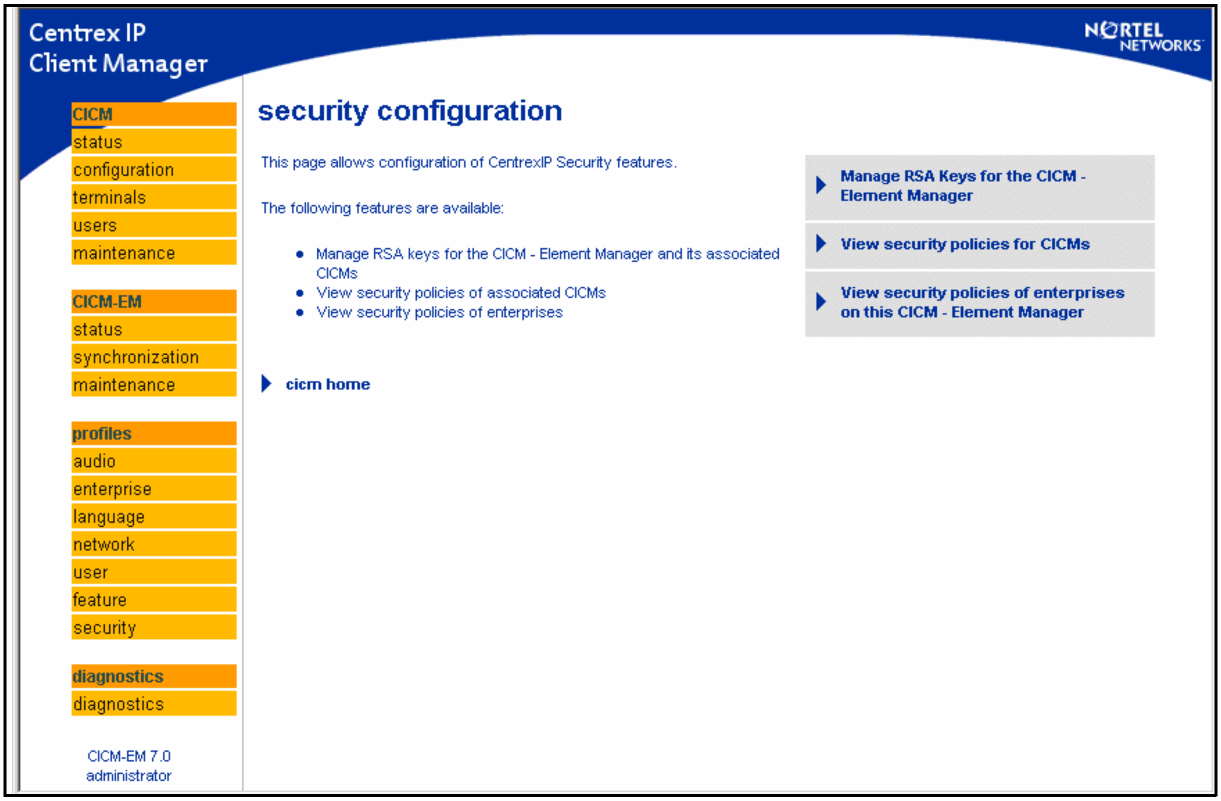
Enterprise	CICM server	Client	Reset Security value	Impact
No	No	No	No	No clients will have their security objects cleared
No	No	Yes	Yes	Only the specific client will have its security objects cleared.
No	Yes	No	Yes	All clients associated with the CICM server will have their security objects cleared.
No	Yes	Yes	Yes	All clients associated with the CICM server will have their security objects cleared.
Yes	No	No	Yes	All clients under the enterprise will have their security objects cleared.
Yes	No	Yes	Yes	All clients under the enterprise will have their security objects cleared.
Yes	Yes	No	Yes	All clients under the enterprise will have their security objects cleared.
Yes	Yes	Yes	Yes	All clients under the enterprise will have their security objects cleared.

Procedure 13 Clear the associated security object from a client

At the Centrex IP Client Manager

1 Click on **security** from the profiles section of the left menu.

Response: The **security configuration** page opens.



security configuration

This page allows configuration of CentrexIP Security features.

The following features are available:

- Manage RSA keys for the CICM - Element Manager and its associated CICMs
- View security policies of associated CICMs
- View security policies of enterprises

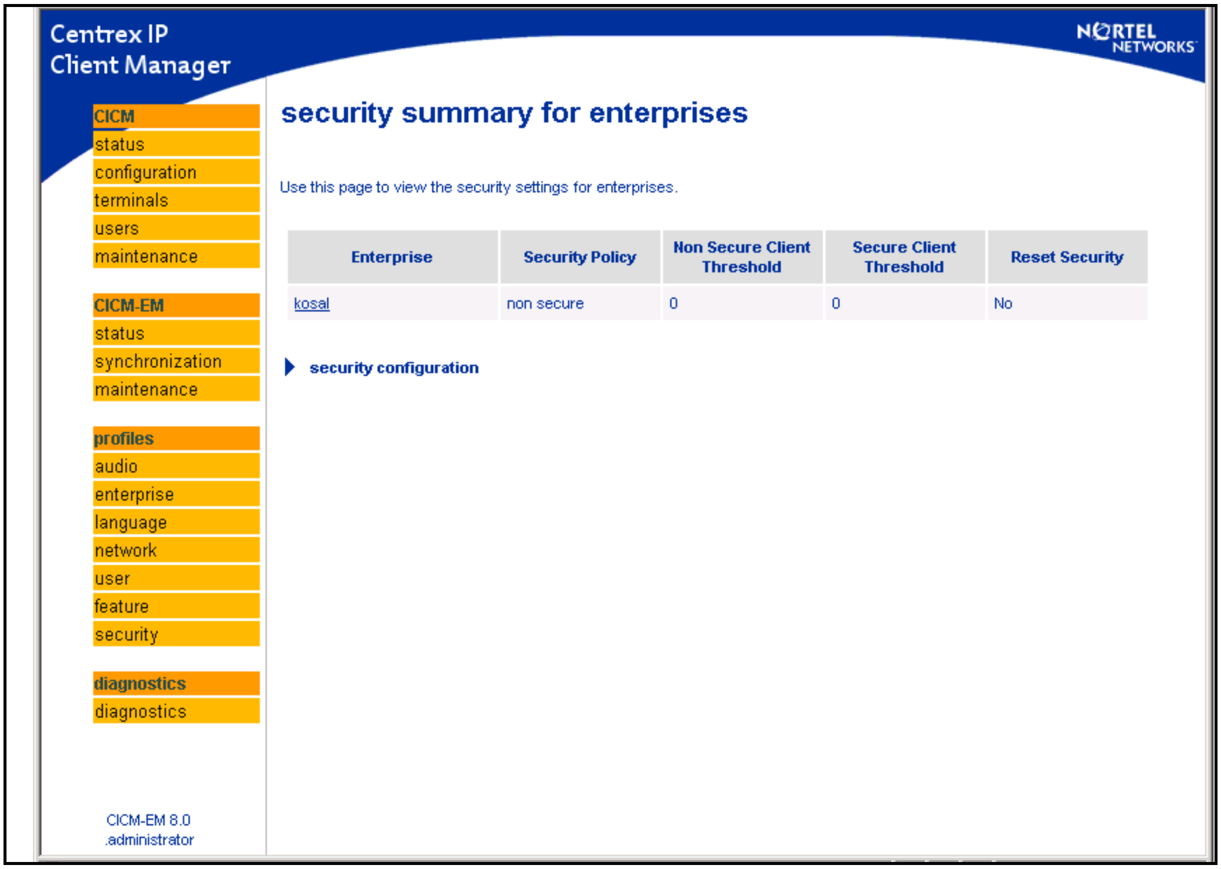
2 Use the following table to determine your next step:

If you want to clear the security object at the	Do
enterprise level	step 3
CICM server level	step 4
client (terminal) level	step 4

3 Clear the security object from all clients associated with CICM servers within an enterprise as follows:

a Click **View security policies of enterprises on this CICM-Element Manager**

Response: The **security summary for enterprises** page opens.



security summary for enterprises

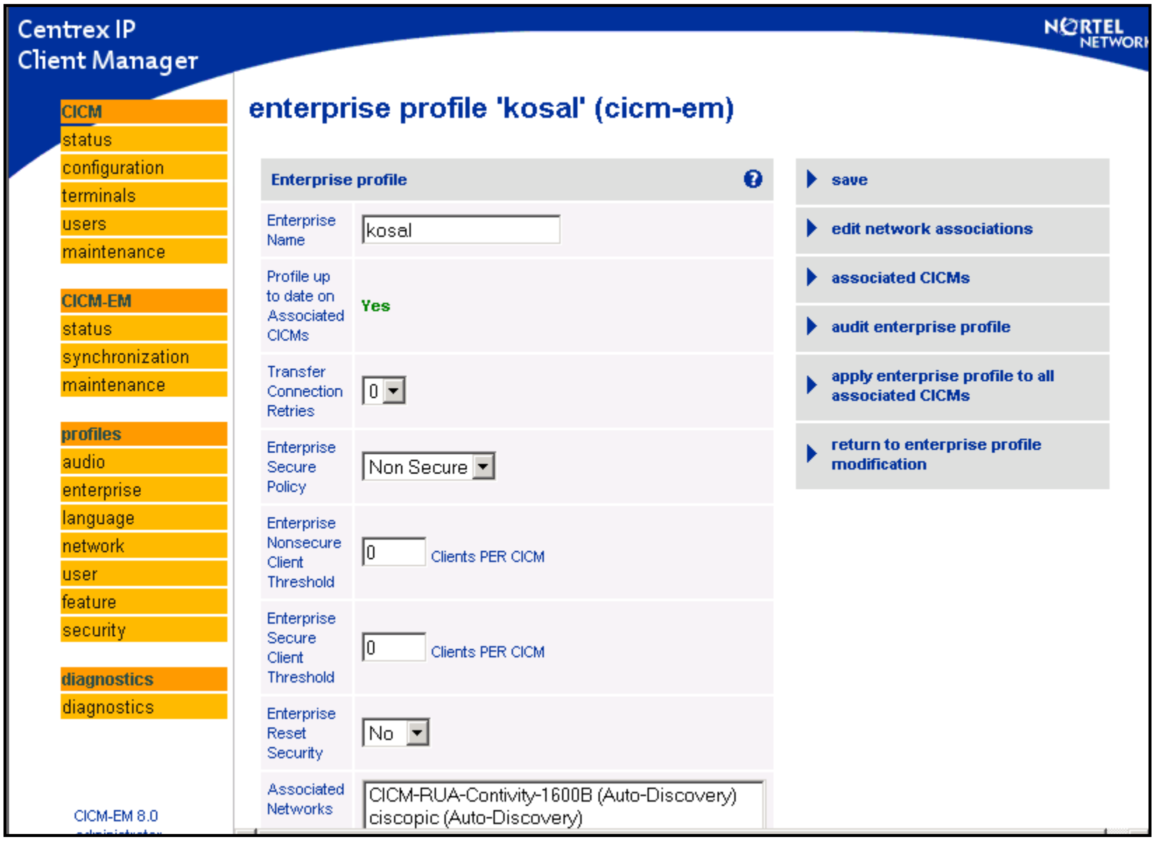
Use this page to view the security settings for enterprises.

Enterprise	Security Policy	Non Secure Client Threshold	Secure Client Threshold	Reset Security
kosal	non secure	0	0	No

security configuration

b Click on an Enterprise link.

Response: The **enterprise profile <enterprise> (cicm-em)** page opens.



enterprise profile 'kosal' (cicm-em)

Enterprise profile	
Enterprise Name	kosal
Profile up to date on Associated CICMs	Yes
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	CICM-RUA-Contivity-1600B (Auto-Discovery) ciscopic (Auto-Discovery)

c Select **Yes** for the Enterprise Reset Security parameter.

d Click on **save**.

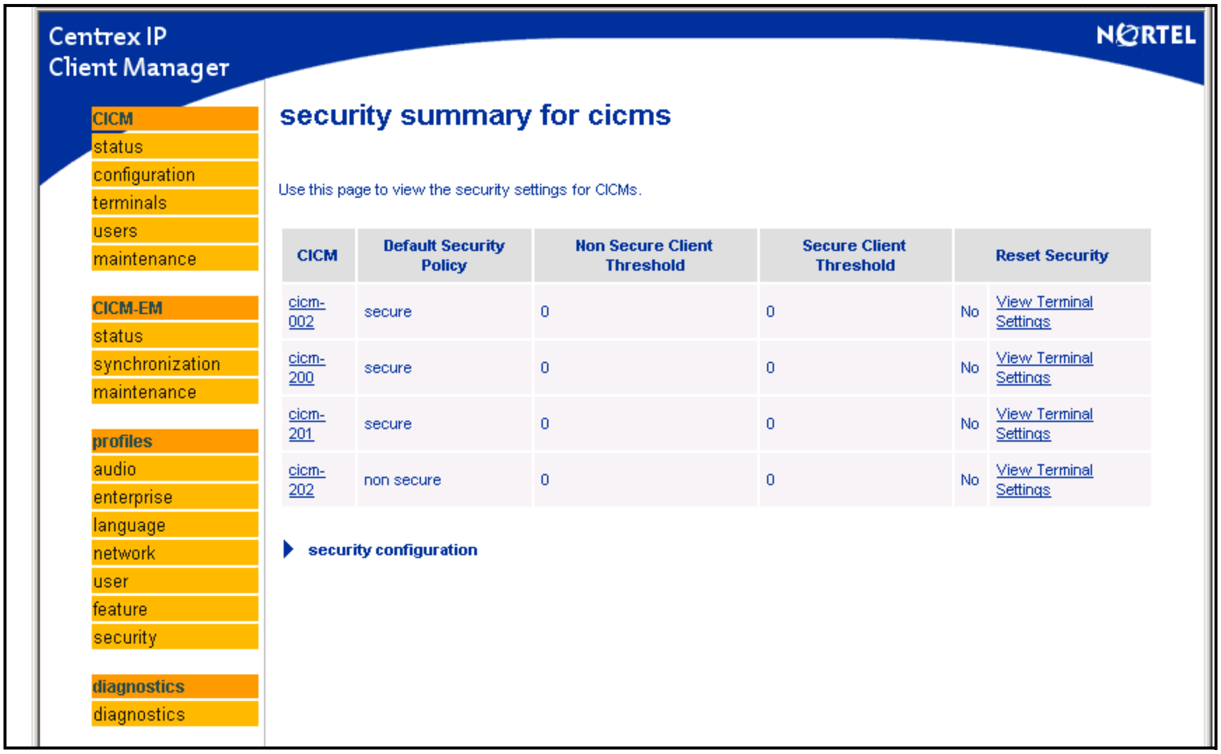
You can now move all the clients associated with each CICM server within the enterprise to other CICM servers.

This procedure is complete.

4 Clear the security object from one or more or all clients associated with a CICM server as follows:

5 Click **View security policies for CICMs**

Response: The **security summary for cicms** page opens.



security summary for cicms

Use this page to view the security settings for CICMs.

CICM	Default Security Policy	Non Secure Client Threshold	Secure Client Threshold	Reset Security	
cicm-002	secure	0	0	No	View Terminal Settings
cicm-200	secure	0	0	No	View Terminal Settings
cicm-201	secure	0	0	No	View Terminal Settings
cicm-202	non secure	0	0	No	View Terminal Settings

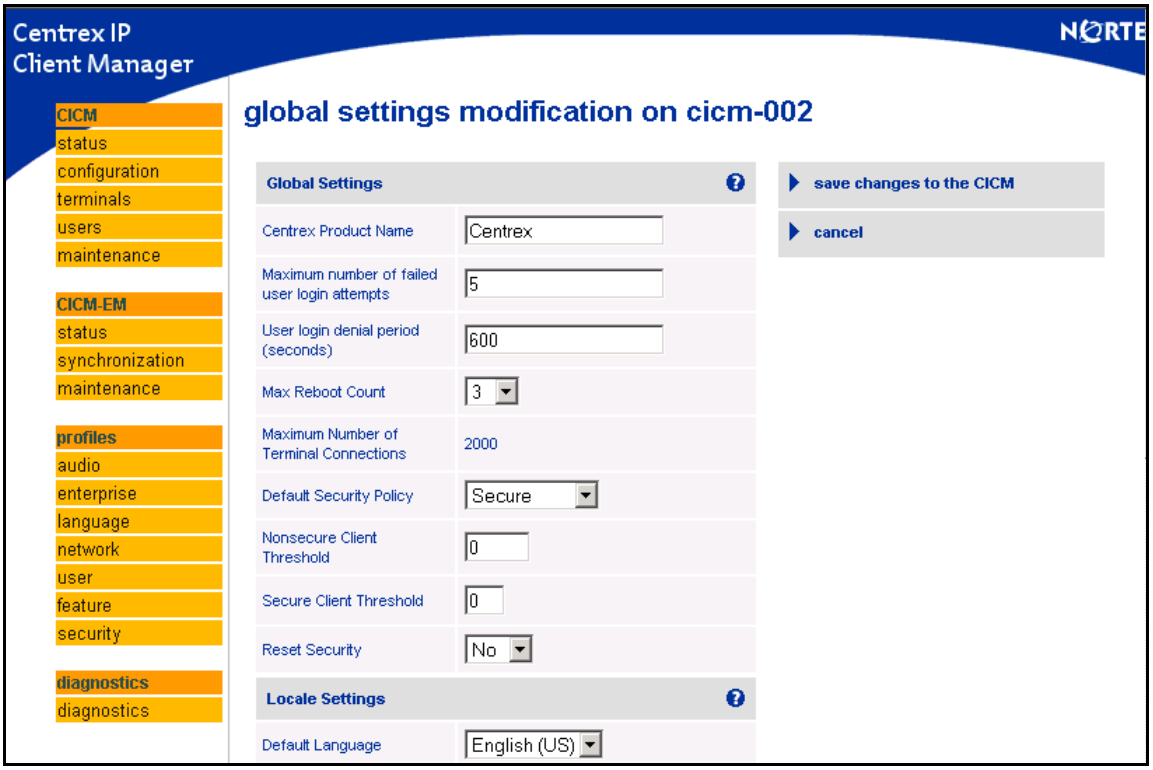
security configuration

If you want to clear the security object at the	Do
CICM server level	step 6
client (terminal) level	step 7

6 Clear the security object from all clients associated with a CICM server as follows:

a Click on a CICM server link.

Response: The **global settings modification on <cicm>** page opens.



global settings modification on cicm-002

Global Settings	
Centrex Product Name	Centrex
Maximum number of failed user login attempts	5
User login denial period (seconds)	600
Max Reboot Count	3
Maximum Number of Terminal Connections	2000
Default Security Policy	Secure
Nonsecure Client Threshold	0
Secure Client Threshold	0
Reset Security	No
Locale Settings	
Default Language	English (US)

b Select **Yes** for the Reset Security parameter.

c Click on **Save changes to the CICM**.

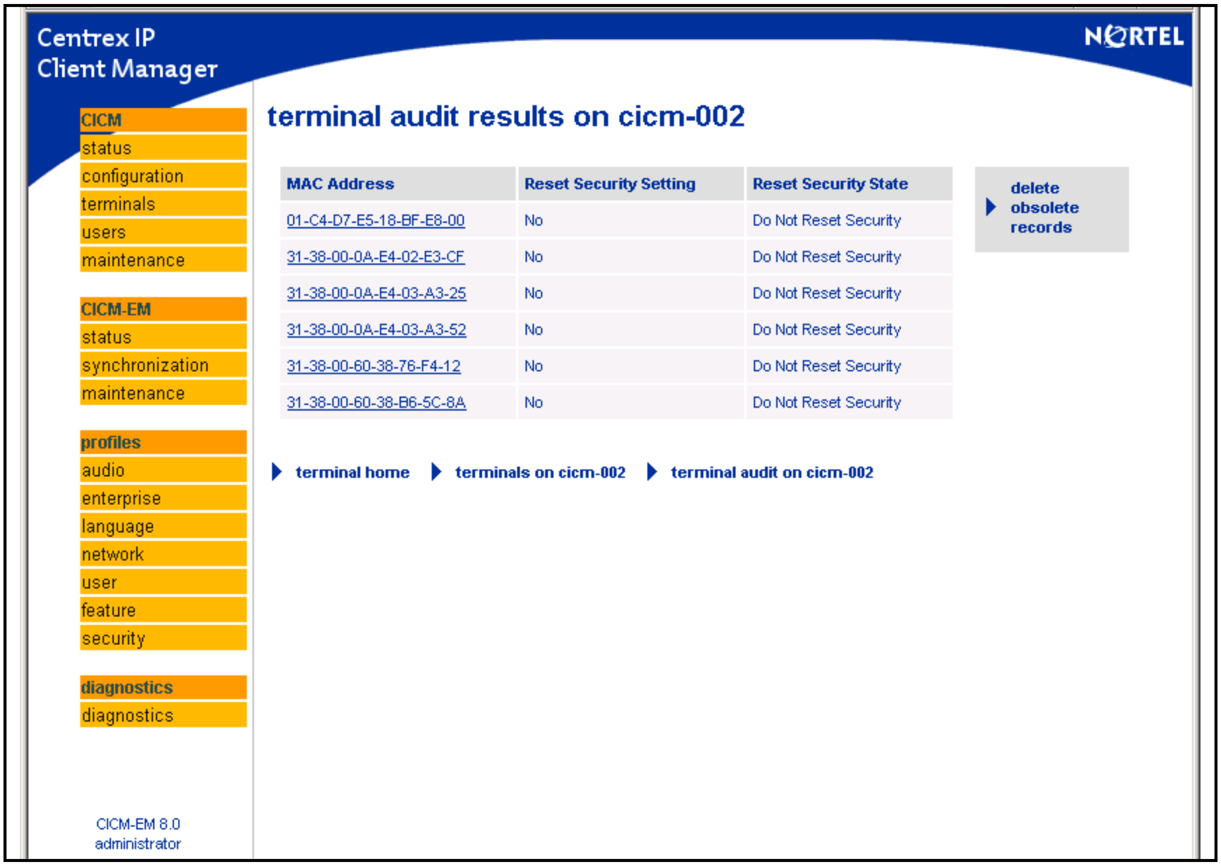
You can now move all the clients associated with this CICM server to another CICM server.

This procedure is complete.

7 Clear the security object from a client associated with a CICM server as follows:

a Click on **View Terminal Settings** for a particular CICM server.

Response: The **terminal audit results on <cicm>** page opens.

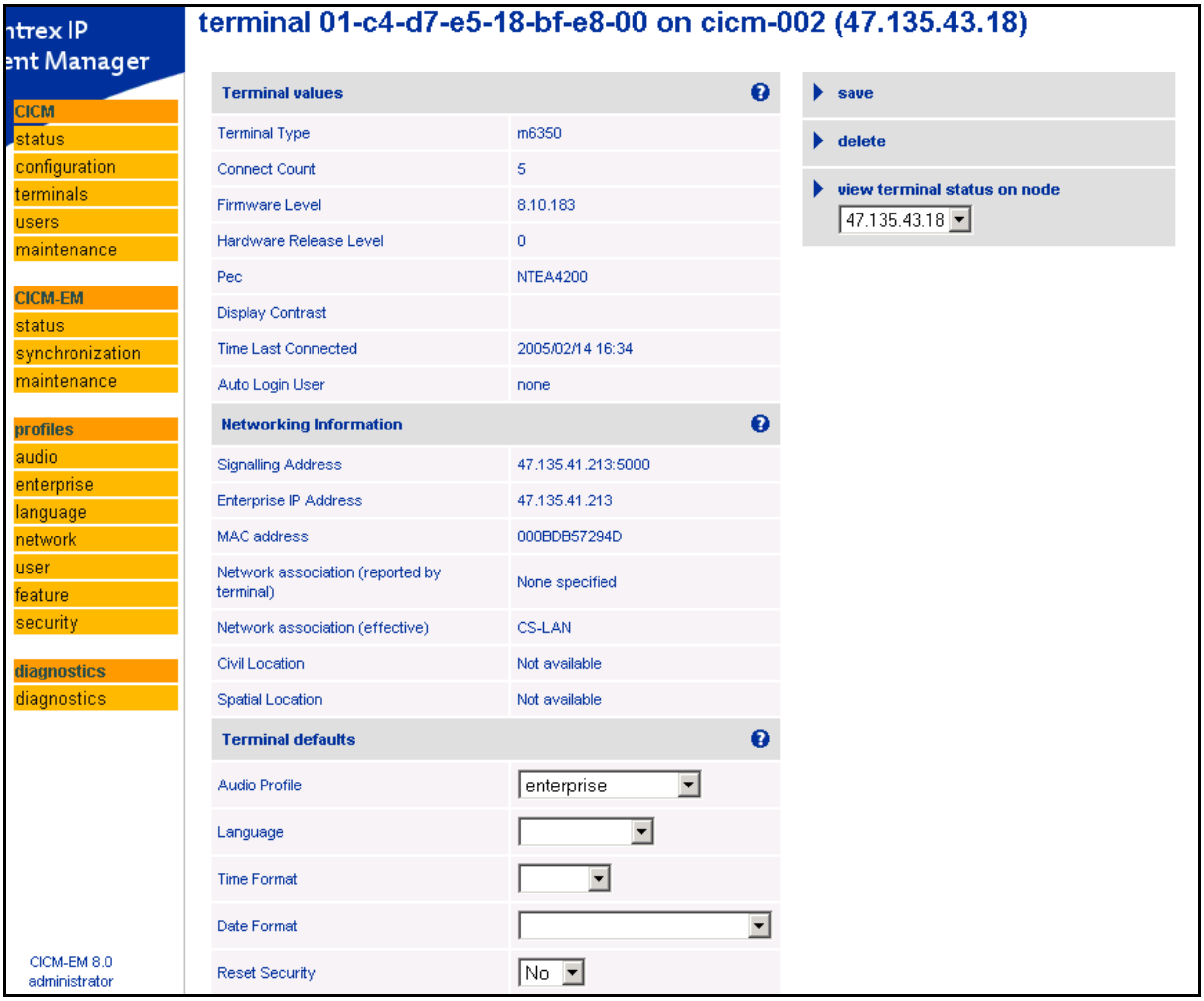


terminal audit results on cicm-002

MAC Address	Reset Security Setting	Reset Security State
01-C4-D7-E5-18-BF-E8-00	No	Do Not Reset Security
31-38-00-0A-E4-02-E3-CF	No	Do Not Reset Security
31-38-00-0A-E4-03-A3-25	No	Do Not Reset Security
31-38-00-0A-E4-03-A3-52	No	Do Not Reset Security
31-38-00-60-38-76-F4-12	No	Do Not Reset Security
31-38-00-60-38-B6-5C-8A	No	Do Not Reset Security

8 Click on the MAC Address for the client (terminal) on which you want to reset the security parameter.

Response: The **terminal <MAC Address> on <cicm>** page opens.



terminal 01-c4-d7-e5-18-bf-e8-00 on cicm-002 (47.135.43.18)

View terminal status on node: 47.135.43.18

Terminal values	
Terminal Type	m6350
Connect Count	5
Firmware Level	8.10.183
Hardware Release Level	0
Pec	NTEA4200
Display Contrast	
Time Last Connected	2005/02/14 16:34
Auto Login User	none
Networking Information	
Signalling Address	47.135.41.213:5000
Enterprise IP Address	47.135.41.213
MAC address	000BDB57294D
Network association (reported by terminal)	None specified
Network association (effective)	CS-LAN
Civil Location	Not available
Spatial Location	Not available
Terminal defaults	
Audio Profile	enterprise
Language	
Time Format	
Date Format	
Reset Security	No

a Select **Yes** for the Reset Security parameter.

b Click on **Save**.

You can now move this client associated with this CICM server to another CICM server.

This procedure is complete.

Deleting a CICM

Use this procedure only under Nortel support direction to delete a CICM node from the CICM-EM.

Procedure 14 Delete a CICM

CAUTION
Loss of all service
Completing this procedure will delete a CICM and result in loss of all CentrexIP service on that CICM.
This procedure must be performed only under direction from Nortel Support.

At the CICM Home page of the element manager web pages

1 Click on the **Change the list of CICMs stored in the CICM-EM** text in the right menu.

*Response: The **CICM modification** page opens.*

2 On the list of CICMs displayed, click the **delete** (trash can) icon for the CICM to be deleted.

Response: A status window displays the status of the deletion operation, and provides notification when complete.

3 This procedure is complete.

Editing CICM nodes

Use this procedure to edit the CICM nodes.

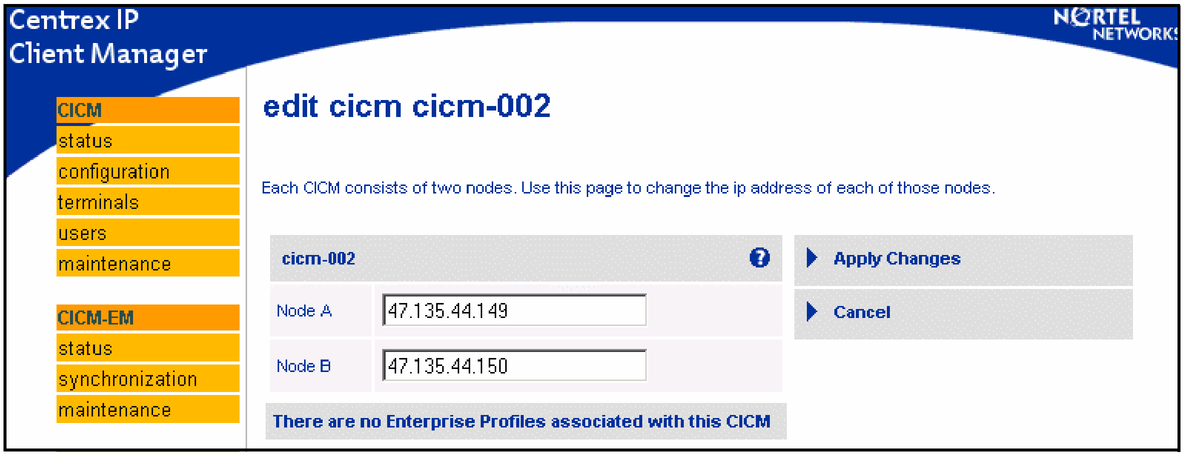
At the cicm home page of the element manager web pages

1 Click on the **Change the list of CICMs stored in the CICM-EM** text in the right menu.

*Response: The **cicm modification** page opens.*

2 On the list of CICMs displayed, click on the CICM to be changed.

*Response: The **edit cicm <cicm-nnn>** page opens.*



edit cicm cicm-002

Each CICM consists of two nodes. Use this page to change the ip address of each of those nodes.

cicm-002

Node A: 47.135.44.149

Node B: 47.135.44.150

There are no Enterprise Profiles associated with this CICM

3 Enter the node IP address for Node A and/or Node B,

Note 1: The nodes of a CICM correspond to the IP address of each side of the CICM (Unit 0 = Node A, Unit 1 = Node B). The IP addresses must be exactly correct, as the CICM-EM accesses the CICM using the IP address.

Note 2: The CICM name is a reference only and is not used for communication with the CICM.

4 Click on **Apply Changes** on the right menu.

5 This procedure is complete.

Monitoring the status of a CICM node

Use this procedure to monitor the status of a CICM node.

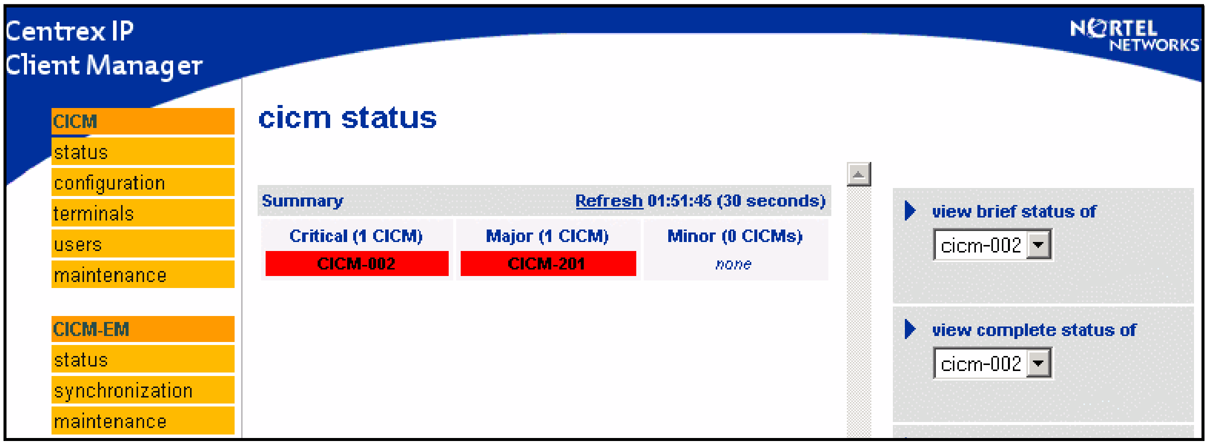
The **CICM status** page is an emulation of the alarm bar panel on the physical CICM. Any alarms that are seen on the alarm bar will be seen within 30 seconds on the Element Manager **CICM Status** page. From this page you can view the status of individual cards and information about their configuration.

This **CICM Status** web page is the best tool to monitor the CICM status. However, it is recommended to also periodically monitor the event logs of both nodes and the Element Manager. The details of event logs should also be viewed if an error occurs to identify the cause of the fault. Refer to the *View Event Logs* procedure of this document.

At the CICM home page on the Element Manager web interface

1 Click on **View the status of the CICMs** from the right menu.

*Response: the **cicm status** page displays a summary of critical, major, and minor faults on the CICM.*



cicm status

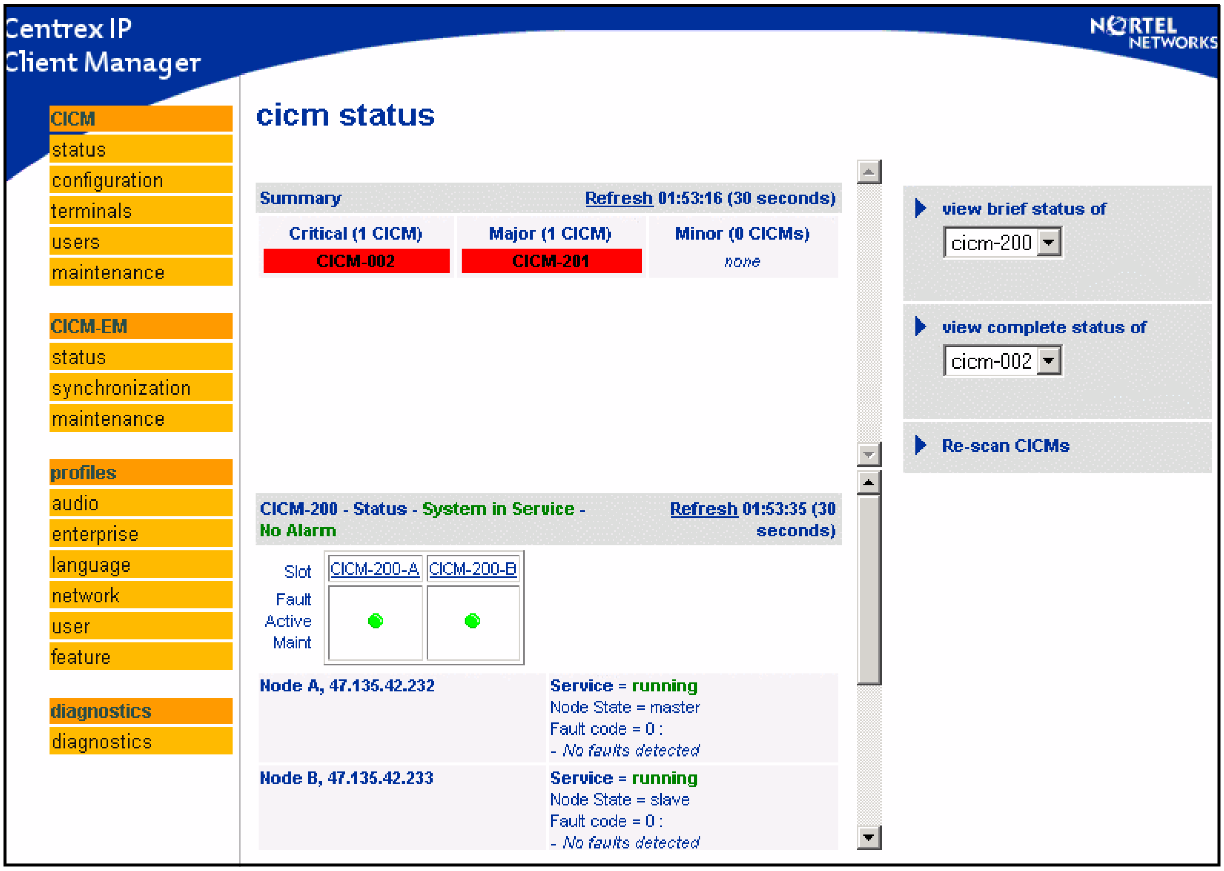
Summary	Refresh 01:51:45 (30 seconds)	
Critical (1 CICM)	Major (1 CICM)	Minor (0 CICMs)
CICM-002	CICM-201	none

view brief status of cicm-002

view complete status of cicm-002

2 To view additional details of the CICM status, click on **view brief status of** on the right.

*Response: The **cicm status** page updates to add additional node and card status information for the CICM.*



cicm status

view brief status of: cicm-200

view complete status of: cicm-002

Summary Refresh 01:53:16 (30 seconds)

Critical (1 CICM)	Major (1 CICM)	Minor (0 CICMs)
CICM-002	CICM-201	*none*

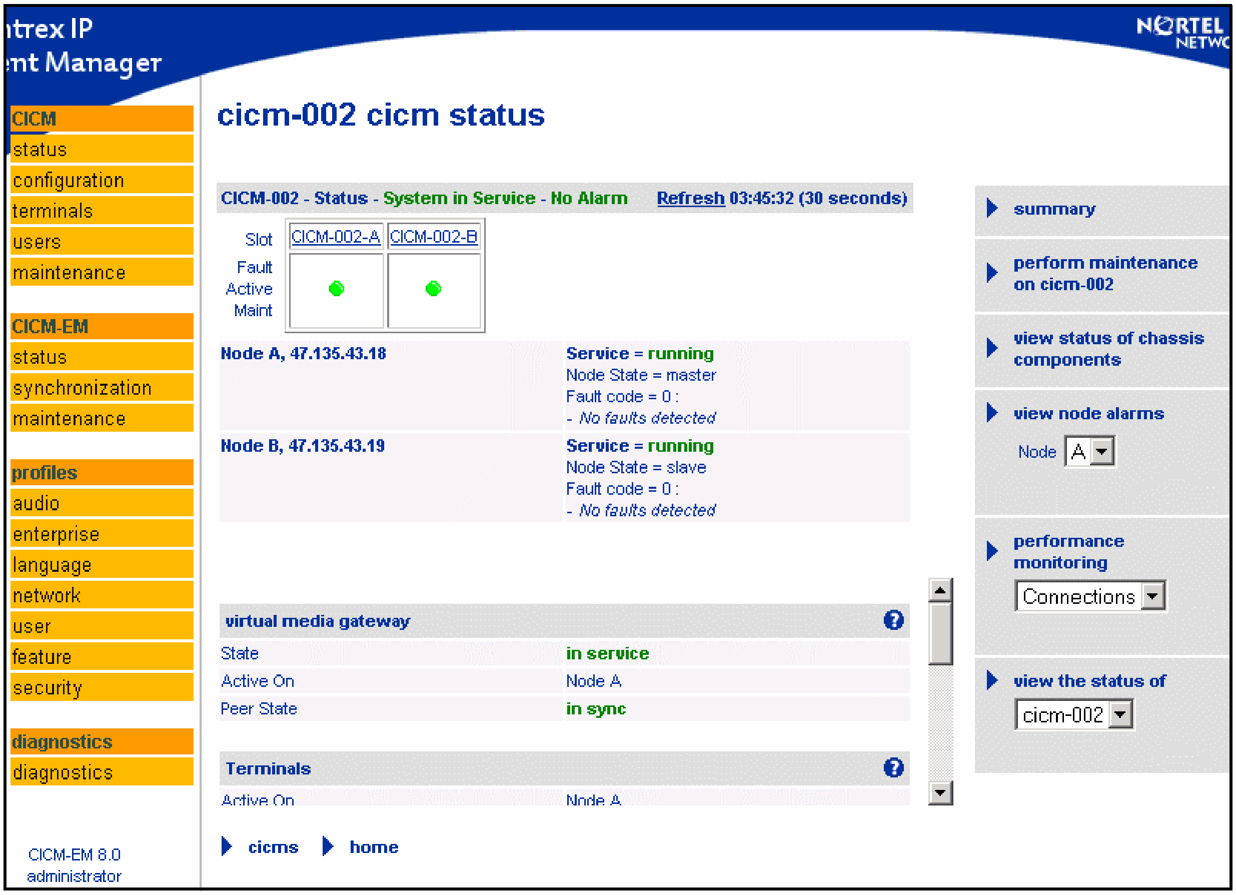
CICM-200 - Status - System in Service - No Alarm Refresh 01:53:35 (30 seconds)

Slot	CICM-200-A	CICM-200-B
Fault Active Maint	●	●

Node A, 47.135.42.232	**Service = running** Node State = master Fault code = 0 : - *No faults detected*
Node B, 47.135.42.233	**Service = running** Node State = slave Fault code = 0 : - *No faults detected*

3 To view the complete CICM status, click the **view complete status of** text box on the right menu.

*Response: The **<cicm-nnn> cicm status** page updates to add additional VMG, node, and network information, and to provide options to view additional detail (see step 4).*



cicm-002 cicm status

CICM-002 - Status - System in Service - No Alarm Refresh 03:45:32 (30 seconds)

Slot	CICM-002-A	CICM-002-B
Fault Active Maint	●	●

Node A, 47.135.43.18	Service = running Node State = master Fault code = 0 : - *No faults detected*
Node B, 47.135.43.19	Service = running Node State = slave Fault code = 0 : - *No faults detected*

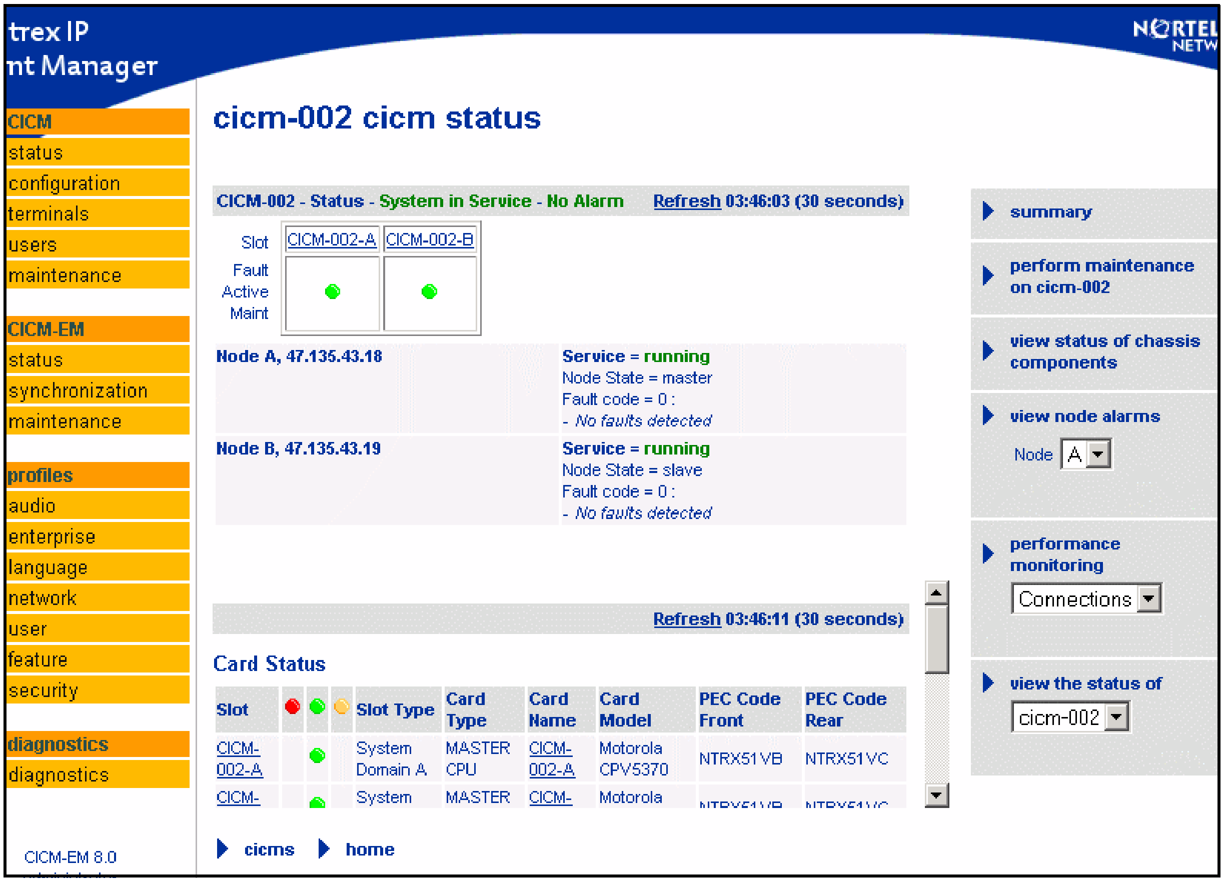
virtual media gateway	
State	in service
Active On	Node A
Peer State	in sync

Terminals	
Active On	Node A

Note: You must scroll down in the details sub-window to view all information.

4 To view details of the chassis components, click on **view status of chassis components** for each option on the right menu.

*Response: The <**cicm-nnn**> **cicm status** page updates with the additional detail selected.*



cicm-002 cicm status

CICM-002 - Status - System in Service - No Alarm Refresh 03:46:03 (30 seconds)

Slot	CICM-002-A	CICM-002-B
Fault Active Maint	●	●

Node A, 47.135.43.18 — Service = running
Node State = master
Fault code = 0 :
- *No faults detected*

Node B, 47.135.43.19 — Service = running
Node State = slave
Fault code = 0 :
- *No faults detected*

Node: A

performance monitoring: Connections

view the status of: cicm-002

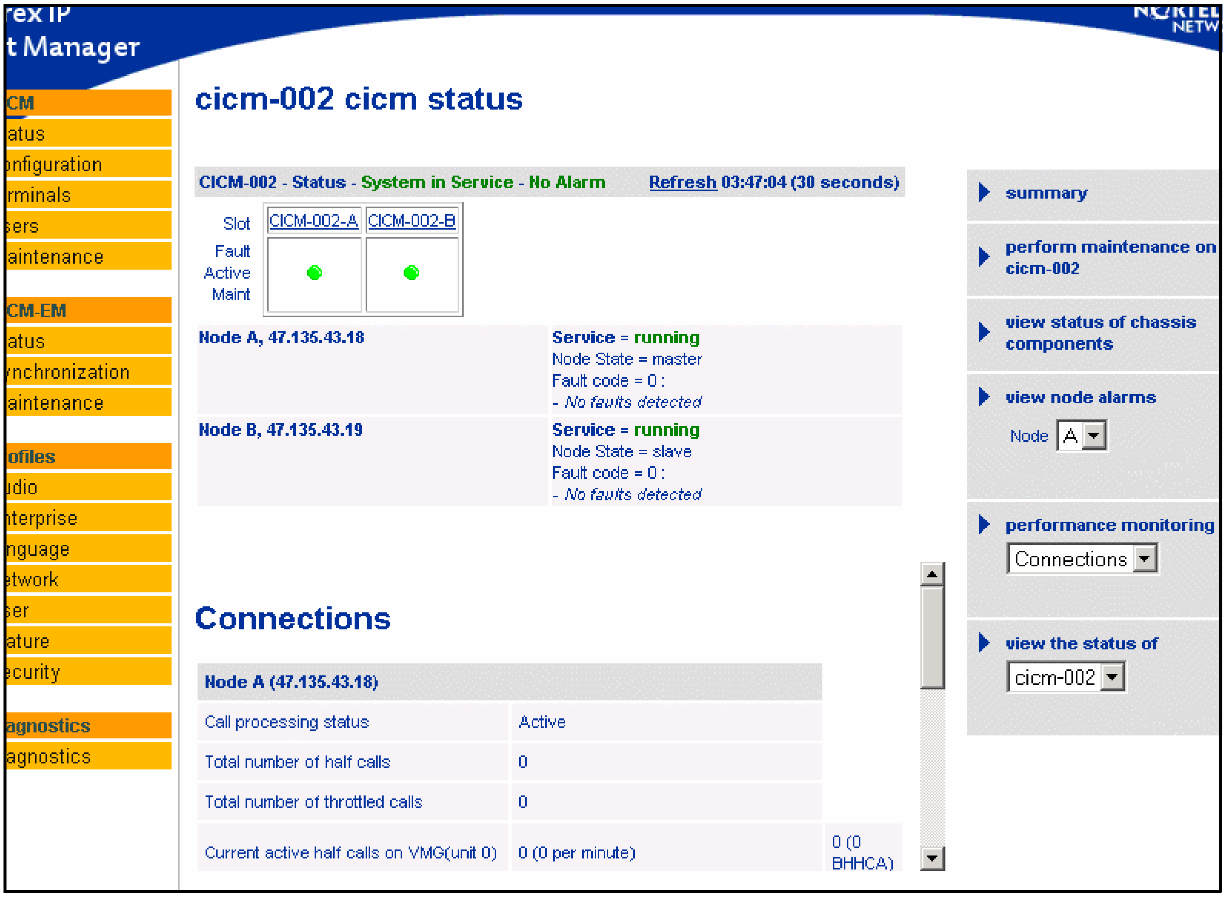
Refresh 03:46:11 (30 seconds)

Card Status

Slot	🔴	🟢	🟡	Slot Type	Card Type	Card Name	Card Model	PEC Code Front	PEC Code Rear
CICM-002-A		●		System Domain A	MASTER CPU	CICM-002-A	Motorola CPV5370	NTRX51VB	NTRX51VC
CICM-		●		System	MASTER	CICM-	Motorola	NTRX51VB	NTRX51VC

5 For performance monitoring of connections or terminals, from the **<cicm-nnn> cicm status** page, click on **Connections**, **Terminals**, or **Packets** from the drop-down menu of **performance monitoring** on the right menu, then click on **performance monitoring**.

Response: the ***<cicm-nnn> cicm status*** *page updates to display the information. The figure below displays connections information.*



cicm-002 cicm status

CICM-002 - Status - System in Service - No Alarm **Refresh 03:47:04 (30 seconds)**

Slot	CICM-002-A	CICM-002-B
Fault Active Maint	●	●

Node A, 47.135.43.18	**Service = running** Node State = master Fault code = 0 : - *No faults detected*
Node B, 47.135.43.19	**Service = running** Node State = slave Fault code = 0 : - *No faults detected*

Connections

Node A (47.135.43.18)		
Call processing status	Active	
Total number of half calls	0	
Total number of throttled calls	0	
Current active half calls on VMG(unit 0)	0 (0 per minute)	0 (0 BHHCA)

6 This procedure is complete.

Performing a sanity check on a CICM

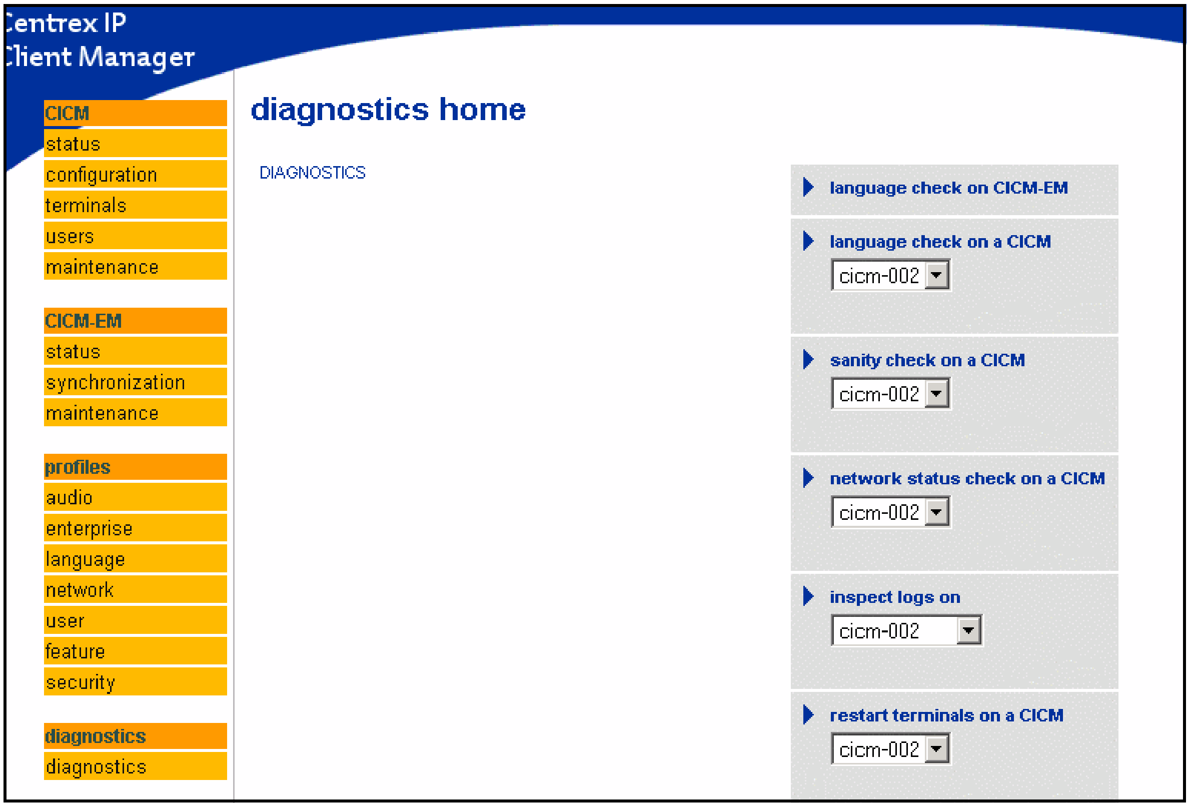
Use this procedure to perform a sanity check on a CICM. It will result in a display of the software release version.

Procedure 15 Perform sanity check on a CICM

At the cicm home page of the element manager web pages

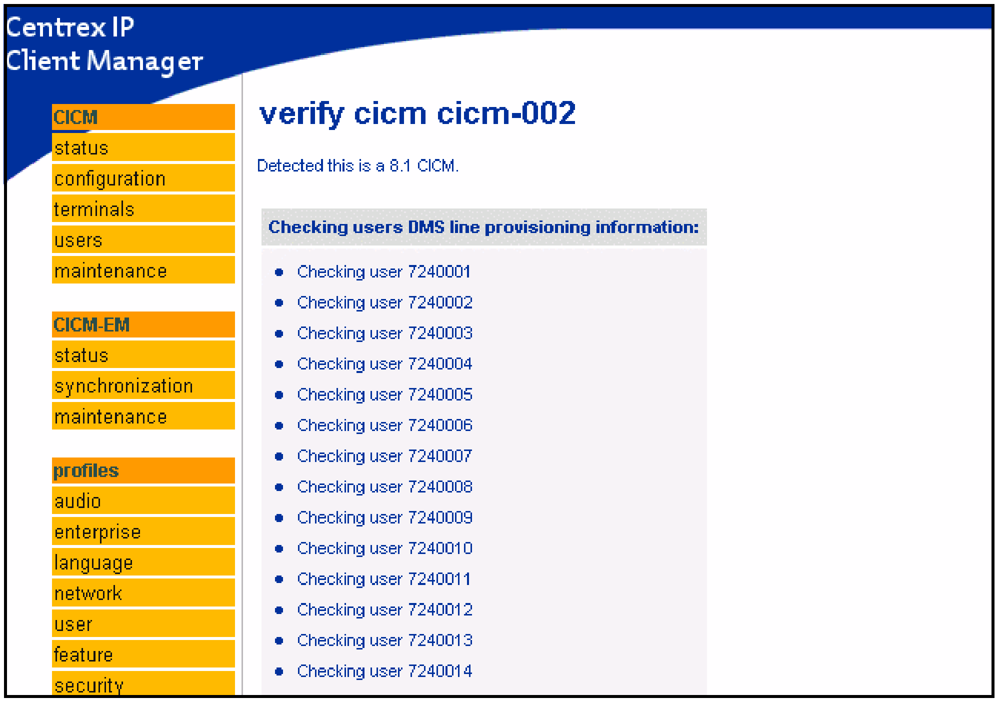
1 Click on **diagnostics** on the left menu.

*Response: The **diagnostics home** page opens.*



2 Choose the CICM from the drop-down menu of **sanity check on a CICM** on the right menu, then click on **sanity check on a CICM**.

*Response: the **verify CICM <cicm-nnn>** page opens and displays the results of the sanity check.*



verify cicm cicm-002

Detected this is a 8.1 CICM.

Checking users DMS line provisioning information:

- Checking user 7240001
- Checking user 7240002
- Checking user 7240003
- Checking user 7240004
- Checking user 7240005
- Checking user 7240006
- Checking user 7240007
- Checking user 7240008
- Checking user 7240009
- Checking user 7240010
- Checking user 7240011
- Checking user 7240012
- Checking user 7240013
- Checking user 7240014

3 This procedure is complete.

Setting up secure communications between a CICM server and its clients

You can set the security parameters at a CICM server level or at an enterprise level. All CICM servers within an enterprise must have the security feature provided in the MR6 release in order for the enterprise to have its security policy set to secure. If one or more CICM servers within the enterprise do not have the security feature, then the security policy for the enterprise can only be set to nonsecure. All CICM servers within an enterprise, are either all secure or all nonsecure as the CICM servers security policy defaults to the security policy of the enterprise. All CICM servers within an enterprise share the same security parameters, which cannot be overridden on a CICM server basis.

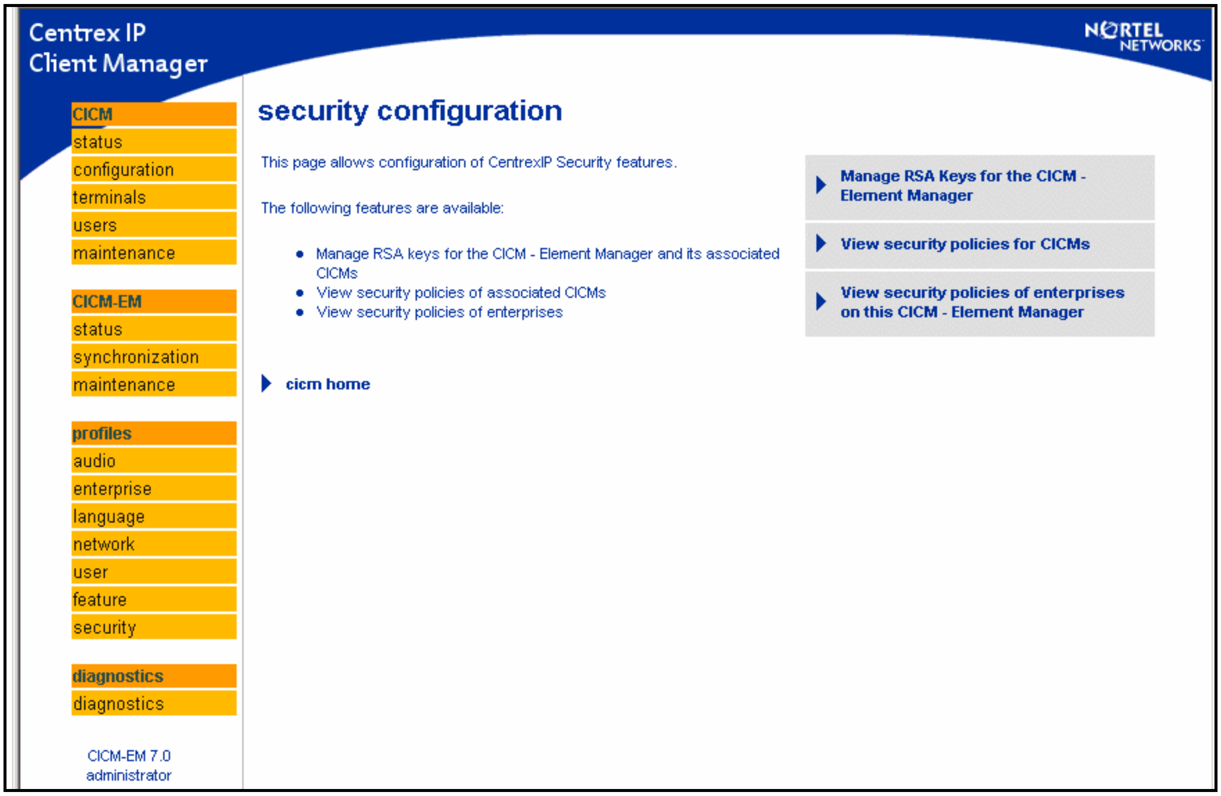
Complete one of the following procedures to set up secure communications between a CICM server and its clients:

- Set the security parameters at a CICM server level
- Set the security parameters at an enterprise level

At the Centrex IP Client Manager

1 Click on **security** from the profiles section of the left menu.

Response: The **security configuration** page opens.



security configuration

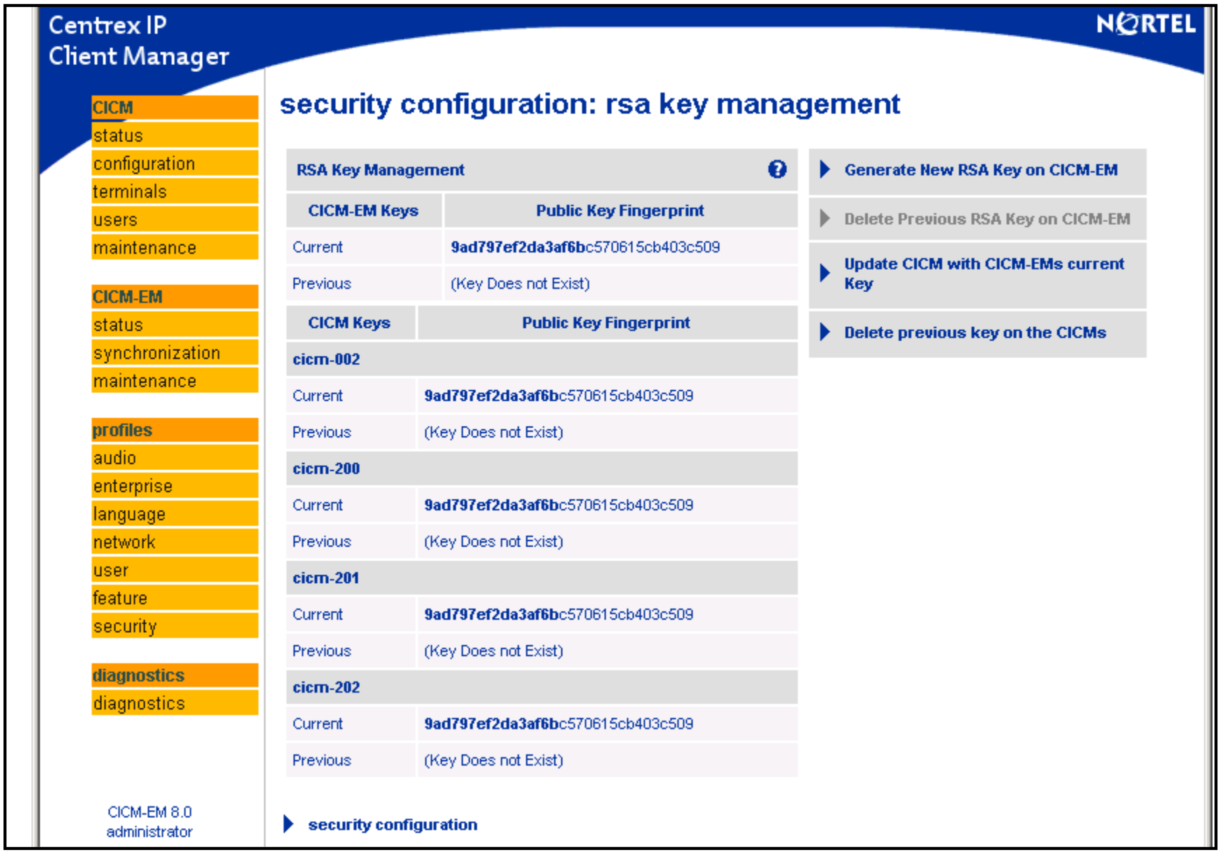
This page allows configuration of CentrexIP Security features.

The following features are available:

- Manage RSA keys for the CICM - Element Manager and its associated CICMs
- View security policies of associated CICMs
- View security policies of enterprises

2 From the right menu, click on **Manage RSA Keys for the CICM Element Manager**.

Response: The **security configuration: rsa key management** page opens.



security configuration: rsa key management

RSA Key Management

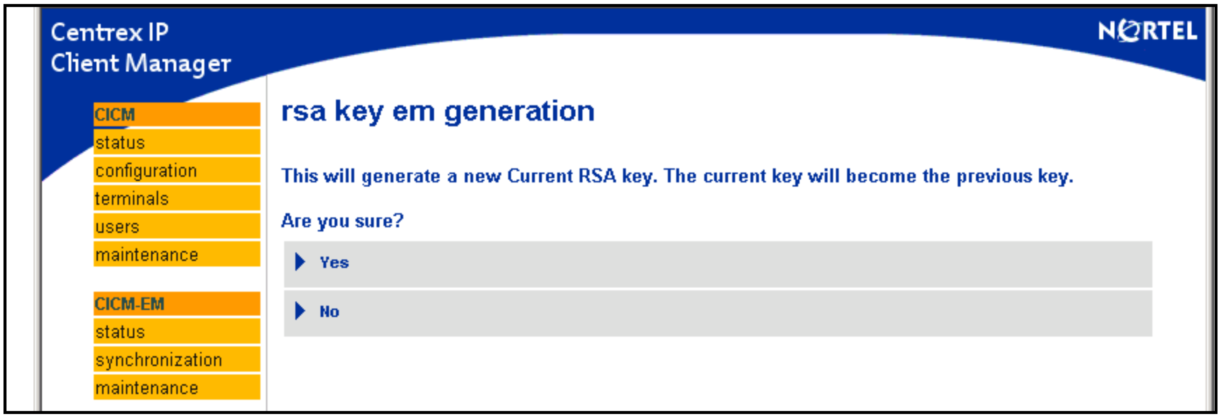
CICM-EM Keys	Public Key Fingerprint
Current	9ad797ef2da3af6bc570615cb403c509
Previous	(Key Does not Exist)

CICM Keys	Public Key Fingerprint
cicm-002	
Current	9ad797ef2da3af6bc570615cb403c509
Previous	(Key Does not Exist)
cicm-200	
Current	9ad797ef2da3af6bc570615cb403c509
Previous	(Key Does not Exist)
cicm-201	
Current	9ad797ef2da3af6bc570615cb403c509
Previous	(Key Does not Exist)
cicm-202	
Current	9ad797ef2da3af6bc570615cb403c509
Previous	(Key Does not Exist)

3 From the right menu, click on **Generate New RSA Key on CICM-EM**.

> ***Note:*** A maximum of two RSA keys can be provisioned on the system at any given time. If an RSA key already exists in the Current field, generating a new RSA key will move the RSA key from the Current field to the Previous field. If an RSA key already existed in the Previous field, it will be removed from the system.

Response: The **rsa key em generation** page opens requesting confirmation to generate a new Current RSA key.



rsa key em generation

This will generate a new Current RSA key. The current key will become the previous key.

Are you sure?

4 Click Yes to confirm you want to generate a new RSA key.

> ***Note:*** Clicking no aborts the procedure and returns you to the rsa key management page.

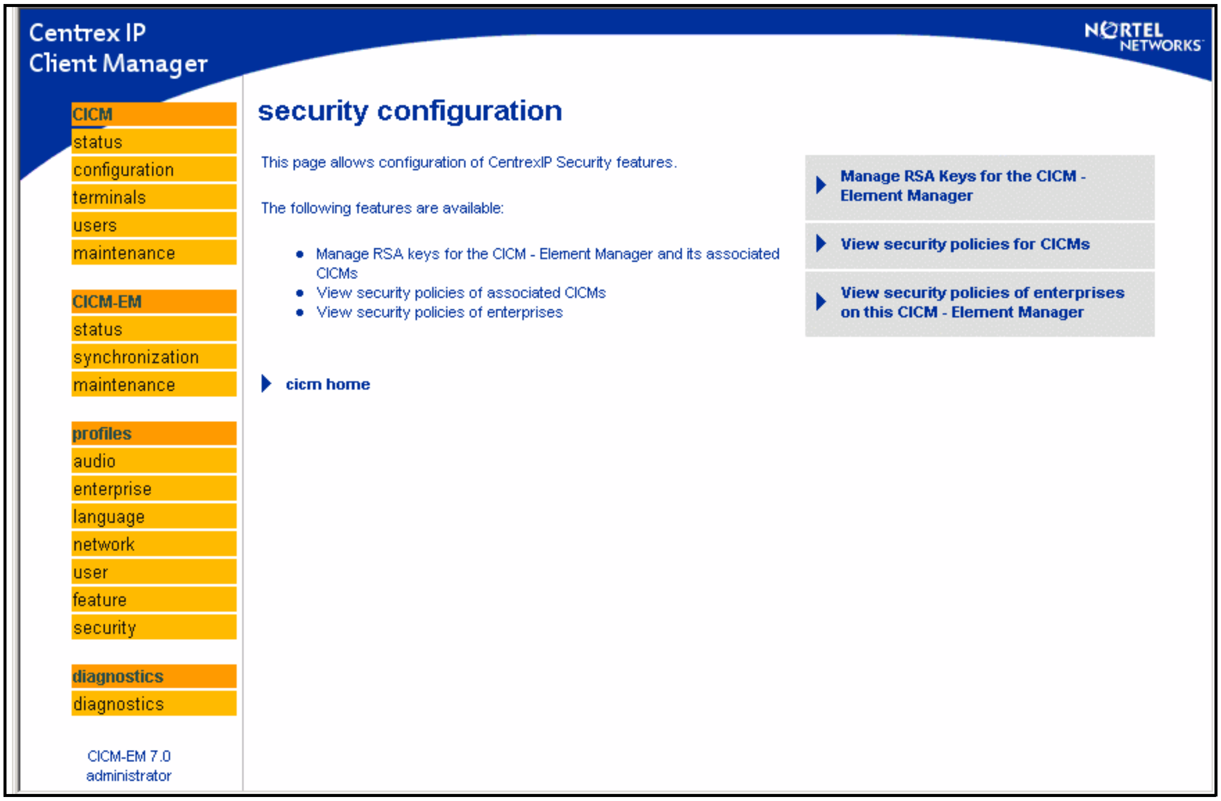
Once you click Yes, the system generates the new RSA key and propagates it to all active CICM servers associated with the CICM element manager on which the RSA key was generated.

> ***Note:*** Removing the previous key in a secure environment, will cause clients that were not in contact with their CICM server when you generated the new RSA key, to be unusable until manual intervention occurs on the client. Manual intervention involves updating the PK fingerprint on the particular client. Therefore, it is recommended that you not remove the previous key until the new key is propagated to all clients associated with the CICM servers served by the CICM element manage on which the new RSA key was generated.

If an error occurs during the generation of the RSA key, log report CH0001 will be generated. Contact your next level of support if required.

5 Click the security configuration link to return to the security configuration page.

Response: The **security configuration** page opens.



security configuration

This page allows configuration of CentrexIP Security features.

The following features are available:

- Manage RSA keys for the CICM - Element Manager and its associated CICMs
- View security policies of associated CICMs
- View security policies of enterprises

This procedure is complete. Proceed to one of the following procedures:

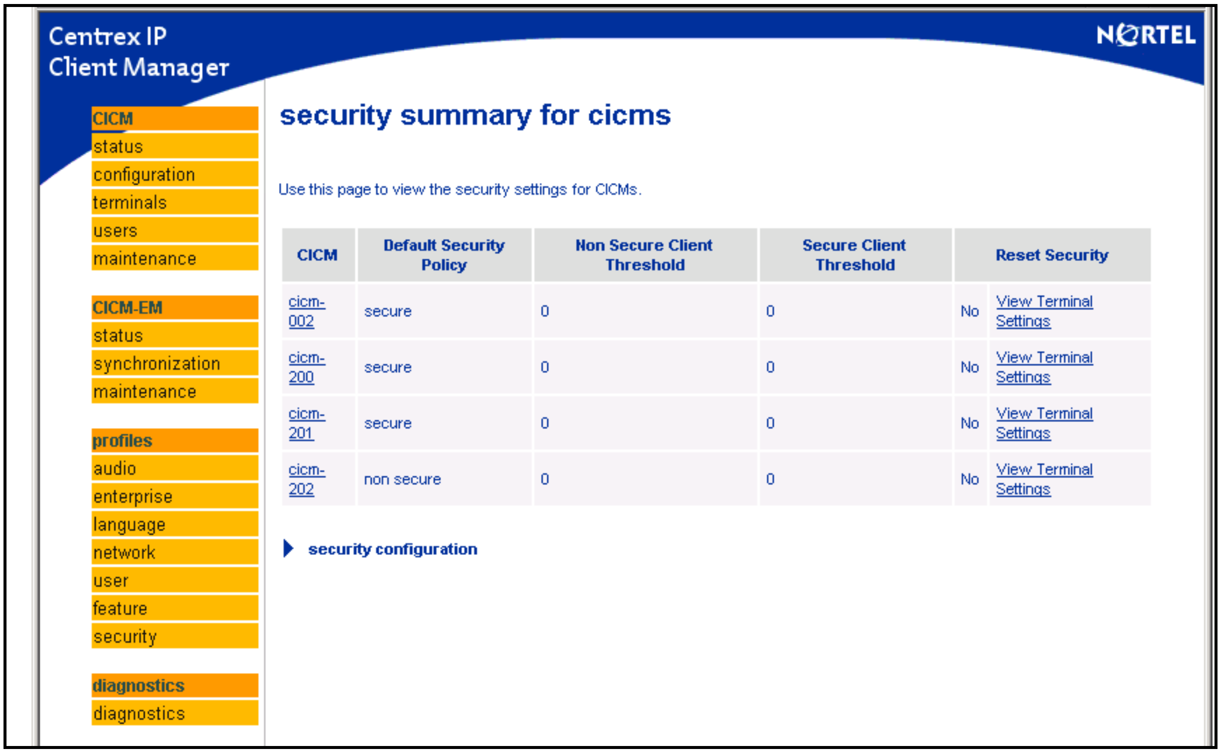
- Set the security parameters at a CICM server level
- Set the security parameters at an enterprise level

Procedure 16 Set the security parameters at a CICM server level

At the security configuration web page

1 Click **View security policies for CICMs**

Response: The **security summary for cicms** page opens.



security summary for cicms

Use this page to view the security settings for CICMs.

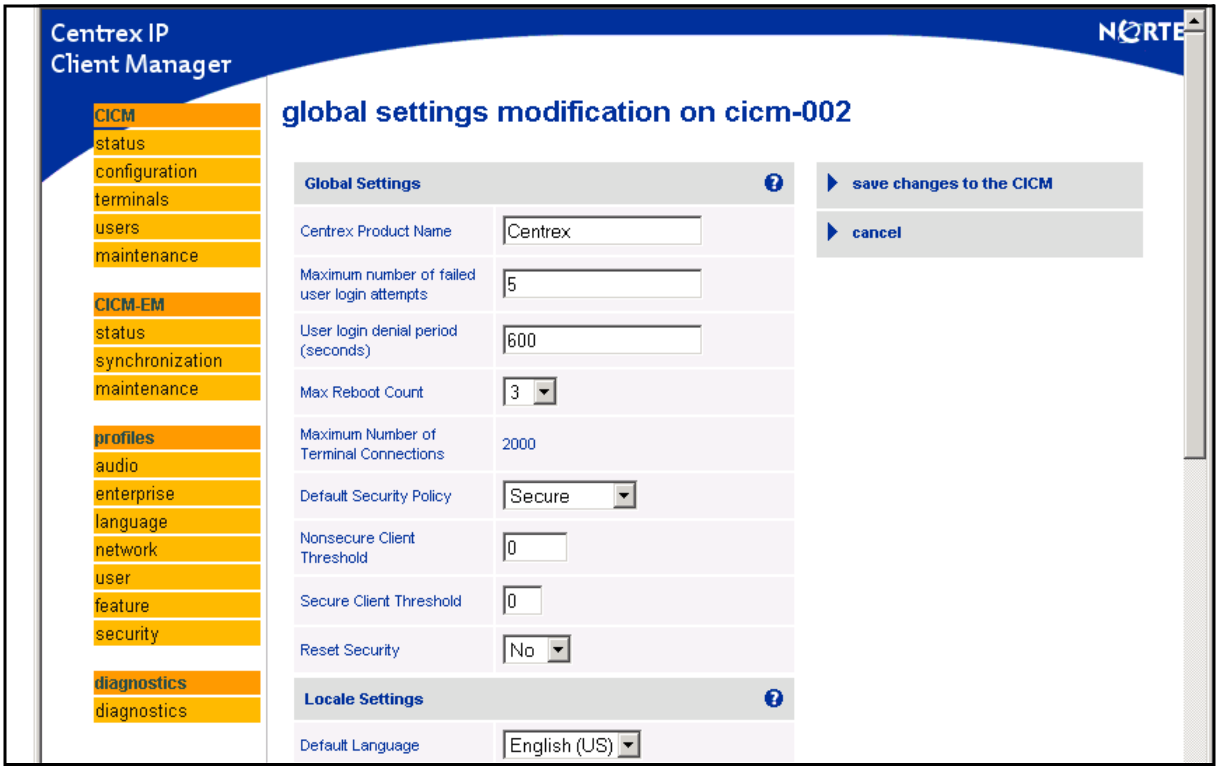
CICM	Default Security Policy	Non Secure Client Threshold	Secure Client Threshold	Reset Security	
cicm-002	secure	0	0	No	View Terminal Settings
cicm-200	secure	0	0	No	View Terminal Settings
cicm-201	secure	0	0	No	View Terminal Settings
cicm-202	non secure	0	0	No	View Terminal Settings

▶ security configuration

2 Set the security parameters for the CICM servers associated with the CICM element manager as follows:

a Click on a CICM server link.

Response: The **global settings modification on <cicm>** page opens.



global settings modification on cicm-002

Global Settings	
Centrex Product Name	Centrex
Maximum number of failed user login attempts	5
User login denial period (seconds)	600
Max Reboot Count	3
Maximum Number of Terminal Connections	2000
Default Security Policy	Secure
Nonsecure Client Threshold	0
Secure Client Threshold	0
Reset Security	No
Locale Settings	
Default Language	English (US)

b Set the security parameters for the CICM server as follows:

- Default Security Policy = Secure

  Note 1: You can only set the Default Security Policy parameter to Secure if the CICM server has an RSA key. If the CICM server does not have an RSA key, you will be prompted to generate one.

  Note 2: If the CICM server is within an enterprise, the enterprise security policy takes precedence.

- Nonsecure Client Threshold = <number of clients permitted to connect in a non-secure fashion to this secure CICM server>

  Note: If you do not want to allow any clients to connect to the secure CICM server in non-secure mode, set the Nonsecure Client Threshold value to 0 (zero).

3 Click on **Save changes to the CICM**.

Once the security parameters are set, the CICM server will propagate the RSA key to its clients and transition the clients to secure mode, which involves a hard reset.

> ***Note:*** The first time the CICM server propagates the RSA key to its clients, it will be done in the clear (no encryption). The clients will only allow for a one-time push of the RSA key in the clear. All other RSA key pushes will be ignored unless the push is done over a secure connection.

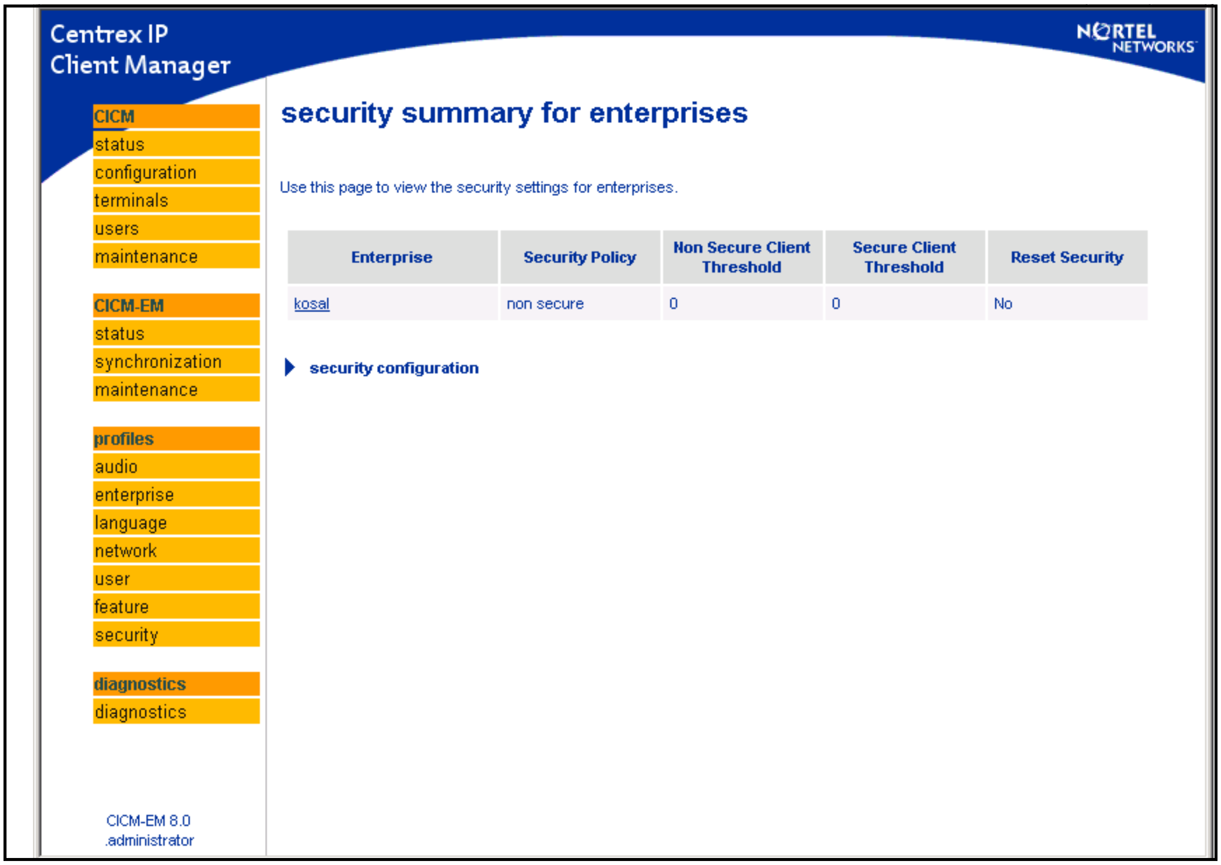
This procedure is complete.

Procedure 17 Set the security parameters at an enterprise level

At the security configuration web page

1 Click **View security policies of enterprises on this CICM-Element Manager**

Response: The **security summary for enterprises** page opens.



security summary for enterprises

Use this page to view the security settings for enterprises.

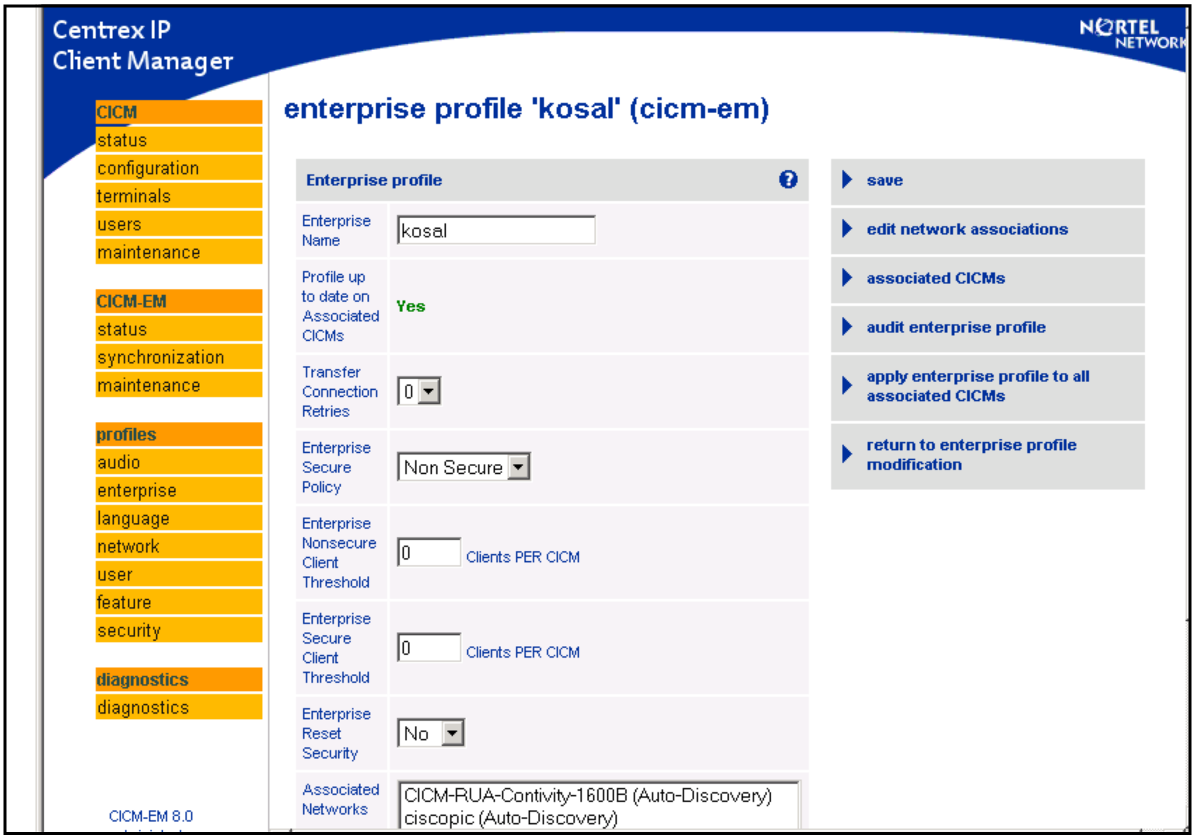
Enterprise	Security Policy	Non Secure Client Threshold	Secure Client Threshold	Reset Security
kosal	non secure	0	0	No

▶ security configuration

2 Set the security parameters for the enterprises associated with the CICM element manager as follows:

a Click on an Enterprise link.

Response: The **enterprise profile <enterprise> (cicm-em)** page opens.



enterprise profile 'kosal' (cicm-em)

Enterprise Name	kosal
Profile up to date on Associated CICMs	Yes
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	CICM-RUA-Contivity-1600B (Auto-Discovery) ciscopic (Auto-Discovery)

b Set the security parameters for the enterprise as follows:

- Enterprise Security Policy = Secure

  Note: You can only set the Enterprise Security Policy parameter to Secure if all the CICM servers within the enterprise support the security feature provided in the MR6 release.

- Enterprise Nonsecure Client Threshold = <number of clients permitted to connect in a non-secure fashion to a secure CICM server within this secure enterprise>

  Note: If you do not want to allow any clients to connect to a secure CICM server in non-secure mode, set the Nonsecure Client Threshold value to 0 (zero).

3 Click on **save**.

4 Click on **apply enterprise profile to all associated CICMs**.

The security parameters are propagated to all the CICM servers associated with the enterprise, and in turn the CICM servers propagate the RSA key to their clients and transition the clients to secure mode, which involves a hard reset.

> ***Note:*** The Profile up to date on Associated CICMs field changes from NO to YES, which indicates that all CICM servers within the enterprise are using the latest settings in the enterprise's profile.

Starting or stopping the CICM service

Stopping the service (call-processing) on a CICM node may be necessary when upgrading or during routine maintenance such as changing cables. When the service is stopped, CICM terminals cannot log in. Use these procedures only under the direction of Nortel Support.

Stop or start CICM service in order to minimize service outage.

Procedure 18

CAUTION
Loss of service
Using the ***Restart*** button can result in loss of service if a terminal transfer is not performed prior to this procedure.
This procedure must be performed only under direction from Nortel Support.

At the CICM-EM home page of the Element Manager web pages

1 Click on **status** on the **CICMs** section of the left menu.

*Response: The **cicm home** page opens*

2 Select the CICM to view from the drop-down list under the **view the status of the following CICM** text on the right menu, then click on the **view the status of the following CICM** text.

*Response: The **<cicm-nnn> cicm status** page opens.*

3 Click on **perform maintenance on <cicm-nnn>** on the right menu.

*Response: The **maintenance status <cicm-nnn>** page opens.*

4 From the drop-down menu of **Node A Service Control** or **Node B Service Control**, click on **Restart** for the applicable node.

Response: A confirmation prompt is displayed.

5 At the confirmation prompt, enter **Yes** to confirm restart (or **no** to decline).

Response:
With confirmation, the CICM resets and attempts to start the service on the node.

The field *Status* updates to display the current service state. Possible states are have the syntax x (y) where:

x

is one of the following:

- *master*
- *master (no slave)*
- *slave*
- *slave (no master - isolated)*
- *swact complete*
- *swacting master -> slave*
- *swacting slave -> master*
- *unavailable*

y

is one of the following:

- *running*
- *start pending*
- *stop pending*
- *stopped*
- *unknown state*

Note: *The node will be in the state "Start Pending" while the hardware is being initialized.*

6 Monitor the node service status from the **maintenance status (<cicm-nnn>)** page.

When the **service state** changes to **running** the service has correctly started.

7 Repeat this procedure to start the second node.

8 This procedure is complete.

Note: If the service fails to start, refer to the CS2K documentation *Remote Line concentrating Module Maintenance Guide* to bring the CentrexIP into service.

Procedure 19 Stop the CICM service

CAUTION
Loss of service
Attempt this procedure only on a slave node. **This procedure must be performed only under direction from Nortel support.**

At the Element Manager home page

1 Click on **status** of the **CICMs** section of the left menu.

*Response: The **cicm home** page opens*

2 Select the CICM to view from the drop-down list on the right, then click on the **view the status of the following CICM** text.

*Response: The **<cicm-nnn> cicm status** page opens.*

3 On the **<cicm-nnn> cicm status** page, click on **perform maintenance on <cicm-nnn>** on the right menu.

*Response: The **maintenance status (<cicm-nnn>)** page opens.*

4 At the **maintenance status (<cicm-nnn>)** page, click on **node A service control** or **node B service control**. **Stop** should be displayed on the drop-down menu (if the node is running, the **Restart** option will be displayed).
Click on the **node A service control** or **node B service control** as applicable.

Response: The node begins the shutdown process, and the results of the action is displayed.

5 On the **maintenance status (<cicm-nnn>)** page, the field *Status* displays **stop pending** for the node selected. The node will be in the **Stop Pending** state while the hardware is shutting down.

6 Monitor the node service state from the **maintenance status (<cicm-nnn>)** page.

When the *Status* changes to **stopped** the service has correctly been shut down.

> ***Note:*** Stopping the CentrexIP service causes alarms. To prevent these alarms, offline the CICM at the CS2K before powering down the CICM. Refer to the documentation *Remote Line Concentrating Module Maintenance Guide*.

7 Repeat this procedure to stop the second node.

8 This procedure is complete.

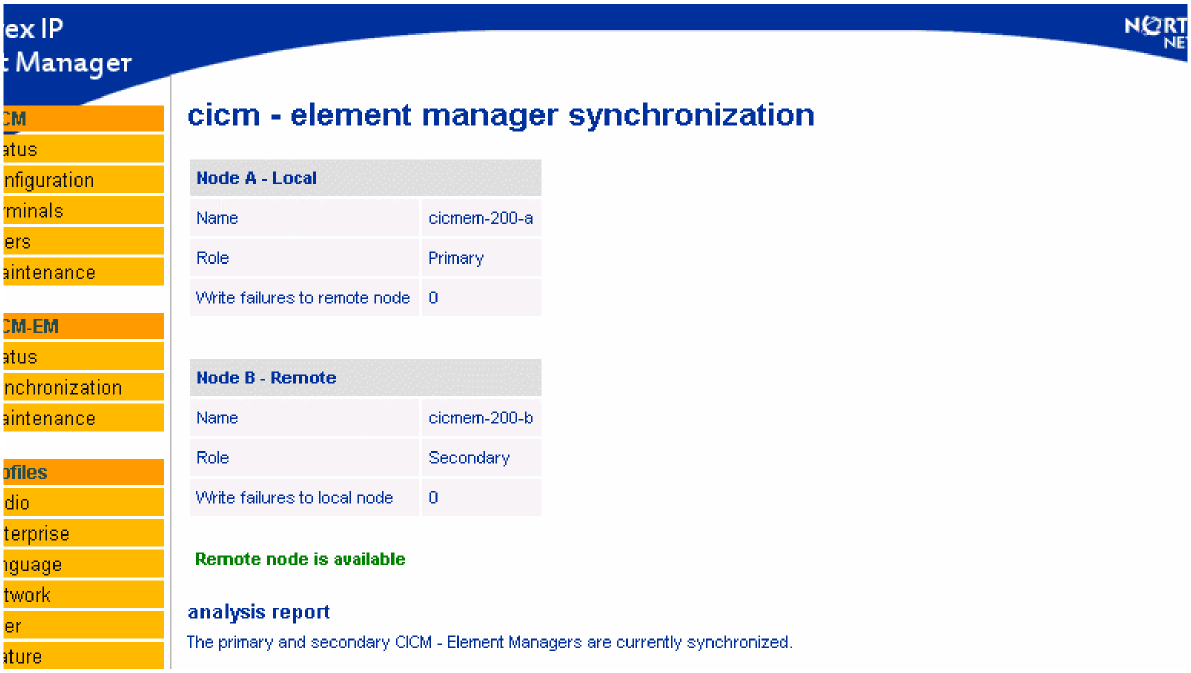
Viewing CICM-EM synchronization

Use this procedure to view and check the synchronization between the Primary and Backup Element Managers.

At the cicm - element manager home page

1 Select **synchronization** from the **CICM-EM** section of the left menu.

*Response: The **cicm - element manager synchronization** page opens.*



cicm - element manager synchronization

Node A - Local	
Name	cicmem-200-a
Role	Primary
Write failures to remote node	0

Node B - Remote	
Name	cicmem-200-b
Role	Secondary
Write failures to local node	0

Remote node is available

analysis report

The primary and secondary CICM - Element Managers are currently synchronized.

2 This procedure is complete.

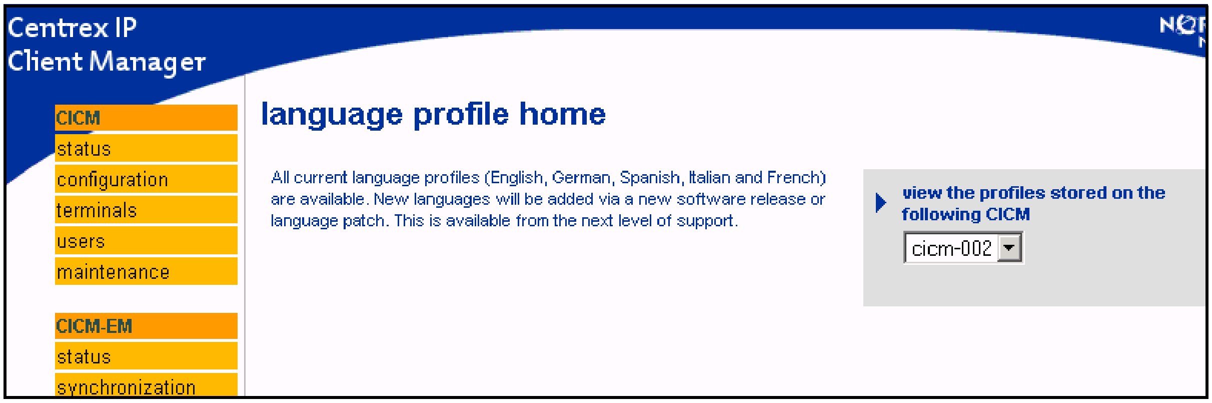
Viewing Language Profiles on a CICM

Use this procedure to view the Language Profiles applied to a CICM. Current Language Profiles available are English, German, Spanish, Italian, and French. New Language Profiles will be added through new software releases.

At the cicm - element manager home page

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

*Response: The **language profile home** page opens.*



language profile home

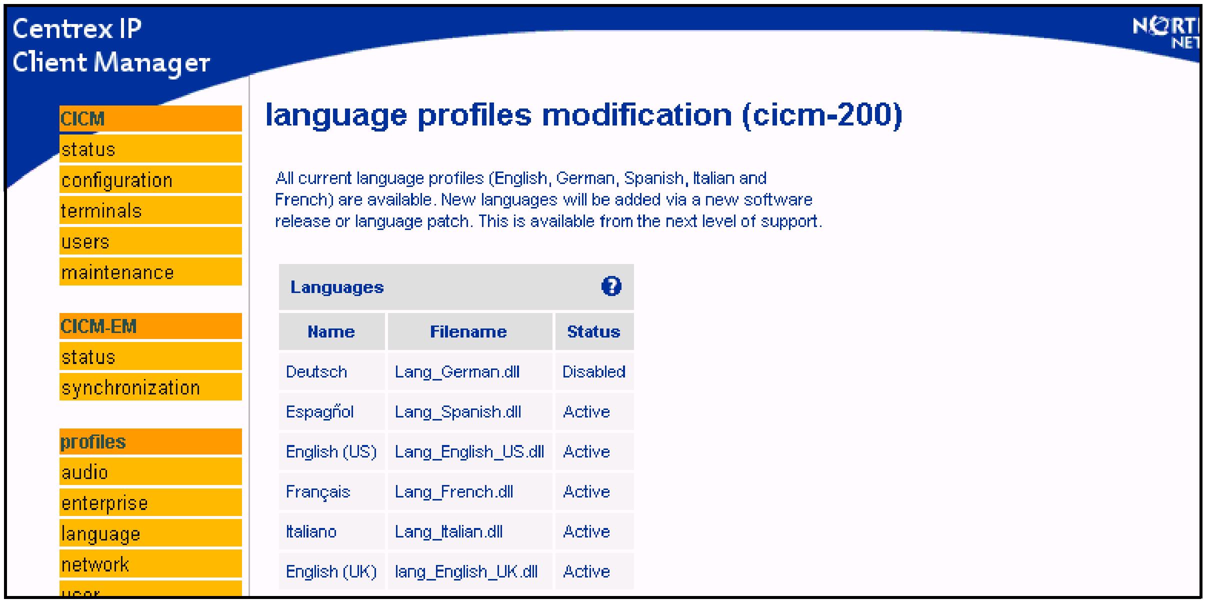
All current language profiles (English, German, Spanish, Italian and French) are available. New languages will be added via a new software release or language patch. This is available from the next level of support.

view the profiles stored on the following CICM

cicm-002

2 To view the language profiles stored on a CICM, select the CICM from the drop-down menu, then click on **view the profiles stored on the following CICM** on the right menu.

*Response: The **language profiles modification (<cicm-nnn>)** page opens and displays the list of language profiles on the CICM.*



language profiles modification (cicm-200)

All current language profiles (English, German, Spanish, Italian and French) are available. New languages will be added via a new software release or language patch. This is available from the next level of support.

Languages

Name	Filename	Status
Deutsch	Lang_German.dll	Disabled
Espagñol	Lang_Spanish.dll	Active
English (US)	Lang_English_US.dll	Active
Français	Lang_French.dll	Active
Italiano	Lang_Italian.dll	Active
English (UK)	lang_English_UK.dll	Active

3 This procedure is complete.

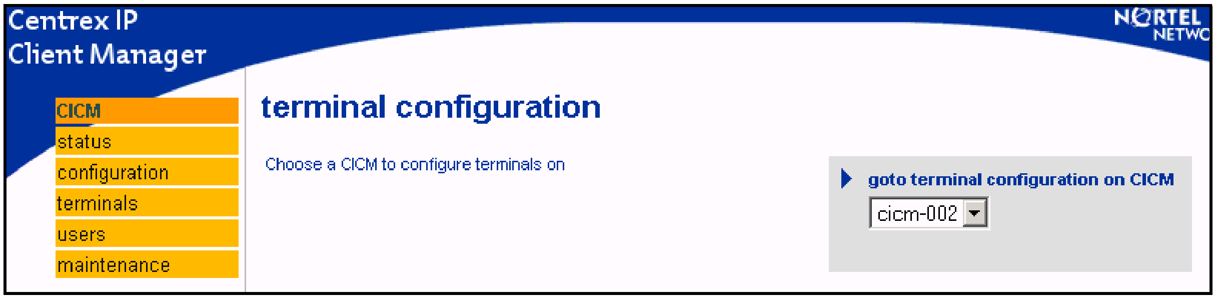
Viewing terminal status

Use this procedure to view a terminal status.

At the CICM - element manager home page

1 Click on **terminals** from the left menu.

*Response: The **terminal configuration** page opens.*



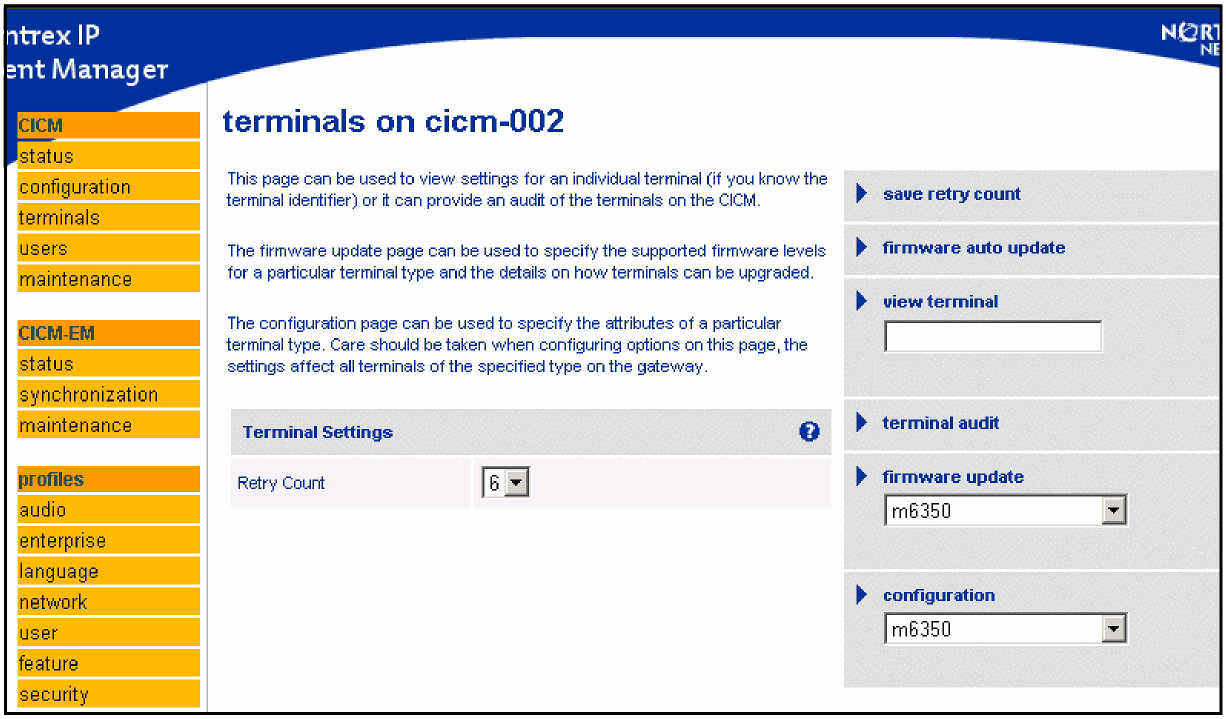
terminal configuration

Choose a CICM to configure terminals on

goto terminal configuration on CICM: cicm-002

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

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



terminals on cicm-002

This page can be used to view settings for an individual terminal (if you know the terminal identifier) or it can provide an audit of the terminals on the CICM.

The firmware update page can be used to specify the supported firmware levels for a particular terminal type and the details on how terminals can be upgraded.

The configuration page can be used to specify the attributes of a particular terminal type. Care should be taken when configuring options on this page, the settings affect all terminals of the specified type on the gateway.

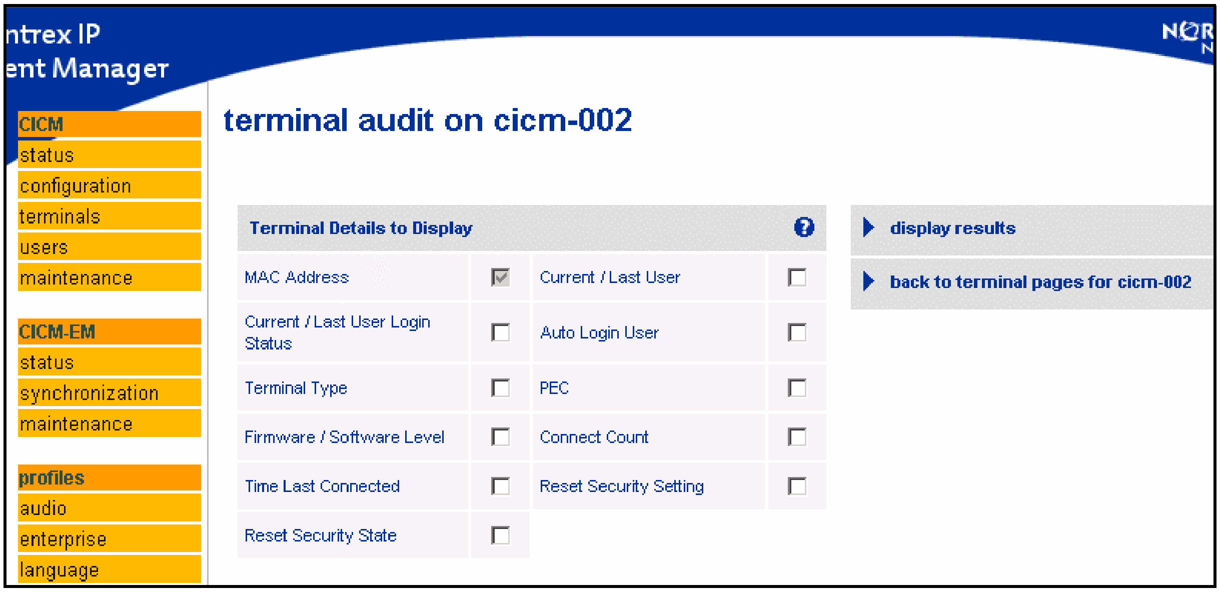
Terminal Settings	
Retry Count	6

firmware update: m6350

configuration: m6350

3 Click on **terminal audit** on the right menu.

*Response: The **terminal audit on <cicm-nnn>** page opens.*

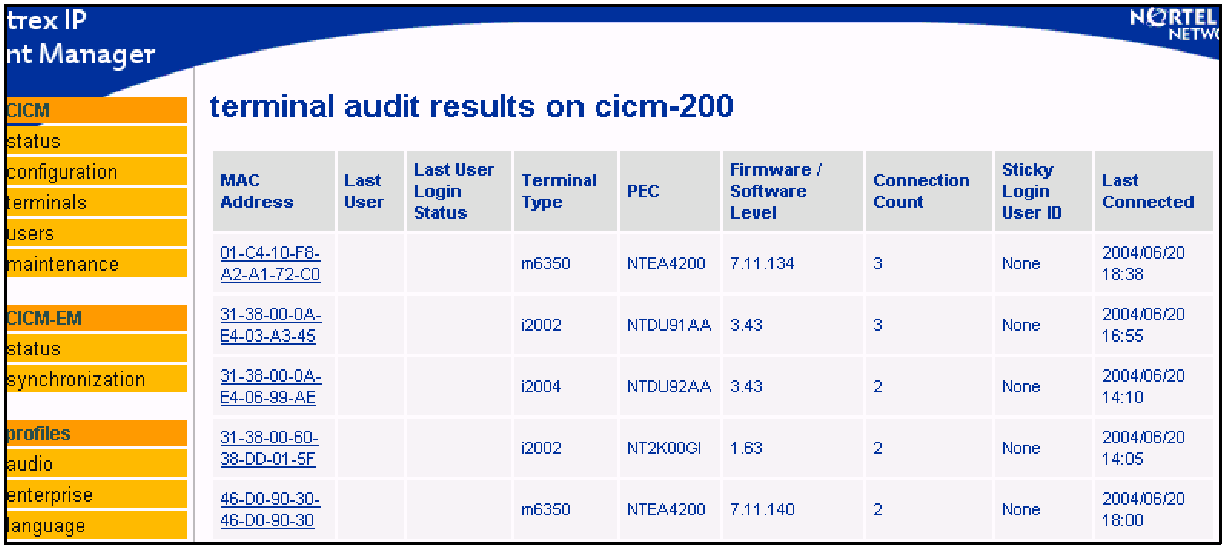


terminal audit on cicm-002

Terminal Details to Display			
MAC Address	☑	Current / Last User	□
Current / Last User Login Status	□	Auto Login User	□
Terminal Type	□	PEC	□
Firmware / Software Level	□	Connect Count	□
Time Last Connected	□	Reset Security Setting	□
Reset Security State	□		

4 Select the terminal details to display in the audit by checking each box, then click on **display results**.

*Response: The **terminal audit results on <cicm-nnn>** page opens.*

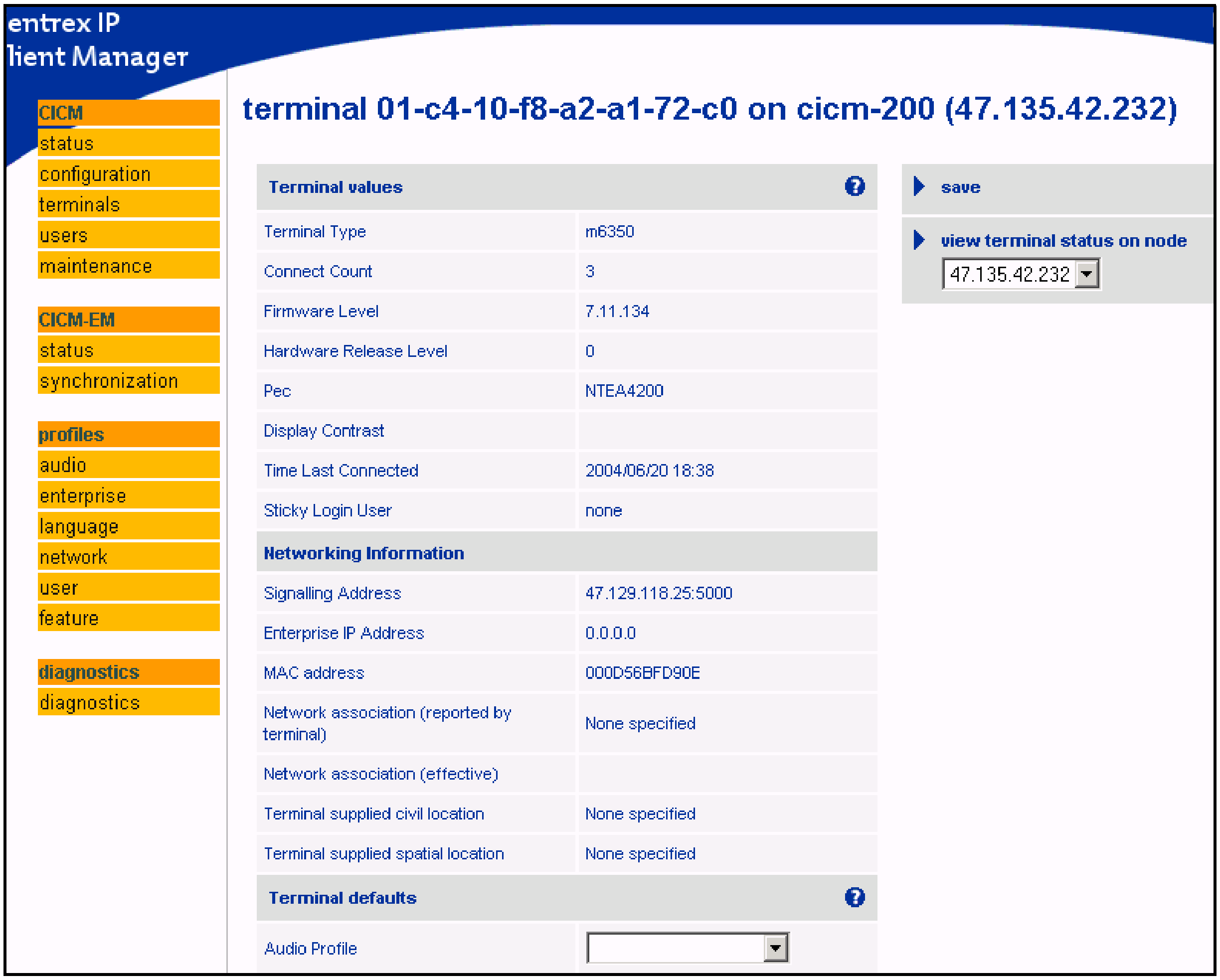


terminal audit results on cicm-200

MAC Address	Last User	Last User Login Status	Terminal Type	PEC	Firmware / Software Level	Connection Count	Sticky Login User ID	Last Connected
01-C4-10-F8-A2-A1-72-C0			m6350	NTEA4200	7.11.134	3	None	2004/06/20 18:38
31-38-00-0A-E4-03-A3-45			i2002	NTDU91AA	3.43	3	None	2004/06/20 16:55
31-38-00-0A-E4-06-99-AE			i2004	NTDU92AA	3.43	2	None	2004/06/20 14:10
31-38-00-60-38-DD-01-5F			i2002	NT2K00GI	1.63	2	None	2004/06/20 14:05
46-D0-90-30-46-D0-90-30			m6350	NTEA4200	7.11.140	2	None	2004/06/20 18:00

5 To view terminal values, networking information, and terminal defaults for a specific terminal, click on the terminal ID (MAC Address) on the list.

*Response: The **terminal <name> on <cicm-nnn> (<IP address>)** page opens.*



terminal 01-c4-10-f8-a2-a1-72-c0 on cicm-200 (47.135.42.232)

Terminal values	
Terminal Type	m6350
Connect Count	3
Firmware Level	7.11.134
Hardware Release Level	0
Pec	NTEA4200
Display Contrast	
Time Last Connected	2004/06/20 18:38
Sticky Login User	none
Networking Information	
Signalling Address	47.129.118.25:5000
Enterprise IP Address	0.0.0.0
MAC address	000D56BFD90E
Network association (reported by terminal)	None specified
Network association (effective)	
Terminal supplied civil location	None specified
Terminal supplied spatial location	None specified
Terminal defaults	
Audio Profile	

6 This procedure is complete.

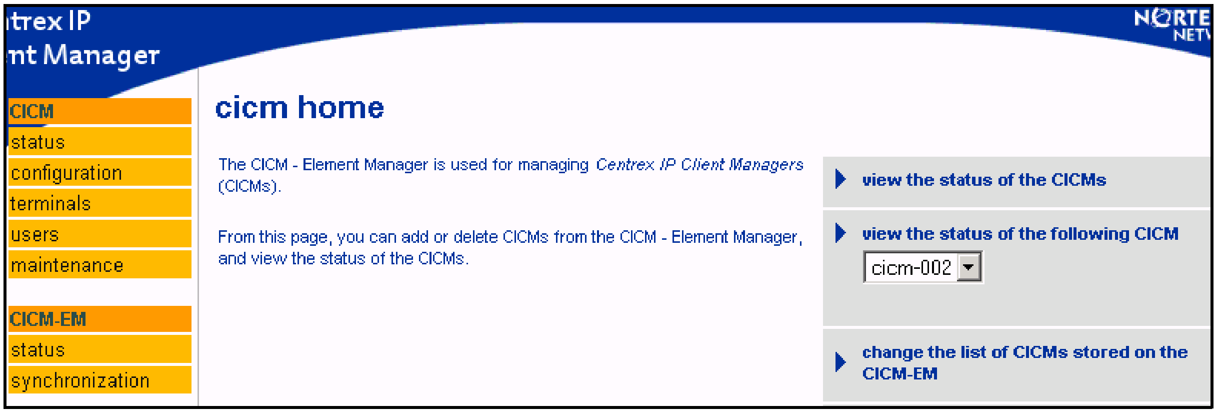
Viewing CICM information at the node level

The web interface can be used to collect statistics about the number of calls that are handled by the CentrexIP International Gateway. These statistics are collected and displayed per node.

At the cicm - element manager home page

1 Click on the **status** link from **CICM** section of the left menu.

*Response: The **cicm home** page opens.*


ıtrex IP
nt Manager
NORTE
NETW
CICM
status
configuration
terminals
users
maintenance
CICM-EM
status
synchronization
view the status of the CICMs
view the status of the following CICM
cicm-002
change the list of CICMs stored on the CICM-EM

cicm home

The CICM - Element Manager is used for managing *Centrex IP Client Managers* (CICMs).

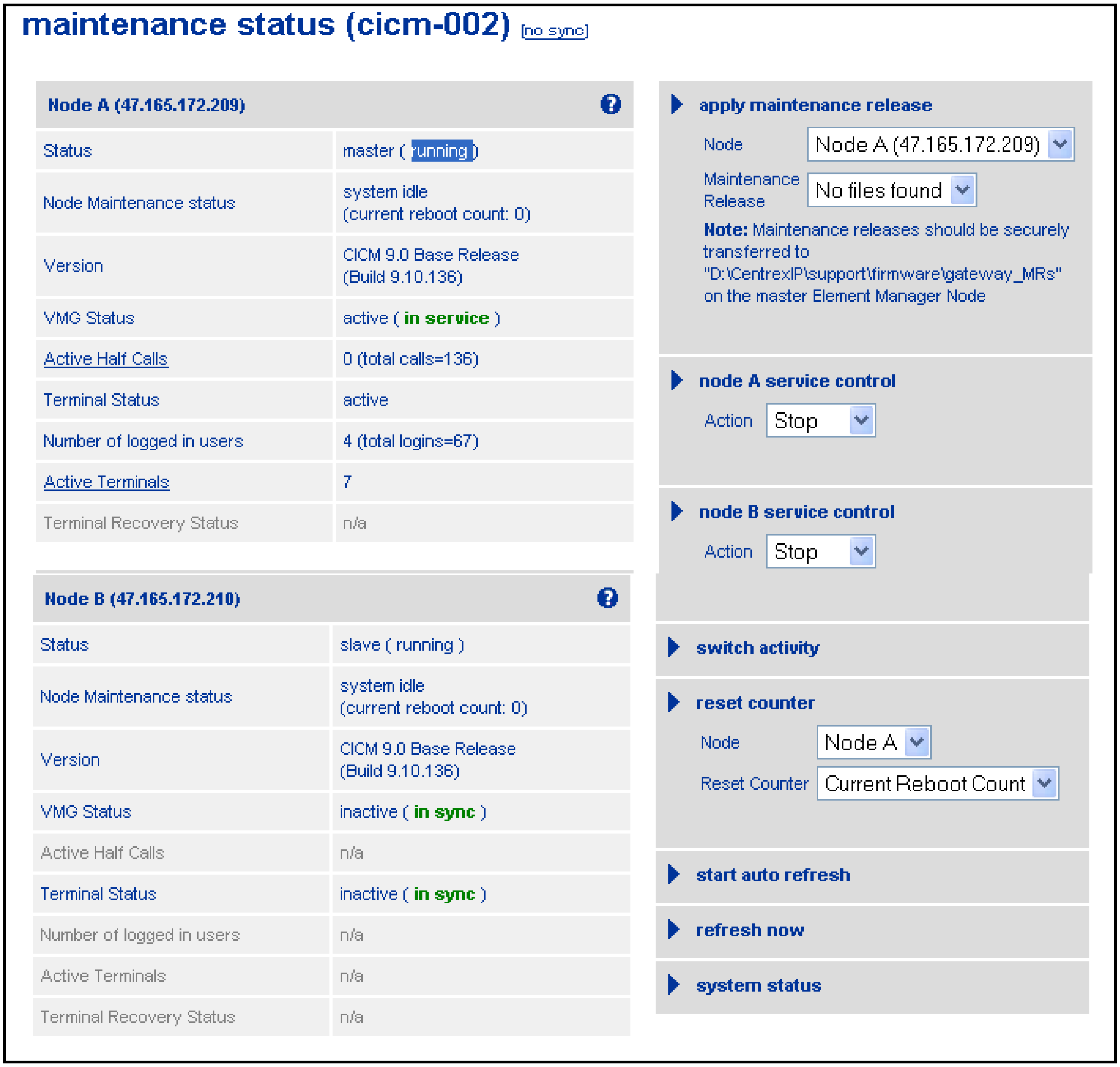
From this page, you can add or delete CICMs from the CICM - Element Manager, and view the status of the CICMs.

2 Select the CICM to be viewed from the drop-down menu of **view the status of the following CICM** on the right menu, then click on **view the status of the following CICM**.

*Response: The **<cicm-nnn> cicm status** page opens.*

3 Click on **perform maintenance on <cicm-nnn>** on the right menu.

*Response: The **maintenance status <cicm-nnn>** page opens. Below is an example.*



maintenance status (cicm-002) [no sync]

Node A (47.165.172.209)	
Status	master (running)
Node Maintenance status	system idle (current reboot count: 0)
Version	CICM 9.0 Base Release (Build 9.10.136)
VMG Status	active (**in service**)
Active Half Calls	0 (total calls=136)
Terminal Status	active
Number of logged in users	4 (total logins=67)
Active Terminals	7
Terminal Recovery Status	n/a

Node B (47.165.172.210)	
Status	slave (running)
Node Maintenance status	system idle (current reboot count: 0)
Version	CICM 9.0 Base Release (Build 9.10.136)
VMG Status	inactive (**in sync**)
Active Half Calls	n/a
Terminal Status	inactive (**in sync**)
Number of logged in users	n/a
Active Terminals	n/a
Terminal Recovery Status	n/a

apply maintenance release

Node: Node A (47.165.172.209)

Maintenance Release: No files found

Note: Maintenance releases should be securely transferred to "D:\CentrexIP\support\firmware\gateway_MRs" on the master Element Manager Node

node A service control

Action: Stop

node B service control

Action: Stop

switch activity

reset counter

Node: Node A

Reset Counter: Current Reboot Count

start auto refresh

refresh now

system status

4 This procedure is complete.

Viewing the record of backup sets for a CICM

Use this procedure to view the record of backup sets (backup execution times) for a CICM.

At the CICM home page of the Element Manager web pages

1 Select the CICM name from the drop-down menu of **show the backup sets available for** on the right menu, then click on **show the backup sets available for.**

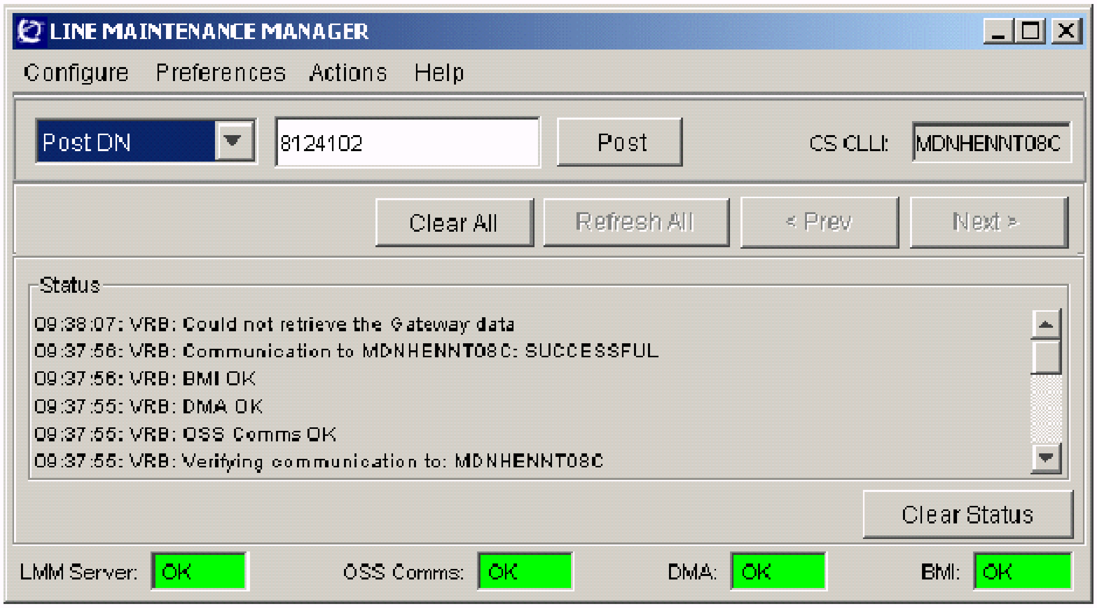
*Response: The **<cicm-nnn> backup sets on <cicm-em_name>** page opens and displays a table of backup sets for the CICM.*

2 This procedure is complete.

Line Maintenance Manager

The Line Maintenance Manager (LMM) is a GUI provided by the CS2000 Management Server to replace/emulate the functionality provided by the MAPCI tool on the CS2000 Core.

Example: Line Maintenance Manager



Post DN: 8124102

CS CLLI: MDNHENNT08C

Status

```
09:38:07: VRB: Could not retrieve the Gateway data
09:37:56: VRB: Communication to MDNHENNT08C: SUCCESSFUL
09:37:56: VRB: BMI OK
09:37:55: VRB: DMA OK
09:37:55: VRB: OSS Comms OK
09:37:55: VRB: Verifying communication to: MDNHENNT08C
```

LMM Server: OK OSS Comms: OK DMA: OK BMI: OK

The LMM provides for the following commands:

- BSY
- RTS
- FRLS
- INB

The LMM also provides the functionality to post a gateway in addition to individual lines.