|  |
| --- |
|  |
|  |
|  |

EXPERiUS Application Server

Security

Release: 11.2

Document Revision: 10.02

[www.genband.com](http://www.genband.com/) NN48111-612

EXPERiUS Application Server Release: 11.2

Publication: NN48111-612 Document status: Standard

Document release date: 12 January 2016

Copyright © 2010-2016 GENBAND. All rights reserved. Use of this documentation and its contents is subject to the terms and conditions of the applicable end user or software license agreement, right to use notice, and all relevant copyright protections.

GENBAND, the GENBAND corporate logo and tagline, and certain of GENBAND's product and solution names are registered trademarks of GENBAND and its affiliates.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, GENBAND AND/OR ITS LICENSORS PROVIDES THIS DOCUMENT "AS IS" WITHOUT

WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

THE INFORMATION CONTAINED HEREIN IS THE PROPERTY OF GENBAND OR ITS LICENSORS AND MUST NOT BE DISCLOSED, OTHER THAN TO EMPLOYEES OF GENBAND OR CUSTOMERS WITH NEED- TO-KNOW, WITHOUT THE PRIOR WRITTEN CONSENT OF GENBAND OR ITS LICENSORS. THE INFORMATION MUST NOT BE DISCLOSED TO SUBCONTRACTORS OR REGULATORY AUTHORITIES. GENBAND MUST BE NOTIFIED OF ANY REQUEST OR ORDER FOR DISCLOSURE PRIOR TO SUCH DISCLOSURE.

For access to the Document Center, log in through the Customer Support website at [http://cust.genband.com](http://cust.genband.com/).

Software and documentation owned by or under license with Nortel Networks included in this Release or in any document provided with this Release is Copyright © 2010 Nortel Networks or its licensors. All rights reserved. Use of this software and/or documentation and its contents is subject to the terms and conditions of the applicable end user or software license agreement, right to use notice, and all relevant copyright protections.

###### 3

**Contents**

### [New in this document 9](#_bookmark0)

### [Introduction 11](#_bookmark3)

### [Platform security configuration 13](#_bookmark4)

[Platform security configuration overview 13](#_bookmark5)

[BIOS password control 13](#_bookmark6)

[Configuring the BIOS administrative password 15](#_bookmark7)

[Administrative users provisioning overview 16](#_bookmark8)

[Administrative user roles 16](#_bookmark9)

[Sudo access control 18](#_bookmark10)

[Administrative account timers 18](#_bookmark11)

[Security logs 19](#_bookmark12)

[Syslog 19](#_bookmark13)

[System audit 19](#_bookmark14)

[Failed log ons 20](#_bookmark15)

[File activity in restricted areas 21](#_bookmark16)

[Backup of security logs 21](#_bookmark17)

[System alarms 21](#_bookmark18)

[Password complexity 22](#_bookmark19)

[Individual user accounts 22](#_bookmark20)

[Preconfigured accounts 23](#_bookmark21)

[Platform user management 24](#_bookmark22)

[Modifying password complexity rules 26](#_bookmark24)

[CLI mode 27](#_bookmark25)

[Changing the password for system accounts 30](#_bookmark26)

[Creating individual user accounts 31](#_bookmark27)

[Menu mode 31](#_bookmark28)

[CLI mode 32](#_bookmark29)

[Deleting a user account 33](#_bookmark30)

[Menu mode 33](#_bookmark31)

[CLI mode 34](#_bookmark32)

[Modifying user roles 34](#_bookmark33)

[Menu mode 34](#_bookmark34)

[CLI mode 35](#_bookmark35)

[Changing the state of a user account 35](#_bookmark36)

[Menu mode 35](#_bookmark37)

[CLI mode 36](#_bookmark40)

[Listing server user accounts 37](#_bookmark41)

[Menu mode 37](#_bookmark42)

[CLI mode 37](#_bookmark43)

[Managing sudo access for local users 38](#_bookmark44) [Menu mode 38](#_bookmark45)

[CLI mode 39](#_bookmark48)

[Managing sudo access for central users 39](#_bookmark49) [Menu Mode 39](#_bookmark50)

[CLI mode 40](#_bookmark51)

[Resetting a user account password 41](#_bookmark52) [Loading user accounts 41](#_bookmark53)

[Listing central users on this system 43](#_bookmark54) [Menu mode 43](#_bookmark55)

[CLI mode 44](#_bookmark56) [Deleting a central user 44](#_bookmark57)

[CLI mode 45](#_bookmark58)

[Configuring warning banners 45](#_bookmark59) [File system integrity administration 46](#_bookmark62)

[Creating an FSI baseline 46](#_bookmark63)

[Verifying the file system against a baseline 46](#_bookmark64) [Managing FSI baselines 47](#_bookmark65)

[Modification of SSH Ciphers and Message Authentication Codes 47](#_bookmark66) [Modifying SSH Ciphers and Message Authentication Codes 47](#_bookmark67)

### [Network security configuration 51](#_bookmark68)

[Access control rules 51](#_bookmark69)

[Access control rules overview 51](#_bookmark70)

[Trusted nodes 52](#_bookmark71)

[Trusted ports 54](#_bookmark72)

[External trusted node 57](#_bookmark73)

[Internal trusted node 57](#_bookmark74)

[Internal trusted node in a two server system 57](#_bookmark75)

[Internal trusted node in a four server system 57](#_bookmark76)

[Internal trusted node in a four plus server system 58](#_bookmark77)

[Access control tools 60](#_bookmark78)

[Access control default system configuration 60](#_bookmark79)

[Access control limitations and restrictions 61](#_bookmark80)

[Access control configuration 61](#_bookmark81)

[Trusted node configuration 62](#_bookmark83)

[Adding a trusted node 63](#_bookmark84)

[Listing trusted nodes 65](#_bookmark88)

[Modifying a trusted node 65](#_bookmark89)

[Removing a trusted node 67](#_bookmark90)

[Specifying Ports For Trusted Nodes and Subnets 67](#_bookmark91)

[Adding Ports for Trusted Nodes and Subnets 68](#_bookmark92)

[Removing Ports for Trusted Nodes and Subnets 68](#_bookmark93)

[Trusted port configuration 68](#_bookmark94)

[Listing the trusted ports 69](#_bookmark95)

[Modifying a trusted port 69](#_bookmark96)

[Enforcing access control rules 70](#_bookmark97)

[Importing access control rules 71](#_bookmark98)

[Viewing all configured access control rules 73](#_bookmark99)

[Rolling back to the previous access control configuration 73](#_bookmark100)

[Restoring the access control default configuration 73](#_bookmark101)

[IPSec configuration overview 74](#_bookmark102) [Secure communication 74](#_bookmark103)

[IPSec configuration on a live AS system 75](#_bookmark104) [BCP7200 Fault Tolerant System 75](#_bookmark105)

[IPsec configuration tools 76](#_bookmark106)

[Certificate and CRL update in IPSec 77](#_bookmark107) [IPsec limitations and restrictions 77](#_bookmark108)

[IPSec configuration 78](#_bookmark109)

[Pre-shared key management 81](#_bookmark111) [Adding a pre-shared key 81](#_bookmark112)

[Importing Pre-shared Keys 82](#_bookmark113) [Modifying a Preshared Key 82](#_bookmark114)

[Deleting Preshared Key Configurations 82](#_bookmark115) [IPsec policy management 83](#_bookmark116)

[Adding a new IPsec policy 83](#_bookmark117) [Importing IPsec policies 84](#_bookmark118) [Listing IPsec policies 86](#_bookmark119) [Modifying an IPsec policy 86](#_bookmark120) [Deleting an IPsec policy 87](#_bookmark121)

[Rolling back to the previous IPsec policy configuration 88](#_bookmark122) [IKE rules management 89](#_bookmark123)

[Adding a new IKE phase 1 rule 89](#_bookmark124) [Adding a new IKE phase 2 rule 91](#_bookmark125) [Importing IKE rules 93](#_bookmark126)

[Listing IKE rules 95](#_bookmark127)

[Modifying an IKE phase 1 rule 96](#_bookmark128) [Modifying an IKE phase 2 rule 97](#_bookmark129) [Deleting an IKE rule 99](#_bookmark130)

[Rolling back to the previous IKE rule configuration 99](#_bookmark131) [Restoring IKE rules default configuration 100](#_bookmark132)

[IPsec service management 101](#_bookmark133)

[Starting or restarting the IPsec service—ipscfg method 101](#_bookmark134) [Starting or restarting the IPsec service—CLI method 102](#_bookmark135) [Stopping the IPsec service—ipscfg method 102](#_bookmark136)

[Stopping the IPsec service—CLI method 103](#_bookmark137) [IPsec configuration between OpenSwan and Racoon 103](#_bookmark138)

[Setting the OpenSwan (PLE4) side 105](#_bookmark139)

[Setting the Preshared Key in OpenSwan 105](#_bookmark140) [Setting the IKE configuration in OpenSwan 105](#_bookmark141) [Starting IPsec on OpenSwan 106](#_bookmark142)

[Setting the Racoon side 106](#_bookmark143)

[Setting the Preshared Key on Racoon 106](#_bookmark144) [IPsec Policy configuration 108](#_bookmark148)

[IPsec IKE configuration 109](#_bookmark152)

[Starting IPsec service on Racoon 111](#_bookmark156)

[Stopping IPsec between OpenSwan and Racoon 111](#_bookmark157) [Stopping IPsec service on OpenSwan 111](#_bookmark158) [Stopping IPsec service on Racoon 111](#_bookmark159)

[Viewing trusted node and port configurations with iptstatus 112](#_bookmark160) [DSCP marking configuration 113](#_bookmark161)

[Listing the DSCP marking configurations 113](#_bookmark162) [Modifying DSCP marking values 114](#_bookmark163)

[Modifying the DSCP marking status 115](#_bookmark164)

[Modifying DSCP Call Signaling and OAMP Values 116](#_bookmark165) [Increasing network security with SNMP 119](#_bookmark166)

[Configuring an SNMP profile 120](#_bookmark167) [Enabling a license key 121](#_bookmark168) [Configuring a server 123](#_bookmark169)

|  |  |  |
| --- | --- | --- |
| [**Central Authentication and Authorization**](#_bookmark170)[Platform Authentication and Authorization 126](#_bookmark171) [Application Authentication and Authorization 127](#_bookmark172) |  | [**125**](#_bookmark170) |
| [RADIUS Proxy 128](#_bookmark173)  [JPAM 128](#_bookmark174)  [Role Mapping 128](#_bookmark175)  [Feature Dependencies and Restrictions 130](#_bookmark176) [Supported Platforms 130](#_bookmark177)  [Configuration of Central Authentication and Authorization 131](#_bookmark178) [SM GUI Configuration 131](#_bookmark179)  [Central Authentication and Authorization Platform CLI (caaMgt.pl)](#_bookmark180) | [132](#_bookmark180) |  |
| [Assigning multiple roles per user 146](#_bookmark181)  [Migrating users to a central RADIUS server 147](#_bookmark182) |  |  |
| [**Certificate management overview**](#_bookmark183) |  | [**149**](#_bookmark183) |
| [**CA certificate management for IPsec**](#_bookmark184)  [Installing a CA certificate 151](#_bookmark185) [Listing installed CA certificates 152](#_bookmark186) [Uninstalling a CA certificate 153](#_bookmark187) [Renewing a CA certificate 153](#_bookmark188) |  | [**151**](#_bookmark184) |
| [**CA-signed certificate management for IPsec**](#_bookmark189)  [Generating the private key 155](#_bookmark190) [Generating a CSR 156](#_bookmark191) [Generating a PKCS12 file 158](#_bookmark192)  [Validating a CA-signed certificate 160](#_bookmark193)  [Installing a CA-signed certificate and private key pair 160](#_bookmark194) |  | [**155**](#_bookmark189) |

[Listing installed CA-signed certificates and private key pairs 161](#_bookmark195) [Uninstalling CA-signed certificates and private key pairs 162](#_bookmark196) [Renewing a CA-signed certificate 163](#_bookmark197)

### [Certificate Revocation List management for IPsec 165](#_bookmark198)

[Listing installed CRLs 165](#_bookmark199)

[Installing a CRL 166](#_bookmark200)

[Uninstalling a CRL 166](#_bookmark201)

[Renewing the CRL 167](#_bookmark202)

### [SSL/TLS certificate management 169](#_bookmark203)

### [CA-signed certificate management 171](#_bookmark204)

### [SSL/TLS certificate management with the System Management](#_bookmark205) [Console 173](#_bookmark205)

[Importing an internal certificate to the keystore 173](#_bookmark206)

[Viewing an internal certificate in the keystore 174](#_bookmark207)

[Removing an internal certificate from the keystore 174](#_bookmark208) [Importing a CA certificate to the truststore 175](#_bookmark209) [Viewing a CA certificate in the truststore 175](#_bookmark210) [Removing a CA certificate from the truststore 176](#_bookmark211) [Importing a CRL 176](#_bookmark212)

[Viewing a CRL 177](#_bookmark213) [Removing a CRL 178](#_bookmark214)

[System security configuration and management 179](#_bookmark215)

[Security configuration and management overview 179](#_bookmark216)

[Administrative security services 179](#_bookmark217)

[Password policies and domains 180](#_bookmark218)

[Administrative user accounts 181](#_bookmark219)

[Domain security 183](#_bookmark220)

[Foreign domains 183](#_bookmark221)

[Administrator security configuration 184](#_bookmark222)

[Configuring database user accounts 184](#_bookmark223)

[Resetting database user accounts 185](#_bookmark224)

[Configuring a new System Management Console role 186](#_bookmark225)

[Configuring a new System Management Console user 191](#_bookmark227)

[Assigning a role to a System Management Console user 192](#_bookmark228)

[Configuring System Management Console password rules 193](#_bookmark229)

[Configuring log on and session rules 194](#_bookmark230)

[Configuring a new Provisioning Client role 196](#_bookmark231)

[Configuring a new Provisioning Client user 197](#_bookmark232)

[Configuring warning banners 198](#_bookmark233)

[Adding an External SIP Proxy 199](#_bookmark234)

[Adding a foreign domain 201](#_bookmark235)

[Administrator security management 203](#_bookmark236)

[Resetting the password for the database sys account 203](#_bookmark237)

[Resetting the password for the database system account 203](#_bookmark238)

[Resetting the passwords for the database internal accounts 204](#_bookmark239)

[Resetting the password for an individual database user account 204](#_bookmark240)

[Changing the password for the database schema user account 205](#_bookmark241)

[Changing the password for the database application account 206](#_bookmark242)

[Modifying log on and session rules 207](#_bookmark244)

[Modifying System Management Console password rules 208](#_bookmark245)

[Modifying a System Management Console role 210](#_bookmark246)

[Modifying a System Management Console user 211](#_bookmark247)

[Disabling a System Management Console user account 212](#_bookmark248)

[Disabling password aging rules for an account 212](#_bookmark249)

[Viewing and forcing off users 213](#_bookmark250)

[Exporting configuration data for System Management Console 213](#_bookmark251)

[Importing configuration data for System Management Console 214](#_bookmark252)

[Deleting a System Management Console role 215](#_bookmark253)

[Deleting a System Management Console user 215](#_bookmark254)

[Resetting the password for the System Manager admin account 215](#_bookmark255)

[Modifying a Provisioning Client role 216](#_bookmark256)

[Listing Provisioning Client users 217](#_bookmark257)

[Deleting a Provisioning Client user 217](#_bookmark258)

[Resetting the password for the Provisioning Manager admin account 218](#_bookmark259)

[Configuring cipher changes 219](#_bookmark261)

[Adjusting the cipher suites 220](#_bookmark262)

# New in this document

The following sections detail what’s new in *EXPERiUS AS — Security*

(NN48111–612):

* [“Document revision 10.02” (page 9)](#_bookmark1)
* [“Document revision 10.01” (page 9)](#_bookmark2)

## Document revision 10.02

January 12, 2016. Release 11.2

### New features

* Added the new procedure [“Modification of SSH Ciphers and Message](#_bookmark66) [Authentication Codes” (page 47)](#_bookmark66).

## Document revision 10.01

July 17, 2015. Release 11.2.

### Modifications

* Added SSL/TLS cipher information and the procedure to configure cipher changes. See [“Configuring cipher changes” (page 219)](#_bookmark261).

# Introduction

This document contains the procedures required to configure and administer security for the Application Server (AS) system.

For more information about AS administration and configuration, see *EXPERiUS Application Server — Administration* (NN48111-611) , and *EXPERiUS Application Server — Configuration* (NN48111–511) or *C20– EXPERiUS — Configuration* (NN10399-110).

**Attention**

Throughout this document, the terms “system” and “server” refer to the AS unless otherwise noted.

**Prerequisites**

* The AS installation is complete.
* You must be familiar with the System Management Console.

**Platform security configuration**

This chapter explains the procedures to configure and manage the security of the platform on which the Application Server (AS) application runs.

## Platform security management navigation

* + [“Platform security configuration overview” (page 13)](#_bookmark5)
  + [“Configuring the BIOS administrative password” (page 15)](#_bookmark7)
  + [“Password complexity” (page 22)](#_bookmark19)
  + [“Administrative user roles” (page 16)](#_bookmark9)
  + [“Individual user accounts” (page 22)](#_bookmark20)
  + [“Preconfigured accounts” (page 23)](#_bookmark21)
  + [“Platform user management” (page 24)](#_bookmark22)
  + [“File system integrity administration” (page 46)](#_bookmark62)

For information about initial BIOS configuration, see *EXPERiUS AS — Installation*.

## Platform security configuration overview

This section contains information related to platform security configuration.

### BIOS password control

The planar BIOS enables the user to configure both an Administrative and Power-on password. The BIOS also refers to the Administrative password as the Privileged Access Password in console messages displayed during BIOS initialization.

BIOS passwords are enforced at the end of BIOS initialization when the message BIOS Installed Successfully displays.

The following table illustrates the password enforcement type performed by the BIOS at this point in the BIOS execution.

**Bios Password Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **BIOS Password Control** | | | |
| **Password Configured** | | **Password Requirement** | |
| **Power-on password** | **Admin** | **BIOS Entry Requested (F1 pressed)** | **Standard Initialization (F1 not pressed)** |
| No | No | None | None |
| No | Yes | Admin | None |
| Yes | No | Power-on password | Power-on password |
| Yes | Yes | Power-on password (limited access) or Admin | Power-on password or Admin |

Two basic scenarios are possible:

* + The administrator presses the F1 key during the early stages of BIOS initialization with the intent of entering BIOS setup when BIOS initialization finishes. If at least one password is configured, the password must be entered to enter into the BIOS setup. If both passwords are configured, specifying the Power-on password gives the administrator only limited access, where no BIOS configuration changes can be made.
  + The administrator does not press the F1 key during the early stages of BIOS initialization. If a Power-on password is configured (not recommended), BIOS requires the administrator to enter the password to allow the system to continue past the BIOS initialization. If configured, the administrative password is also accepted.

If an Administrator password is configured, an administrator entering BIOS with only a Power-on password receives access to the following menus:

* + System Summary—This menu provides information such as processor model, USB devices, and memory information.
  + System Information—This menu provides information such as the machine type and model number, serial number, firmware levels, and installed system cards.

When configuring the Administrator password, changing the value of the Power-on password changeable by user field to Yes provides limited BIOS access to the administrator. The following are the additional menu items available:

* + System Security—This menu provides the facility to change or delete the Power-on password.

The following general points also apply to Administrative and Power-on BIOS passwords:

* + Each password can be up to seven characters in length.
  + The passwords can consist of any characters.
  + If both passwords are configured, a forgotten Power-on password can be reset (deleted and re-configured) by entering the BIOS with the Administrative password.
  + If a single password is set, and is forgotten, it cannot be recovered using the BIOS menu.
  + If both the Administrative and Power-on password are set, and the Administrative password is forgotten, it cannot be recovered using the BIOS menu.
  + Neither passwords are affected when the factory defaults of the main BIOS are restored to factory default.

## Configuring the BIOS administrative password

Use this procedure to configure the planar BIOS administrative password for a server, only if your local security policy requires that you secure access to the BIOS.



**WARNING**

GENBAND does not recommend that you configure the planar BIOS administrative password. If you forget the configured password, you cannot reset the password or access the BIOS for configuration purposes. If you require access to the BIOS and do not know the password, you must replace the server motherboard (planar).

### Procedure steps

###### Step Action

1. Press **F1** to enter the BIOS Configuration/Setup Utility during startup.
2. Select **System Security, Administrator Password** from the top level of the BIOS Configuration/Setup Utility.
3. Use the **Up** and **Down** arrow keys to position the cursor in the **Enter Administrator Password** text box.
4. Type the password (maximum of 7 characters).
5. Use the **Down** arrow key to position the cursor in the **Enter Administrator Password Again** text box.
6. Type the password again.
7. Highlight **Change Administrator Password** and press **Enter**.

The following message appears:

*The new administrator password will replace any existing*

*administrator password. Your password can be up to seven characters long.*

1. Press **Enter** to proceed with the password change. You can press Esc to abort the change.
2. Press **Esc** repeatedly until the top menu of the BIOS Configuration/Setup Utility appears.
3. Select **Exit Setup** to exit.

**--End--**

## Administrative users provisioning overview

This section contains information about administrative user roles.

### Administrative user roles

The following administrative user roles are defined for the system:

* + System Security Administrator (SSA)—

This is equivalent to what is commonly thought of as the system administrator, but includes additional security responsibilities. The function of the SSA includes the following responsibilities:

* + - Maintain the operating system configuration.
    - Maintain the hardware and network configuration.
    - Maintain the security configuration (including IPsec and IP Tables configuration).
    - Perform backup and restore of all elements on the system (including any application-specific data).
    - Perform user management (add, delete, modify users) and password configuration.
    - Perform IPSec and certificate management.
    - Manage IP Tables access control.
    - Run the File System Integrity tools.
  + Database Administrator (DBA)—

The function of the DBA includes the following responsibilities:

* + - Maintain the database schemas and files.
    - Perform database backup and table management as required.
  + Security Auditor (SA)—

The function of the SA includes the following responsibilities:

* + - Collect and read the security audit log and syslogs at the platform level.
    - Back security logs up to a remote server.
  + Application Administrator (AA)—

The function of the AA includes the following responsibilities:

* + - Install, patch, and upgrade the AS software.
    - Manage AS software configuration.
  + Backup Administrator (BA)—

These users can perform only system backups. BAs cannot:

* + - Perform any operation on the server except backups.
    - Perform restores: Only the SSA or root user can perform restores.
  + OSS Administrator (OSS)—

This role allows the account to be used by downstream processors to connect to the server and collect OSS logs.

* + RPS Administrator (RPS)—

This role allows the account to be used to deliver patches through the GENBAND patch delivery system.

Roles grant users group access permissions to certain files. When you add a new user to the system, you assign the user to one or more of the above roles. The user can then perform the functions associated with that role.

A primary role of the administrator defines the administrator’s primary group. This setting configures permissions and group ownership for any files that are generated by the administrator. Any tools in this system that extract or create files uses the administrator’s primary role to determine the appropriate group settings. The primary role is automatically assigned when the administrator is created because it is the first role assigned. The primary role can be changed.

All roles, other than the Backup Administrator role, are intended to manage some aspect of the system. Because of this and the use of discretionary access groups to control access to system resources, administrators with a primary role of SSA, SA, AA, or DBA have a primary GID that is traditionally reserved for system accounts (less than 500).

### Sudo access control

Most tools on the server require root level access to system files. This is achieved through the use of sudo. The following are two methods to allow administrators to run commands under sudo:

* + Define a set of commands that can be executed as root for a given role
  + Grant an administrator root level access to all system commands

By default, when an administrator is assigned a role, they are granted access to all commands defined for that role. However, if required, the root administrator can grant all root access controls to an individual administrator.

Commands that are executed as sudo are recorded in /var/log/secure and only the security administrator can view these logs. Administrators who are granted sudo access do not need to know the root password of the system to invoke root level commands; they use their own current password.

Only the root user has the privilege to grant or deny all sudo level access to administrators. If an administrator is already logged on before being granted sudo access, the sudo access will be invoked only the next time the administrator logs in.

The sudo menu option in the userMgt script is only visible when the script is executed by root.

### Administrative account timers

The idle session timer is used to automatically log out administrators that are not actively using their sessions. After the configured time has elapsed and there is no administrator activity, the session closes automatically.

Changes to the idle session timer value do not effect currently existing sessions. Administrators must log out and log in for this setting to take effect.

The pwConfig tool configures the timeout value by configuring the Idle session timeout (seconds) field. The value can be configured also by an SSA using the command line interface.

To reduce the effectiveness of password guessing attacks, account lockout can be configured on the system. If account lockout is enabled, the system temporarily locks an account after a specified number of log on failures.

To enable account lockout, use the pwConfig tool to configure the value of the 'Deny after this many log on failures' field to a value other than zero. To subsequently disable account lockout, configure the value back to zero.

You can also configure this value using the command line interface.

The amount of time that the account is locked out is configured using the pwConfig tool to configure the value of the Unlock account duration (seconds) field. If account lockout is disabled, this field has no effect. You can also configure this value using the command line interface.

When an account reaches the lockout threshold, a security log is generated. An SSA user can unlock an administrator’s account using the userMgt tool to disable and subsequently enable the locked out administrator.

### Security logs

This section contains information about security logs.

### Syslog

System syslogs are stored in /var/log/messages. Security related syslogs are stored in /var/log/secure. Both of these syslogs can be viewed by administrators who have the role of SA or SSA. Syslogs cannot be deleted from the system, except by root. However, the SA can force the logs to rotate using the logrotate command.

Syslogs are rotated daily and will store up to 15 days of logs. After 15 days, the oldest log is deleted on a daily basis. It is recommended that the logs be transferred from the server within 15 days to prevent the loss of any log files due to file rotation.

Syslogs can also be sent to a syslog server. This is normally configured during system installation but the SSA may choose to configure this at run time by issuing the reconfigure script. You must configure the remote syslog server as a trusted node, if an ACL firewall is configured on the system.

### System audit

Audit logs track and monitor administrative user behavior. The system generates these logs and they can only be viewed by the SA or SSA. Logs cannot be modified or deleted by the SA or SSA, except by root.

Audit logs are stored in /var/log/audit and can be viewed by administrators who have the SSA or SA roles. Audit logs can be forced to rotate by issuing the logrotate command.

Audit logs record the following data:

* + time and date of incursion
  + userID and PID of incursion
  + command issued
  + success or fail status
  + object operated on
  + terminal type
  + exit code

Audit logs are rotated daily and will store up to 15 days of logs. After 15 days, the oldest log is deleted on a daily basis. In the event, the /var/log partition fills up, and any SSA with root access can log on and delete these logs. GENBAND recommends that you backup the logs before deleting.

If the system cannot write to the audit log, a message is sent to syslog indicating the failure. When the free disk space for this partition drops below 750 MB, a warning message is sent to syslog.

When the free disk space for this partition drops below 250 MB, another message is sent to syslog indicating that the disk is full, and logging may be interrupted. In the event the disk partition fills up, GENBAND recommends that you log on as root and delete the logs after first backing them up.

System audit is normally configured during initial installation, but the SSA can configure audit log settings by issuing the following command:

>auditConfig

If the setting is changed, the system must be rebooted. System audit can also be configured through the reconfigure script.

The following tools can be used by any SSA or SA users to view audit logs:

* + >aureport – used to get a summarized report on audit logs.
  + >ausearch – search for patterns in audit log. (use

--help

for instructions)

Users with SSA or SA roles can also view the audit logs using vi and grep, if required.

### Failed log ons

Failed Login attempts can be viewed by issuing the grep command for the audit log files to search for the words "authentication" and "failed".

The resulting output displays the following data:

* + record ID for audit
  + user ID and log on name
  + host where the log on was attempted

The summary report also displays the number of failed attempts.

### File activity in restricted areas

The file system is locked down mainly by using file permissions appropriate to the administrator’s role. However, these files require traceability to any modifications or additions.

Auditing is based on watch rules on files and directories. The watch rule on directories includes all the files in that directory. Most of the watch rules are on write or append to the directory and files.

When audited, the record includes the following data:

* + UID of user accessing the file
  + process ID
  + the file or directory in question
  + success or fail status
  + command executed on the file or directory

### Backup of security logs

Security logs can be transferred from the server to a secured server. This action does not delete the security logs from the server as only a copy of the logs are transferred. If deleting logs is required to free up disk space, this must be performed by the root user.

### System alarms

The following disk partitions can be monitored from the SM for utilization:

* + boot
  + /var
  + /var/mcp
  + /var/log
  + /admin
  + /home
  + /opt
  + /tmp

In the SM console, select Server, Monitor, Disk Utilization. Configure the alarm thresholds for setting the alarm when the disk partition fills up past a specified limit, and clear the alarm when the disk space is freed up.

### Password complexity

You manage password complexity on a per-server basis. There is no automatic password complexity synchronization performed between servers. Therefore, if you change any value on one server, you must manually change it on all of the other servers.

If a user's account is locked because of successive failed attempts to log on, the user cannot log on to the system until the lockout period expires. However, the system administrator can manually re-enable the account within the lockout period if necessary. Additionally, after 3 consecutive failed access attempts, the SSH or SFTP connection terminates and the user must re-establish the connection to log on.

The root user password does not adhere to the password complexity rules. Ensure that only a very limited number of individuals know the root password for the servers.

The backup and restore process includes all files related to password complexity.

### Individual user accounts

Individual user accounts allow for full accountability and monitoring of individual actions. If the installer chooses this option during server installation, the System Security Administrator (SSA) must create each individual user account after the installation is complete. You manage user accounts on a per-server basis. Therefore, the SSA must create identical users on each server within the system.

The SSA uses the User Management Configuration tool to create, modify, and delete users. Administrator user names must adhere to the following rules:

* + Be between 6 and 30 characters in length.
  + Begin with an alphabetic character [a-z] or [A-Z].
  + Contain any of the following characters: [a-z], [A-Z], [0-9], ‘\_’
  + Contain no spaces or tabs.

Each individual user account has its own password, which is subject to the password complexity rules. The SSA can disable or re-enable each individual user account as necessary. Individual user accounts have a home directory in /home/<userid>. If the SSA removes the user account, the home directory is also removed.

System data files associated with individual user accounts are included in the backup and restore process.

### Preconfigured accounts

If the installer chooses the preconfigured account option during server installation, the installation software creates the following user accounts:

* + ntappadm—created by the installation software. This user account's primary role is of the Application Administrator (AA) role, which replaces the GENBAND user found on previous systems.
  + ntdbadm—created by the installation software. This user account's primary role is of the database administrator (DBA) role.
  + ntsysadm—created by the installation software. This user account's primary role is the System Security Administrator (SSA) role. The ntsysadm account, by default, has ALL sudo root access. Full sudo access can be removed if required by invoking the userMgt tool as root. This account replaces the sysadmin user found on previous systems.
  + ntsecadm—created by the installation software. This user account's primary role is of the security auditor (SA) role.
  + ntbackup—created by the installation software. This user account's primary role is of the backup administrator (BA) role.

Each preconfigured account has its own password, which is subject to the password complexity rules. However, because these accounts are shared (and therefore, the password is shared) amongst multiple individuals, there is no accountability at the individual user level for these accounts. If more than one person knows the password for an account, that account is immediately less secure than if only one person knew the password.

The SSA can create additional individual user accounts. Additional individual accounts are subject to the same password complexity profile as the preconfigured accounts. The SSA user can delete preconfigured accounts. All preconfigured accounts are backed up and restored during backup and restore procedures.

The ntossadm and nortelrps accounts are protected using password authentication. These accounts are also susceptible to lockout if the password is entered incorrectly and the account lockout is configured for the system. The password on these accounts can be changed by logging in as either ntossadm or nortelrps, as appropriate, and issuing the command: **#>passwd**. Additionally, the passwords can be reset using the userMgt tool.

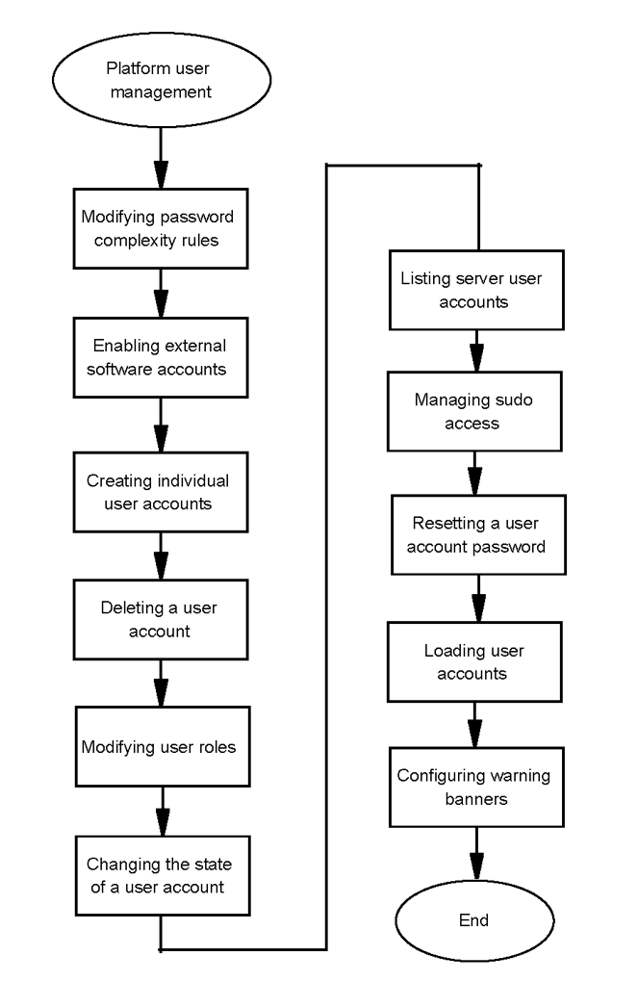
## Platform user management

This section describes how to manage password complexity requirements, create individual user accounts, and manage user role assignments to control access to the AS servers.

### Platform user management procedures

This task flow provides the procedures that you require to manage platform users. To link to any procedure, click on the link from [“Platform user](#_bookmark23) [management navigation” (page 25)](#_bookmark23).

**Platform user management**



### Platform user management navigation

* + [“Modifying password complexity rules” (page 26)](#_bookmark24)
  + [“Changing the password for system accounts” (page 30)](#_bookmark26)
  + [“Creating individual user accounts” (page 31)](#_bookmark27)
  + [“Deleting a user account” (page 33)](#_bookmark30)
  + [“Modifying user roles” (page 34)](#_bookmark33)
  + [“Changing the state of a user account” (page 35)](#_bookmark36)
  + [“Listing server user accounts” (page 37)](#_bookmark41)
  + [“Managing sudo access for local users” (page 38)](#_bookmark44)
  + [“Managing sudo access for central users” (page 39)](#_bookmark49)
  + [“Resetting a user account password” (page 41)](#_bookmark52)
  + [“Loading user accounts” (page 41)](#_bookmark53)
  + [“Listing central users on this system” (page 43)](#_bookmark54)
  + [“Deleting a central user” (page 44)](#_bookmark57)
  + [“Configuring warning banners” (page 45)](#_bookmark59)

### Modifying password complexity rules

Use this procedure to modify password complexity rules to ensure that user passwords are more secure. Password complexity rules apply only to subsequently configured passwords.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. Run the script to configure password complexity:

###### pwConfig

1. If you receive a prompt, enter your password.
2. Enter **1** to view the current configuration.
3. Press **Enter** to continue.
4. Enter **2** to change the current configuration.
5. Enter a value for **Minimum lowercase chars**.
6. Enter a value for **Minimum uppercase chars**.
7. Enter a value for **Minimum digits**.
8. Enter a value for **Minimum special chars**.
9. Enter a value for **Minimum change chars**.
10. Enter a value for **Minimum password length**.
11. Enter a value for **Deny after this many log on failures**.
12. Enter a value for **Unlock account duration (seconds)**.
13. Enter a value for **Old passwords to remember**.
14. Enter a value for **Maximum password age (days)**.
15. Enter a value for **Minimum password age (days)**.
16. Enter a value for **Password change warning (days)**.
17. Enter a value for **Idle session timeout (seconds)**.
18. Press **Enter** to continue.
19. (Optional) If you want to cancel pending (unsaved) changes, enter **3**.
20. Enter **4** to save pending changes.
21. Press **Enter** to continue.
22. Enter **5** to exit.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as an SSA.
2. Configure the minimum password length:

**pwConfig –nl <number\_of\_characters>**

1. Configure the minimum number of lowercase characters:

**pwConfig –l <number\_of\_characters>**

1. Configure the minimum number of uppercase characters:

**pwConfig –u <number\_of\_characters>**

1. Configure the minimum number of digits:

**pwConfig –d <number\_of\_characters>**

1. Configure the minimum number of special characters:

**pwConfig –s <number\_of\_characters>**

1. Configure the minimum number of changed characters:

**pwConfig –dif <number\_of\_characters>**

1. Configure the number of passwords to remember:

**pwConfig -old <number\_of\_passwords>**

1. Configure the value for deny after this many log on failures:

**pwConfig -den <number\_of\_log on\_failures>**

1. Configure the value for unlock account duration (seconds):

**pwConfig -unl <unlock\_account\_duration>**

1. Configure the maximum password age (in days):

**pwConfig –xd <number\_of\_days>**

1. Configure the minimum password age (in days):

**pwConfig –nd <number\_of\_days>**

1. Configure the number of days in advance for password expiration warnings:

**pwConfig –wd <number\_of\_days>**

1. Configure the value for idle session timeout:

**pwConfig -tmout <idle\_session\_timeout>**

**--End--**

### Modifying password complexity rules job aid

This job aid provides lists of parameters that you can modify, and those that you cannot.

You can modify the following parameters at any time:

**Parameters**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Minimum number lowercase chars | This parameter specifies the minimum number of lowercase characters (a–z) that the password must contain. The system rejects passwords that contain fewer lowercase characters.  Default: 2 |
| Minimum number uppercase chars | This parameter specifies the minimum number of uppercase characters (A–Z) that the password must contain. The system rejects passwords that contain fewer uppercase characters.  Default: 2 |
| Minimum number digits | This parameter specifies the minimum number of digit characters (0–9) that the password must contain. The system rejects passwords that contain fewer digit characters.  Default: 2 |
| Minimum special chars | This parameter specifies the minimum number of special characters (not a number or alphabetic character; for example, ! @ # $ % ^ & \*) that the password must contain. The system rejects passwords that contain fewer special characters. Default: 0 |

**Parameters (cont'd)**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Minimum change chars | This parameter specifies the minimum number of characters by which the new password must differ from the previous password. The system ignores this value if either one half of the characters in the new password are different, or if there are more than 23 characters in the new password.  Default: 0 |
| Minimum password length | This parameter specifies the minimum number of total characters a password can contain. The system rejects passwords that contain fewer characters.  Default: 8 |
| Deny after this many log on failures | This parameter specifies the number of failed attempts to log on to an account before the account is locked.  Default: 0 |
| Unlock account duration (seconds) | This parameter specifies the amount of time for which the account remains locked after log on failures.  Default: 60 |
| Old passwords to remember | This parameter specifies the number of previous passwords the system remembers. Administrators cannot reuse any password on the remembered list. Regardless of the value of this field, administrators cannot ever reuse the current password.  Default: 0 |
| Maximum password age (days) | This parameter specifies the maximum number of days that an administrator’s password can be used. After the specified number of days, the administrator must change the password to access the server. If you reduce this value, some existing passwords can immediately expire.  Default: 90 |
| Minimum password age (days) | This parameter specifies the minimum number of days between password changes. This setting discourages administrators from immediately changing their passwords back to a previously used password (password flipping).  Default: 1 |
| Password change warning (days) | This parameter specifies the number of days in advance that administrators receive warning that their passwords will expire. If an administrator logs on within this number of days before expiry, a |

**Parameters (cont'd)**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
|  | message appears to indicate that their password will expire soon.  Default: 7 |
| Idle session timeout (seconds) | This parameter specifies the number of seconds a session can be idle before it times out.  Default: 600 (10 minutes) |

The following non-configurable parameters apply to password complexity:

* + The Linux CrackLib library is used to ensure that the password is not based on the username or on a dictionary word. This library manipulates the new password in various ways to try and determine if the new password is based on the username or a dictionary word.
  + Users must change their passwords during initial log on.

Users cannot access the system with the temporary passwords.

* + The password cannot be a palindrome.

### Changing the password for system accounts

Use this procedure to change the password for internal system accounts.

The passwords for these accounts are subject to password complexity rules. Because the initial (during installation) password complexity rules are minimal, It is recommended that you change the passwords for any accounts created prior to completing the procedure to configure (harden) password complexity rules.

**Attention**

The ntossadm and nortelrps accounts should never be used by anyone other than the external software for which each is intended. You cannot delete these accounts from the system.

### Prerequisites

You must know the current password for the internal account.

### Procedure steps

###### Step Action

1. Log on to the server as the account for which you want to change the password.
2. Change the password:

###### #>passwd

1. Enter the new password.
2. Enter the new password to confirm.

**--End--**

### Creating individual user accounts

If the system uses individual accounts, the System Security Administrator (SSA) must create new accounts for each administrative user. If the system uses preconfigured accounts, the SSA user can create additional individual accounts.

### Menu mode

###### Step Action

1. Log on to the server as SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If prompted, enter your password.
2. Enter **1** to add a new user.
3. Enter a username for the new user.
4. Specify a user ID:

|  |  |
| --- | --- |
| **To** | **Do this** |
| Manually specify a user ID | Enter a number between 1000 and 10 000. |
| Have the system select a user ID | Press Enter. |

1. Enter the corresponding numbers for the user's roles.

The first role is the user's primary role. Separate multiple role entries with a comma (,).

1. Enter **Y** to continue adding users.
2. Enter the initial password for the user.

The user must change this password during the initial log on to gain access to the server.

1. Enter the initial password again.

You receive a prompt to continue adding users or to return to the main menu.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt add <username> <userid> <roles>

Separate multiple roles with a comma (,).

1. To add the administrator with an encrypted password, use -p '<passwd>'

###### userMgt add <username> <userid> <roles> -p '<passwd>'

Separate multiple roles with a comma (,).

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <userid> | This value is the user ID for the new user. |
| <username> | This value is the username for the new user. |
| <roles> | This value specifies the primary and any other roles for the user, separated by commas (,). |
| <passwd> | This value is the initial password for the user. |

**Creating individual user accounts job aid**

This job aid lists and describes the system groups defined on the system, and provides the role to groups mapping. The system groups are:

* + ntsysgrp—group for system related files
  + ntsecgrp—group for security logs
  + ntappgrp—group for MCP application files
  + ntdbgrp—group for database related files
  + ntossgrp—group for OSS files
  + ntbackupgrp—group for backup files
  + ntdropboxgrp—group for RPS files

**Role to groups mapping**

|  |  |
| --- | --- |
| **Role** | **Groups** |
| SSA—System Security Administrator | ntsysgrp, ntsecgrp, ntbackupgrp |
| SA—Security Auditor | ntsecgrp |
| AA—Application Administrator | ntappgrp, ntossgrp, ntdropboxgrp |
| BA—Backup Administrator | ntbackupgrp |
| DBA—Database Administrator | ntdbgrp, ntappgrp |

### Deleting a user account

You can delete individual users who no longer require access to the server. The User Management Configuration tool does not manage the following system accounts, and you cannot delete them:

* + ntossadm
  + nortelrps
  + root
  + ntappsw
  + ntdbsw (database systems only)
  + ntdblsnr (database systems only)

**Attention**

Any files owned by a deleted user account are orphaned. The root user is responsible for the management of orphaned files.

### Menu mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If prompted, enter your password.
2. Enter **2** to delete a user.
3. From the list of users, select the user that you want to delete by entering the corresponding number.
4. Enter **Y** to confirm the delete.

You receive a prompt to continue deleting users or to return to the main menu.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt delete <username>

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | This value is the name of the user account. |

**Modifying user roles**

Use this procedure to modify roles for a server administrator. You can also change the primary role of the administrator.

### Menu mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If you receive a prompt, enter your password.
2. Enter **3** to modify a user's roles.
3. From the list of users, enter the corresponding number for the user account that you want to modify.
4. Enter the corresponding number for the user's roles (primary role first), separated by commas (,).
5. Enter **Y** to continue making modifications.

You receive a prompt to continue modifying roles for users or to return to the main menu.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt modify <username> <roles>

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | This value is the name of user account. |
| <roles> | This value contains the roles that you want to assign to the user account. You must enter the primary role first, and separate multiple roles with a comma (,).  Example: SSA, AA |

**Changing the state of a user account**

Disable a user's account to temporarily prevent access to the server with that account. Enable the account to restore access.

If a user's account becomes locked because of failed attempts to log on, you can clear the lock by disabling and then enabling the account again.

### Menu mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If you receive a prompt, enter your password.
2. Enter **4** to enable or disable a user account.
3. Enter the corresponding number for the user account that you want to enable or disable.
4. Enable or disable the account:

|  |  |
| --- | --- |
| **If the account is currently** | **Do this** |
| Enabled | Enter Y to disable the account, and go to [Step 9](#_bookmark39). |
| Disabled | Enter Y to enable the account, and go to [Step 7](#_bookmark38). |

1. Enter a new password for the user account.

The user must change this password during initial log on.

1. Enter the new password again.
2. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Change another account state | Enter Y |
| Not change another account state | Enter N |
| Exit | Enter 8 |

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

|  |  |
| --- | --- |
| **Choose to** | **Enter this command** |
| Enable a user account | userMgt state <username> enable  The initial password must be supplied and confirmed when enabling a user account. |
| Disable a user account | userMgt state <username> disable |

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | This value is the name of user account. |

**Listing server user accounts**

You can view a list of users currently configured on the server. The display shows 20 entries for each page, and lists the user name, userID, the user's configured state, and whether the user has sudo access to the system.

### Menu mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If you receive a prompt, enter your password.
2. Enter **5** to list the users currently configured on the server. The screen displays up to 20 users.
3. You can choose to display the next 20 users or quit to the main menu.

|  |  |
| --- | --- |
| **To choose this** | **Do this** |
| Show the next 20 users (if applicable) | Press **Enter** . |
| Return to the main menu | Type **q** and press **Enter**. |

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt show

1. You can choose to display the next 20 users or quit to the main menu.

|  |  |
| --- | --- |
| **To choose this** | **Do this** |
| Show the next 20 users (if applicable) | Press **Enter** . |
| Return to the main menu | Type **q** and press **Enter**. |

**--End--**

### Managing sudo access for local users

Use this procedure to grant or revoke sudo access for user accounts.

### Prerequisites

* + You must be the root user. **OR**
  + You must be an SSA user with sudo privileges.

### Menu mode

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. If you are an SSA, change to the root:

###### su - root

1. Enter the root password.
2. Run the User Management Configuration tool:

###### userMgt.pl

1. Enter **6** to manage sudo access.
2. Enter the corresponding number for the user account for which you want to grant or deny sudo access.
3. Grant or remove sudo access:

|  |  |
| --- | --- |
| **If the account currently** | **Do this** |
| Has sudo access | Enter Y to remove sudo access. |
| Does not have sudo access | Enter Y to enable sudo access. |

1. Choose whether to manage sudo access for another user account.

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Manage sudo access for another user account | Enter Y, and repeat [Step 6](#_bookmark46) to [Step 8](#_bookmark47). |
| Not manage sudo access for another user account | Enter N to go back to the main menu. |

1. Enter **9** to exit.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as the SSA user and su to root.

###### su - root

1. Enter the root password.
2. At the command prompt:

|  |  |
| --- | --- |
| **Choose to** | **Enter this command** |
| Grant sudo for a user | userMgt sudo <username> allow |
| Revoke sudo for a user | userMgt sudo <username> deny |

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | This value is the name of user account. |

**Managing sudo access for central users**

Use this procedure to grant or revoke sudo access for central users.

### Prerequisites

* + You must be the root user

###### OR

* + You must be an SSA user with sudo privileges.

### Menu Mode

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. If you are an SSA, change to root. At the command prompt: **su**

###### – root

1. 3. Run the User Management Configuration tool. At the comment prompt: **userMgt.pl**
2. Enter **8** to manage sudo access for central users
3. Enter the number of the user account for which you want to grant or deny sudo access.
4. Grant or remove sudo access:

|  |  |
| --- | --- |
| **If the account currently** | **Do This** |
| Has sudo access | Enter Y to remove sudo access |
| Does not have sudo access | Enter Y to enable sudo access |

1. Choose whether to add sudo access for another account:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Manage sudo access for another account | Enter Y and repeat steps 6-7 |
| Not manage sudo access for another account | Enter N to go back to the main menu |

1. Enter **13** to exit.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as the SSA user and su to root **su – root**
2. Enter the root password
3. At the command prompt:

|  |  |
| --- | --- |
| **Choose to** | **Enter this command** |
| Grant sudo for a user | **userMgt.pl sudo <username> allow** |
| Revoke sudo for a user | **userMgt.pl sudo <username> deny** |

**--End--**

### Variable Definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | The name of the central user account |

**Resetting a user account password**

If an administrator is locked out of the server because of failed attempts to log on, you can reset the user account password to clear the lock.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA (for example, ntsysadm).
2. At the command prompt:

###### userMgt

1. If you receive a prompt, enter your password.
2. Enter **6** to reset a user password.
3. Enter the corresponding number for the user whose password you want to reset.
4. Enter a new password for the user account and confirm by entering the new password again.

A prompt displays asking to reset a password for another user or return to the main menu.

1. Reply to the prompt with the desired action.

**--End--**

### Loading user accounts

Use this procedure to configure all of the admin users on a single server and then replicate this configuration to all other servers in the system.

In this procedure, you import the user database from System A to System

B. Both systems are installed with the same accounts as chosen during installation (individual accounts or preconfigured).

The passwords for the accounts loaded to server B are the same as the passwords configured for admin users on Server A.

**Attention**

Perform this procedure only after a fresh installation of the server.

### Prerequisites

* + You must be logged on as root on both servers.
  + The user database file must be imported from a system that shares the same type of accounts as determined during initial installation (individual or preconfigured).
  + Ensure that no additional users were added to System B after initial installation.

### Procedure steps

###### Step Action

1. Log on to both system A and system B servers as root.
2. On system A, run the following command from the home directory:

###### userMgt.pl backup

1. Copy the following files from system A to the home directory of system B:
   * /admin/.userConfig.txt
   * /admin/userPass.txt
   * /admin/sudoUsers.txt
2. On system B, make a copy of the user database file.

###### # cp /admin/.userConfig.txt / admin/.userConfig.bak

1. Copy the files from the home directory to /admin:

###### # cp /home/<account>/.userConfig.txt / admin/.userConfig.txt

**# cp /home/<account>/userPass.txt /admin/ userPass.txt**

**# cp /home/<account>/sudoUsers.txt /admin/ sudoUsers.txt**

1. Ensure the file permissions in /admin are as follows:

###### -rw-r----- 1 root root sudoUsers.txt

**-rw-r--r-- 1 root root .userConfig.txt**

**-rw-r----- 1 root root userPass.txt**

1. Edit sudoUsers.txt to remove existing sudo users. Use VI to edit the file /admin/sudoUsers.txt.

If server B was configured with preconfigured accounts, remove ntsysadm from sudoUsers.txt.

If server B was configured with individual accounts, remove the system administrator name that was selected during initial installation from sudoUsers.txt

1. Run the userMgt load command:

###### # userMgt.pl load

Ignore any error messages regarding existing user accounts.

1. Verify that all users are there:

###### # userMgt.pl show

**--End--**

### Listing central users on this system

Use this procedure to list the central users on the system.

### Prerequisites

* + You must be the root user.

###### OR

* + You must be an SSA user with sudo privileges.

### Menu mode

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. If you are an SSA, change to the root: **su - root**
3. Enter the root password.
4. Run the User Management Configuration tool: **userMgt.pl**
5. Enter **11** to list central users.
6. Press Enter to go to main menu
7. Enter **13** to exit

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. At the command prompt: **userMgt.pl showcentral**
3. You can choose to display the next twenty users or press Enter to return to the Main menu.

**--End--**

### Deleting a central user

Use this procedure to delete a central user from the system.

### Prerequisites

* + You must be the root user.

###### OR

* + You must be an SSA user with sudo privileges.

### Procedure steps

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. If you are an SSA, change to the root: **su - root**
3. Enter the root password.
4. Run the User Management Configuration tool: **userMgt.pl**
5. Enter **12** to delete central users.
6. Enter the corresponding number for the central user account for which you want to delete.
7. If you want to delete central user, enter Y. If you don’t want to delete central user, enter N.
8. If you want to delete another user, enter Y. Otherwise enter N.
9. Enter **13** to exit.

**--End--**

### CLI mode

###### Step Action

1. Log on to the server as root or an SSA (for example, ntsysadm).
2. At the command prompt: **userMgmt.pl deletecentral**

###### <username>

**--End--**

### Variable Definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <username> | The name of the temporary central user to delete |

**Configuring warning banners**

Use this procedure to configure warning banners to display a message before users enter their usernames and passwords, and another after a successful log on. Warning banners typically state the legal implications of logging on to a system.

### Prerequisites

You are an SSA (for example, nysysadm).

### Procedure steps

###### Step Action

1. Use a text editor to create <issue\_filename>
2. Use a text editor to create <motd\_filename>
3. Connect to the server as SSA user by using SFTP or SCP.
4. Transfer <issue\_filename> and <motd\_filename> to /var/tmp.
5. Log on to the server as SSA user with SSH.
6. Copy the files from /var/tmp to /etc directory:

###### cp /var/tmp/<issue\_filename> /etc/issue cp /var/tmp/<motd\_filename> /etc/motd

1. Repeat [Step 3](#_bookmark60) to [Step 6](#_bookmark61) for each server.

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <issue\_filename> | This value is the name of the text file that contains the message that appears before log on. |
| <motd\_filename> | This value is the name of the text file that contains the message that appears after a successful log on. |

**File system integrity administration**

**Note**: This feature is not applicable to the platform types which run on HP CC3310 and BellMicro-SAMXTS servers.

The installation software contains a file system integrity tool called Fcheck. Use this tool to monitor changes in the file system for unauthorized modifications.

### Creating an FSI baseline

A file system integrity (FSI) baseline is the snapshot of all the system files including their size and permissions. This snapshot is specific to the time the baseline is taken. Create a baseline on a weekly basis or after any significant changes to the system, such as software installation.

### Prerequisites

The administrator must be a System Security Administrator (SSA)

### Procedure steps

###### Step Action

**1** At the prompt, enter the following command:

###### fsibaseline

**--End--**

### Verifying the file system against a baseline

Routinely verify the file system against the baselines. The verification process identifies the following changes:

* + Addition or removal of files
  + Modification of files and attributes
  + File sizes and MD5 signatures

### Prerequisites

The administrator must be a System Security Administrator (SSA).

### Procedure steps

###### Step Action

**1** At the prompt, enter the following command:

###### fsiverify

**--End--**

### Managing FSI baselines

You can list all of the file system integrity (FSI) baselines currently stored on the server. The system uses the file marked baseline for verification. You can select a different baseline file to use for verification.

### Prerequisites

The administrator must be a System Security Administrator (SSA).

### Procedure steps

###### Step Action

1. At the prompt, enter the following command:

###### fsibaselineMgt

1. Select a management action:

|  |  |
| --- | --- |
| **Choose to** | **Enter selection number** |
| List available baselines | 1 |
| Set the verification baseline | 2 |
| Unset the verification baseline | 3 |
| Exit | 4 |

**--End--**

## Modification of SSH Ciphers and Message Authentication Codes

For organizations that have a prescribed set of encryption ciphers to be used for SSH, this section describes the procedure that specifies how to modify the supported set.

### Modifying SSH Ciphers and Message Authentication Codes

###### Step Action

1. Open a SSH connection to the server that is to be modified.

**Attention**

Keep this session open until this procedure is fully completed. If connection testing fails, you must have this session available to repair/ revert the SSH configuration.

1. Check the list of supported Ciphers and Message Authentication Codes (MAC) and decide on the Ciphers and MACs required.

‘man sshd\_config’ displays the list of supported ciphers in the Cipher section. The list of supported MACs are in the MACs section. These lists are dependent on version of the SSH software currently in use.

For PLE4 images this would include:

* + Ciphers 3des-cbc,aes128-cbc,aes192-cbc,aes256- cbc,aes128-ctr,aes192-ctr,aes256- ctr,arcfour128,arcfour256,arcfour,blowfish-cbc,cast128-cbc
  + MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac- ripemd160,hmac-sha1-96,hmac-md5-96,hmac-

sha2-256,hmac-sha2-512

For PLE2 images this would include:

* + Ciphers des-cbc,aes128-cbc,aes192-cbc,aes256- cbc,aes128-ctr,aes192-ctr,aes256- ctr,arcfour128,arcfour256,arcfour,blowfish-cbc,cast128-cbc
  + MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac- ripemd160,hmac-sha1-96,hmac-md5-96,hmac-

sha2-256,hmac-sha2-512

1. Back up the existing configuration.

cd /etc/ssh

cp –rp sshd\_config sshd\_config.orig.`date +%Y%m

%d`

1. Change the supported Ciphers. If the Ciphers entry does not exist in the sshd\_config file, then the default list detailed in ‘man sshd\_config’ is in effect.

If the Ciphers entry exists, then modify the entry as appropriate. If it does not exist, then add the entry to the end; that is,

Ciphers aes128-ctr,aes192-ctr,aes256- ctr,arcfour256,arcfour128

1. Change the support Message Authentication Codes

If the MACs entry does not exist in the sshd\_config file, then the default list detailed in ‘man sshd\_config’ is in effect.

If the MACs entry does exist, then modify the entry as appropriate. If it does not exist then add the entry to the end; that is,

MACs hmac-sha1,umac-64@openssh.com,hmac- ripemd160

1. Save the sshd\_config changes.
2. Restart the SSH Daemon.

service restart sshd

1. Open a new SSH session to the server and ensure it successfully connects.

If testing fails, return to step 4 to adjust the Ciphers and MACs, or revert the configuration.

**--End--**

###### 51

**Network security configuration**

This chapter provides the procedures that you require to configure network security on the Application (AS) servers.

## Network security configuration navigation

* + [“Access control configuration” (page 61)](#_bookmark81)
  + [“IPSec configuration” (page 78)](#_bookmark109)
  + [“DSCP marking configuration” (page 113)](#_bookmark161)
  + [“Increasing network security with SNMP” (page 119)](#_bookmark166)

## Access control rules

This section describes information about access control rules.

### Access control rules navigation

* + [“Access control rules overview” (page 51)](#_bookmark70)
  + [“Access control tools” (page 60)](#_bookmark78)
  + [“Access control default system configuration” (page 60)](#_bookmark79)
  + [“Access control limitations and restrictions” (page 61)](#_bookmark80)

### Access control rules overview

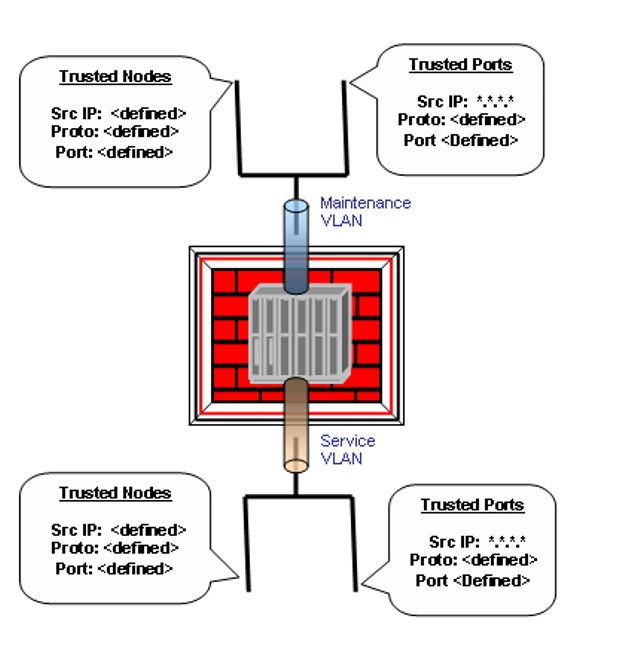
The system controls the access to its servers by enforcing a set of designated access control rules on each server. These access control rules reject all communications except for those with trusted nodes and those using trusted ports. The IPTables utility (the firewall utility offered in the Linux system) enforces the access control rules.

**Attention**

The host based ACL/filtering capability is generally only applicable to system deployments where a filtering/firewall function for the AS IP flows is not performed by a network device such as a (next hop) router/L3 switch or network firewall. The overall network infrastructure and security posture of the AS LAN and WAN should be considered when deciding to implement host based ACLs/filtering.

The following diagram illustrates the concept of Trusted Nodes and Trusted Ports for the ACLs/filtering rules which may be configured against each IP interface.

**ACL firewall**



### Trusted nodes

Trusted nodes are nodes with which communication is permitted. Each AS node can control its access by configuring a list of TCP and UDP ports for which a particular trusted node may communicate through. It can also accept or drop ICMP messages per trusted node.

Trusted nodes are typically classified into two groups: internal and external:

* + **Internal trusted nodes** are nodes considered to be part of the AS mesh. Internal trusted nodes typically require full access and should be provisioned to allow communication across all ports and protocols including ICMP.
  + **External trusted nodes** are nodes which are not part of the AS mesh such as an OAM client or server in the management network (such as OSS/NOC). These nodes typically require specific access to a particular AS node and should be restricted to only allow communication through the specific ports and protocols it requires.

Trusted nodes (internal and external) are determined by the system/ network security administrator and can be either a single node or a subnet.

If a trusted node is a single node, its configuration is converted into the following iptables rules:

**IPTables Rules for an Internal Trusted Node**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Src Addr** | **Src Port** | **Dst Addr** | **Dst Port** | **Protoc ol** | **ICMP** |
| Filter | Input | Truste d Node Addr | Any | Local Node Addr | Any | TCP | Yes |
| Filter | Input | Truste d Node Addr | Any | Local Node Addr | Any | UDP | Yes |

**IPTables Rules for an External Trusted Node**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Src Addr** | **Src Port** | **Dst Addr** | **Dst Port** | **Protoc ol** | **ICMP** |
| Filter | Input | Truste d Node Addr | Any | Local Node Addr | All | None | List of Ports | TCP | Yes | No |
| Filter | Input | Truste d Node Addr | Any | Local Node Addr | All | None | List of Ports | UDP | Yes | No |

If a trusted node is a subnet, its configuration is converted into the following iptables rules:

**IPTables Rules for an Internal Trusted Subnet**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Src Addr** | **Src Port** | **Dst Addr** | **Dst Port** | **Protoc ol** | **ICMP** |
| Filter | Input | Trusted Node Subnet ID and Subnet Mask | Any | Local Node Addr | Any | TCP | Yes |
| Filter | Input | Trusted Node Subnet ID and Subnet Mask | Any | Local Node Addr | Any | UDP | Yes |

**IPTables Rules for an External Trusted Subnet**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Scr Addr** | **Scr Port** | **Dst Addr** | **Dst Port** | **Protoc ol** | **ICMP** |
| Filter | Input | Truste d Node Subnet ID and Subnet Mask | Any | Local Node Addr | All | None | List of Ports | TCP | Yes | No |
| Filter | Input | Truste d Node Subnet ID and Subnet Mask | Any | Local Node Addr | All | None | List of Ports | UDP | Yes | No |

### Trusted ports

Trusted ports are server ports on which the system permits all ingress traffic of a particular protocol from anywhere, if it is an input port, or, all egress traffic of a particular protocol to anywhere, if it is an output port.

Trusted ports are predetermined. The administrator can open or close a trusted port or change to use an alternate port number, but cannot add a new trusted port or delete an existing trusted port.

The following table lists the predetermined trusted ports in the system.

**Trusted ports in the system**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Port Number (Default)** | **Redirect Port Number (Default)** |
| SIP UDP | UDP | 5060 | N/A |
| SIP TCP | TCP | 5060 | N/A |
| SIP TCP TLS | TCP | 5061 | N/A |
| UNISTIM | UDP | 5000 | N/A |
| PA HTTP | TCP | 80 | 8081 |
| PA HTTPS | TCP | 443 | 8043 |

The SIP UDP trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the SIP UDP Trusted Port**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | |
| **Source address** | **Source port** | **Destinati on address** | **Destinati on port** | **Protocol** |
| Filter | Input | Any | 5060 | Any | Any | UDP |
| Filter | Input | Any | Any | Any | 5060 | UDP |

The SIP TCP trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the SIP TCP Trusted Port**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | |
| **Source Address** | **Source Port** | **Destinati on Address** | **Destinati on Port** | **Protocol** |
| Filter | Input | Any | 5060 | Any | Any | TCP |
| Filter | Input | Any | Any | Any | 5060 | TCP |

The SIP TCP TLS trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the SIP TCP TLS Trusted Port**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | |
| **Source Address** | **Source Port** | **Destinati on Address** | **Destinati on Port** | **Protocol** |
| Filter | Input | Any | 5060 | Any | Any | TCP |
| Filter | Input | Any | Any | Any | 5061 | TCP |

The UNISTIM trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the UNISTIM Trusted Port**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | |
| **Source Address** | **Source Port** | **Destinati on Address** | **Destinati on Port** | **Protocol** |
| Filter | Input | Any | Any | Any | 5000 | UDP |

The PA HTTP trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the PA HTTP Trusted Port**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Source Addres s** | **Source Port** | **Destin ation Addres s** | **Destin ation Port** | **Redire ct Port** | **Protoc ol** |
| Filter | Input | Any | Any | Any | 8041 | N/A | TCP |
| Nat | Prerou ting | Any | Any | Any | 80 | 8081 | TCP |

The PA HTTPS trusted port configuration converts into the following IPTables rules.

**IPTables Rules for the PA HTTPS Trusted Port**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Table** | **Chain** | **Rule** | | | | | |
| **Source Addres s** | **Source Port** | **Destin ation Addres s** | **Destin ation Port** | **Redire ct Port** | **Protoc ol** |
| Filter | Input | Any | Any | Any | 8043 | N/A | TCP |
| Nat | Prerou ting | Any | Any | Any | 443 | 8043 | TCP |

### External trusted node

External trusted nodes and subnets are generally defined for OAM protocol flows between AS nodes and OAM clients/servers in the Management network. The AS can limit its exposure to the OSS by specifying the ports and protocols it will accept for each external trusted node or subnet.

### Internal trusted node

In addition to configuring external trusted nodes to secure the AS system's communications with the external world, the internal trusted node is also required to secure the interserver communications within the AS system. This is achieved by configuring an internal trusted node among AS servers.

###### Internal trusted node in a two server system

On a two server AS system, the Internal Trusted Node is configured on each server with the following trusted nodes on each machine.

**Internal trusted node setup in two server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on other server |
| Service VLAN local IP | System Manager Floating IP |
| System Manager Floating IP | Service VLAN IP on other server |
| Service VLAN local IP | AM Floating IP |
| AM Floating IP | Service VLAN IP on other server |
| Service VLAN local IP | Session Manager Floating IP |
| Session Manager Floating IP | Service VLAN IP on other server |

Note that the System Manager Floating IP, the AM Floating IP, and the Session Manager Floating IP refer to their service addresses. The service address of System Manager, AM, or Session Manager only exists on the server where the network element’s active instance is running.

###### Internal trusted node in a four server system

On a four server AS system which consists of EMS server 1, EMS server 2, NES server 1 and NES server 2, the internal trusted node mesh is configured on each server with the following trusted nodes on each machine.

**Internal trusted node setup on EMS server in four server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SM Floating IP |

**Internal trusted node setup on EMS server in four server system (cont'd)**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| SM Floating IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | AM Floating IP |
| AM Floating IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SESM Floating IP |

**Internal trusted node setup on NES server in four server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SM Floating IP |
| Service VLAN local IP | AM Floating IP |
| Service VLAN local IP | SESM Floating IP |
| SESM Floating IP | Service VLAN IP on each of other servers |

Note that in a four server system, the SM Floating IP and the AM Floating IP only switch in between the two EMS servers, and the SESM Floating IP in between the two NES servers.

###### Internal trusted node in a four plus server system

To enhance the capability of the system, additional servers can be included in the AS system to add more Session Managers. For example, an enhanced AS system consists of six servers: EMS server 1, EMS server 2, NES server 1, NES server 2, NES server 3, and NES server 4. This system includes two Session Managers: Session Manager 1 on NES server 1 and NES server 2, Session Manager 2 on NES server 3 and NES server 4.

The configuration of the internal trusted node on a four plus server system is similar to that on the four server system, except that the additional NES servers and Session Managers must be considered.

The six server system serves as an example for the internal trusted node configuration on a four plus server system. On a six server system, configure the internal trusted node on each server with the following trusted nodes on each server.

**Internal trusted node setup on EMS server in four plus server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SM Floating IP |
| SM Floating IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | AM Floating IP |
| AM Floating IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SESM1 Floating IP |
| Service VLAN local IP | SESM2 Floating IP |

**Internal trusted node setup on NES server 1/2 in four plus server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SM Floating IP |
| Service VLAN local IP | AM Floating IP |
| Service VLAN local IP | SESM1 Floating IP |
| Service VLAN local IP | SESM2 Floating IP |
| SESM1 Floating IP | Service VLAN IP on each of other servers |

**Internal trusted node setup on NES server 3/4 in four plus server system**

|  |  |
| --- | --- |
| **Local node address** | **Trusted node address** |
| Service VLAN local IP | Service VLAN IP on each of other servers |
| Service VLAN local IP | SM Floating IP |
| Service VLAN local IP | AM Floating IP |
| Service VLAN local IP | SESM1 Floating IP |
| Service VLAN local IP | SESM2 Floating IP |
| SESM2 Floating IP | Service VLAN IP on each of other servers |

Note that the SESM1 Floating IP switches in between NES server 1 and NES server 2, and the SESM2 Floating IP switches in between NES server 3 and NES server 4.

### Access control tools

Use the following tools to manage and configure firewall rules for server access control.

**Access control tools**

|  |  |
| --- | --- |
| **Tool** | **Description** |
| iptcfg | This tool allows the administrator to configure trusted nodes and trusted ports and to enforce access control rules according to the configured trusted nodes and trusted ports. |
| iptstatus | This tool allows the administrator to verify and view the trusted node and trusted port configurations and the access control rules from outside of the iptcfg tool. |

Access each tool by typing its name at the command prompt.

For more information about iptstatus, see [“Viewing trusted node and port](#_bookmark160) [configurations with iptstatus” (page 112)](#_bookmark160).

### Access control default system configuration

By default, there are no trusted nodes configured and no corresponding firewall rules in place after initial system installation.

After installation, there are no firewall rules for trusted ports configured except for the PA port redirection rules, which redirect the PA HTTP port from port 80 to port 8041, and the PA HTTPS port from port 443 to port 8043.

Except for the PA ports, other trusted ports are in the Unconfigured state after installation.

By default, DSCP marking is disabled. The three default values configuration exists, but the system does not apply the values until after you enable DSCP marking.

The applications and communication channels to which DSCP marking applies, are predefined and assigned a DSCP marking category. You cannot modify the predefined applications or assignments.

**Predefined DSCP marking categories**

|  |  |
| --- | --- |
| **Application** | **DSCP marking category** |
| Secure Shell log on | Low Latency Data |
| Network Time Protocol | Low Latency Data |
| Database connections | Low Latency Data |
| IPsec negotiation | Network Signaling |

**Predefined DSCP marking categories (cont'd)**

|  |  |
| --- | --- |
| **Application** | **DSCP marking category** |
| Simple Network Management Protocol | Low Latency Data |
| Syslog | High Throughput Data |
| NED | Low Latency Data |
| SSL FTP | Low Latency Data |
| ICMP messages | Network Signaling |

### Access control limitations and restrictions

The administrator cannot add new or delete existing trusted ports.

The iptcfg tool is specially designed for configuring or modifying the firewall rules in the system. GENBAND does not guarantee the integrity of the firewall settings in the system if you use any other firewall configuration tool.

The iptcfg tool provides a rollback capability to permit reset of the firewall or access control to the previous configuration. However, this rollback is limited to only the most recent previous version.

## Access control configuration

This section provides the tasks that you must complete to configure access control.



**WARNING**

The iptcfg tool is specially designed to configure and manage the firewall (iptables) rules in the AS system. GENBAND does not guarantee the integrity of the firewall configuration if any other firewall configuration tool is used.

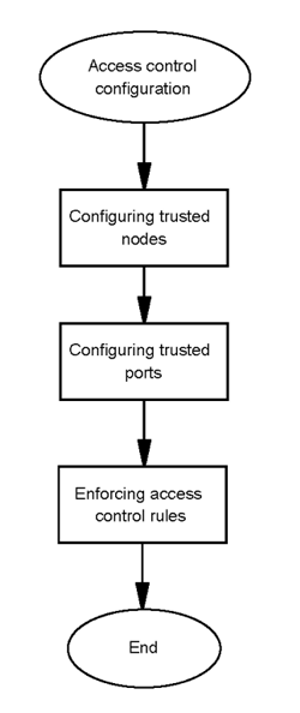
The system controls external access to its servers by enforcing a set of designated access control rules on each server. These rules reject all server communications with external nodes except for those with trusted nodes and communication over trusted ports.

### Access control configuration tasks

This task flow shows the sequence of tasks you perform to configure access control for the system. To locate more information about how to perform each task, see [“Access control configuration navigation”](#_bookmark82)

[(page 62)](#_bookmark82).

**Access control configuration**



### Access control configuration navigation

* + [“Trusted node configuration” (page 62)](#_bookmark83)
  + [“Trusted port configuration” (page 68)](#_bookmark94)
  + [“Enforcing access control rules” (page 70)](#_bookmark97)
  + [“Importing access control rules” (page 71)](#_bookmark98)
  + [“Viewing all configured access control rules” (page 73)](#_bookmark99)
  + [“Rolling back to the previous access control configuration” (page 73)](#_bookmark100)
  + [“Restoring the access control default configuration” (page 73)](#_bookmark101)

### Trusted node configuration

This section provides the procedures that you require to configure trusted nodes.

### Trusted node configuration navigation

* + [“Adding a trusted node” (page 63)](#_bookmark84)
  + [“Listing trusted nodes” (page 65)](#_bookmark88)
  + [“Modifying a trusted node” (page 65)](#_bookmark89)
  + [“Removing a trusted node” (page 67)](#_bookmark90)

### Adding a trusted node

Use this procedure to add a trusted node.

**Attention**

The administrator must add the node from which they can log into the AS servers as a trusted node. Otherwise, the administrator will lose the accessibility to the AS servers after the firewall rules for access control are in place.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **1** to select **Configure Trusted Nodes**.
5. Enter **2** to select **Add a new trusted node configuration**.
6. Enter the local node address.
7. Specify the trusted node type.

|  |  |
| --- | --- |
| **Choose** | **Do this** |
| Single node | Enter 1, and go to [Step 10](#_bookmark86). |
| Subnet | Enter 2, and go to [Step 8](#_bookmark85). |

1. Enter the subnet-hosted IP address.
2. Enter the trusted node subnet mask.
3. Do one of the following:

If you did not enter the subnet-hosted IP address in [Step 8](#_bookmark85), enter the trusted node address.

###### OR

Continue to the next step.

1. Enter “Y” to accept or “N” to drop ICMP messages from the trusted node.
2. Enter “Y” to specify ports and protocols accepted from the trusted node, or “N” to accept all ports and protocols.
3. If “Y” is selected, follow the steps in [“Adding Ports for Trusted](#_bookmark92) [Nodes and Subnets” (page 68)](#_bookmark92) to specify ports and protocols otherwise enter “Y” to confirm.
4. Review the configuration and enter **Y** to confirm.
5. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, or 4. |
| Return to the main menu and make another selection | Enter 5, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 6, and then confirm that you want to exit the tool. |

**--End--**

###### Adding a Trusted Node job aid

This job aid lists and describes the parameters for trusted node configuration.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Local node address | This is the local node IP address. |
| Trusted node type | The types of trusted nodes are 1-single node and 2- subnet. |
| Trusted node address | This is the trusted node IP address. (dot-notation) |
| Trusted node subnet id or subnet-hosted address | The iptcfg tool either prompts for a single trusted node address or prompts for a subnet id/subnet-hosted address and a subnet mask, depending on the trusted node type you select. (dot-notation) |
| Trusted node subnet mask | The iptcfg tool either prompts for a single trusted node address or prompts for a subnet id/subnet-hosted address and a subnet mask, depending on the trusted node type you select. (dot-notation) |

### Listing trusted nodes

Use this procedure to list all configured trusted nodes. You can use this procedure to identify the ID for a trusted node that you want to modify or remove.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **1** to select **Configure Trusted Nodes**.
5. Enter option **1** to select **List all trusted node configurations**. Trusted nodes are listed by ID.
6. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, or 4. |
| Return to the main menu and make another selection | Enter 5, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 6, and then confirm that you want to exit the tool. |

**--End--**

### Modifying a trusted node

Use this procedure to modify a trusted node.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **1** to select **Configure Trusted Nodes**.
5. Enter option **3** to select **Modify a trusted node configuration**.
6. Enter the ID of the trusted node that you want to modify. The tool displays the current parameters.
7. Enter the local node address.
8. Specify the trusted node type.

|  |  |
| --- | --- |
| **Choose** | **Do this** |
| Single node | Enter 1, and go to Step 11. |
| Subnet | Enter 2, and go to Step 9. |

1. Enter the subnet-hosted IP address.
2. Enter the trusted node subnet mask.
3. If you chose Single node in Step 8, enter the trusted node address.

Otherwise, continue to the next step.

1. Enter “Y” to specify ports and protocols accepted from the trusted node, or “N” to accept all ports and protocols.
2. If “Y” is selected, then follow the steps in [“Removing Ports for](#_bookmark93) [Trusted Nodes and Subnets” (page 68)](#_bookmark93) to specify ports and protocols otherwise enter “Y” to confirm.
3. Review the configuration and enter **Y** to confirm.
4. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, or 4. |
| Return to the main menu and make another selection | Enter 5, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 6, and then confirm that you want to exit the tool. |

**--End--**

###### Modifying a Trusted Node job aid

Refer to [“Adding a Trusted Node job aid” (page 64)](#_bookmark87) for a list and description of the parameters for trusted node modification.

### Removing a trusted node

Use this procedure to remove a trusted node.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **1** to select **Configure Trusted Nodes**.
5. Enter option **4** to select **Remove a trusted node configuration**.
6. Enter the ID of the trusted node that you want to remove.
7. Enter **Y** to confirm.
8. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, or 4. |
| Return to the main menu and make another selection | Enter 5, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 6, and then confirm that you want to exit the tool. |

**--End--**

### Specifying Ports For Trusted Nodes and Subnets

As part of the Add and Modify trusted node procedures, a prompt is given to configure ports for the trusted node. This controls access to the AS from the trusted node by restricting ports and protocols to only those provisioned.

* + Adding Ports for Trusted Nodes and Subnets
  + Removing Ports for Trusted Nodes and Subnets

###### Adding Ports for Trusted Nodes and Subnets

**Step Action**

1. Select “1” to Add ports.
2. Make a selection from the predefined list or “Other” to specify a particular port and protocol.
3. If “Other” was chosen:
   * Select the protocol.
   * Enter a list of ports to accept packets through. The values are separated by a comma and can contain a single port or a port range in the form <start port>:<end port> (such as 5000,6000:6050,4050).
   * If there are more ports to be configured, enter “Y” at the prompt and repeat steps 1-3.

**--End--**

###### Removing Ports for Trusted Nodes and Subnets

**Step Action**

1. Select “3” to list ports. A list of ports that has been configured for the trusted node will be presented.
2. Select “2” to remove ports.
3. Make a selection from the predefined list or “Other” to specify a particular port and protocol.
4. If “Other” was chosen:
   * Select the protocol.
   * Enter a list of ports to remove. The values are separated by a comma and can contain a single port or a port range in the form <start port>:<end port> (such as 7080,6000-6050).
5. If there are more ports to be configured, enter “Y” at the prompt and repeat the above steps.

**--End--**

### Trusted port configuration

This section provides the procedures that you require to configure trusted ports.

**Attention**

Trusted ports are predefined; you cannot add a new trusted port.

### Trusted port configuration navigation

* + [“Listing the trusted ports” (page 69)](#_bookmark95)
  + [“Modifying a trusted port” (page 69)](#_bookmark96)

### Listing the trusted ports

Use this procedure to list the trusted ports. You can use this procedure to identify the ID for a trusted port that you want to modify.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **2** to select **Configure Trusted Ports**.
5. Enter **1** to select **List all trusted port configurations**.

The tool displays the current trusted port configurations, listed by ID.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1 or 2. |
| Return to the main menu and make another selection | Enter 3, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 4, and then confirm that you want to exit the tool. |

**--End--**

### Modifying a trusted port

Use this procedure to modify the configuration of a trusted port.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **2** to select **Configure Trusted Ports**.
5. Enter **2** to select **Modify a trusted port configuration**.
6. Enter the ID of the trusted port that you want to modify.
7. Enter the port number.
8. Configure the port status.

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Allow communications | Enter 1 |
| Disallow communications | Enter 0 |

1. Enter **Y** to confirm the changes.
2. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1 or 2. |
| Return to the main menu and make another selection | Enter 3, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 4, and then confirm that you want to exit the tool. |

**--End--**

### Enforcing access control rules

Enforce (commit) the access control configuration rules so that the system applies the rules for trusted nodes and trusted ports.

**Attention**

To prevent the administrator from being locked out of the server, the tool requires that at least one trusted node be configured. If at least one configured trusted node does not exist, the tool cannot commit the changes.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **5** to select **Commit IP Tables Rules**.
5. Enter **Y** to confirm.
6. Enter **Y** if trusted nodes used to perform system maintenance operations are included.

**--End--**

### Importing access control rules

Use this procedure to perform bulk data entry for access control configuration. The tool converts the import data into corresponding firewall rules and commits the changes.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **4** to select **Import Configurations**.
5. Enter **Y** to proceed with the import.
6. Enter the full path and name of the import file.
7. Enter **Y** if trusted nodes used to perform system maintenance operations are included.

**--End--**

### Importing access control rules job aid

The import data file is a plain text file. This job aid lists the requirements for the data specifications in the file.

* + The words trustednode, sipudpport, siptcpport, siptcptlsport, unistimport, httpport, and httpsport are reserved as headers of the specs.
  + The tool ignores any line that does not start with a header.
  + The tool allows multiple "trustednode" specs.
  + At least one "trustednode" specification must exist.
  + The tool allows only a single specification for each port.
  + The tool requires that specifications for each port exist.
  + The syntax for the specifications is:
    - trustednode <local node ip> <trusted node ip>|<subnet id> [<subnet mask>]> [<ICMP Allowed> <TCP port list> <UDP port list>]

where:

<ICMP Allowed> values are: 0 - drop

1 - accept

<TCP port list> is:

* + - * a list of accepted tcp ports and port ranges separate by comma (such as 22,8043,10000:10500)
      * or "None" to drop all tcp ports
      * or "All" to accept all tcp ports

<UDP port list> is:

* + - * a list of accepted tcp ports and port ranges separate by comma (such as 22,8043,10000:10500)
      * or "None" to drop all udp ports
      * or "All" to accept all udp ports
    - sipudpport <port number> <status>
    - siptcpport <port number> <status>
    - siptcptlsport <port number> <status>
    - unistimport <port number> <status>
    - httpport <original port number> <redirected port number> <status>
    - httpsport <original port number> <redirected port number> <status>
  + The valid status values are:
    - 1—Traffic on the port is allowed.
    - 0—Traffic on the port is not allowed.
  + If a trusted node is a single node, provide <trusted node ip> only.
  + For a trusted node subnet, provide both <subnet id> and <subnet mask>, or, provide <trusted node ip> and <subnet mask> (<trusted node ip> is any node address within the subnet).

### Viewing all configured access control rules

Use this procedure to display all of the configured access control rules.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. tEonsteerle**8**ct **Show Current IPTables Rules** .

**--End--**

### Rolling back to the previous access control configuration

Use this procedure to roll access control rules back to the previous configuration.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **6** to select **Rollback**.
5. Enter **Y** to confirm the rollback to the previous access control configuration.

**--End--**

### Restoring the access control default configuration

**Prerequisites**

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **7** to select **Restore System Defaults**.
5. Enter **Y** to confirm the rollback to the previous access control configuration.

**--End--**

## IPSec configuration overview

This section contains information about IPSec configuration.

### IPSec configuration navigation

* + [“Secure communication” (page 74)](#_bookmark103)
  + [“IPSec configuration on a live AS system” (page 75)](#_bookmark104)
  + [“BCP7200 Fault Tolerant System” (page 75)](#_bookmark105)
  + [“IPsec configuration tools” (page 76)](#_bookmark106)
  + [“Certificate and CRL update in IPSec” (page 77)](#_bookmark107)
  + [“IPsec limitations and restrictions” (page 77)](#_bookmark108)

### Secure communication

The system supports IPSec for securing certain communication flows between Network Elements. Both public key cryptography technology using X.509 certificates and pre-shared keys may be used in IPSec for server authentication. The Internet Key Exchange (IKE) protocol provides the mutual authentication and key exchange when establishing IPSec Security Associations (SAs) between nodes.

Pre-shared keys are recommended for IPsec/IKE server authentication in most deployments.

The use of X.509 certificates requires an external Certificate Authority (CA) in the solution for signing X.509 certificates.

IPSec is supported and may be configured to secure the communication between following AS components:

* + BCP7200 and System Manager Server (SM)
  + BCP7200 and Database Server (DB)
  + BCP7200 and Session Manager Server (SESM)

Outside of AS components, IPSec is also enabled between BCP7200 and C20 GWC.

### IPSec configuration on a live AS system

If IPSec configuration must be performed on a live AS system, the administrator is required to perform the following steps:

### Procedure steps

###### Step Action

1. Perform the IPSec service configuration or the IPSec service configuration update, if needed.
2. **Start**/ **Restart**/ **Stop** the IPSec service on all servers that are involved in the IPSec setup.
3. Restart the BCP7200 instance that is involved in the IPSec setup via the SM Console.

If calls are up during the time that IPSec is restarting, the call server will no longer be able to control those calls (hold/retrieve, disconnect, etc).

If the call server attempts to communicate with the BCP when IPSec is down, the call server may raise an alarm and temporarily remove the BCP from its resource pool until IPSec comes back up.

It is recommended to start the IPSec configuration change on the standby node.

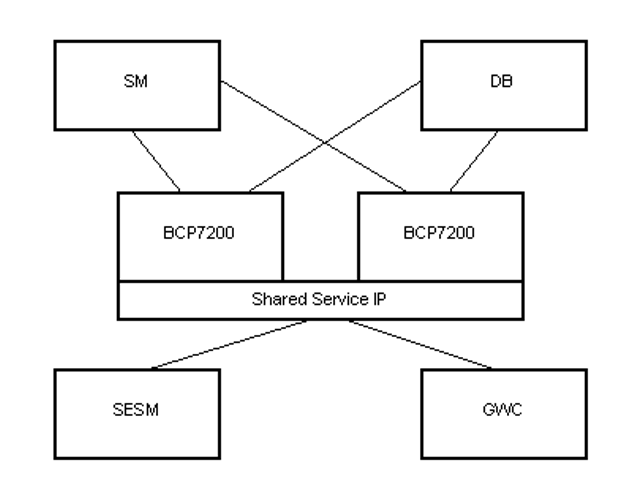
If the user does not follow the above steps in these cases, the AS system could behave abnormally in its OAM and server monitoring functions.

**--End--**

### BCP7200 Fault Tolerant System

The media portal fault tolerant system consists of the BCP7200, SM, DB, SESM(s), and GWC(s). The media portal fault tolerant system can switch between BCPs to ensure high availability of the media portal service.

**BCP7200 Fault Tolerant System**



A BCP7200 fault tolerant system may include redundant SMs and replicated DBs.

In a system that contains a single SM, the SM may be configured to use a service logical IP address for Network Element (NE) communications between the SM and other AS components. If the SM is so configured, the IPSec setup between the SM and the BCP7200 must include both the server IP address and the service IP address of the SM.

### IPsec configuration tools

The administrator uses the following tools to facilitate the configuration of the IPsec , the utilization of the X.509 certificate in IPsec, and the management of the IPsec service.

Start each tool by typing the name at the command prompt. The administrator must have sudo privileges to use these tools.

**IPsec configuration tools**

|  |  |
| --- | --- |
| **Tool** | **Function** |
| certmgr | Manage the certificates in IPsec |
| ipscfg | Configure the IPsec and manage the IPsec service |
| startipsec | Start or restart the IPsec service on a server |

**IPsec configuration tools (cont'd)**

|  |  |
| --- | --- |
| **Tool** | **Function** |
| stopipsec | Stop a running IPsec service |
| ipsecstatus | View and verify the connection status of all configured IPsec links |



**WARNING**

It is prohibited to use any tool other than the provided tools to configure or change the IPsec configurations in an AS system. The integrity of the AS IPsec configuration is not guaranteed if you use other tools to alter the IPsec configuration.

### Certificate and CRL update in IPSec

For information about renewing a CA certificate, see [“Renewing a CA](#_bookmark188) [certificate” (page 153)](#_bookmark188).

For information about renewing a CA-signed certificate, see [“Renewing a](#_bookmark197) [CA-signed certificate” (page 163)](#_bookmark197).

For information about renewing a CRL, see [“Renewing the CRL”](#_bookmark202) [(page 167)](#_bookmark202).

### IPsec limitations and restrictions

The AS does not support the live update of the IPsec policies and the IKE rules. To update any of those settings in an established IPsec , you must stop the running IPsec service, update the settings, and then restart the IPsec service.

When certificates are used, the renewal of the CA certificate, the server certificate, and the CRL must be well-planned. It is the administrator's responsibility to ensure the renewal occurs before the certificate expires or before the CRLs next update date has passed. Otherwise, a service interruption occurs when the certificate expires or when the CRLs next update date has passed.

After the CA certificate renewal, the server certificate renewal, or the CRL installation or update, the new certificate or CRL only becomes effective when the IPsec Phase 1 connection is renewed. It is not effective immediately.

The ipscfg tool is specially designed for configuring or modifying the IPsec configurations in an AS system. The integrity of the IPsec settings in the system is not guaranteed if other IPsec configuration tools are used to alter the IPsec settings.

The ipscfg tool provides a rollback capability allowing IPsec policy configuration and IKE rule configuration to be reset to their previous settings. However, this rollback is limited to only the most recent previous version.

## IPSec configuration

This section provides the tasks that you must complete to configure IPSec.

Use the procedures in this section to commission the IPSec service. The IPSec package is included in the server image. The installation of the IPSec package is part of the server installation process.

### Prerequisites to IPSec configuration

Server installation and commissioning must be completed.

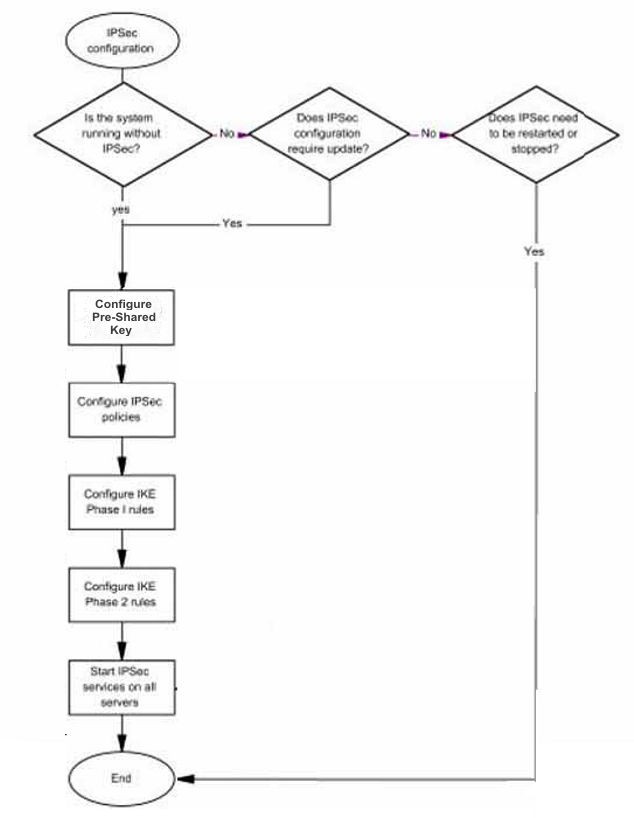
### IPSec configuration tasks

This following task flows show the sequence of tasks you must perform to configure IPSec for the system. To locate more information about how to perform each task, see [“IPSec configuration navigation” (page 80)](#_bookmark110).

**IPSec configuration with certificate**

|  |
| --- |
|  |

**IPSec configuration with pre-shared keys (no certificate)**



### IPSec configuration navigation

* + Obtain certificate from CA.

Use your preferred method to obtain the certificate from the CA.

* + Install the CA certificate on the server

For more information about installing a CA certificate, see [“Installing a](#_bookmark185) [CA certificate” (page 151)](#_bookmark185).

* + Generate a private key

For more information see [“Generating the private key” (page 155)](#_bookmark190).

**Attention**

The above three bullet points are only necessary when Certificates are used for IPsec/IKE authentication

* + For more information about configuring Pre-Shared keys, see [“Pre-](#_bookmark111) [shared key management” (page 81)](#_bookmark111)
  + For more information about configuring IPsec policies, see [“IPsec](#_bookmark116) [policy management” (page 83)](#_bookmark116).
  + For information about configuring IKE phase 1 rules (individually or in bulk), see [“IKE rules management” (page 89)](#_bookmark123).
  + For information about configuring IKE phase 2 rules (individually or in bulk), see [“IKE rules management” (page 89)](#_bookmark123).
  + For information about starting the IPsec service, see [“IPsec service](#_bookmark133) [management” (page 101)](#_bookmark133).

### Pre-shared key management

This section provides the procedures that you require to manage pre- shared keys for the AS system.

### Adding a pre-shared key

Use this procedure to configure a pre-shared key

###### Procedure steps Step Action

1. Log on to the server as an SSA
2. Run the IPsec/IKE Configuration tool:

/opt/mcp/ipsec/ipscfg.pl

1. Choose option 1: in the ipscfg tools main menu.

***the preshared key configuration submenu opens***

1. Select option 3: Add a Preshared key configuration.
2. Enter the IP address of the server to which this server needs to communicate in "Enter Remote Node Address" field.
3. Enter the key shared between the two servers in "Enter preshared key" field.
4. Confirm the data by entering "Y" at the prompt "Confirm (Y or N)".
5. To save the new preshared key select option 6: Save Preshared key configurations
6. To return to the main menu select option 8: Return to main menu

**--End--**

###### Importing Pre-shared Keys

To facilitate the bulk data entry for IPSec policy, the ipscfg tool provides an IPSec policy import capability. Use this procedure to import IPSec policies.

**Procedure steps**

###### Step Action

1. Log on to the server as an SSA
2. Run the IPsec/IKE Configuration tool:

/opt/mcp/ipsec/ipscfg.pl

1. Choose option 1: in the ipscfg tools main menu.

#### *the preshared key configuration submenu opens*

1. Choose Option 2) in the IPSec policy configuration submenu.
2. Confirm the import operation by entering "Y" at the prompt "Proceed (Y or N)"

**--End--**

###### Modifying a Preshared Key

Use this procedure to update preshared key configuration on a server

**Procedure steps**

###### Step Action

1. Log on to the server as an SSA
2. Run the IPsec/IKE Configuration tool:

/opt/mcp/ipsec/ipscfg.pl

1. Choose option 1: in the ipscfg tools main menu.

#### *the preshared key configuration submenu opens*

1. Select option 1: List all preshared key configuration.
2. Select option 4: Modify a Preshared key configuration.
3. Enter ID of the preshared key configuration to be updated, enter the new IP address and/or new key and finally confirm the update.
4. Select option 6: Save preshared key configuration.
5. Select option 8: Return to main menu or option 9: Exit.

**--End--**

###### Deleting Preshared Key Configurations

Use this procedure to delete preshared key configuration on a server.

**Procedure steps**

###### Step Action

1. Log on to the server as an SSA
2. Run the IPsec/IKE Configuration tool:

/opt/mcp/ipsec/ipscfg.pl

1. Choose option 1: in the ipscfg tools main menu.

#### *the preshared key configuration submenu opens*

1. Select option 1: List all preshared key configuration.
2. Select option 5: Delete a Preshared key configuration.
3. Enter ID of the preshared key configuration to be deleted.
4. Select option 6: Save preshared key configuration.
5. Select option 7: Return to main menu or option 8: Exit.

**--End--**

### IPsec policy management

This section provides the procedures that you require to manage the IPsec for the AS system.

### Adding a new IPsec policy

Use this procedure to add a new IPsec policy.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **3** to select **Add an IPsec policy**.
3. At the prompt, enter the local node IP address (dot-notation).
4. At the prompt, enter the remote node IP address (dot-notation).
5. Enter **Y** to confirm the new addition.
6. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, or 7. |
| Save all configured IPsec policies | If all IPsec configurations are complete, enter 6. |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

###### Adding new IPsec policy job aid

This job aid provides the syntax for adding a new IPsec policy.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| local node IP address (dot- notation) | The IP address of the local node (in dot- notation). |
| remote node IP address (dot- notation) | The IP address of the remote node (in dot- notation). |

### Importing IPsec policies

Use this procedure to bulk-import IPsec policies. The IPsec policy import file is a plain text file.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **2** to select **Import IPsec policies**.
3. Enter **Y** to continue with the import and overwrite all current IPsec policies with the imported version of the IPsec policies.
4. Enter the name of the import file.

<ipsec\_import>

After the import completes, the following message appears:

The import has succeeded and the imported IPsec policy configurations have been saved.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5 or 7. |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

###### Importing IPsec policies job aid

The following table provides variable definitions for the Importing IPsec policies procedure.

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <ipsec\_import> | This value is the path and name of the file containing the imported IPSec policies. The file can be a plain text file. |

The following table provides the syntax for the IPsec policy import file. The syntax for the IPsec policies specified in the file is:

<local\_IP\_address>[space]<remote\_IP\_address>

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| <local\_IP\_address> | The IP address of the local node (in dot-notation). |
| <remote\_IP\_address> | The IP address of the remote node (in dot-notation). |

### Listing IPsec policies

Use this procedure to list all of the currently configured IPsec policies. You can use this procedure to identify the ID for a particular IPsec policy that you want to modify or delete.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **1** to select **List all IPsec policies**.

The tool displays the policies by ID, and lists the local node and remote node addresses for each.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5 or 7. |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

### Modifying an IPsec policy

Use this procedure to modify an existing IPsec policy.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **4** to select **Modify an IPsec policy**.
3. Enter the ID of the IPsec policy that you want to modify.
4. At the prompt, enter the local node IP address (dot-notation).
5. At the prompt, enter the remote node IP address (dot-notation).
6. Enter **Y** to confirm the new configuration.
7. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5 or 7. |
| Save all configured IPsec policies | Enter 6. |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

### Deleting an IPsec policy

Use this procedure to delete an IPsec policy.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **5** to select **Delete an IPsec policy**.
3. Enter the ID of the IPsec policy that you want to delete.
4. Enter **Y** to confirm the delete.
5. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5 or 7. |
| Save all configured IPsec policies | Enter 6 |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

### Rolling back to the previous IPsec policy configuration

Use this procedure to roll back to (restore) the previous IPsec policy configuration

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **2** to select **Configure IPsec Policies**.
2. Enter **7** to select **Rollback**.
3. Enter **Y** to confirm the rollback and overwrite all current IPsec policies with the rollback version of the IPsec policies.
4. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5 or 7. |
| Save all configured IPsec policies | Enter 6. |
| Return to the main menu | Enter 8, and then enter Y to confirm the save. |
| Exit the tool | Enter 9, and then enter Y to confirm the save. |

If you select option 8 or 9, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IPsec policy configuration file.

**--End--**

### IKE rules management

Use the procedures in this section to manage IKE rules.

### Adding a new IKE phase 1 rule

Use this procedure to add a new IKE phase 1 rule.

**Attention**

The parameters selected for the IKE phase 1 and phase2 rules, such as encryption algorithm, hash algorithm, authentication algorithm, dh group, authentication method, lifetime, and generate policy must be identical at both ends of an IPsec connection. Otherwise, the IPsec connection cannot be established.

**Attention**

In an AS system, the floating IP of a network element, such as the SM floating IP, the AM floating IP, and the SESM floating IP, is a virtual network interface added onto the same network interface (card) to which the service vlan IP of a server is bound. You must specify the same IKE rule parameters for all IPsec connections that end at the same network interface. Otherwise, the IPsec connections cannot be established.

###### Prerequisites

* + You must be assigned the SSA role.
  + The certificate and private key, referenced by the new phase 1 rule, are installed (optional - only when Certificates are used with IPsec/IKE).
  + The CA certificate and CRL, if any, are installed (optional - only when Certificates are used with IPsec/IKE).

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **3** to select **Add an IKE configuration**.
3. At the prompt to add a phase 1 spec or a phase 2 spec, enter **1**.
4. At the prompt, enter the remote node IP address (dot-notation).

You can specify the IP address as anonymous (\*.\*.\*.\*). Because this rule applies to all IKE phase 1 negotiation, you can create only one rule (per server) that specifies the remote node IP address as anonymous.

1. At the prompt, enter the corresponding number for the Generate Policy (1-on, 2-off) This value must be set as off as the default. If the configuration is set between PLE4 the value must be set as on.
2. At the prompt, enter the phase 1 lifetime (30 to 2592000 seconds).
3. At the prompt, enter the corresponding number tor the Encryption Algorithm (1-des, 2-3des, 3-aes).
4. At the prompt, enter the corresponding number tor the Hash Algorithm (1-md5, 2-sha1, 3-sha256).
5. At the prompt, enter the Authentication Method (1- x509\_certificate, 2-pre\_shared\_key)

###### For Certificates:

* + At the prompt, enter the X.509 certificate file name.
  + At the prompt, enter the Private key file name.

1. At the prompt, enter the DH Group (1, 2, 5, 14, 15, 16, 17, or 18).
2. Review the configuration, and enter **Y** to confirm the new addition.
3. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

###### Adding a new IKE phase 1 rule job aid

When the remote node IP address is specified as anonymous, only one IKE phase 1 rule on a server is required as it applies to the IKE phase 1 negotiation for all IPsec connections. Therefore, the ipscfg tool does not permit a new IKE phase 1 rule to be added if an IKE phase 1 rule with an anonymous remote node IP address already exists. Multiple IKE phase 1 rules can only be added if each rule specifies a distinct remote node IP address.

It is recommended that only one IKE phase 1 rule with an anonymous remote node address be configured on a server, unless it is necessary to configure multiple IKE phase 1 rules with each having a distinct remote node address.

When using certificates, the certificate and private key must be installed prior to modifying a new IKE phase 1 rule that uses them. Otherwise, the ipscfg tool does not allow the rule to be modified.

### Adding a new IKE phase 2 rule

Use this procedure to add a new IKE phase 2 rule.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **3** to select **Add an IKE configuration**.
3. At the prompt to add a phase 1 spec or a phase 2 spec, enter **2**.
4. At the prompt, enter the local node IP address (dot-notation).

You can specify the local and remote node IP addresses as anonymous (\*.\*.\*.\*). Because this rule applies to all IKE phase 1 negotiation, you can create only one rule (per server) that specifies the remote node IP address as anonymous.

1. At the prompt, enter the remote node IP address (dot-notation).

If you specify the local node IP address as anonymous, you must specify the remote node IP address as anonymous. If you specify a particular IP address for the local node IP address, you must specify a particular IP address for the remote node IP address.

1. At the prompt, enter the Phase 2 lifetime (30 to 86400 seconds).
2. At the prompt, enter the corresponding number tor the Encryption Algorithm (1-des, 2-3des, 3-aes, 4-null\_enc).
3. At the prompt, enter the corresponding number tor the Authentication Algorithm (1-hmac\_md5, 2-hmac\_sha1, 3-hmac- sha256).
4. Review the configuration, and enter **Y** to confirm the new addition.
5. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

###### Adding a new IKE phase 2 rule job aid

Local node and remote node IP addresses can either be both anonymous (\*.\*.\*.\*) or both specific, but not a combination of each.

When an existing IKE phase 2 rule is configured with both the local and remote node IP addresses as anonymous, only one IKE phase 2 rule is required as it applies to the IKE phase 2 rule negotiations for all IPsec connections. Therefore, the ipscfg tool does not permit a new IKE phase 2 rule to be added if an IKE phase 2 rule with anonymous local and remote node IP addresses already exists. Multiple IKE phase 2 rules can only be added if each rule specifies a distinct local and remote node IP address.

It is recommended that only one IKE phase 2 rule with anonymous local and remote node IP addresses be configured on a server, unless it is necessary to configure multiple IKE phase 2 rules with each having a distinct local and remote node IP address.

### Importing IKE rules

Use this procedure to bulk-import IKE rules. The IKE rules import file is a plain text file.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **2** to select **Import IKE configurations**.
3. tEoncteorn**Y**tinue with the import and overwrite all existing IKE configurations with import data.
4. Enter the name of and full path to the import file. There are no specific requirements for the name and path location of the import file; it can be a plain text file or another file type of your choosing.

You must restart the IPsec service for the new configuration to take effect.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

###### Importing IKE rules job aid

This job aid provides the syntax for the IPsec policy import file. The syntax for the IKE phase 1 rules specified in the file is: p1[space]<remote node address>([space]<generate policy>)[space]<lifetime>lspace]<enc alg>[space]<hash alg>[space]<dh group>[space]<auth mthd>([space]<cert file>[space]<key file>)

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| p1 | This is a phase 1 rule. |
| <remote node address> | IP address of the remote node (in dot-notation)— can be anonymous or a specific IP. |
| <generate policy> | Generate policy: on, off |
| <lifetime> | Lifetime: number of seconds, from 30 to 2592000 seconds (30 days) |
| <end alg> | Encryption algorithm: des, 3des, or aes |
| <hash alg> | Hash algorithm: md5, sha1, or sha256 |
| <dh group> | DH group: 1, 2, 5, 14, 15, 16, 17, or 18 |
| <auth methd> | Authentication method: x509\_certificate or pre\_shared\_key. |
| <cert file> | x.509 certificate file name (if certificate is used) |
| <key file> | Private key file name (if certificate is used) |

The syntax for the IKE phase 2 rules specified in the file is: p2[space]<local node address>[space]<remote node address>[space]<lifetime>[space]<enc alg>[space]<auth alg>

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| p2 | This is a phase 2 rule. |
| <local node address> | IP address of the local node (in dot-notation)—can be anonymous or a specific IP and must be anonymous if the remote node address is anonymous. |
| <remote node address> | IP address of the remote node (in dot-notation)— can be anonymous or a specific IP and must be anonymous if the local node address is anonymous. |
| <lifetime> | Lifetime: number of seconds, from 30 to 86400 seconds (24 hours) |
| <end alg> | Encryption algorithm: des, 3des, aes, or null\_enc |
| <auth alg> | Authorization algorithm: hmac\_md5, hmac\_sha1, or hmac\_sha256 |

### Listing IKE rules

Use this procedure to list all of the currently configured IKE rules. You can use this procedure to identify the ID for a particular IKE rule that you want to modify or delete.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **1** to select **List all IKE configurations**.

The tool displays the policies by ID, and lists the phase (1 or 2) along with all of the parameters for each.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

For an example of an IKE rules listing, see IKE rules listing example.

### Modifying an IKE phase 1 rule

Use this procedure to modify an IKE phase 1 rule.

###### Prerequisites

* + You must be assigned the SSA role.
  + The certificate and private key, referenced by the phase 1 rule, are installed if certificates are used for IPSec/IKE authentication.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **4** to select **Modify an IKE configuration**.
3. Enter the ID of the IKE phase 1 rule that you want to modify.
4. At the prompt, enter the remote node IP address (dot-notation).

You can specify the IP address as anonymous (\*.\*.\*.\*). Because this rule applies to all IKE phase 1 negotiation, you can create only one rule (per server) that specifies the remote node IP address as anonymous.

1. At the prompt, enter the corresponding number for the Generate Policy (1-on, 2-off). This value must be set as off as default. If the configuration is set between PLE4 the value must be set as on
2. At the prompt, enter the phase 1 lifetime (30 to 2592000 seconds).
3. At the prompt, enter the corresponding number tor the Encryption Algorithm (1-des, 2-3des, 3-aes).
4. At the prompt, enter the corresponding number tor the Hash Algorithm (1-md5, 2-sha1, 3-sha256).
5. At the prompt, enter the Authentication Method (1- x509\_certificate, 2-pre\_shared\_key)

###### For Certificates:

* + At the prompt, enter the X.509 certificate file name.
  + At the prompt, enter the Private key file name.

1. At the prompt, enter the DH Group (1, 2, 5, 14, 15, 16, 17, or 18).
2. Review the configuration, and enter **Y** to confirm the new addition.
3. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

### Modifying an IKE phase 2 rule

Use this procedure to modify an IKE phase 2 rule.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **4** to select **Modify an IKE configuration**.
3. the ID of the IKE phase 2 rule that you want to modify.
4. At the prompt, enter the local node IP address (dot-notation).

You can specify the local and remote node IP addresses as anonymous (\*.\*.\*.\*). Because this rule applies to all IKE phase 2 negotiation, you can create only one rule (per server) that specifies the remote node IP address as anonymous.

1. At the prompt, enter the remote node IP address (dot-notation).

If you specify the local node IP address as anonymous, you must specify the remote node IP address as anonymous. If you specify a particular IP address for the local node IP address, you must specify a particular IP address for the remote node IP address.

1. At the prompt, enter the Phase 2 lifetime (30 to 86400 seconds).
2. At the prompt, enter the corresponding number tor the Encryption Algorithm (1-des, 2-3des, 3-aes, 4-null\_enc).
3. At the prompt, enter the corresponding number tor the Authentication Algorithm (1-hmac\_md5, 2-hmac\_sha1, 3-hmac- sha256).
4. Review the configuration, and enter **Y** to confirm the new addition.
5. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

### Deleting an IKE rule

Use this procedure to delete a phase 1 or phase 2 IKE rule.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **5** to select **Delete an IKE configuration**.
3. Enter the ID of the IKE rule that you want to delete.
4. Enter **Y** to confirm the delete.
5. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

### Rolling back to the previous IKE rule configuration

Use this procedure to roll back to (restore) previously saved IKE rule configurations.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **7** to select **Rollback**.
3. Enter **Y** to confirm the rollback and overwrite all current IKE rules with the rollback version of the IKE rules.
4. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

### Restoring IKE rules default configuration

Use this procedure to restore the system default IKE rules.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **3** to select **Configure IKE Rules**.
2. Enter **8** to select **Restore system defaults**.
3. Enter **Y** to overwrite all current IKE rules with the system default IKE configuration.
4. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, 3, 4, 5, 7 or 8. |
| Save IKE rule configuration | Enter 6. |
| Return to the main menu and make another selection | Enter 9, and then enter Y to confirm the save. |
| Exit the tool | Enter 10, and then enter Y to confirm the save. |

If you select option 9 or 10, you receive a prompt to confirm the save operation only if the session data is different than the data stored in the current IKE rule configuration file.

**--End--**

### IPsec service management

The following procedures enable you to manage the IPsec service:

* + [“Starting or restarting the IPsec service—ipscfg method” (page 101)](#_bookmark134)
  + [“Starting or restarting the IPsec service—CLI method” (page 102)](#_bookmark135)
  + [“Stopping the IPsec service—ipscfg method” (page 102)](#_bookmark136)
  + [“Stopping the IPsec service—CLI method” (page 103)](#_bookmark137)

### Starting or restarting the IPsec service—ipscfg method

Use this procedure to start or restart the IPsec service.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### /opt/mcp/ipsec/ipscfg.pl

1. Enter **4** to select **Start IPsec Service**.

A warning message appears to notify you that this operation can disrupt traffic between this server and other servers.

1. Enter **Y** to confirm.

**--End--**

### Starting or restarting the IPsec service—CLI method

Use this procedure to start or restart the IPsec service.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the command prompt, enter the following command:

###### startipsec

**--End--**

### Stopping the IPsec service—ipscfg method

Use this procedure to stop the IPsec service.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. Run the IPsec/IKE Configuration tool:

###### ipscfg

1. Enter **5** to select **Stop IPsec Service**.

A warning message appears to notify you that this operation can disrupt traffic between this server and other servers.

1. tEoncteorn**Y**firm.

**--End--**

### Stopping the IPsec service—CLI method

Use this procedure to stop the IPsec service.

###### Prerequisites

You must be assigned the SSA role.

###### Procedure steps Step Action

1. Log on to the server as an SSA.
2. At the command prompt, enter the following command:

###### stopipsec

**--End--**

## IPsec configuration between OpenSwan and Racoon

This section contains the procedures for configuring IPsec connections between OpenSwan and Racoon using a preshared key (PSK).

###### System Layout

In cryptography, a PSK is a shared secret shared previously between the two parties using a secure channel. The preshared key used in an OpenSwan to Racoon connection must be a hexadecimal number in the AS system. Configurations on the OpenSwan and Racoon sides must be same.

The supported algorithms in IPsec Policy for OpenSwan and Racoon are shown in the following table.

|  |  |  |
| --- | --- | --- |
| **Supported algorithm** | **OpenSwan** | **Racoon** |
| Encryption algorithm | 3des | 3des |
| Hash algorithm | md5 | sd5 |
| sha1 | sha1 |
| Authentication algorithm | hmac\_md5 | hmac\_md5 |
| hmac\_sha1 | hmac\_sha1 |

The Diffie-Hellman group is called “dh group” in the Linux IKE policy. The following values of the Diffie-Hellman group parameter are supported:

• 2: modp1024

• 5: modp1536

The remainder of the Diffie-Helman group is not configurable for a tunnel between OpenSwan and Racoon.

As a default, the generate\_policy value on Racoon is in the “off” setting. This value must be set to “on” for configuration between OpenSwan and Racoon.

###### Recommendations

For purposes of backup and recovery, each network element should be treated as if it is on physically separate hardware.

The following parameter values are recommended in the IKE configuration for the Racoon system:

* + P1 lifetime: 86400 seconds (= 24 hours)
  + P2 lifetime: 86400 seconds

The following parameter values are recommended in the IKE configuration for the OpenSwan system:

* + ikelifetime=86400s
  + salifetime=86400s

###### Limitations

The following are limitations that should be considered when this functionality is used:

* + A certificate exchange procedure is not supported; this configuration only works with PSK exchange.
  + OpenSwan must be configured manually; no script is available to configure IPsec on OpenSwan.

**Navigation**

The IPsec package is included in the server image. The installation of the IPsec package is part of the server installation process. PLE1(RHEL 3), PLE2(RHEL 5), PLE3(RHEL 5) servers use Racoon IPsec and the PLE4(RHEL 6) server uses OpenSwan IPsec.

* + [“Setting the OpenSwan (PLE4) side” (page 105)](#_bookmark139)
  + [“Setting the Racoon side” (page 106)](#_bookmark143)
  + [“Stopping IPsec between OpenSwan and Racoon” (page 111)](#_bookmark157)

**Attention**

In the procedures that follow in this section, the IP address 47.168.1.1 is used for OpenSwan and the IP address 47.168.1.2 is used for Racoon.

### Setting the OpenSwan (PLE4) side

Perform the following procedures to set the OpenSwan (PLE4) side:

* + [“Setting the Preshared Key in OpenSwan” (page 105)](#_bookmark140)
  + [“Setting the IKE configuration in OpenSwan” (page 105)](#_bookmark141)
  + [“Starting IPsec on OpenSwan” (page 106)](#_bookmark142)

### Setting the Preshared Key in OpenSwan

Use this procedure to set the Preshared Key in OpenSwan

###### Procedure steps Step Action

1. Log in to the sever that uses OpenSwan for IPsec.
2. Generate the preshared key on the server on which OpenSwan is installed.

**ipsec ranbits --continuous 128**

The following is sample output:

**0xf6aae763af1d42fc65a023ec957dce8d**

1. Modify /etc/ipsec.secrets file to add preshared key configuration on the OpenSwan side:

***left-side-IP-address right-side-IP-address* : PSK**

***Generated key at step 1***

**Attention**

The left side IP address is the IP address of this server; the right side IP address is the remote IP address of the server that will be connected.

**--End--**

### Setting the IKE configuration in OpenSwan

Use this procedure to set the IKE configuration in OpenSwan.

###### Procedure steps Step Action

**1** Modify the “/etc/ipsec.conf” file for IPsec configuration for the preshared key on the OpenSwan site.

**Attention**

Make sure that the indentation is retained on the configuration file.

The following is a sample of configuration between OpenSwan and Racoon:

conn net-to-net type=tunnel

left=*left side IP address* right=*right side IP address* authby=secret

ike=3des-sha1;modp1024 ikelifetime=86400s saliftime=86400s phase2=ah ah=hmac\_sha1 auto=start

**--End--**

### Starting IPsec on OpenSwan

Use this procedure to start IPsec on OpenSwan.

###### Procedure steps Step Action

**1** Start IPsec service

**service ipsec start**

**--End--**

### Setting the Racoon side

Perform the following procedures to set the Racoon side:

* + [“Setting the Preshared Key on Racoon” (page 106)](#_bookmark144)
  + [“IPsec Policy configuration” (page 108)](#_bookmark148)
  + [“IPsec IKE configuration” (page 109)](#_bookmark152)
  + [“Starting IPsec service on Racoon” (page 111)](#_bookmark156)

### Setting the Preshared Key on Racoon

Use this procedure to set the Preshared Key on Racoon.

###### Procedure steps Step Action

1. Log in to the server that uses Racoon for IPSec.
2. Change directory to the following:

**cd /opt/mcp/ipsec/**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 1: Configure Preshared Keys
2. There are two methods for configuring preshared keys. Only one of these methods can be used to set the PSK of Racoon; the other one, then, should be skipped. The two methods are:
   * Add preshared key configuration one by one using option Import preshared key configurations. To perform this procedure go to step [Step 6](#_bookmark145)
   * Import all preshared key configurations at once using Add a preshared key configuration. To perform this procedure go to step [Step 11](#_bookmark146)
3. Select option 3: Add a preshared key configuration

**Prompt remote note IP address and PSK.**

**Enter Remote Node Address (dot-notation): 47.168.1.1**

**Enter preshared key (0xhex): 0xf6aae763af1d42fc65a023ec957dce8d**

1. Select Option 1: List all preshared key configurations, to ensure no mistake was made in the data entry in the previous step.
2. Select Option 6: Save preshared key configuration.
3. Select Option 8: Return to main menu, or Option 9: Exit
4. Go to step [Step 20](#_bookmark147)
5. Prepare a preshared key configuration import file. If it is in a conventional system, the import file contains the following specification: 47.168.1.1 0xf6aae763af1d42fc65a023ec957dce8d
6. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 1: Configure Preshared Keys, to enter the preshared key configuration submenu.
2. Select Option 2: Import preshared key configuration.
3. Select the import option “Overwrite” and enter the import file name.
4. Select Option 6: Save preshared key configurations.
5. Select Option 8: Return to main menu, or Option 9: Exit.
6. Erase the preshared key configuration import file, since it could be a security risk if left on the machine where it can be seen.
7. Procedure is complete.

**--End--**

### IPsec Policy configuration

Use this procedure to set IPsec policy.

###### Procedure steps Step Action

1. There are two approaches to configuring IPsec policies. Only one of these methods can be used to set policies of Racoon; the other method should, then, be skipped. These two methods are:
   * Add IPsec policy configuration one by one. To perform this procedure go to step [Step 2](#_bookmark149)
   * Import all IPsec policy configurations at once. To perform this procedure go to step [Step 11](#_bookmark150)
2. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 2: Configure IPsec Policies, to enter the IPSec policy configuration submenu.
2. Select Option 3: Add an IPSec policy.
3. Add local and remote server IP addresses.

**Enter local node address (dot-notation):47.168.1.2 Enter remote node address (dot-notation): 47.168.1.1**

**Add the following IPSec policy configuration: Local Node Address: 47.168.1.2; Remote Node Address: 47.168.1.1**

1. Select Option 1: List all IPSec policies, to ensure no mistake in the data entry in the previous steps.
2. Select Option 6: Save policies.
3. Select Option 8: Return to main menu, or Option 9: Exit
4. Go to step [Step 19](#_bookmark151)
5. Prepare an IPsec policy configuration import file. The import file contains the following IPsec policy configuration: 47.168.1.2 47.168.1.1
6. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 2: Configure IPSec Policies, to enter the IPSec policy configuration submenu.
2. Select Option 2: Import IPSec policies.
3. Select the import option “Overwrite” and enter the import file name.
4. Select Option 6: Save IPSec policies.
5. Select Option 8: Return to main menu, or Option 9: Exit
6. Procedure is complete.

**--End--**

### IPsec IKE configuration

Use this procedure to set IPsec IKE.

###### Procedure steps Step Action

1. There are two methods for configuring the IKE. Only one of these methods can be used to set IKE of Racoon; the other method should, then, be skipped. The two methods are:
   * Add IKE configurations one by one. To perform this procedure go to step [Step 2](#_bookmark153)
   * Import all IKE configurations at once. To perform this procedure go to step [Step 11](#_bookmark154)
2. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 3: Configure IKE Rules , to enter the IKE Configuration Submenu.
2. Select Option 3: Add an IKE configuration, to add a remote node specification.
3. Enter data and confirm the action for phase1. A sample configuration is as follows:

Phase 1 lifetime = 86400 sec Generate Policy = on Encryption Algorithm = 3des Hash Algorithm = sha1

Authentication Method = pre\_shared\_key DH Group =2

1. Enter data and confirm the action for phase2. A sample configuration is as follows:

Phase 2 lifetime = 86400 Encryption algorithm = 3des

Authentication algorithm = hmac\_sha1

1. Select Option 6: Save IKE configurations
2. Select Option 9: Return to main menu, or Option 10: Exit
3. Go to step [Step 19](#_bookmark155)
4. Prepare an IKE configuration import file that contains the specifications shown below:

**p1 *remote-node-address lifetime enc-alg hash-alg dh- group auth-mthd***

**p2 *local-node-address remote-node-address lifetime enc-alg auth-alg***

**p1 47.168.1.1 on 86400 3des sha1 2 pre\_shared\_key**

**p2 47.168.1.2 47.168.1.1 86400 3des hmac\_sha1**

1. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscf g.pl**

1. Select Option 3: Configure IKE Rules, to enter the IKE configuration submenu.
2. Select Option 2: Import IKE configurations.
3. Select the import option “Overwrite” and enter the import file name.
4. Select Option 6: Save IKE configurations.
5. Select Option 9: Return to main menu, or Option 10: Exit.
6. Procedure is complete.

**--End--**

### Starting IPsec service on Racoon

Use this procedure to set IPsec service on Racoon.

###### Procedure steps Step Action

1. Change directory to the following:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 4: Start IPSec Service to start IPsec.
2. Select Option 6: Show IPSec Service Status to see IPSec status.

**--End--**

### Stopping IPsec between OpenSwan and Racoon

When no IPsec is required between OpenSwan and Racoon, services have to be stoped on both sides. If IPsec configuration is required, however, DO NOT stop IPsec.

**Attention**

IPsec also supports VLan tagging.

### Stopping IPsec service on OpenSwan

Use this procedure to stop IPsec service on OpenSwan.

###### Procedure steps Step Action

**1** To stop IPsec service, enter the following command:

**service ipsec stop**

**--End--**

### Stopping IPsec service on Racoon

Use this procedure to stop IPsec service on Racoon.

###### Procedure steps Step Action

1. To stop IPsec service, enter the following command:

**cd /opt/mcp/ipsec**

1. Run the tool ipscfg

**./ipscfg**

1. Select Option 5: Stop IPsec Service to stop IPsec.

**--End--**

## Viewing trusted node and port configurations with iptstatus

Use this procedure to display all of the configured trusted nodes and ports using the iptstatus command.

### Procedure steps

###### Step Action

**1** At the command line, run the iptstatus tool:

###### /opt/mcp/ipt/iptstatus.pl

**--End--**

### Viewing trusted node and port configurations with iptstatus job aid

The iptstatus tool includes the following command line options:

|  |  |
| --- | --- |
| **Option** | **Description** |
| h | Displays the Help information. |
| n | Displays all current trusted node configurations. This option provides the same functionality as the List trusted nodes option provided by the iptcfg tool. |
| p | Displays all current trusted post configurations. This option provides the same functionality as the List trusted ports option provided by the iptcfg tool. |
| a | Displays all current access control rules. This option provides the same functionality as the Show Current Access Control Rules option provided by the iptcfg tool. |
| r | Displays all current access control rules in a raw format that is convenient for the user to further process the data, if desired.  The syntax for the iptstatus command in the raw format is as follows: |

|  |  |
| --- | --- |
| **Option** | **Description** |
|  | <Type of Rule>, <Source IP>, <Source Subnet Mask>,  <Destination IP>, <Destination Subnet Mask>, <Protocol>, <Source Port>, <Destination Port>, <To-Port> |
| j | Displays all current access control rules in a justified format based on the raw format. |

## DSCP marking configuration

Configure DSCP marking to differentiate packet types according to type of traffic. For traffic types, see [“Access control configuration” (page 61)](#_bookmark81).

### Navigation

* + [“Listing the DSCP marking configurations” (page 113)](#_bookmark162)
  + [“Modifying DSCP marking values” (page 114)](#_bookmark163)
  + [“Modifying the DSCP marking status” (page 115)](#_bookmark164)
  + [“Modifying DSCP Call Signaling and OAMP Values” (page 116)](#_bookmark165)

### Listing the DSCP marking configurations

Use this procedure to view the current DSCP marking configurations. You can use this procedure to identify the ID for a DSCP marking value that you want to modify.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **3** to select **Configure DSCP Marking**.
5. Enter **1** to select **Show DSCP marking configurations**.

The tool displays the current values for the network traffic categories by ID and the current DSCP marking status.

1. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 2 or 3. |
| Return to the main menu and make another selection | Enter 4, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 5, and then confirm that you want to exit the tool. |

**--End--**

### Modifying DSCP marking values

Modify the DSCP values to specify the value for each category of network traffic.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **3** to select **Configure DSCP Marking**.
5. Enter **2** to select **Modify DSCP marking values**.
6. Enter the ID of the DSCP value (network traffic category) that you want to modify.
7. Enter the new value.
8. Enter **Y** to confirm the changes.
9. Choose an action:

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1, 2, or 3. |
| Return to the main menu and make another selection | Enter 4, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 5, and then confirm that you want to exit the tool. |

**--End--**

### Modifying the DSCP marking status

Modify the DSCP marking status to enable or disable DSCP marking.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/ipt/iptcfg.pl**.
3. If you receive a prompt, enter your password.
4. Enter **3** to select **Configure DSCP Marking**.
5. Enter **3** to select **Modify DSCP marking status**.
6. Configure the DSCP marking state.

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Enable DSCP marking | Enter 1 |
| Disable DSCP marking | Enter 0 |

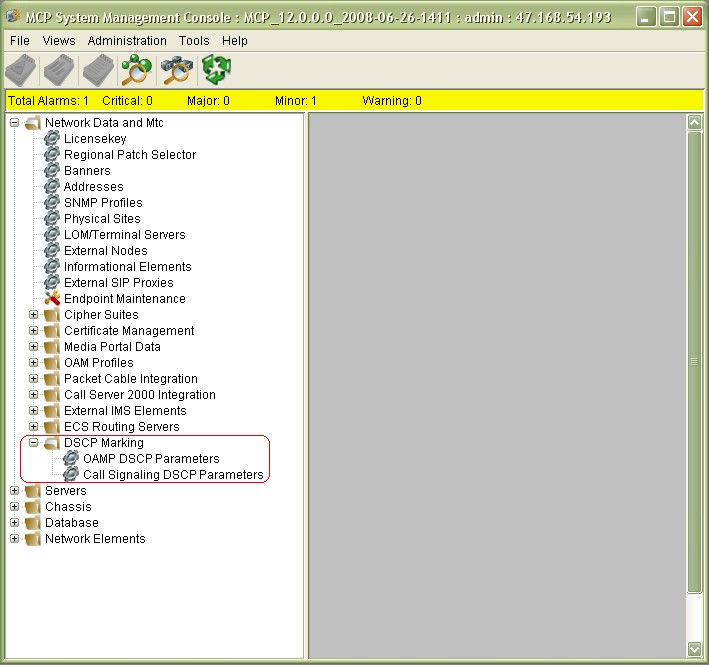
1. Enter **Y** to confirm the changes.
2. Choose an action:

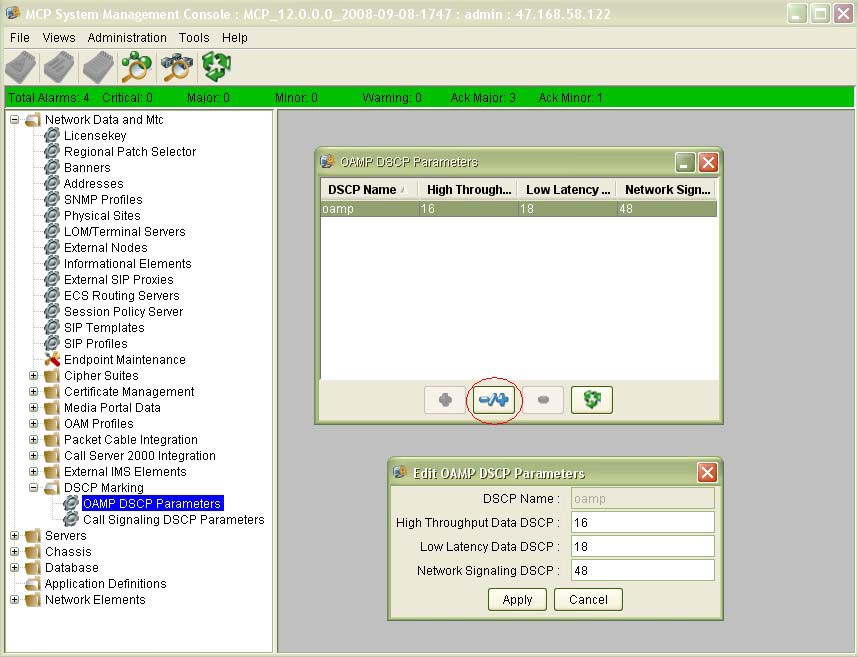
|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Select another configuration option | Enter 1 or 2. |
| Return to the main menu and make another selection | Enter 4, and then choose to keep or discard uncommitted changes. |
| Exit | Enter 5, and then confirm that you want to exit the tool. |

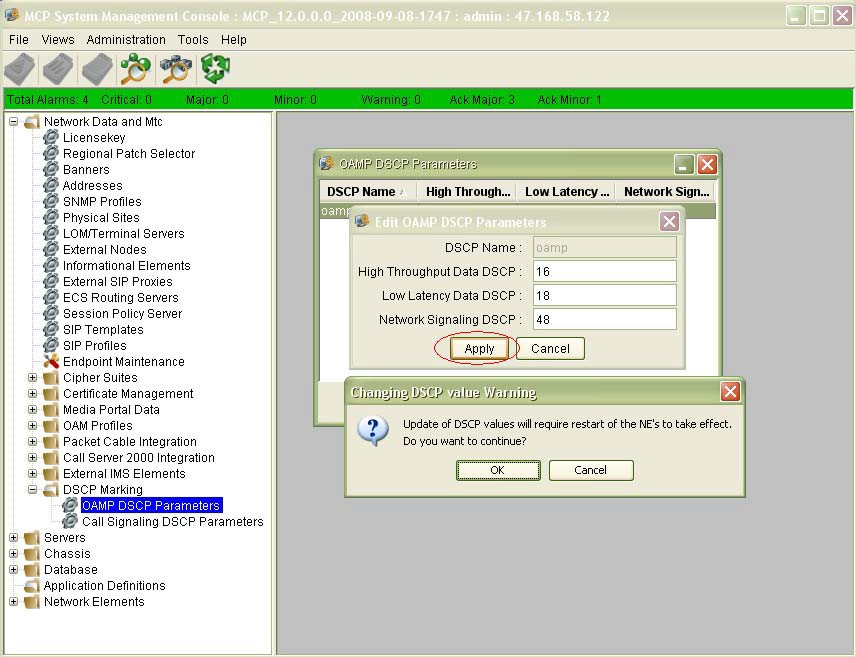
**--End--**

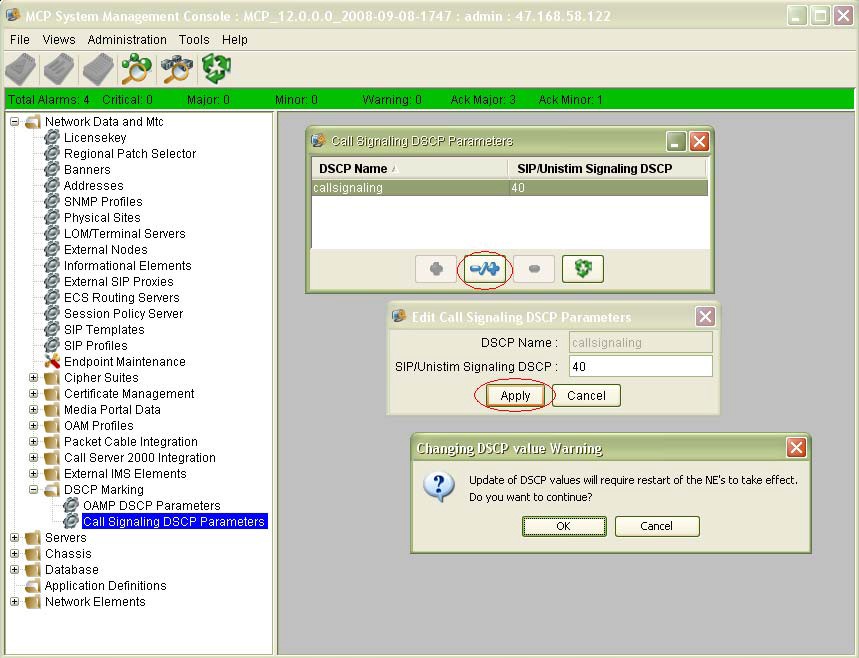
### Modifying DSCP Call Signaling and OAMP Values

The following System Management console screens are used to configure Call Signaling and OAMP DSCP values.

**SM GUI – DSCP Marking contains DSCP Parameter and Call Signaling groups**

**SM GUI – OAMP DSCP Parameters and Edit Dialog**

**SM GUI - OAMP DSCP Parameters Dialog**

**Call Signaling DSCP Parameters Configuration Dialog**

## Increasing network security with SNMP

During the installation, The AS is configured with a default SNMP profile with *public* as the read community string. This default profile is used between the SM and its managed AS core elements. After the initial installation, it is recommended to replace the default SNMP with a unique read community string. Use the following procedures to replace the default SNMP profile and assign the new SNMP profile.

### Prerequisites

* + You can access the System Management Console
  + You are assigned an administrative role with SnmpProfileService privilege.

### Navigation

* + [“Configuring an SNMP profile” (page 120)](#_bookmark167)
  + [“Enabling a license key” (page 121)](#_bookmark168)
  + [“Configuring a server” (page 123)](#_bookmark169)

### Configuring an SNMP profile

Configure an Simple Network Management Protocol (SNMP) profile to establish consistent SNMP parameters that the System Manager uses to monitor the condition of the operating system and server hardware for the managed and monitored network elements.

### Prerequisites

* + You can access the System Management Console.
  + You have SnmpProfileService privileges.
  + The license key is updated. For more information about how to update the license key, see [“Enabling a license key” (page 121)](#_bookmark168).

### Procedure steps

###### Step Action

1. From the configuration view of the System Management Console, select **Network Data and Mtc, SNMP Profiles**.
2. Click **Add (+)**. **OR**

Select an entry and click **Edit (-/+)**.

1. Configure the **Profile Name**, **SNMP Port**, **Read Community String**, and **Write Community String** parameters.
2. Click **Apply**.

**--End--**

### Configuring an SNMP profile job aid

The following table describes the parameters that you use to configure an SNMP profile.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Profile Name | This (text) value is a unique name to identify the profile. |
| SNMP Port | This (read only) value is the SNMP port. |
| Read Community String | This (text) value is the name of the Read Community String.  Default: Public |
| Write Community String | This (text) value is the name of the Write Community String.  Default: Private |

**Attention**

The default values are Public and Private. To increase security, GENBAND recommends that you use values other than Public and Private.

### Enabling a license key

Use this procedure to enable a license key.

A license key is used to activate specific features and services, (for example, Application Manager service and Network-based call log service) which require license keys for activation.

Before performing this procedure ensure that you have met the following requirements:

* + You can access the System Management Console.
  + Ensure that you have downloaded the license keys using the Keycode Retrieval System (KRS). For more information, see *EXPERiUS AS — Fundamentals* (NN48111-111). For additional information about license keys, see *EXPERiUS AS — Administration* (NN48111-611).

### Procedure steps

###### Step Action

1. Select **Network Data and Mtc, Licensekey** from the System Management Console.

*The Licensekey window appears.*

1. On the Select Licence dialog box, click the **Edit** button. **3**

**Attention**

Remember this is the license key that you generated using the Keycode Retrieval System.

Navigate to the license key file on the local workstation, select the file, and click **Open**.

**4** Click all of the tabs to see the list of enabled features and services.

**--End--**

### Job aid

This job aid provides a list of major AS services that are activated with their license keys. Note this is not a comprehensive list of license keys.

* + Advanced Screening
  + Network Call Log
  + Presence
  + Unified Communications
  + Wireless Client
  + Application Manager service
  + Teen service
  + SH Interface
  + Vertical Service Codes
    - Call Forward Variants Subscribers
    - Do Not Disturb Subscribers
    - Anonymous Call Rejection Subscribers
    - Network Call Waiting Subscribers
    - Calling Line ID Restriction Subscribers
    - Call Return Subscribers
    - Short Dialing Codes Subscribers
    - Malicious Call Trace subscribers (existing)
  + Call Type Based Screening and Selective Call Reject
    - Call Type Based
    - Deny All Calls service
    - Selective Reject service
  + Embedded Web Service Gateway
    - Presence web service
    - Multimedia messaging web service
    - Third Party Call web service
    - E911 Public IP
  + XMPP Gateway Subscriber
  + PBX Communicator Subscribers
  + Session Policy Server
  + Uniform Call Distribution (UCD)
  + SLR Mobility Subscribers
  + Mobile Extension Subscribers
  + Call Grabber Subscribers
  + Hunt Group
  + Equal Access Subscribers
  + SLR Domain License Key
  + SLR Mobility License Key

### Configuring a server

The addition of new servers and server configuration typically occurs during installation and commissioning.

### Prerequisites

* + You can access the System Management Console.
  + You have PhysicalServerService privileges.
  + You have PhysicalSiteService privileges.
  + You have IPAdddressService privileges.
  + You have SnmpProfileService privileges.

### Procedure steps

###### Step Action

1. From the configuration view of the System Management Console, select **Servers**.
2. Click **Add (+)**.
3. In the **Server** dialog box, configure the **Server Name**, **Long Server Name**, **Physical Site**, **Interface 1**, **Interface 2 (mgmt)**, **Operating System**, **Server Type**, **SNMP Profile**, and **Host Name** parameters.
4. Click **Apply**.

Use the new data to configure a network element instance.

**--End--**

### Configuring a server job aid

This job aid lists and describes the parameters that appear on the Server dialog box.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Server Name | This parameter is the unique name that identifies the server, for example, EMS1. You use this parameter to associate the network element application with the server. |
| Server Name Long | This parameter is the long name of the server, for example, EMS1Server. |

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Physical Site | This parameter (select from a list), specifies the location of the server. |
| Interface 1 | This parameter (select from a list), specifies the Logical Name of the IP address for this server. |
| Interface 2 (mgmt) | This optional parameter (select from a list) is for management LAN configuration. If you configure this parameter, all northbound OAM feeds use this interface. |
| Operating System | This parameter (select from a list) indicates the operating system running on the server. Do not configure the value to windows. If the value is windows, memory information is not polled from the server. The system also uses this parameter to determine file paths. |
| Server Type | This parameter (select from a list) indicates the server model: BladeServer, CC3310, Other, SAM-XTS, or X3550. |
| SNMP Profile | This parameter (select from a list) specifies the SNMP Profile the server uses. Ensure that the operating system SNMP daemon configuration matches the defined SNMP profile. |
| Host Name | This parameter specifies the hostname of the server. |

# Central Authentication and Authorization

**125**

Central Authentication and Authorization applies to the following devices and applications in an Application Server (AS) system:

* + Platform users for blades hosting the SM, SESM, PROV, AM, AppMan, IPCM, DB, and BCP
  + SM administrators
  + Provisioning administrators

Authentication, or validation of the user ID and password, is available in two basic varieties:

* + **Local** – The user is authenticated using locally-defined account information.
  + **Central** – The user is authenticated with an external server.

Authorization, or determining what level of access an authenticated user has, also can be performed centrally or locally.

Central Authentication and Authorization is performed using RADIUS through an external RADIUS server. While a local RADIUS proxy is not required, it can be used to provide additional functionality not available directly to the platform and applications. A variety of modes allows the service provider maximum flexibility in configuring the solution to make use of Central Authentication and Authorization. This flexibility allows the product to be integrated with solutions that support only Central Authentication, but not Central Authorization.

A RADIUS proxy is available on a platform blade, with OAM access, so that any blades without OAM access can still use Central Authentication and Authorization.

When accounts are managed in a central location, it is easier for the service provider to manage information and maintain its security. And since a single RADIUS server can serve multiple systems, an administrator

needs to use only a single user ID and password for all the systems to be accessed. By reducing the number of secrets and keeping them in a single location, the overall security of the network is increased.

Other developments provided by this feature include:

* + RADIUS proxy. Since not all AS servers have OAM access, they are unable to connect to an external RADIUS server. Therefore, a RADIUS proxy is packaged with the AS system that can be deployed on any server with OAM access. Other servers can be configured to point to the proxy, which mediates requests between the external server and the client.
  + Multiple roles per user. The existing implementation of the AS application only allows a single role to be assigned to a user. With multiple roles available for each user, roles can be created that contain logically cohesive functions, which can then be assigned to existing users without having to define specific roles for each user.
  + The default staging certificate is replaced with a stronger hash.

## Platform Authentication and Authorization

Central authentication and authorization for platform users is enabled through the platform CAA Management CLI (caaMgt.pl). The caaMgt CLI is used to define and provision the RADIUS server groups, and to set the CAA mode to enable central authentication. Access types for platform users include sshd, login (console), su, and sudo.

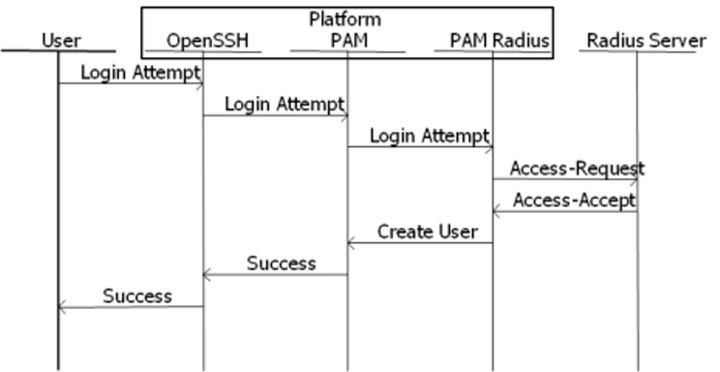
Before enabling CAA on the AS, one or more external RADIUS servers must be available. Every RADIUS server that will process AS central authentication requests must include the AS node information in its list of known RADIUS clients.

Since RADIUS requests can be proxied, the IP address of the proxy server should be configured on the RADIUS server for purposes of filtering devices from which to expect requests. The NAS IP address (that is, the IP address of the client being proxied) should be used for determining policies.

Using the caaMgt CLI, each RADIUS server group that has a primary RADIUS server and, optionally, a backup RADIUS server, is first defined. The secret for each RADIUS server defined must match the secret provisioned in the clients list at the RADIUS server.

An example of central authentication is shown in the following diagram.

**Central Authentication example**



When a server times out, a login attempt request is sent to the next server in the group. If all the servers timeout, or if a rejection is received, then the request is sent to the next group. If no groups remain, then authentication fails.

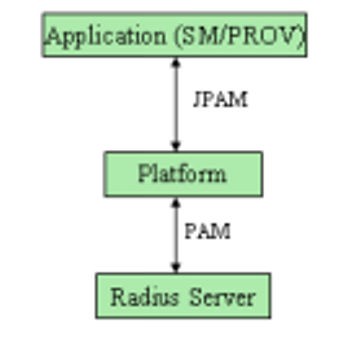
When the selected CAA mode includes local authorization, a successfully authenticated central user is subject to the locally-defined account privileges. This applies to local users who are made to authenticate centrally by the user password for that account being disabled.

When the selected CAA mode includes central authorization, a successfully authenticated central user will have a temporary account created on the platform. If a local account already exists for the user, however, the temporary account cannot be created and the authorization fails.

## Application Authentication and Authorization

The Application Authentication and Authorization component provides central authentication and central authorization for the existing system. The System Manager (SM) and Provisioning Manager (PROV) provide the ability for users to log in. Central Authentication is implemented in the application by interaction with the platform using JPAM. The platform, in turn, interacts with the external RADIUS server using the PAM module for authentication. Central Authorization is implemented by creating a temporary user for the central user in the application. This temporary user is created based on the roles/domains retrieved from the platform. The following figure depicts the flow of interaction for performing central authentication and central authorization.

**Application central authentication**



In order to operate properly, the platform on which the application is running must be configured for Central Authentication since the application will use JPAM to access the platform’s PAM configuration.

## RADIUS Proxy

RADIUS proxy is an intermediate server between third-party RADIUS servers and RADIUS clients (AS platform and application). The AS server that does not have the OAM address or direct access to external RADIUS server uses the RADIUS proxy to communicate with the third-party server. Multiple RADIUS clients and servers can be configured in a RADIUS proxy.

Unlike the platform, the proxy cannot be configured with multiple groups. Thus, when a reject is received, authentication will fail immediately since there are no other groups to which a request can be sent. Timeouts, however, still result in attempting to access the next server.

## JPAM

JPAM is the Java – PAM Bridge configured on the AS platform, which provides the facility for AS applications interaction with PAM, configured on the AS platform. All external Java application/GUI users can be authenticated centrally by a third-party RADIUS server using JPAM, which uses the Pam RADIUS authentication module (PAM) implicitly to communicate with the RADIUS server.

## Role Mapping

The following platform roles are defined for AS:

* + SSA – System Security Administrator
  + SA – Security Auditor
  + AA – Application Administrator
  + BA – Backup Administrator
  + DBA – Database Administrator
  + OSS - OSS Administrator
  + RPS - Patching (RPS) Administrator

These roles are standard CVAS Security roles. As such, a mapping of CVAS roles to AS roles is done when the VSA is received from the RADIUS server by the platform doing Central Authorization.

The mapping is as follows:

**Role mapping**

|  |  |
| --- | --- |
| **Succession Group / Role** | **AS Platform Role(s)** |
| secadm | SSA |
| A2\_SSA | SSA |
| secrw | SA |
| secmtc | SA |
| secro | SA |
| A2\_SA | SA |
| emsadm | AA, BA |
| A2\_AA | AA |
| emsmtc | BA |
| emsrw | BA |
| A2\_BA | BA |
| A2\_DBA | DBA |
| A2\_OSS | OSS |
| A2\_RPS | RPS |

In the examples below, the Central users are already configures in the RADIUS server:

**test90 Cleartext-Password := "Li69nux"** (central user - test90 will have "RPS" role on AS Platform)

AAE-User-Role := "A2\_RPS” AAE-User-Domain := "system"

**test92 Cleartext-Password := "Li69nux"** (central user - test92 will have "SSA" role on AS Platform)

AAE-User-Role := "A2\_SSA" AAE-User-Domain := "system"

**test5 Cleartext-Password := "Li69nux"** (central user - test5 will have "SSA, AA and BA” roles on AS Platform)

AAE-User-Role := "secadm,emsrw,emsadm" AAE-User-Domain := "system"

**Note:** The AS Platform role "PAUD" is defined only for the SFTP user role. It is used between two systems (CMT to AS Prov) and is not used by real operational users. It has therefore been excluded from the external AAA system. It is used only for Local Authentication / Local user.

For the SM and the PROV, there is no specific mapping comparable to AS Platform mapping. For example, if you need a central user for the AS application with the "secadmin" role, you can configure the central user in the RADIUS server using the "secadmin" role as the VSA attribute.

## Feature Dependencies and Restrictions

* + Password change and expiry is not supported from the AS when Central Authentication is used. In order to implement a password expiry mechanism, the central RADIUS server is responsible for determining when passwords are about to expire and triggering the sending of notifications to users. If a password must be changed, the operation must be performed on the central server instead of the platform/ application.
  + Centrally authorized accounts do not support account lockout checking and account-disabled checking since it requires details of the last login history.
  + Since the data of central users are stored in the cache only after authentication is successful, details about the last login history of central users cannot be accurately maintained.
  + Security of the RADIUS protocol should be ensured with IPSec because the RADIUS does not provide adequate security of the user ID and password contained in the Access-Request message.

## Supported Platforms

The following hardware platforms are supported in Central Authentication and Authorization:

* + HT Langley
  + aTCA (C20)
  + IBM BC-T

• CC3310

## Configuration of Central Authentication and Authorization

Central Authentication and Authorization is an optional configuration option. Only by explicitly enabling Central Authentication and Authorization can the central server be used. If Central Authentication and Authorization is not configured, system behavior with respect to authentication and authorization is unchanged from previous releases. Central authentication requires an external RADIUS server. The RADIUS server must be configured to include the AS nodes in its list of valid known clients. The RADIUS Server needs to be centrally configured if Central Authentication/ Authorization is to be used. The Central Authentication and Authorization option is used in the AS whenever a user is to be authenticated centrally from the RADIUS server.

### SM GUI Configuration

SM and PROV network elements associated with Central Authentication and Authorization have their own AAA profile. Initially, after upgrade, a default AAA profile is loaded into the system. The default profile contains the following information:

1. Central Authentication mode configured as LOCAL\_ONLY
2. Central Authorization mode configured as LOCAL
3. AAA profile name

The AAA profile is configured through the System Management Console, with the following information:

* + Central Authentication Mode
    - CENTRAL\_LOCAL. Central authentication is attempted first. If central authentication fails, it is followed by local authentication.
    - LOCAL\_CENTRAL. Local authentication is attempted first. If local authentication fails, it is followed by central authentication using an external RADIUS server.
    - LOCAL\_ONLY. The authentication is performed locally, based on local data.
  + Central Authorization Mode
    - CENTRAL. A temporary user is created, based on the roles/ domains retrieved from the RADIUS server.
    - LOCAL. The roles/domains of the user are defined locally.
  + Cache Expiry time (configured only for PROV). The cache expiry time (maximum length of one 24-hour day) for a PROV application provides the time interval after which the cache is cleared. When a PROV user is centrally authorized the first time, a temporary account is created for that user. In order to provide efficient authentication in the event of multiple SOAP requests (over OPI) for the same user (that is, to avoid

RADIUS requests sent every time), the user’s authentication information is cached. Any subsequent login attempts made within the expiry time do not go to the RADIUS server, but to the cache, where the following rules are applied:

* + - If the cache contains the given user name and password the cached authentication result is used without querying the central server.
    - If the user name and password combination is not present in the cache, it is checked to see if the given user name already has a successful authentication using a different password. If so, authentication with the given password is rejected.
    - Otherwise the central RADIUS server is used to centrally authenticate.

If the result is a failure, the user name/password is stored in the cache with a failed authentication result. If the result is a pass, all failed cache entries for the user are deleted and the single successful entry is inserted.

A limited number of attempts are made to centrally authenticate a cached user since the attempts could be associated with a DoS attack. When the expiry time has elapsed, the next authentication attempt will go to the central RADIUS server. Since existing mechanisms for account expiry are used, there is no performance impact.

* + AAA Profile Name

The AAA profile can be associated with either an SM or a PROV.

For the procedure used to configure the AAA profile, see *Configuring an AAA profile* in *EXPERiUS Application Server — Configuration* (NN48111– 511).

### Central Authentication and Authorization Platform CLI (caaMgt.pl)

The Central Authentication and Authorization (CAA) Management CLI (caaMgt.pl) allows setting the platform to CAA mode, provisioning the PAM RADIUS server details, and configuring the RADIUS proxy. Only administrators assigned the SSA role, belonging to the ntsysgrp group, can run this CLI. Since root access is required, the CLI is under sudo control for all SSA users.

For platform users, central authentication is supported for the following access types:

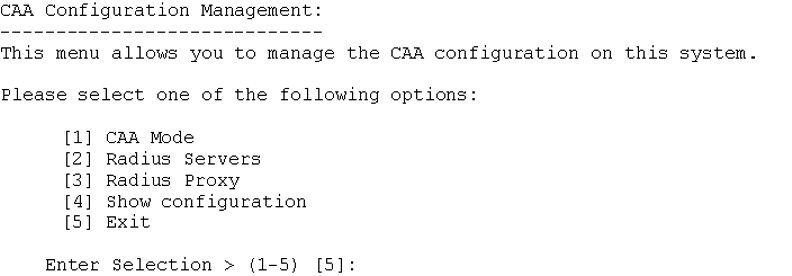
##### *ssh*

* + *login* (console)

##### *su*

* + *sudo*

The following figure shows the CAA Configuration Management menu when the caaMgt CLI is invoked.

**CAA Configuration Management menu**

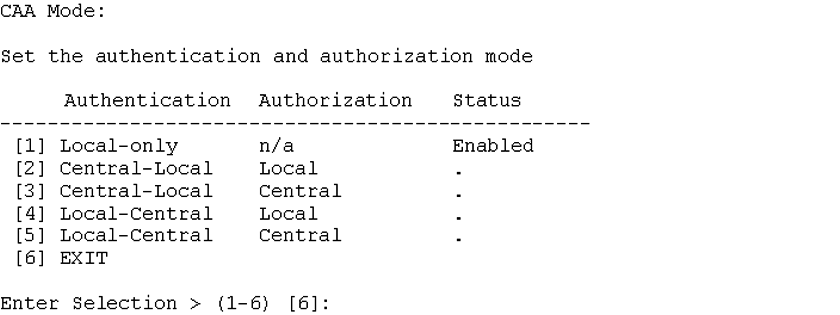
###### Configuring CAA Mode

The following figure shows the CAA Mode sub-menu. CAA is disabled when the mode is Local-Only. CAA is enabled for all other modes.

Provisioning the RADIUS servers is a prerequisite to setting the CAA mode to support central authentication.

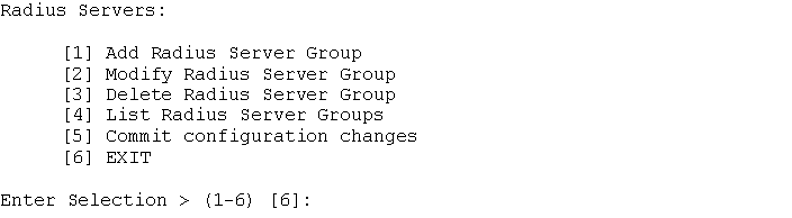
**Attention**

Fully removing the RADIUS server datafill is only permitted when CAA is disabled (that is, CAA mode is set to local-only).

**CAA Mode sub-menu**

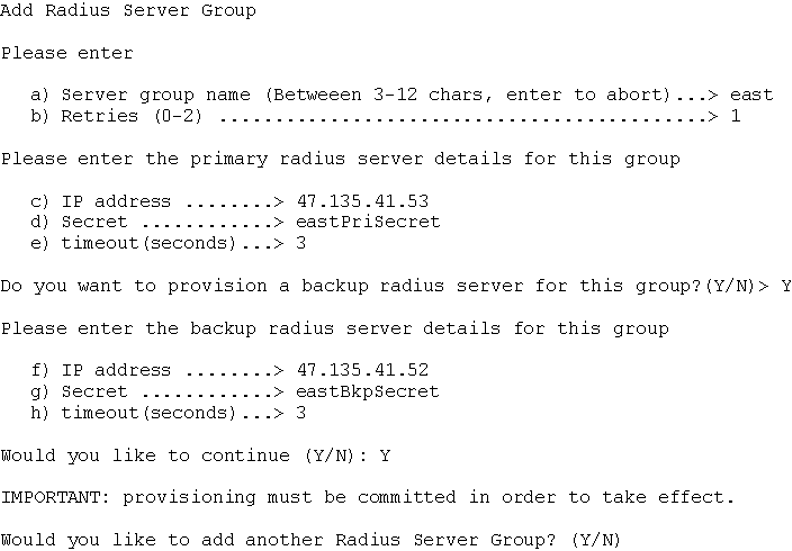
###### Configuring RADIUS Servers

The following figure shows the RADIUS Servers sub-menu. To enable CAA, at least one RADIUS server group must be added that contains a primary RADIUS server.

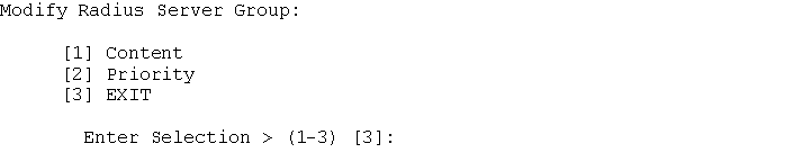
**RADIUS Servers sub-menu**

The following figure shows a sample Add RADIUS Server Group configuration dialog. This dialog allows definition of the RADIUS server group-name, the retries value for the group, the primary RADIUS server details, and the backup RADIUS server details. All servers in a group should share the same configuration. The following parameters are entered:

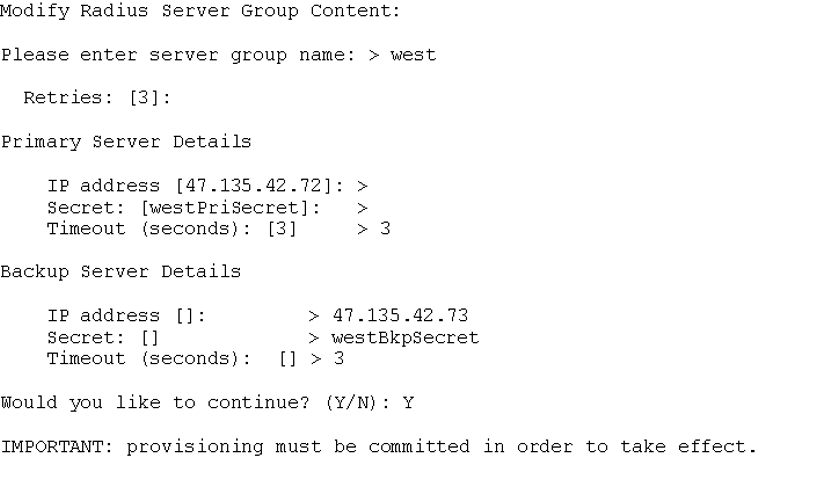
* + The group name is an arbitrary string, but could be the location of the servers.
  + The number of retries is applicable to all the servers in the group and applies when a message times out.
  + The IP address of each server is the address to which RADIUS messages will be sent when attempts to communicate to the server are being made.
  + The secret is used to validate the identities of the parties involved in the connection between the RADIUS server and the platform. This secret must also be configured on the RADIUS server.
  + The timeout indicates how long to wait for a response from a server before considering that the request has timed-out. The timeout is specific to the server.

**Add a RADIUS Server Group**

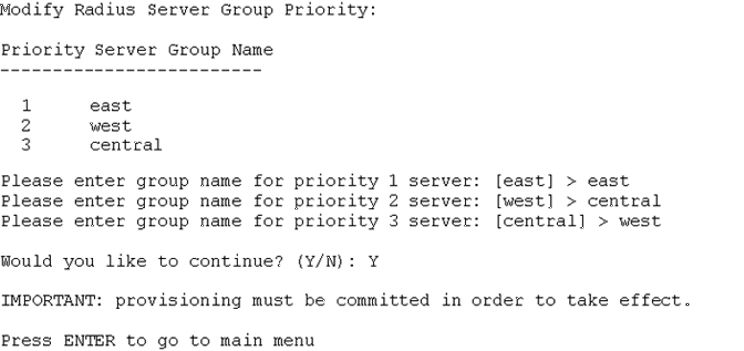
The following figure shows the Modify RADIUS Server Group sub-menu. This sub-menu allows the user to modify the RADIUS server group details and/or the RADIUS server group priority.

**Modify RADIUS Server Group**

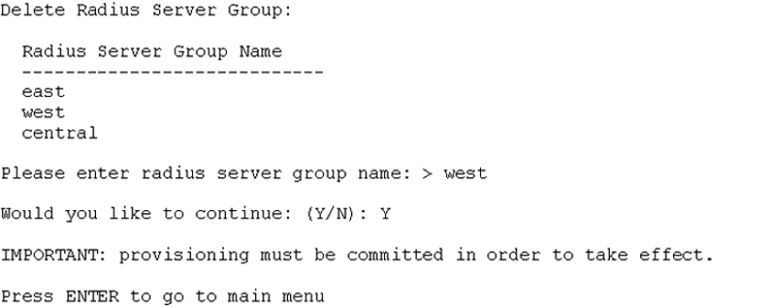
The following figure shows the Modify RADIUS Server Group Content sub- menu. This sub-menu is used to modify the retries count and the primary and backup RADIUS server details.

**Modify RADIUS Server Group Content**

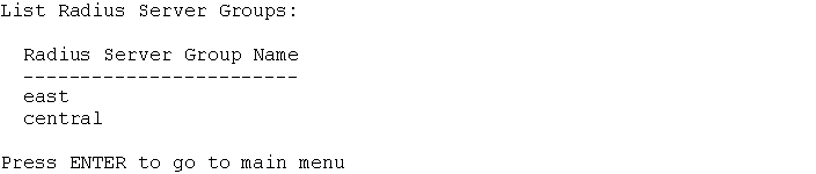
The following figure shows the Modify RADIUS Server Group priority sub- menu. This sub-menu is used to change the priority of the RADIUS server groups. The priority of the RADIUS server groups determines the order in which they are called by PAM RADIUS during central authentication.

**Modify RADIUS Server Group priority**

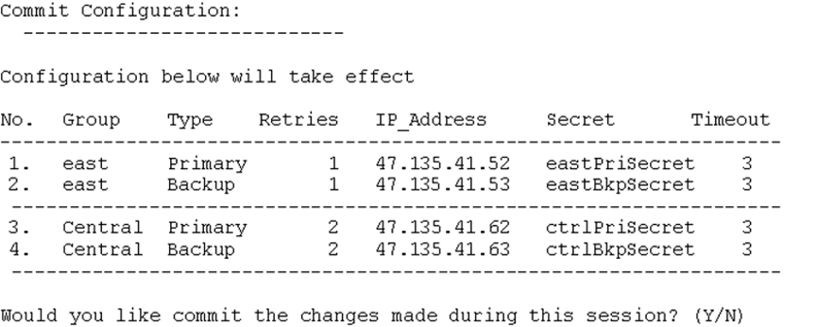
The following figure shows the Delete RADIUS Server Group sub-menu. This sub-menu is used to delete a RADIUS Server Group. If there is only one RADIUS Server Group defined, this group can only be deleted when the CAA mode is Local-Only. When the last RADIUS server group is being deleted, central authentication must be disabled for the SM and PROV applications.

**Delete RADIUS Server Group**

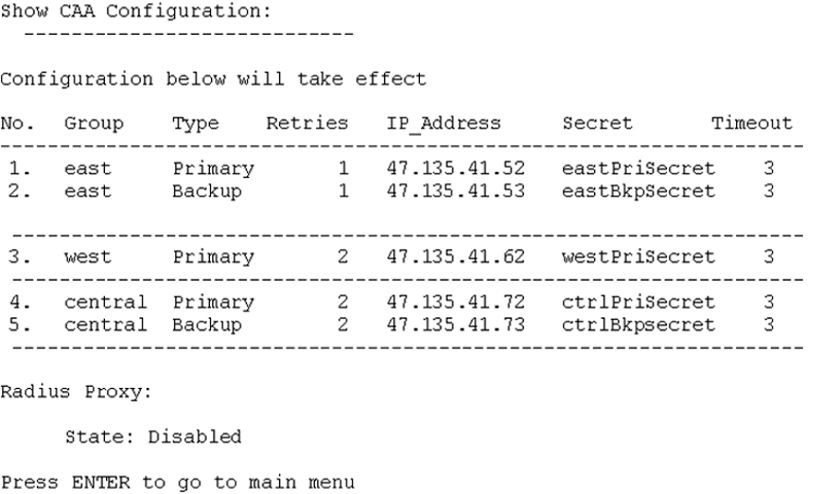
The following figure shows the List RADIUS Server Groups sub-menu, which is used for listing defined RADIUS Server Groups.

**List RADIUS Server Groups**

The following figure shows an example of a datafilled Commit Configuration sub-menu. This sub-menu is used to commit any RADIUS Server Group provisioning at the system level. If the CLI is exited before RADIUS Server Group provisioning is committed, a warning and confirmation is presented to ensure the user wishes to exit without committing.

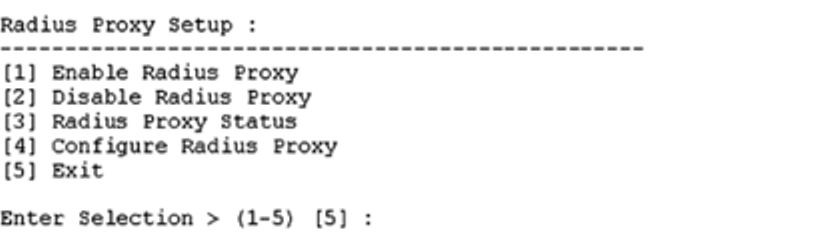
**Commit RADIUS Server Configuration example**

The following figure contains the Show CAA Configuration sub-menu, which is used to display all the CAA Management details, including CAA mode, RADIUS Server Group details, and RADIUS Proxy details.

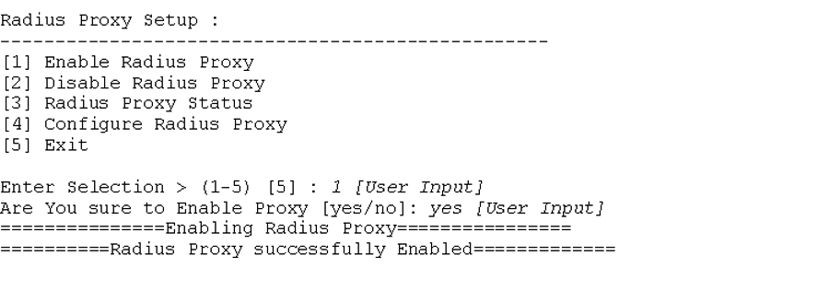
**Show CAA Configuration**

###### Configuring a RADIUS Proxy

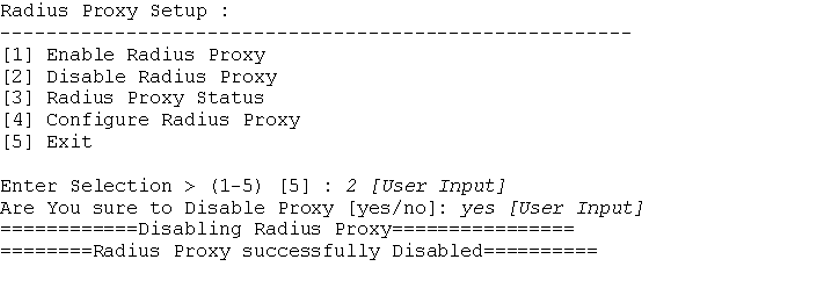
The following figure shows the RADIUS Proxy Setup sub-menu.

**Configuring a RADIUS proxy**

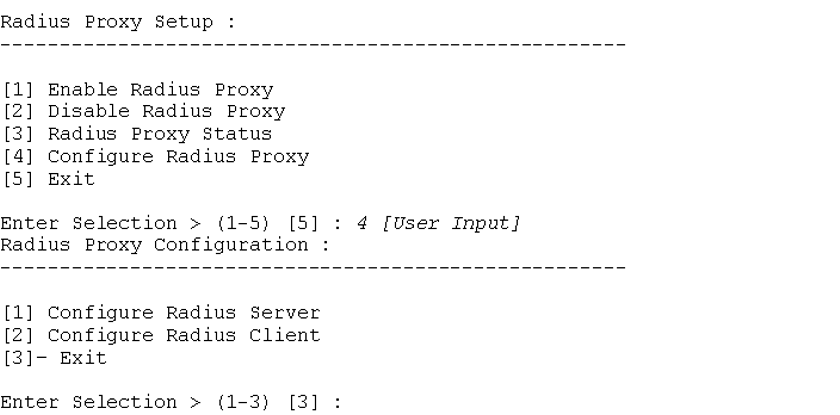
The following figure shows selection of the Enable RADIUS Proxy option. This option enables a RADIUS proxy on the AS blade or platform. It updates the radiusd.conf file of FreeRADIUS with proper parameters or configurations. If the radiusd.conf file is not present, the CLI tool will display an error message. If the proxy is already enabled, it displays the message, *Proxy is already Enabled*.

**Enable RADIUS Proxy**

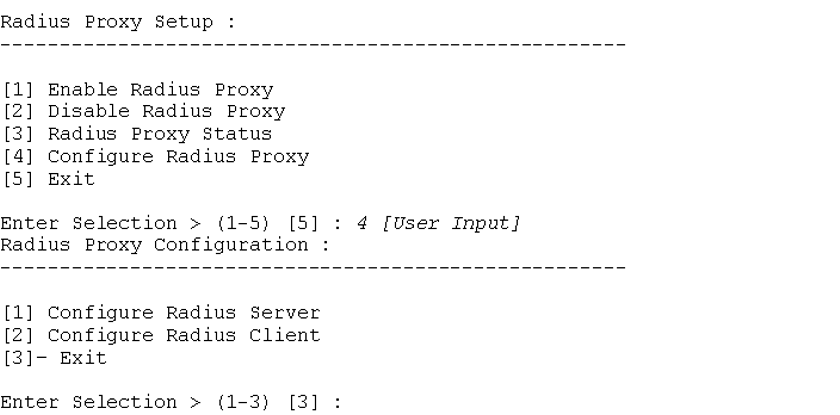
The following figure shows selection of the Disable RADIUS Proxy option. This option provides the ability to disable the RADIUS proxy on a particular AS platform. It restores the proxy parameters to the default configurations in the radiusd.conf file.

**Disable RADIUS Proxy**

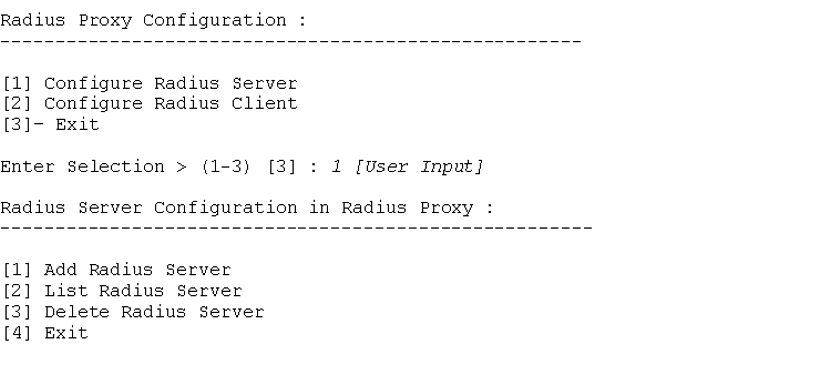
The following figure shows selection of the RADIUS Proxy Status option. This option displays the status of RADIUS proxy on a particular AS platform, based on the configuration data found in the radiusd.conf file.

**RADIUS Proxy Status**

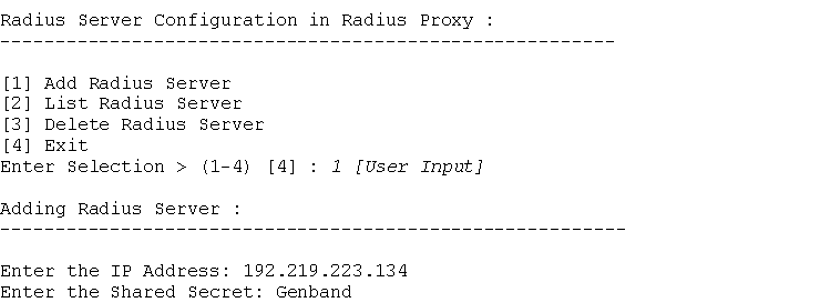
The following figure shows selection of the Configure RADIUS Proxy option. This option provides an interactive facility used to configure the RADIUS servers and clients in the RADIUS proxy. Multiple RADIUS servers and clients can be configured in the RADIUS proxy.

**Configure RADIUS Proxy**

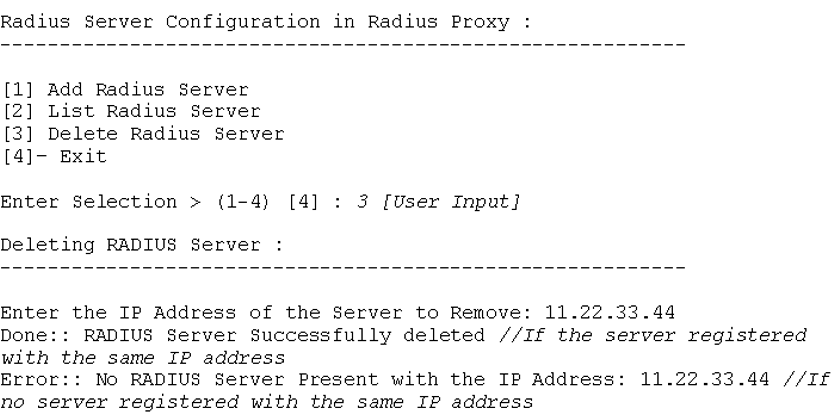
The following figure shows selection of the Configure RADIUS Server option. The RADIUS proxy is an intermediate server between a third-party RADIUS server and a RADIUS client. In the RADIUS proxy, multiple RADIUS servers or home servers can be configured to which access- request messages from external registered clients can be forwarded.

**Configure RADIUS Server**

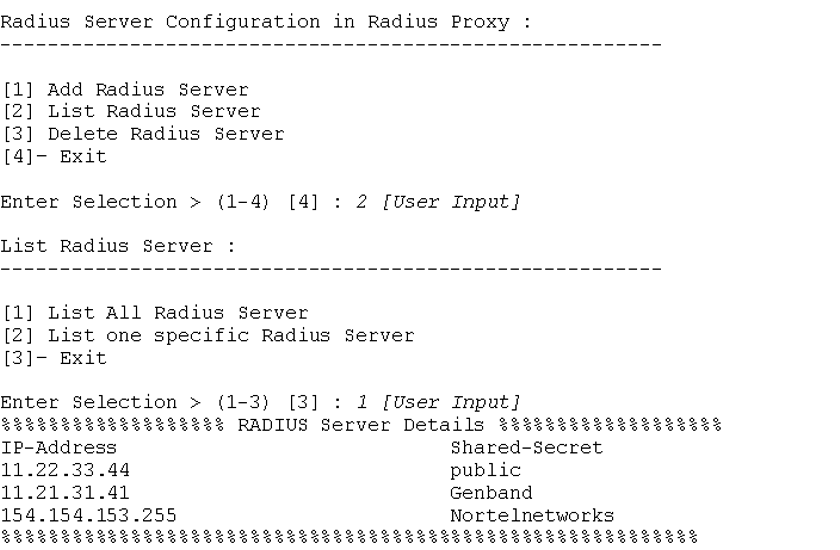
The following figure shows selection of the Add RADIUS Server option. This option enables adding or registering RADIUS server details to a proxy server. These details are stored in one file used for back up of all registered RADIUS servers. New data entries are added to the backup file and server configurations are added to the *proxy.conf* file.

**Add RADIUS Server**

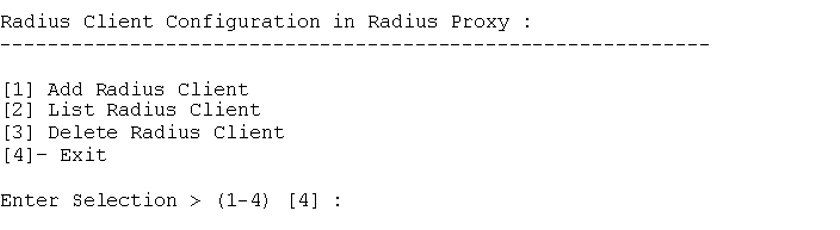
The following figure shows selection of the Delete RADIUS Server option. This option removes or unregisters the RADIUS servers from the proxy server. Entries for the deleted RADIUS server are removed from the *proxy.conf* file and also from backup RADIUS server list file.

**Delete RADIUS server**

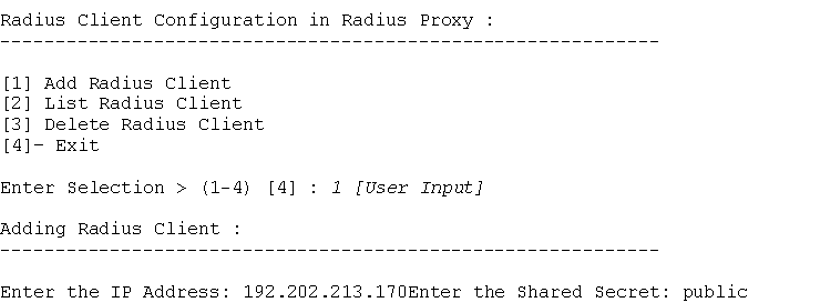
The following figure shows selection of the List RADIUS Server option. This option displays the details for registered RADIUS servers.

**List RADIUS Server**

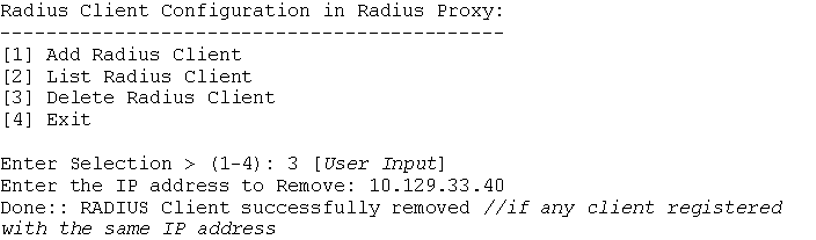
The following figure shows selection of the Configure RADIUS Client option. This option enables adding, listing, or deleting RADIUS client details in a proxy server. The proxy server forwards a request only for clients who have been registered to the proxy server.

**Configure RADIUS Client**

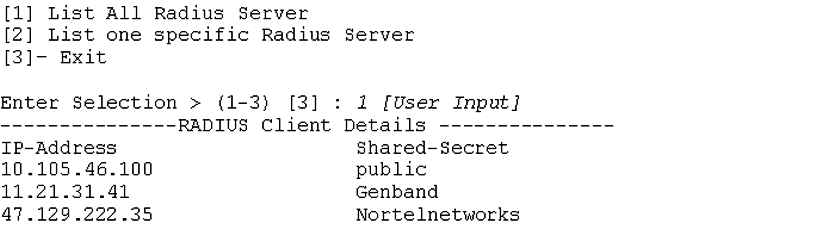
The following figure shows selection of the Add RADIUS Client option. This option adds or registers RADIUS client details to the clients.conf file in the proxy server. A client list file stores, for backup, all registered RADIUS clients and their details. New entries are added to the list file and client configurations are added to the **clients.conf** file.

**Add RADIUS Client**

The following figure shows selection of the Delete RADIUS Client option. This option removes or unregisters RADIUS clients from a proxy server. Entries are deleted from the *client.conf* file and from the backup list file.

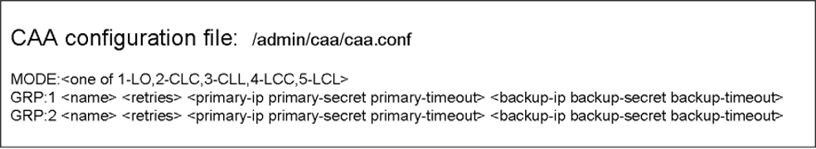
**Delete RADIUS Client**

The following figure shows selection of the List RADIUS Client option. This option displays the details for RADIUS clients registered in a proxy server.

**List RADIUS Client**

###### Configuration Files

The following figure shows a sample platform CAA Management CLI configuration file. This configuration file contains the CAA mode and RADIUS Server Group information. The file should not be updated manually since the data in the file is used by the CLI to configure other PAM RADIUS configuration files (for sshd, login, su, sudo and jpam) and RADIUS server files.

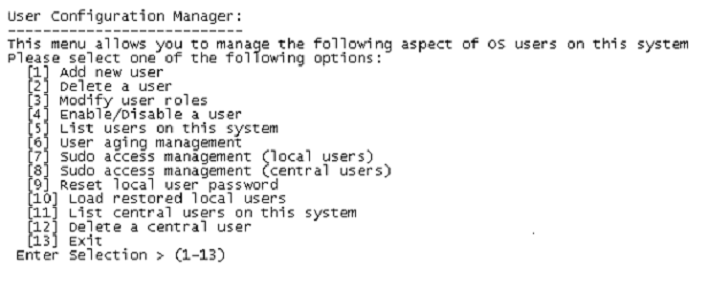
**caa conf (Platform CAA Management CLI configuration file)**

###### User Management CLI (userMgt.pl) modification

Temporary accounts are created for platform users who are centrally- authorized. These accounts are not deleted automatically since it is not possible to always detect when a user logs out. Therefore, these temporary accounts can remain in the system indefinitely unless manually removed.

In order to remove these stale accounts, the userMgt tool is modified to provide an option that deletes any temporary accounts that have been created. The following figure shows this Delete temporary central users option in the User Management CLI menu.

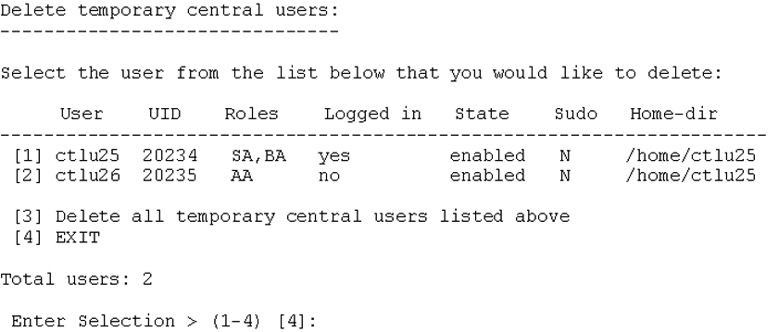
**User Management CLI menu – Delete temporary central users option**



The following figure shows an example of *Delete temporary central users*

option selection.

**User Management CLI menu – Delete temporary central users option selection**



###### Configuring a Platform RADIUS Server Group

Perform the following steps to define and provision a Platform RADIUS Server Group.

**Attention**

To perform these steps, the administrator must be assigned the SSA role (that is, belong to the ntsysgrp group). The administrator must also have the IP address for the RADIUS server and the RADIUS secret.

1. At the AS platform, execute the caaMgt.pl CLI.
2. From the CAA Configuration Management menu, select [2] RADIUS Servers.
3. From the RADIUS Servers menu, select [1] Add RADIUS Server Group.
4. In the Add RADIUS Server Group dialog, enter the server group name, retries value, and primary and backup server details. In response to the final question in the dialog, “Would you like to add another RADIUS Server Group?”, enter Y if another RADIUS server group is being defined at this time or N if another RADIUS server group is not being defined at this time.

###### Enabling Central Authentication for platform users

Perform the following steps to enable central authentication.

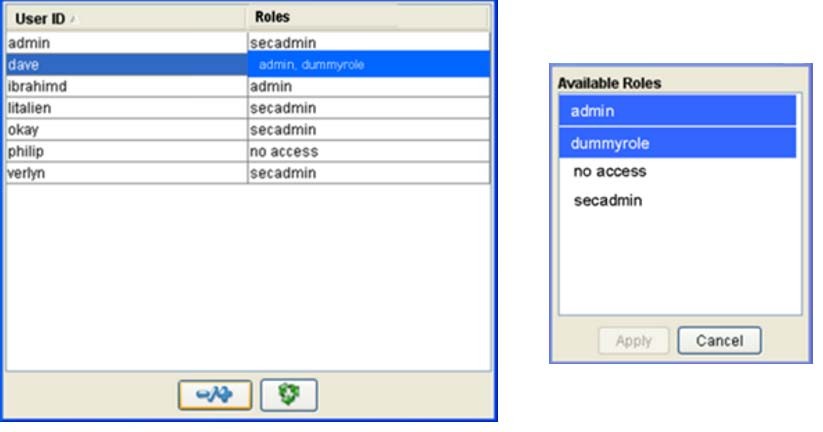
**Attention**

To perform these steps, the administrator must be have previously added a platform RADIUS Server Group to the system.

1. At the AS platform, execute the caaMgt.pl CLI.
2. From the CAA Configuration Management menu, select [1] CAA Mode.
3. In the CAA Mode menu, select the desired central mode.

### Assigning multiple roles per user

With the introduction of this feature, a user can be assigned more than one role. In previous releases, only single role assignment was possible. Using the SM GUI interface, multiple items can be selected from the list of roles by using the *Ctrl* key when clicking on listed items, as shown in the figure below.

**Assigning multiple roles to a user**

For the procedure to use to assign roles to a System Manager GUI user, see [“Assigning a role to a System Management Console user” (page 192)](#_bookmark228).

### Migrating users to a central RADIUS server

When the service provider decides to enable Central Authentication and Authorization, users that are to be centrally-managed must be migrated to the central RADIUS server. Migration of platform, SM, and PROV accounts is performed using the procedures shown in the following tables.

**Platform Account Migration**

|  |  |
| --- | --- |
| **Purpose:** | Platform Account Migration |
| **Prerequisites:** | RADIUS Server should be configured. Central Authentication should be enabled on the platform. |
| **Supporting info:** | Refer to [“Configuration of Central Authentication and](#_bookmark178) [Authorization” (page 131)](#_bookmark178). |
| **Procedure steps:** | 1. Login to the device where the user is defined 2. Record the user’s role(s). 3. Create the user with the appropriate role(s) on the central RADIUS server. 4. Delete the account on the device . |

**SM Account Migration**

|  |  |
| --- | --- |
| **Purpose:** | To migrate SM accounts currently defined locally to the central RADIUS server. |
| **Prerequisites:** | RADIUS Server should be configured. Central Authentication should be enabled on the platform (including JPAM) and SM application. |
| **Supporting info:** | Refer to [“Configuration of Central Authentication and](#_bookmark178) [Authorization” (page 131)](#_bookmark178) Any SM role that is not predefined must be created on the central server. |
| **Procedure steps:** | 1. Login to the SM as an administrator with the   *ConfigRoleAssignmentService* Read right.   1. Record the user’s role(s). 2. Create the user with the appropriate role(s) on the central RADIUS server. 3. Delete the account on the SM. |

**PROV Account Migration**

|  |  |
| --- | --- |
| **Purpose:** | To migrate PROV accounts currently defined locally to the central RADIUS server. |
| **Prerequisites:** | RADIUS server should be configured. Central Authentication should be enabled on the platform. |
| **Supporting info:** | Refer to [“Configuration of Central Authentication and](#_bookmark178) [Authorization” (page 131)](#_bookmark178) Any PROV role that is not predefined must be created on the Central server. |
| **Procedure steps:** | 1. Log in to the PROV client as an administrator with the Admin Read right. 2. Record the user’s role(s) and domain(s). 3. Create the user with the appropriate role(s) and domain(s) on the central RADIUS server. 4. Delete the account on the PROV. |

# Certificate management overview

The system supports the use of public-key cryptography technology with X. 509 certificates in its SIP/TLS, IPSec/IKE and HTTPS security applications. The certmgr certificate management tool may be used to manage X.509 certificates for these security applications.

An administrator with sudo privileges can start the certmgr tool by typing the name of the tool at the prompt.

The certmgr tool includes the utilities that support the generation of private keys, the generation of Certificate Signing Requests (CSR) , and the generation of PKCS#12 files. These functions may be used in obtaining CA signed certificates for the IPSec/IKE, SIP/TLS and HTTPS security applications. This generally should be done as part of initial system installation and commissioning or soon after (when enabling security applications) in order to replace the default certificates.

**Attention**

Default certificates for IPSec/IKE (if used in place of pre-shared keys), SIP/TLS (if enabled) and HTTPS need to be replaced by CA (or local CA) signed certificates. The Default certificates are staging certificates which are shipped with the system and use a common public and private key pair. These key pairs need to be changed so they are unique for each system installation.

The certmgr tool also includes other utilities that support the certificate management in IPSec.

The certmgr tool does not provide the support to obtain the CA certificate, send the CSR to the CA, obtain the signed certificate from the CA, and obtain the CRL from the CA. How to obtain these files and transfer them to the servers is the administrator’s choice. For example, the administrator can use the secure FTP (SFTP) for this purpose.

In the AS system, two RSA key sizes 1024 and 2048 are supported when generating a private key, and the message digest algorithm SHA1 is used when generating a CSR.

# CA certificate management for IPsec

Use these procedures to manage CA certificates for IPsec.

For more information about installing and managing CA-signed certificates, see [“CA-signed certificate management” (page 171)](#_bookmark204) .

## Navigation

* [“Installing a CA certificate” (page 151)](#_bookmark185)
* [“Listing installed CA certificates” (page 152)](#_bookmark186)
* [“Uninstalling a CA certificate” (page 153)](#_bookmark187)
* [“Renewing a CA certificate” (page 153)](#_bookmark188)

## Installing a CA certificate

Use this procedure to install a CA certificate.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **6** to select **Manage CA Certificate**.

The CA Certificate Management Options menu displays.

1. From the CA Certificate Management Options menu, enter **3** to select **Install a new CA certificate**.
2. Enter the source CA certificate filename and the destination CA certificate filename.
3. Confirm the data entered.

**--End--**

### Installing a CA certificate job aid

|  |  |
| --- | --- |
| **Item** | **Description** |
| Source CA certificate file name | Enter the full path of the source file location. You do not have to enter the full path if the source file is in the current working directory. |
| Destination CA certificate file name | Enter a unique file name only. Full path information is not required because the certmgr tool installs the CA certificate to a predetermined directory. |

**Listing installed CA certificates**

Use this procedure to list all installed CA certificates.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **6** to select **Manage CA Certificate**.

The CA Certificate Management Options menu displays.

1. From the CA Certificate Management Options menu, enter **1** to select **List all CA certificates**.

The list of installed certificates displays.

**--End--**

### Listing installed CA certificates job aid

The following example shows the result of the List all CA certificates option.

All CA certificates: [1]: slfcacrt.pem

[2]: cacert.pem

Renewing a CA certificate **153**

## Uninstalling a CA certificate

Use this procedure to uninstall a CA certificate.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **6** to select **Manage CA Certificate**.

The CA Certificate Management Options menu displays.

1. From the CA Certificate Management Options menu, enter **2** to select **Uninstall a CA certificate**.

The following message displays:

*WARNING: If a CA certificate is uninstalled, all installed server certificates issued by that CA become unusable for IPsec.*

1. Enter **Y** to proceed.
2. Enter the ID of the CA certificate to delete.
3. Enter **Y** to confirm.

A message displays confirming the deletion of the CA certificate.

**--End--**

## Renewing a CA certificate

Renew a CA certificate in the IPsec to maintain communications secured by IPsec.

**Attention**

The renewal must be complete before the currently installed CA certificate expires. Otherwise, the system cannot establish new IPsec connections and existing IPsec connections drop when the system renews the connections.

### Prerequisites

* + You are familiar with the procedure to uninstall a CA certificate. For more information, see [“Uninstalling a CA certificate” (page 153)](#_bookmark187).
  + You are familiar with the procedure to install a CA certificate. For more information, see [“Installing a CA certificate” (page 151)](#_bookmark185).

### Procedure steps

###### Step Action

1. Use your preferred method to obtain a new CA certificate.
2. Uninstall the current CA certificate.
3. Install the new CA certificate.

**--End--**

You need not restart the IPsec service after you renew the CA certificate. The new CA certificate becomes effective after the IPsec Phase 1 connection renews.

###### 155

**CA-signed certificate management for IPsec**

Use these procedures to manage CA-signed server certificates for IPsec.

**Attention**

Some of the following procedures also apply to certificates for SIP/TLS and HTTPS (HTTP over SSL or TLS). Unless otherwise specified, the term "SSL/TLS" will be used in conjunction with certificates used for either SIP/TLS or HTTPS.

## Navigation

* [“Generating the private key” (page 155)](#_bookmark190)
* [“Generating a CSR” (page 156)](#_bookmark191)
* [“Generating a PKCS12 file” (page 158)](#_bookmark192)
* [“Validating a CA-signed certificate” (page 160)](#_bookmark193)
* [“Installing a CA-signed certificate and private key pair” (page 160)](#_bookmark194)
* [“Listing installed CA-signed certificates and private key pairs”](#_bookmark195) [(page 161)](#_bookmark195)
* [“Uninstalling CA-signed certificates and private key pairs” (page 162)](#_bookmark196)
* [“Renewing a CA-signed certificate” (page 163)](#_bookmark197)

## Generating the private key

Use this procedure to generate the private key for a server.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. Enter **certmgr** at the prompt.
3. If you receive a prompt, enter your password.
4. Enter **1** to select **Generate Private Key**.
5. Enter the RSA modulus size.
6. Enter the private key file name.
7. Specify the Private key file encryption password.

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Encrypt the private key file | Enter a password (4 or more alphanumeric characters) |
| Not encrypt the private key file | Press Enter |

1. If you entered a password, enter the password again.
2. At the Confirm (Y or N) [Y] prompt, enter **Y**.

**--End--**

### Generating the private key job aid

This job aid lists and describes the parameters required to generate a private key for a server.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| RSA modulus size (1024 or 2048) | The RSA modulus size can be 1024 or 2048. |
| Output private key file name (full path) | For the output private key file, enter a full path file name, unless the file is to be saved in the current working directory. |
| Private key file encryption password (4 or more alphanumeric chars) (optional) | For IPsec, you must not encrypt the private key file; do not enter a password.  For SSL/TLS, you can encrypt the private key file; enter a password (optional). |

## Generating a CSR

Use this procedure to generate a certificate signing request (CSR).

### Prerequisites

* + You must be assigned the SSA role.
  + Generate the private key. For more information, see [“Generating the](#_bookmark190) [private key” (page 155)](#_bookmark190).

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **2** to select **Generate Certificate Signing Request**.
5. Enter the private key file name.
6. Enter the Output CSR file name.
7. (Optional) Enter the Country name.
8. Enter the private key file encryption password (if the private key file is encrypted)
9. (Optional) Enter the State or province name.
10. (Optional) Enter the Locality name
11. (Optional) Enter the Organizational name
12. (Optional) Enter the Organizational unit name.
13. Enter the Common name.
14. (Optional) Enter the Email address.
15. (Optional) Enter the IP address for SubjAltName.
16. (Optional) Enter a Challenge password.
17. To confirm, enter **Y**.

**--End--**

### Generating a CSR job aid

This job aid lists and describes the parameters required to generate a CSR.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Private key file name | For the private key file, enter a full path file name unless the file is in the current working directory. |
| Output CSR file name | For the output CSR file, enter a full path file name unless the file is to be saved in the current working directory. |
| Country name (optional) | This is the two-letter country code. |

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Private key file encryption password | This is the Private key file encryption password; it is only required if the private key file is encrypted. |
| State or province name (optional) | This is the name of the state or province in less than 40 characters. |
| Locality name (optional) | This is the name of the locality in less than 40 characters. |
| Organizational name (optional) | This is the name of the company or subidiary. |
| Organizational unit name (optional) | This is the name of the department or division. |
| Common name | This is the common name in less than 40 characters. |
| Email address (<= 60 chars) (optional) | This is the e-mail address |
| IP address for SubjAltName (IP in dot-notation) (optional) | This is the IP in the dot-notation. It is recommended that you not provide the IP address for SubjAltName when you generate a CSR for IPsec, because the IPsec/IKE mechanism for the AS system ignores it. However, SSL/TLS can require this data. |
| Challenge password (4 to 20 alphanumeric chars) (optional) | It is recommended that you provide a challenge password. Some CAs require a challenge password to submit a CSR for signing. |

## Generating a PKCS12 file

Use this procedure to generate a PKCS#12 file to use for SSL/TLS.

### Prerequisites

* + You must be assigned the SSA role.
  + For SSL/TLS the CA signed certificate must be transferred by SFTP to the AS system running the certmgr tool where the certificate signing request was generated.
  + You must be familiar with the procedure to generate the private key. For more information, see [“Generating the private key” (page 155)](#_bookmark190).

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **3** to select **Generate PKCS12 File**.
5. Enter the private key file name.
6. Enter the private key file encryption password (if the private key file is encrypted).
7. Enter the certificate file name.
8. Select an option for CA certificate inclusion.

Do not select the CA certificate chain option, which is not supported in the current release of AS.

|  |  |
| --- | --- |
| **Choose to** | **Do this** |
| Not include a CA certificate | Enter 0 |
| Include a single file | Enter 1 |

1. Enter the CA certificate file name (if included).
2. (Optional) Enter the friendly name of the certificate.
3. Enter the PKCS12 file name.

**Attention**

The extension of PKSC12 file must be "p12".

1. Enter the export password (if the private key file is not encrypted).
2. To confirm, enter **Y**.

**--End--**

### Generating a PKCS12 file Job Aid

The following information applies to PKCS12 file generation.

* + If the private key file is encrypted, the encryption password is also used for the export password, thus no prompt for the export password data is present. Otherwise, the prompt for entering an export password is present.
  + The generated PKCS#12 file is readable by an SSA user and is protected by the export password.
  + The friend name of the certificate is optional; however, it is required by some certificate management systems.
  + For SSL/TLS the PKCS12 file must transferred by SFTP to the SM console platform for it to be imported into the SM.

## Validating a CA-signed certificate

Use this procedure to ensure that the digital signature on a certification authority (CA)-signed certificate is valid (issued by a trusted CA).

### Prerequisites

* + You must be assigned the SSA role.
  + The CA certificate to use for validation is installed.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **4** to select **Validate Certificate**.

The certmgr tool prompts for confirmation that the CA certificate to be used for validation is installed.

1. Enter **Y** to continue.
2. Enter the full path and name of the CA-signed certificate that you want to validate.
3. Enter **Y** to continue.

**--End--**

## Installing a CA-signed certificate and private key pair

Use this procedure to install a CA-signed certificate and private key pair.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **5** to select **Manage Server Certificate and Private Key**.

The Server Certificate and Key Management Options menu appears.

1. Enter **3** to select **Install a new server certificate and private key pair**.
2. Enter the full path and file name of the source CA-signed certificate.
3. Enter the full path and file name of the source private key pair.
4. Enter the file name of the destination CA-signed certificate.
5. Enter the file name of the destination private key pair.
6. Review the summary and enter **Y** to continue.

**--End--**

### Installing a CA-signed certificate and private key pair job aid

This job aid lists and describes the information you must enter to install a CA-signed certificate and private key pair.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Source CA-signed certificate file name (full path) | Enter the full path and file name, unless the file is in the current working directory. |
| Destination CA-signed certificate file name | Enter the file name only; the certmgr tool only installs the CA-signed certificate into a predetermined destination directory. |
| Source private key file name | Enter the full path and file name, unless the file is in the current working directory. |
| Destination private key file name | Enter the file name only; the certmgr tool only installs the private key into a predetermined destination directory. |

## Listing installed CA-signed certificates and private key pairs

Use this procedure to list the all installed server CA-signed certificates and private key pairs. You can use this procedure to locate the ID for a CA- signed certificate and private key pair that you want to delete.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **5** to select **Manage Server Certificate and Private Key**.

The Server Certificate and Key Management Options menu appears.

1. Enter **1** to select **List all server certificates and private key pairs**.

Each CA-signed certificate and private key pair is listed by ID number.

**--End--**

## Uninstalling CA-signed certificates and private key pairs

Use this procedure to uninstall a CA-signed certificate and private key pair.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **5** to select **Manage Server Certificate and Private Key**.

The Server Certificate and Key Management Options menu appears.

1. Enter **2** to select **Uninstall a server certificate and private key pair**.
2. Enter the ID of the CA-signed certificate and private key pair that you want to uninstall.
3. Enter **Y** to confirm the uninstall.

**--End--**

## Renewing a CA-signed certificate

Renew a CA-signed certificate in the IPsec to maintain communications secured by IPsec.

**Attention**

The renewal must be complete before the currently installed CA-signed certificate expires. Otherwise, the system cannot establish new IPsec connections and existing IPsec connections drop when the system renews the connections.

### Prerequisites

* + You are familiar with the procedure to generate a CSR. For more information, see [“Generating a CSR” (page 156)](#_bookmark191).
  + You are familiar with the procedure to uninstall the current CA-signed certificate and private key pair. For more information, see [“Uninstalling](#_bookmark196) [CA-signed certificates and private key pairs” (page 162)](#_bookmark196).
  + You are familiar with the procedure to install the new CA-signed certificate and private key pair. For more information, see [“Installing a](#_bookmark194) [CA-signed certificate and private key pair” (page 160)](#_bookmark194).

### Procedure steps

###### Step Action

1. Generate a CSR.
2. Use your preferred method to obtain the new CA-signed certificate from the CA.
3. Uninstall the current CA-signed certificate and private key pair.
4. Install the new CA-signed certificate and private key pair.

**--End--**

### Renewing a CA-signed certificate job aid

The following information applies to CA-signed certificate renewals.

• You need not restart the IPsec service after you renew the CA-signed server certificate. The new CA-signed server certificate becomes effective after the IPsec Phase 1 connection renews.

• You can choose to create a new private key or continue to use the existing private key when you create the new CSR.

• The file names of the new CA-signed server certificate and the new private key must be the same as the ones to be replaced. Otherwise, you must modify the certificate and private key file names specified in the IKE phase 1 rule, after which you must restart the IPsec service.

###### 165

**Certificate Revocation List management for IPsec**

Use these procedures to manage Certificate Revocation Lists (CRL).

## Certificate Revocation List management for IPsec navigation

* + [“Listing installed CRLs” (page 165)](#_bookmark199)
  + [“Installing a CRL” (page 166)](#_bookmark200)
  + [“Uninstalling a CRL” (page 166)](#_bookmark201)
  + [“Renewing the CRL” (page 167)](#_bookmark202)

## Listing installed CRLs

Use this procedure to list installed CRLs. You can use this procedure to locate the ID for a CRL that you want to delete.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **7** to select **Manage CRL**.

The CRL Management Options menu displays.

1. Enter **1** to select **List all CRLs**.

The list of CRLs appears, organized by ID.

**--End--**

## Installing a CRL

Use this procedure to install a CRL.

### Prerequisites

You must be assigned the SSA role.

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **7** to select **Manage CRL**.

The CRL Management Options menu displays.

1. Enter **3** to select Install a new CRL.
2. Enter the full path and file name of the source CRL file.
3. Enter the file name of the destination CRL file.
4. Review the summary and enter **Y** to continue.

**--End--**

### Installing a CRL job aid

This job aid lists and describes the information you must enter to install a CRL.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Source CRL file name (full path) | Enter the full path and file name, unless the file is in the current working directory. |
| Destination CRL file name | Enter the file name; the certmgr tool only installs the CRL into a predetermined destination directory. |

## Uninstalling a CRL

Use this procedure to uninstall a CRL.

### Prerequisites

You must be assigned the SSA role.

Renewing the CRL **167**

### Procedure steps

###### Step Action

1. Log on to the server as an SSA.
2. At the prompt, enter **/opt/mcp/cm/certmgr.pl**.
3. If you receive a prompt, enter your password.
4. Enter **7** to select **Manage CRL**.

The CRL Management Options menu displays.

1. Enter **2** to select **Uninstall a CRL**.
2. Enter the ID of the CRL that you want to uninstall.
3. Enter **Y** to confirm.

**--End--**

## Renewing the CRL

Renew a CRL in the IPsec before the current CRL passes the next-update date or when the CA issues a new CRL.

**Attention**

You must complete the renewal before the CRL next-update date passes. Otherwise, the system cannot establish new IPsec connections and existing IPsec connections drop when the system renews the connections.

### Prerequisites

* + You are familiar with the procedure to uninstall a CRL. For more information, see [“Uninstalling a CRL” (page 166)](#_bookmark201).
  + You are familiar with the procedure to install a CRL. For more information, see [“Installing a CRL” (page 166)](#_bookmark200).

### Procedure steps

###### Step Action

1. Use your preferred method to obtain the CRL from the CA.
2. Uninstall the current CRL.
3. Install the new CRL.

**--End--**

The following information applies to CRL renewals.

* + You do not need to restart the IPsec service after renewing the CRL. The CRL becomes effective after the IPsec Phase 1 connection renews.
  + You can configure an IPsec without installing a CRL. For example, you do not need to install the CRL when configuring the IPsec using the default server certificate provided. However, when configuring the IPsec using the customer server certificate, obtain and install the CRL issued by the CA that signed the customer server certificate. After installing the CRL in the IPsec , you must keep it up to date.

# SSL/TLS certificate management

For out of the box installations, a self-signed certificate is preconfigured for all Session Initiation Protocol (SIP) transport layer security (TLS) and Hypertext Transfer Protocol Secure (HTTPS) ports of the system. It is recommended that you replace the self-signed certificate with a certificate signed by a certification authority (CA) for each component in the network. The CA can be public or part of an internal public key infrastructure (PKI).

**Attention**

The out of box Default certificate is not secure. The same private key is shared across all AS installations and cannot be considered "private". A new CA signed certificate must be installed when the SIP/TLS and HTTPS are enabled.

**SSL/TLS certificate management procedures**

The following task flow shows the sequence of procedures that you perform to manage (generate and install) a certificate for SSL/TLS.

**SSL/TLS certificate management**

|  |
| --- |
|  |

# CA-signed certificate management

Use these procedures to manage CA-signed server certificates.

**Attention**

The following procedures apply to SIP/TLS and HTTPS.

**Navigation**

* [“Generating the private key” (page 155)](#_bookmark190)
* [“Generating a CSR” (page 156)](#_bookmark191)
* [“Generating a PKCS12 file” (page 158)](#_bookmark192)

**SSL/TLS certificate management with the System Management Console**

This section provides the procedures that you require to use the System Management Console to manage Transport Layer Security (TLS)/Secure Socket Layer (SSL) certificates and certificate revocation lists (CRL).

## Importing an internal certificate to the keystore

Use this procedure to import an internal certificate. The only supported format is PKCS #12. The system expects the PKCS #12 file to contain only one end entity certificate and the corresponding private key. Only the node that is assigned this certificate can retrieve the private key. When you import a PKCS#12 file that also includes a certificate chain, you automatically import the rest of the chain into the truststore, if an entry does not already exist for each CA in the chain.

Keystore (internal) certificates are the certificates for the network elements (NE) that are part of the system. This does not include external nodes, such as gateways.

### Prerequisites

* + You can access the System Management Console.
  + The PKCS#12 file exists in a location accessible to the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Keystore**.
2. Click **Add (+)**.
3. Configure the **Logical Name**, **PKCS#12 file**, **Password**, and **Export Password** parameters.
4. Click **Apply**.

**--End--**

### Importing an internal certificate to the keystore job aid

This job aid lists and describes the parameters for importing an internal certificate to the keystore.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Logical Name | The logical name to identify the certificate. |
| PKCS#12 File | Browse to the location of the PKCS#12 file. |
| Password | The password. |
| Export Password | The export password. |

## Viewing an internal certificate in the keystore

Use this procedure to view the details for internal certificates in the keystore.

### Prerequisites

You can access the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Keystore**.
2. From the **Keystore** panel, select a certificate.
3. Click **Edit (-/+)**.

**--End--**

## Removing an internal certificate from the keystore

Use this procedure to remove an internal certificate from the keystore.

### Prerequisites

* + You can access the System Management Console.
  + The certificate must not be associated with a SSL/TLS port.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Keystore**.
2. From the **Keystore** panel, select a certificate.
3. Click **Delete (-)**.
4. Click **Yes** to confirm the delete.

A successful delete removes the private key as well.

**--End--**

## Importing a CA certificate to the truststore

Use this procedure to import a certification authority (CA) root or intermediate certificate to the truststore.

Truststore (root CA and intermediate CA) certificates are the certificates the system uses to authenticate signed certificates. To authenticate a certificate stored in the keystore, the signing chain must exist in the truststore. The signing chain for other certificates, such as for gateways, must exist in the truststore. If the system uses a self-signed certificate, it must exist in the truststore.

### Prerequisites

* + You can access the System Management Console.
  + The CA root or intermediate certificate file already exists in a location accessible to the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Truststore**.
2. Click **Add (+)**.
3. Click **Browse**, and navigate to the file location.
4. Select the CA root or intermediate certificate file, and click **Open**.

**--End--**

## Viewing a CA certificate in the truststore

Use this procedure to view the details for CA root and intermediate certificates in the keystore.

### Prerequisites

You can access the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Keystore**.
2. From the **Truststore** panel, select a root or intermediate certificate.
3. Click **Edit (-/+)**.

**--End--**

## Removing a CA certificate from the truststore

Use this procedure to remove a CA root or intermediate certificate from the truststore.



**WARNING**

Use extreme caution when you perform this procedure. The removal of a trusted CA can disrupt service.

### Prerequisites

You can access the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Keystore**.
2. From the **Keystore** panel, select a certificate.
3. Click **Delete (-)**.
4. Click **Yes** to confirm the delete.

**--End--**

## Importing a CRL

Use this procedure to import a certificate revocation list (CRL).

If the private key for a certificate is compromised, the CA can revoke the certificate prior to the expiry time. The CA is responsible for posting revocation information. A CRL is a periodic publication of revoked certificates. The system treats CRLs as public and does not require a password or private key to import them.

**Attention**

AS supports only the Complete CRL format. CRL Distribution Points, Redirect CRLs, Delta CRLs, and the Online Certificate Status Protocol (OCSP) formats are not supported. The Complete CRL file size must be less than 4000 bytes. This file size limit accommodates approximately 100 revoked certificate entries.

### Prerequisites

* + You can access the System Management Console.
  + The certificate revocation list file already exists in a location accessible to the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Certificate Revocation List**.
2. Click **Add (+)**.
3. Click **Browse**, and navigate to the file location.
4. Select the CRL file, and click **Open**.

**--End--**

## Viewing a CRL

Use this procedure to view the details for a certificate revocation list (CRL).

### Prerequisites

* + You can access the System Management Console.
  + A CRL is installed.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Certificate Revocation List**.
2. From the **Certificate Revocation List** panel, select a CRL.
3. Click **Edit (-/+)**.

**--End--**

## Removing a CRL

Use this procedure to remove a CRL after you import a new CRL for the CA, or after you remove the CA from the truststore.

### Prerequisites

* + You can access the System Management Console.
  + A CRL is installed.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Certificate Management, Certificate Revocation List**.
2. From the **Certificate Revocation List** panel, select a certificate.
3. Click **Delete (-)**.
4. Click **Yes** to confirm the delete.

**--End--**

###### 179

# System security configuration and management

This chapter contains procedures for initial Application Server (AS) security configuration and management.

## Security configuration and management overview

This section contains information about security configuration and management.

### Administrative security services

When creating and managing System Manager administrative user roles, protect access to the services used to control System Manager security configuration. These services include:

###### AdminUserService

This service controls the adding, editing, and removal of administrative users (System Management Console administration menu item User Administration). It also controls force-out operations and password administration (administration menu items Set Administrator Password and Force Password Change).

###### BannerConfigService

This service controls configuration of the system log on banners (Banners application in the Network Data and Mtc folder of the System Management Console topology tree).

###### ConfigRoleAssignmentService

This service controls the assignment of roles to administrative users (System Management Console administration menu item Role Assignment).

###### ConfigRoleDefinitionService

This service manages the adding, editing, and removal of administrative roles (System Management Console administration menu item Role Definition).

###### DebugSecurityService

This service controls the management of debug roles and debug security settings (System Management Console administration menu items Debug Security Settings and Debug Role Assignment). Debugging control is only supported for GENBAND technicians, and debugging security access should be limited to the administrators who interface with GENBAND technicians.

###### Log onRulesService

This service controls the management of system log on rules for both the System and Provisioning Manager (System Management Console administration menu item Log on Rules).

###### PasswordRulesService

This service controls the management of system password rules for both the SM and Provisioning Manager (System Management Console administration menu item Password Rules).

###### LogProcessingRulesService

This service controls Log Processing configuration for FPs (the System Manager and any Fault Performance Managers in the system). Part of the configuration controlled by this service is the ability to configure where Security Logs are stored, as well as which remote destinations these Security Logs can be pushed using FTP. These points should be considered very carefully before granting write access to this service. It is highly recommended that only Security Administrators have write access to this service.

###### LogBrowserFeedService

This service controls the configuration of the Log Browser Feed functionality on the System Manager. As the Log Browser Feed is available to anyone that can log in to the System Manager, care should be take to ensure the Log Browser Feed is configured so that security logs are filtered out, if desired.

### Password policies and domains

A password policy is not enforceable on subscribers until it is associated with a domain. When a password policy is associated with a domain, all subscribers in that domain must conform to that password policy. When you create a password policy, you can either select the policy during the creation of a domain or update a domain and select the policy to use.

You can explicitly identify a password policy association when creating a new domain. You can change the password policy of a domain through the domain modification process. If you do not explicitly select a password policy when creating a new domain, the domain is given the Default password policy.

If a subscriber is moved from one domain to another domain, the subscriber's password is not verified against the new domain password policy at the time of the move. The password is validated for conformance during any subsequent attempt to access the Personal Agent (by the subscriber) or any subsequent data change attempted on the subscriber account by an administrator.

The password policy prevents subscribers from maintaining passwords that do not conform to the password policy associated with the domain in which they are assigned (they can actually have a noncompliant password for a while). They can keep their passwords as long as they do not log on to their Personal Agent account. If they log on to their Personal Agent with a nonconforming password, they are directed to the password change page and are not permitted to do anything on Personal Agent before changing their password.

A subscriber’s account is marked to have the initial password reset at the time of creation. There is no affect on whether or not an initial password reset is required when moving between domains.

The subscriber lockout parameters, Max Failed Attempts and LockoutDuration, are associated with a domain and not a subscriber. A subscriber’s authorization attempt is evaluated against the values associated with the current domain at the time that the authentication attempt occurs.

### Administrative user accounts

By default, the system defines the following administrative user account roles for the System Management Console and Provisioning Client.

**System Management Console administrative user account roles**

|  |  |
| --- | --- |
| **Role** | **Definition** |
| secadmin | Administrators assigned to this role are authorized for all System Management Console services. The admin user is assigned this role by default. Only a user with the secadmin role can assign the secadmin role to another user or make modifications to this account. You can |

**System Management Console administrative user account roles (cont'd)**

|  |  |
| --- | --- |
| **Role** | **Definition** |
|  | delete the admin user only if another user is assigned to the secadmin role. In addition, this role has the following properties and limitations:   * at least one secadmin account must be enabled (for example, you cannot delete the default admin user unless another user is assigned to the secadmin role) * only a user assigned to the secadmin role can add, modify or delete another account assigned to the secadmin role * only a user assigned to the secadmin role can reset the password of another user with secadmin role * users assigned to the secadmin role are immune to lockout * users assigned to the secadmin role can log on to the system even if the Maximum session limit is reached |
| admin | Administrators assigned this role are authorized for all System Management Console services. |
| no access | This is the default role. All new users are automatically assigned to this role. Users assigned to this role have no authorization privileges at the System Management Console except for those services not requiring authorization. |

**Provisioning client administrative user account roles**

|  |  |
| --- | --- |
| **Role** | **Definition** |
| SuperUser | This role has no initial users. This role cannot be modified or deleted by any administrator. Care should be taken when assigning this role to any administrator as this role will give full access to all the provisioning data. |
| secadmin | The admin user is assigned to this role by default and has full access to all provisioning data. In addition, this role has the following properties and limitations:   * at least one secadmin account must be enabled (for example, you cannot delete the default admin user unless another user is assigned to the secadmin role) * only a user assigned to the secadmin role can add, modify or delete another account assigned to the secadmin role |

**Provisioning client administrative user account roles**

|  |  |
| --- | --- |
| **Role** | **Definition** |
|  | * only a user assigned to the secadmin role can reset   the password of another user with secadmin role   * users assigned to the secadmin role are immune to lockout * users assigned to the secadmin role can log on to the system even if the Maximum session limit is reached |

### Domain security

UNIStim encryption (USEC) must be enabled for a domain, to support UNIStim signaling between the AS and connected 1100-Series IP Phones.

The current AS defaults the UNIStim Encryption Enabled setting to True in the IPCM Parameters for a domain. This automatically enables encryption on each 1100-Series IP Phone assigned to the domain. When encryption is enabled on both the domain and the assigned 1100-Series IP Phones, UNIStim encrypted signaling occurs between the server and the 1100- Series IP Phones.

Additional settings for IPCM, media, and security must be provisioned for a domain that control both the type of media and type of signaling permitted in the domain.

**Attention**

While it is possible to provision a domain and the assigned 1100-Series IP Phones such that signaling between them is not encrypted, this is not a supported configuration in this release.

### Foreign domains

Foreign domains are associated with an External SIP proxy that is defined on the System Management Console. External SIP Proxy refers to all external SIP proxies that are not part of the SM managed network.

When configuring foreign domains, you must know the IP address of the foreign route destination as DNS resolution of foreign domains is not supported in this release. You must configure foreign domains using the SIP Proxy IP address option.

Foreign domains must be provisioned on both the local and the foreign destination system. For example, the local system has an external node that is provisioned with the proxy service address of the foreign destination system and the foreign destination has an external node provisioned with the proxy service address of the local system.

Use the Provisioning Client to administer foreign domains.

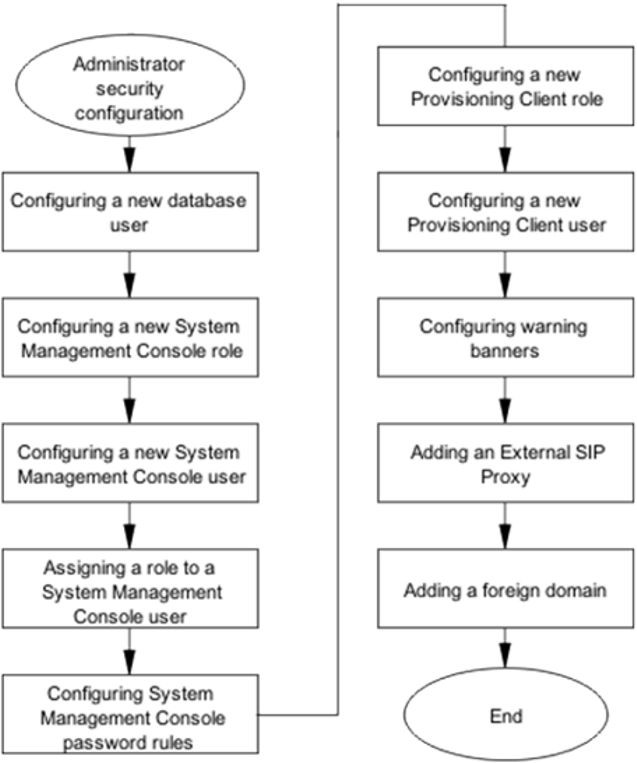
## Administrator security configuration

To enhance system security, configure log on security and create individual accounts for administrative users of the database, System Management Console, and Provisioning Client.

### Administrator security configuration procedures

This task flow shows the sequence of procedures you perform to configure log on security for administrators.

**Administrator security configuration**



### Configuring database user accounts

To provide accountability when individual users log on to the database, It is recommended that you create an individual account for each user.

### Prerequisites

You must belong to the SSA (for example, nysysadm) role.

### Procedure steps

###### Step Action

1. Log on to the primary System Manager (SM) as the SSA role.
2. Choose an action:

|  |  |
| --- | --- |
| **To do this** | **Type this** |
| Add a new user account | **sudo /opt/mcp/db/sbin/ addDbUserAcct.pl** |
| Delete a user account | **sudo /opt/mcp/db/sbin/ deleteDbUserAcct.pl** |

**--End--**

### Resetting database user accounts

Use this procedure to reset individual database user accounts.

### Prerequisites

You must belong to the SSA (for example, nysysadm) role.

### Procedure steps

###### Step Action

1. Log on to the primary database server as the SSA role.
2. Type the command:

###### sudo /opt/mcp/db/sbin/resetDbUserPasswd.pl –u

**<username>**

1. If the password prompt appears, enter the password for the user you are logged on as.
2. Enter a new password for the given user that complies to database password rules.
3. Enter the new password again to confirm.

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Definition** |
| <username> | The name of the user account to be reset. |

### Configuring a new System Management Console role

Configure new roles for the System Management Console and assign the roles to users to specify admin privileges and level of access.

### Prerequisites

You must have ConfigRoleDefinitionService READ and WRITE privileges.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Role Definition**.
2. On the **Role Definition** panel, click **Add (+)**.
3. In the **Add Role** dialog box, in the **Role Name** field, type a name to identify the new role.
4. Select the required **READ**, **WRITE**, and **MAINT** to configure privileges for each service.
5. Click **Apply**.

**--End--**

### Configuring System Management Console roles job aid

The effects of the READ, WRITE, and MAINT privileges differ according to the service that is selected; however, the following points generally apply:

* + The READ privilege typically allows you to view, but not modify configuration data.
  + The WRITE privilege enables READ automatically and allows you to add and modify configuration data.
  + The MAINT privilege allows you to start and stop services, but does not allow you to change configuration data. Typically you must also have the READ privilege in addition to MAINT.

The following job aid lists and describes the services for which you can add READ, WRITE, and MAINT privileges to roles.

|  |  |
| --- | --- |
| **Service** | **Description** |
| AcctProcessingRuleService | Account processing rule configuration |
| AdminUserService | Administrative users configuration |
| AgcfMsanService | A collection of AGCF and MSAN configurations |
| AlarmMgmtService | Alarms configuration |

|  |  |
| --- | --- |
| **Service** | **Description** |
| AlarmMtcService | Acknowledgement/clearing of alarms |
| AlarmQueryService | Alarm viewing |
| AMOssProfileService | OSS Profile data configuration—distributed to the Accounting Manager (AM) |
| ApplicationInstances | Application instances configuration |
| Applications | application configuring |
| ArtsElementService | A collection of MFSS and LSC configurations |
| AsacBudgetService | Audio Budget Profiles configuration |
| AsacCallCountProfileService | Audio Profiles configuration |
| AudioCodesNumMapIP2TelSer vice | IPToTelephonyMap configuration |
| AudioCodesServerService | AudioCodes gateway configuration |
| AudioCodesServerStateService | AudioCodes gateway state configuration |
| AudioCodesTrunkService | AudioCodes trunk configuration |
| AuthenticationService | SessMgr trusted node authorized method configuration |
| BannerConfigService | Log on banner configuration |
| CallAgentService | C20 Call Agent configuration |
| CertificateService | Certificate configuration |
| ChassisMonitorService | Blade Center Chassis monitoring |
| ChassisService | Blade Center Chassis configuration |
| CipherSuiteService | OAMP SSL/TLS cipher suite configuration |
| ConfigParmService | Configuration parameters |
| ConfigRoleAssignmentService | Administrative user role assignment |
| ConfigRoleDefinitionService | Administrative role configuration |
| CopsPolicyServerLinkService | CopsPolicyServer configuration |
| CopsPolicyServerService | CopsPolicyServer configuration |
| CscfService | CSCF configuration |
| DBInstanceService | Database instance configuration |
| DBMonitorConfigService | Database monitor threshold configuration |
| DBMonitorService | Database instance monitoring |
| DebugSecurityService | Role and security settings debugging |

|  |  |
| --- | --- |
| **Service** | **Description** |
| DeviceService | IPCM device maintenance |
| DfLinkService | Delivery Function Server configuration |
| DSCPConfigService | DSCP configuration |
| ECSService | ECS Routing Server configuration |
| ExternalAppMgrService | External Application Manager configuration |
| EndpointMtcService | Endpoint Maintenance configuration and monitoring |
| EngParmService | Engineering parameters configuration |
| ExportImportService | Bulk configuration export and import tools |
| ExternalAppMgrService | External Application Manager configuration |
| ExternalElementConfigService | External Element information |
| ExternalOAMPCipherSuiteServ ice | External OAMP CipherSuite configuration (distributed to SM, WSG, PROV/PA) |
| FPOssProfileService | OSS profile data configuration (distributed to FPM) |
| FlowSpecCodecService | FlowSpecService Video FlowSpec configuration (in Packet Cable Integration, Codec) |
| FlowSpecService | FlowSpec configuration |
| GatewayControllerLinkMtcServi ce | Gateway Controller Link Maintenance/ monitoring |
| GatewayControllerService | C20 Gateway Controller configuration |
| GatewayService | Gateway configuration |
| HSSService | HSS configuration |
| HSSSesmService | HSS SESM configuration |
| HttpsCipherSuiteService | HTTPS cipher suite configuration |
| IPAddressService | IP address configuration |
| InfoElementService | Informational Element configuration |
| LawfulInterceptConfigService | Lawful Intercept configuration |
| LogBrowserFeedService | Log browser feed configuration |
| LogProcessingRuleService | Log processing configuration |
| Log onRulesService | System log on rules configuration |
| LOMServerService | LOM and Terminal server configuration |
| LicenseKeyService | License key configuration |

|  |  |
| --- | --- |
| **Service** | **Description** |
| LocationServiceMgr | DNS server configuration for the Session Manager |
| LogicalDBService | Database configuration |
| LogStreamService | Log viewing |
| MASService | Media Application Server configuration |
| MPClusterConfigParmsService | Media Portal Cluster Configuration Parms |
| MPClusterFaultToleranceServi ce | Media Portal Cluster Fault Tolerance configuration |
| MPClusterGwcCallSvrService | Media Portal Cluster Gateway Controllers configuration |
| MPClusterMultiGwy | Multiple Network Gateway Routers configuration for Media Portal Cluster |
| MPClusterNet2RouteService | Choosing the Net2 Routable Networks configuration for a Media Portal |
| MPClusterService | Media Portal Cluster configuration |
| MPClusterSessionMgrService | Media Portal Cluster Session Managers configuration |
| MPClusterStaticRouteService | Media Portal Cluster Static Routes configuration |
| MPClusterSvcInstanceService | Media Portal Cluster Service Instance configuration |
| MPClusterVlan | Choosing the Vlan topology configuration for a Media Portal |
| NEInstanceService | Network element instance configuration and maintenance |
| NERecordStreamService | NE log, OM and accounting format path configuration |
| NEService | Network element configuration |
| NcasLinkMtcService | NCAS Link Maintenance configuration |
| Net2RouteService | Net2 Routable Networks configuration |
| NetworkAddrService | Network Addresses configuration |
| NetworkTypeService | Choosing Network type for Media Portal Static Routes – Control, Net1, Net2 or OAM |
| NodeService | Node configuration |
| OMProcessingRuleService | OM Processing Rule configuration |
| OMQueryService | OM viewing |

|  |  |
| --- | --- |
| **Service** | **Description** |
| OMViewerService | Service to handle historical OM query requests |
| OssProfileService | OSS Profile data configuration (distributed to all Element Managers) |
| PasswordRulesService | User password rules configuration |
| PhysicalServerService | Server configuration |
| PhysicalSiteService | Physical site configuration |
| PolicyServerConnectionService | Choose Policy Server Connection data Application Manager ID (AMID) for a Session Manager |
| PolicyServerService | Policy Servers configuration |
| RTPPortalBladeService | RTP Portal blade configuration |
| RegisteredGwcService | Registered gateway controller service configuration |
| SAConfigService | Federal configuration |
| ServerAnalysisService | MCS System Servers configuration |
| ServerLOMCommandService | Server maintenance for servers that are configured with a LOM server |
| ServerMonitorConfigService | Server monitor threshold configuration |
| ServerMonitorService | Server monitoring |
| SessionPolicyServerLinkServic e | Session Policy Server configuration |
| SessionPolicyServerService | Session Policy Server configuration |
| SignalingCipherSuiteService | Signaling cipher suite configuration |
| SipPbxService | SIP PBX configuration |
| SIPProfileService | SIP Profile configuration |
| SIPProxyService | SIP proxy configuration |
| SipRSService | SIP Redirect Server configuration |
| SIPTemplateService | SIP Template configuration |
| SMDIServerService | SMDI Server configuration |
| SnmpProfileService | SNMP profile configuration |
| StaticRouteService | Static Routes configuration |
| SubnetMaskService | Subnet Masks configuration |
| UpgradeManagerService | Upgrade Manager configuration |

|  |  |
| --- | --- |
| **Service** | **Description** |
| VMGAppearanceService | Virtual Media Gateway Appearance Configuration |
| VlanService | VLANs configuration |
| WebServicesService | Web services configuration |
| WMGService | Wireless Media Gateway configuration |

### Configuring a new System Management Console user

Use this procedure to configure a new administrative user for the System Management Console.

### Prerequisites

The administrator must know the Global Administrator account password.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, User Administration**.
2. On the **User Administration** panel, click **Add (+)**.
3. In the **Add User Account** dialog box, configure the **User ID**, **User Name**, **Password**, **Password Confirm**, **Account Disabled**, **Immune to Expiry**, and **Force Password Change** fields.

###### 4

**Attention**

The new user account has no access. You must assign roles to new users so that they can perform the administrative functions associated with their roles.

Click **Apply**.

The system validates the configuration data. If the change is valid, the Add User Account dialog box closes and the new account appears on the User Administration panel.

**--End--**

### Configuring a new System Management Console user job aid

The following job aid lists and describes the parameters that you configure on the Add User Account dialog box.

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| User ID | This parameter (text) contains the account identity—the new administrator uses this ID to log on. |
| User Name | This parameter (text) contains the administrator's first and last names. |
| Password | This parameter (text) contains the administrator's password (subject to password complexity rules). |
| Password Confirm | This parameter (text) must match the Password parameter— used to reduce typing errors. |
| Account Disabled | This parameter (check box) specifies the state of the account. If you select this check box, the account is disabled and the administrator cannot log on. |
| Immune to Expiry | This parameter (check box) specifies whether the password aging rules apply to the account. If you select this check box, the password rules do not apply. All password complexity rules still apply. This option is intended for nonhuman accounts. |
| Force Password Change | This parameter (check box) specifies whether the administrator must change the account password during the initial log on. If you select this check box, the administrator must change the password. |

### Assigning a role to a System Management Console user

Use this procedure to assign a role to a new System Management Console user, or to change the role currently assigned to an existing user.

### Prerequisites

* + The administrator must know the Global Administrator account password or be assigned the admin role.
  + Ensure the user account exists.
  + Ensure the role to be assigned is already configured.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Role Assignment**.
2. From the **Role Assignment** panel, select the user for which you want to assign a role, and click **Edit (-/+)**.
3. From the Available Roles list, select a role and click **Apply**.

**--End--**

### Configuring System Management Console password rules

Configure the password complexity rules and password aging rules to enhance the security of System Management Console passwords.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Password Rules**.
2. In the **Password Rules** panel, under **Password Complexity Rules**, configure the **Minimum Password Length**, **Minimum Lowercase Characters**, **Minimum Uppercase Characters**, **Minimum Digit Characters**, **Minimum Special Characters**, **Password History**, and **User ID Permitted in Password** fields.
3. In the **Password Rules** panel, under **Password Aging Rules**, configure the **Maximum Password Life (days)**, **Minimum Password Life (hours)**, **Expiry Notification (days)** fields.
4. Click **Apply**.

**--End--**

### Configuring System Management Console password rules job aid

The following job aid lists and describes the parameters on the Password Rules panel.

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| Minimum Password Length | This rule defines the minimum number of characters that a password must include. The range of values allowed is 4–  16. The minimum password length cannot be less than the summation of the minimum lowercase, uppercase, digit and special character rules. |
| Minimum Lowercase Characters | This rule defines the minimum number lowercase characters a password must contain. The range of values allowed is 0–4. Lowercase characters are defined by the US-ASCII character set, a–z. |
| Minimum Uppercase Characters | This rule defines the minimum number of uppercase characters that a password must contain. The range of values allowed is 0–4. Uppercase characters are defined by the US-ASCII character set, A–Z. |
| Minimum Digit Characters | This rule defines the minimum number digit characters that a password must contain. The range of values allowed is 0–4. Digit characters are defined by the US-ASCII character set, 0–9. |

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| Minimum Special Characters | This rule defines the minimum number of special characters that a password must include. The range of values allowed is 0–4. Special characters are defined by the following US-ASCII character set:  !#$%&()\*+,-./:;<=>?@[]^\_{|}~ |
| Password History | This rule defines the size of the password history maintained by the system for each user. The range of values allowed is 0–24. The system rejects the reuse of any password found in the user's history. Configure the value to 0 (zero) to disable password history validation. |
| User ID Permitted in Password | This rule indicates whether a password can include the user's ID, or a component of the user's name. |
| Maximum Password Life (days) | This rule defines the maximum number of days before a user's password expires. The range of values allowed is 0– 180 days. Configure the value to 0 (zero) to disable password expiration. |
| Minimum Password Life (hours) | This rule defines the minimum number of hours that a user's password must exist before the user can change it. The range of values allowed is 0–480 hours (20 days).  Configure the value to 0 (zero) to permit users to change their passwords as often as they wish. If not zero, the minimum password life must be less than the maximum password life. |
| Notification (days) | This rule defines the number of days the user is notified in advance of pending password expiration. The range of values allowed is 0–30 days. Configure the value to 0 (zero) to disable expiry notification. If not zero, the value must be less than the maximum password life and greater than the minimum password life. |

### Configuring log on and session rules

Configure log on and session rules for the following interfaces:

* + System Management Console
  + Provisioning Client

You maintain log on and session rules for each interface basis.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Log on Rules**.
2. In the **Log on Rules** panel, configure the **Log on Interface**, **Session Timeout (minutes)**, **Failed Log on Attempts before Lockout**, and **Lockout Duration (minutes)** fields.
3. Click **Apply**.

**--End--**

### Configuring log on and session rules job aid

The following job aid lists and describes the parameters on the Log on Rules panel.

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| System Interface | This parameter specifies the system interface for which the configuration options apply. |
| Session Timeout (minutes) | This rule defines the maximum number of minutes a session can be idle before the user must re-authenticate. The range of values allowed is 0–120. Configure the value to 0 (zero) to disable session timeout. For the System Management Console, after a session times out, any write operations must be re-authenticated.  You cannot disable session timeout for the Provisioning Client interface. |
| Failed Log on Attempts before Lockout | This rule defines the maximum number of successive failed log on attempts allowed before the user's account is locked. The range of values allowed is 0–10. Configure the value to 0 (zero) to disable lockout and permit unlimited successive failed log on attempts.  If not zero, the value represents an inclusive number of attempts. Therefore, if the value is 1 (one), a single failure causes the user's account is immediately locked. Until the account is unlocked, the system rejects further attempts to log on. |
| Lockout Duration (minutes) | This rule defines the number of minutes that a user's account remains locked after reaching the maximum number of successive failed log on attempts. The range of values allowed is 1–60. |

### Configuring Debug user job aid

Use this procedure to configure and manage the debug user GENBAND uses for access to the software debugging tools. The debug user should only be used by GENBAND support. No instance restart is required for these operations

* + Set login/logout Banner
    - Network Data and Mtc --> Banners
    - Set the login /logout message for selected banner.
  + Set session timeout
    - Administration --> Login Rules --> Session Timeout
    - *Session timeout parameters* sets timeout for each session.
  + Set idle timeout
    - Administration --> Debug Security Settings --> Session Timers
    - *Idle timeout (mins)* sets the timeout parameters for Debug mode (ssh)

### Configuring a new Provisioning Client role

Use this procedure to configure new roles for the Provisioning Client and assign the roles to users to specify administrator privileges and level of access.

### Prerequisites

* + You have administration management rights.
  + You know the System Administrator (SA) password. The SA is assigned the SuperUser or secadmin role.

### Procedure steps

###### Step Action

1. From the Provisioning Client menu bar, select **Admin, Role** to access the Admin Role portlet.
2. On the **Add** tab, in the **Role Name** field, type a name for the new role.
3. In the **Role description** field, type a brief description of the role.
4. Under the **Select All** option, check the **Read**, **Write**, or **Delete** boxes if you want the administrator to have a specific privilege or check all boxes to provide all privileges.
5. Under the **Data Layer Management** option, check the **Write** and **Delete** boxes if you want the administrator to have one or both privileges on the **System**, **Domain**, and **User** level.
6. Select the necessary **Read**, **Write**, and **Delete** check boxes to configure access for each Admin privilege.
7. Click **Save**.

**--End--**

### Configuring a new Provisioning Client user

Use this procedure to configure new administrative users for the Provisioning Client. Assign each new user a role so they can perform the administrative functions associated with that role.

### Prerequisites

* + The administrator has administration management right.
  + The administrator knows the System Administrator (SA) password. The SA is assigned the SuperUser or secadmin role.

### Procedure steps

###### Step Action

1. From the Provisioning Client menu bar, select **Admin, Add** to access the Admin portlet.
2. On the **Add** tab, configure the **Name**, **First Name**, **Last Name**, **Password**, **Confirm Password**, **Disable Password Aging**, **Enforce Password Change**, **Enable Account**, **Email**, **Business Phone**, **Home Phone**, **Cell Phone**, **Pager**, **Time Zone**, and **Locale** fields as necessary.
3. Click **Save**.

**--End--**

### Configuring a new Provisioning Client user job aid

The following job aid describes the parameters that appear on the Add tab of the Admin portlet.

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| Name | This parameter contains the account user name (maximum 120 characters). |
| First Name | This parameter contains the user's first name (maximum 30 characters). |
| Last Name | This parameter contains the user's last name (maximum 30 characters). |

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| Password | This parameter contains the password for the user account. |
| Confirm Password | This parameter must match the Password parameter. |
| Disable Password Aging | Select this check box to disable password aging. |
| Enforce Password Change | Select this check box to enforce password change. |
| Enable Account | Select this check box to enable the account. |
| Email | This parameter contains the user's e-mail address (if available). |
| Business Phone | This parameter contains the user's business telephone number (if available). |
| Home Phone | This parameter contains the user's home phone number (if available). |
| Cell Phone | This parameter contains the user's cell phone number (if available). |
| Pager | This parameter contains the user's pager number (if available). |
| Time Zone | This parameter (select from the list) contains the user's time zone. |
| Locale | This parameter (select from the list) contains the user's preferred language. |

### Configuring warning banners

Configure banner text to display advisory warnings before and after log on for the OPI, Provisioning Client, System Management Console, and Debug interfaces.

### Prerequisites

You can access the System Management Console.

### Procedure steps

###### Step Action

1. In the configuration view of the System Management Console, select **Network Data and Mtc, Banners**.
2. On the Banners panel, from the **Banner Type** list, select a banner type.

|  |  |
| --- | --- |
| **To configure** | **Do this** |
| A warning banner to appear before administrators log on. | Select Admin Pre Log on. |
| A warning banner to appear after administrators log on. | Select Admin Post Log on. |
| A warning banner to appear before debug log on. | Select Debug Pre Log on. |
| A warning banner to appear after debug log on. | Select Debug Post Log on. |
| A warning banner to appear before users log on. | Select User Pre Log on. |
| A warning banner to appear after users log on. | Select User Post Log on |

1. In the **Banner Data** section, select the **Enabled** check box.
2. Type the message to display.
3. Click **Apply**.

**--End--**

### Adding an External SIP Proxy

Use this procedure to add an External SIP Proxy. External SIP Proxies are associated with the configuration of foreign domains.

### Prerequisites

* + You must have access to the System Management Console.
  + You must know the IP address of the remote foreign destination.

### Procedure steps

###### Step Action

1. From the navigation pane of the System Management Console, select **Network Data and Mtc, External SIP Proxies**.
2. Cinlitchke**A**E**d**x**d**ternal SIP Proxies window.
3. Enter the SIP Proxy **Short Name**.
4. Enter the SIP Proxy **Long Name**.
5. Select the **Trusted** check box.
6. Select the **ExemptDoSProtection** check box.
7. Type **0** in the **Port** box. This enables all ports to send incoming messages.
8. From the **Node** list, select the node that corresponds to the External Node that is defined on the System Management Console for the foreign destination IP.
9. Enable the SIP transport method by selecting the appropriate UDP, TCP, and SSL/TLS check boxes. The SIP transport methods selected must match those on the foreign destination system.
10. Enter the port numbers for the selected SIP transport methods.

Each port box requires an integer value, even if you did not enable that specific transport method. The default values are acceptable.

1. Click **Apply**.

**--End--**

### Adding an External SIP Proxy job aid

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Short Name | A unique short name for the SIP Proxy. Range: up to 6 alphanumeric characters |
| Long Name | A unique long name for the SIP Proxy. Range: up to 32 alphanumeric characters |
| Trusted | Select to configure the SIP Proxy as a Trusted Node. |
| ExemptDoSProte ction | Select to allow an exemption for DOS protection. |
| Port | Set as 0 to allow all ports to send incoming messages. |
| Node | The name of the node. |
| Enable SIP UDP Port | Select to enable SIP UDP as the SIP Proxy transport method. |
| Enable SIP TCP Port | Select to enable SIP TCP as the SIP Proxy transport method. |
| Enable SIP TLS Port | Select to enable SIP TLS as the SIP Proxy transport method. |
| SIP UDP Port | The corresponding port used for SIP UDP. Range: integer between 1024 and 65534 |
| SIP TCP Port | The corresponding port used for SIP TCP. Range: integer between 1024 and 65534 |
| SIP TLS Port | The corresponding port used for SIP TLS. Range: integer between 1024 and 65534 |

### Adding a foreign domain

Use this procedure to add a foreign domain.

### Prerequisites

You must know the IP address of the remote foreign destination.

### Procedure steps

###### Step Action

1. From the Provisioning Client menu bar, select **Domain, Foreign Domain** to access the Foreign Domain portlet.
2. On the **Add** tab, configure **Name**, **SIP proxy name**, **SIP URI params**, **Foreign destination**, and **Domain aliases** fields.
3. Click **Save**.

**--End--**

### Adding a foreign domain job aid

This job aid describes the parameters that appear on the Add tab in the Foreign Domain portlet.

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Name | Enter the name of the Foreign Domain in this field. The name of the foreign domain must match the name of the domain hosted by the external SIP proxy. |
| SIP proxy name | A foreign domain proxy can be defined by either using an external SIP proxy provisioned on the System Manager or by specifying an IP address. A fully-qualified domain name (FQDN) can be used instead of the IP Address.  Select either External Domain or Address Name.  External Domain should be selected if an IP address is unavailable for the foreign route. If this field is selected, the domain URL entered in the address field must be a DNS-resolvable external domain name or hostname.  If Address Name is selected, an address should be selected from the drop-down menu in the address box. The address name is the Long Name of the external SIP proxy, defined through the System Management GUI. |

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| SIP URI params | URI parameters include:   * authenticated   This parameter allows all incoming request messages from a foreign domain defined with a FQDN to be accepted without an authentication challenge. The resolved IP addresses are added to the SESM authentication table.  A DNS server with an entry matching the FQDN must be set up on all of the SESMs on which the Foreign Domain will be used.   * trusted   This allows all outgoing messages going to this domain to be handled as going to a “trusted” domain.   * nt\_info=proxy   This parameter should be added when the Foreign Domain SIP Proxy represents an AS system. This parameter is used to tell the foreign server that the call has been forwarded by another AS system.   * nt\_im   This parameter should be added when the Foreign Domain SIP Proxy represents an AS system. This parameter is used to determine the capability of the SIP Proxy to understand GENBAND-specific content for Instant Messages. Valid parameter/values pairs include: nt\_im=nt-im-2.0, nt\_im=nt-im-1.0, nt\_im=enhanced. It is recommended that you add the nt\_im=nt-im-2.0 parameter for AS systems. |
| Foreign Destination | Clicking the ADD button adds a SIP proxy route with its corresponding SIP URI parameters in the Foreign Destination field. Clicking the REMOVE button removes the entries in this field. |
| Domain Aliases | Select one or more aliases associated with informational elements that are configured as the General type. The alias is used as an alias for the foreign domain.  For additional information about informational elements, see "Configuring a trusted node" in  *EXPERiUS Application Server — Configuration*  (NN48111–511). |

## Administrator security management

This chapter provides the procedures that you require to manage administrator security for the database and the following tools:

* + System Management Console
  + Provisioning Client

### Resetting the password for the database sys account

Use this procedure to reset the password for the database sys account.

### Prerequisites

You must belong to the System Security Administrator (SSA) role (for example, nysysadm).

### Procedure steps

###### Step Action

1. Log on to the Primary DB server as an SSA.
2. Enter the command:

###### sudo /opt/mcp/db/sbin/ resetDbSystemUserPasswd.pl sys

1. If prompted for a password, enter the password of the user you are logged on as.
2. At the prompt, enter a new password that complies with the database password rules.
3. At the prompt, enter the new password again.

**--End--**

### Resetting the password for the database system account

Use this procedure to reset the password for the database system account.

### Prerequisites

You must belong to the System Security Administrator (SSA) role (for example, nysysadm).

### Procedure steps

###### Step Action

1. Log on to the Primary DB server as an SSA.
2. Enter the command:

###### sudo /opt/mcp/db/sbin/ resetDbSystemUserPasswd.pl system

If prompted for a password, enter the password of the user you are logged on as.

The system prompts for a new system password.

1. At the prompt, enter a new password that compiles with the database password rules.
2. At the prompt, enter the new password again.

**--End--**

### Resetting the passwords for the database internal accounts

Policy can require that you change all system passwords. Use this procedure to change the passwords for the database internal accounts.

**Attention**

Only the database software uses the internal accounts. To prevent users from logging on to these accounts, the passwords are randomly generated and not available to users. These accounts are also locked.

### Prerequisites

You must belong to the System Security Administrator (SSA) role (for example, nysysadm).

### Procedure steps

###### Step Action

1. Log on to the Primary DB server as an SSA.
2. Change to root:

###### su - root

1. Enter the root password.
2. Change directory:

###### cd /opt/mcp/db/sbin

1. Run the script to change the password:

###### ./resetDbSystemUserPasswd.pl internal

The script changes the internal passwords to new random passwords.

**--End--**

### Resetting the password for an individual database user account

Use this procedure to change your database user account.

**Attention**

If you share the password for your individual user account, you reduce system security and individual accountability. It is recommended that you do not share the password for your individual user account.

### Prerequisites

Your user account is assigned the Database Administrator (DBA) role (ntdbadm).

### Procedure steps

###### Step Action

1. Log on to the Primary DB server using your DBA account.
2. Enter the command:

###### sudo /opt/mcp/db/sbin/resetDbUserPasswd.pl –u

**<user-name>**

1. If prompted, enter the password of the user you are logged on as.
2. At the prompt, enter a new password that complies with the database password rules.
3. At the prompt, enter the new password again to confirm.

**--End--**

### Variable definitions

|  |  |
| --- | --- |
| **Variable** | **Value** |
| <user-name> | This value is the username for the account being modified. |

### Changing the password for the database schema user account

Use this procedure to change the password for the database schema user account.

### Prerequisites

Your user account is assigned the Application Administrator (AA) role (ntappadm).

### Procedure steps

###### Step Action

1. Log on to the Primary System Manager (SM) server as an AA (ntappadm).
2. Change directory:

###### cd /var/mcp/install

1. Run the script to change the password:

###### ./chgDbSchemaUserPasswd.pl

1. At the prompt, enter the current password.
2. At the prompt, enter a new password that complies with the database password rules.
3. At the prompt, enter the new password again.

**--End--**

### Changing the password for the database application account

Use this procedure to change the password for the database application account. For information about how to change the password during a patch or maintenance release (MR) upgrade, see *EXPERiUS Application Server*

*— Installation* (NN48111-316).

### Prerequisites

* + You are assigned to the Application Administrator (AA) role (ntappadm).
  + Be familiar with the procedures to stop, deploy, and start a network element (NE). For more information about how to stop, deploy, and start network elements, see *EXPERiUS Application Server — Configuration* (NN48111–511).

### Procedure steps

###### Step Action

1. Log on to the Primary System Manager (SM) server as an AA (ntappadm).
2. Change directory:

###### cd /var/mcp/install

1. Run the script to change the password:

###### ./chgDbAppUserPasswd.pl

1. At the prompt, enter the current password.
2. At the prompt, enter a new password that compiles with the database password rules.
3. At the prompt, enter the new password again.
4. Change directory:

###### cd /var/mcp/install

1. Run the script to restart the SM instances:

###### ./smUpgrade.pl

This script stops all SM instances, deploys the load specified in installprops.txt (the current load), and then starts all instances

1. Use the System Management Console to stop, deploy, and restart the other NEs in the following order:
   * Fault Performance Manager (FPM)
   * Accounting Manager (AM)
   * PROV Manager
   * Personal Agent (PA) Manager
   * Session Manager (SESM)
   * IP Client Manager (IPCM)

If you miss any of the NEs, you will receive an error message after you run the script in [Step 12](#_bookmark243).

1. Log on to the Primary System Manager (SM) server as an AA (ntappadm).
2. Change directory:

###### cd /var/mcp/install

1. Run the script to change the password:

###### ./chgDbAppUserPasswd.pl

The script removes the old application account.

**--End--**

### Modifying log on and session rules

You can modify log on and session rules for the following interfaces:

* + Configuration Management (OMI)
  + Provisioning Client

You maintain log on and session rules for each interface basis.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Log on Rules**.
2. In the **Log on Rules** panel, configure the **System Interface**, **Session Timeout (minutes)**, **Failed Log on Attempts before Lockout**, and **Lockout Duration (minutes)** fields.
3. Click **Apply**.

**--End--**

### Modifying log on and session rules job aid

The following job aid lists and describes the fields on the Log on Rules panel.

|  |  |
| --- | --- |
| **Field** | **Description** |
| System Interface | This field specifies the system interface for which the configuration options apply. |
| Session Timeout (minutes) | This rule defines the maximum number of minutes a session can be idle before the user must reauthenticate. The range of values allowed is 0–120. Configure the value to 0 (zero) to disable session timeout. For OMI clients and the System Management Console, after a session times out, any write operations must be re-authenticated.  You cannot disable session timeout for the Provisioning Client interface. |
| Failed Log on Attempts before Lockout | This rule defines the maximum number of successive failed log on attempts allowed before the user's account is locked. The range of values allowed is 0–10. Configure the value to 0 (zero) to disable lockout and permit unlimited successive failed log on attempts.  If not zero, the value represents an inclusive number of attempts. Therefore, if the value is 1 (one), a single failure causes the user's account is immediately locked. Until the account is unlocked, the system rejects further attempts to log on. |
| Lockout Duration (minutes) | This rule defines the number of minutes that a user's account remains locked after reaching the maximum number of successive failed log on attempts. The range of values allowed is 1–60. |

### Modifying System Management Console password rules

You can modify the password complexity rules and password aging rules to enhance the security of System Management Console passwords.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Password Rules**.
2. In the **Password Rules** panel, under **Password Complexity Rules**, configure the **Minimum Password Length**, **Minimum Lowercase Characters**, **Minimum Uppercase Characters**, **Minimum Digit Characters**, **Minimum Special Characters**, **Password History**, and **User ID Permitted in Password** fields.
3. In the **Password Rules** panel, under **Password Aging**, configure the **Maximum Password Life (days)**, **Minimum Password Life (hours)**, **Expiry Notification (days)** fields.
4. Click **Apply**.

**--End--**

### Modifying System Management Console password rules job aid

The following job aid lists and describes the fields on the Password Rules panel.

|  |  |
| --- | --- |
| **Field** | **Description** |
| Minimum Password Length | This rule defines the minimum number of characters that a password must include. The range of values allowed is 4–  32. The minimum password length cannot be less than the summation of the minimum lowercase, uppercase, digit and special character rules. |
| Minimum Lowercase Characters | This rule defines the minimum number lowercase characters a password must contain. The range of values allowed is 0–4. Lowercase characters are defined by the US-ASCII character set, a–z. |
| Minimum Uppercase Characters | This rule defines the minimum number of uppercase characters that a password must contain. The range of values allowed is 0–4. Uppercase characters are defined by the US-ASCII character set, A–Z. |
| Minimum Digit Characters | This rule defines the minimum number digit characters that a password must contain. The range of values allowed is 0–4. Digit characters are defined by the US-ASCII character set, 0–9. |
| Minimum Special Characters | This rule defines the minimum number of special characters that a password must include. The range of values allowed is 0–4. Special characters are defined by the following US-ASCII character set:  !#$%&()\*+,-./:;<=>?@[]^\_{|}~ |

|  |  |
| --- | --- |
| **Field** | **Description** |
| Password History | This rule defines the size of the password history maintained by the system for each user. The range of values allowed is 0–24. The system rejects the reuse of any password found in the user's history. Configure the value to 0 (zero) to disable password history validation. |
| User ID permitted in Password | This rule indicates whether a password can include the user's ID, or a component of the user's name. |
| Maximum Password Life (days) | This rule defines the maximum number of days before a user's password expires. The range of values allowed is 0– 180 days. Configure the value to 0 (zero) to disable password expiration. |
| Minimum Password Life (hours) | This rule defines the minimum number of hours that a user's password must exist before the user can change it. The range of values allowed is 0–480 hours (20 days).  Configure the value to 0 (zero) to permit users to change their passwords as often as they wish. If not zero, the minimum password life must be less than the maximum password life. |
| Expiry Notification (days) | This rule defines the number of days the user is notified in advance of pending password expiration. The range of values allowed is 0–30 days. Configure the value to 0 (zero) to disable expiry notification. If not zero, the value must be less than the maximum password life and equal or greater than the minimum password life. |

### Modifying a System Management Console role

You can modify roles for the System Management Console to specify admin privileges and level of access.

### Prerequisites

You must have ConfigRoleDefinitionService READ and WRITE privileges.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, Role Definition**.
2. On the **Role Definition** panel, click **Edit (-/+)**.
3. Select the required **READ**, **WRITE**, and **MAINT** to configure privileges for each service.
4. Click **Apply**.

**--End--**

### Modifying a new System Management Console role job aid

The effects of the READ, WRITE, and MAINT privileges differ according to the service that is selected; however, the following points generally apply:

* + The READ privilege typically allows you to view, but not modify configuration data.
  + The WRITE privilege enables READ automatically and allows you to add and modify configuration data.
  + The MAINT privilege allows you to start and stop services, but does not allow you to change configuration data. Typically you must also have the READ privilege in addition to MAINT.

Refer to [“Configuring System Management Console roles job aid”](#_bookmark226)

[(page 186)](#_bookmark226) for a list and description of the services for which you can add READ, WRITE, and MAINT privileges to roles.

### Modifying a System Management Console user

Modify roles for the System Management Console to define the administrative functions users assigned to the role can perform.

### Prerequisites

You must know the Global Administrator account password.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, User Administration**.
2. On the **User Administration** panel, select the User to be modified and click **Edit (-/+)**.
3. In the **Edit User Account** dialog box, configure the **User Name**, **Account Disabled**, and **Immune to Expiry** fields.
4. Click **Apply**.

If the change is valid, the **Edit User Account** dialog box closes and the modification appears on the **User Administration** panel.

**--End--**

### Modifying a System Management Console user job aid

This job aid lists and describes the fields that you configure on the Add User Account dialog box.

|  |  |
| --- | --- |
| **Field** | **Description** |
| User Name | This field (text) contains the administrator's first and last names. |
| Account Disabled | This field (check box) specifies the state of the account. If you select this check box, the account is disabled and the administrator cannot log on. |
| Immune to Expiry | This field (check box) specifies whether the password aging rules apply to the account. If you select this check box, the password rules do not apply. All password complexity rules still apply. This option is intended for nonhuman accounts. |

### Disabling a System Management Console user account

You can disable a System Management Console user account.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, User Administration**.
2. On the **User Administration** panel, select the user to be disabled and click **Edit (-/+)**.
3. In the **Edit User Account** dialog box, select the **Account Disabled** check box.
4. Click **Apply**.

**--End--**

### Disabling password aging rules for an account

You can disable the password aging rules for a particular account. This option is intended for system (non-human) accounts. All password complexity rules still apply.

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Administration, User Administration**.
2. On the **User Administration** panel, select the User to be disabled and click **Edit (-/+)**.
3. In the **Edit User Account** dialog box, select the **Immune to Expiry** check box.
4. Click **Apply**.

**--End--**

### Viewing and forcing off users

You can view all System Management Console users who are logged on. If necessary you can force another administrator off the system.

### Prerequisites

You must have AdminUserService privileges.

### Procedure steps

###### Step Action

1. From the System Management Console menu bar, select **Administration, User Display/Forceoff**.
2. To force an administrator off the system, from the **Logged-in Users** panel, select an entry and click **Force Off**.
3. Ctoliccokn**Y**fi**e**rm**s** the Force Off.

**--End--**

### Exporting configuration data for System Management Console

You can export configuration data for the System Management Console (SMC).

### Prerequisites

* + You must have ExportImportService privileges.
  + You must be assigned to the AA role (ntappadm).

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Tools, DB Export**.
2. In the **DB Export** panel, click **Choose**.
3. In the **Save** dialog box, browse to the location where you want to save the file.
4. In the **File name** field, type a name for the file.
5. Click **Save**.
6. Select the **Export Selected Services** radio button.
7. From the **Services Available for Export** list, select the desired service.
8. Click **Export Now**.
9. In the FTP log on screen, enter the AA (ntappadm) username and password.
10. Click **Apply**.

**--End--**

### Importing configuration data for System Management Console

You can import configuration data for the System Management Console .

### Prerequisites

* + You must have ExportImportService privileges.
  + You must be assigned to the AA role (ntappadm).

### Procedure steps

###### Step Action

1. From the menu bar of the System Management Console, select **Tools, DB Import**.
2. In the **DB Import** panel, under **Import File**, click **Choose**.
3. In the **Open** dialog box, browse to the location from which you want to select the file.
4. Select the file that you want to restore.

The file name appears in the File name field.

1. Click **Open**.
2. In the **DB Import** panel, under **Result File**, click **Choose**.
3. In the **Save** dialog box, browse to the location where you want to save the log output file.
4. In the **File name** field, type a name for the log output file.
5. Click **Save**.
6. Click **Import Now**.
7. In the FTP log on screen, enter the AA (ntappadm) user name and password.
8. Click **Apply**.

**--End--**

### Deleting a System Management Console role

You can delete any role which is not required.

### Prerequisites

You must reassign any users assigned to the role.

### Procedure steps

###### Step Action

1. From the System Management Console menu bar, select **Administration, Role Definition**.
2. From the **Roles Definition panel** panel, select the role that you want to delete and click **Delete**.
3. Click **Yes** to confirm.

If the role is not referenced by any users, the entry disappears from the Roles Definition panel.

**--End--**

### Deleting a System Management Console user

You can delete the user accounts for administrators who no longer require access to the System Management Console.

### Procedure steps

###### Step Action

1. From the System Management Console menu bar, select **Administration, User Administration**.
2. From the **User Administration** panel, select the entry for the user and click **Delete**.
3. Ctoliccokn**Y**fi**e**rm**s** .

**--End--**

### Resetting the password for the System Manager admin account

Use this procedure to reset the password for the initial System Manager admin account if there are no other administrative users who have sufficient privileges to reset the password.

### Prerequisites

* + You must belong to the Database Administrator role (ntdbadm).
  + You must belong to the Application Administrator role (ntappadm).

### Procedure steps

###### Step Action

1. Log on to the primary database (DB) server as a DBA (ntdbadm).
2. Change directory:

###### cd /var/mcp/run/MCP\_<rel>/<dbName>/bin/util

1. Run the script to change the password:

###### ./resetSMAdminPasswd.pl

1. Log on to the primary System Manager as an AA.
2. Change directory:

###### cd /var/mcp/install

1. Run the script to restart the System Manager:

###### ./smUpgrade.pl

This script stops all System Manager instances, redeploys the load specified in installprops.txt, and restarts all System Manager instances.

1. Log on to the System Management Console with the admin account.
2. At the prompt to change the password, type a new password that complies with the password rules.
3. Type the new password again to confirm.
4. Type the current password (the default password is admin).
5. Click **OK** to save the new password and complete the log on.

**--End--**

### Modifying a Provisioning Client role

You can modify roles for the Provisioning Client to specify admin privileges and level of access.

### Prerequisites

You must know the System Administrator (SA) password. The SA is assigned the SuperUser role.

### Procedure steps

###### Step Action

1. From the Provisioning Client navigation pane, select **Administrator, List Role**.
2. On the **Admin Role** page, click **Role Name** for the role to be modified.
3. In the **Role Description** field, type a brief description of the role.
4. Select the necessary **Read**, **Write**, and **Delete** check boxes to configure access for each Admin privilege.
5. Click **Save**.

**--End--**

### Modifying a Provisioning Client role job aid

Refer to [“Configuring a new Provisioning Client role” (page 196)](#_bookmark231) for a list and description of each of the Admin privileges listed on the Add a New Role page.

### Listing Provisioning Client users

Use this procedure to search for administrator user accounts for the Provisioning Client.

### Procedure steps

###### Step Action

1. From the Provisioning Client menu bar, select **Admin, List** to access the Admin portlet. In the Admin portlet, click the **Search** tab.
2. Enter a value in the **Inactive time in days** field. **OR**

Click **Search**.

*The Search page shows you the list of administrator user accounts.*

**--End--**

### Deleting a Provisioning Client user

Use this procedure to remove Provisioning Client user accounts that are no longer required.

### Procedure steps

###### Step Action

1. From the Provisioning Client navigation pane, select **Administrator, List Admin**.
2. Click **Delete** for the user account you want to delete.

**--End--**

### Resetting the password for the Provisioning Manager admin account

Use this procedure to reset the password for the initial Provisioning Manager admin account if there are no other administrative users who have sufficient privileges to reset the password.

### Prerequisites

You must belong to the Database Administrator role (ntdbadm).

### Procedure steps

###### Step Action

1. Log on to the primary database server as a DBA (ntdbadm).
2. Change directory:

###### cd /var/mcp/run/MCP\_<rel>/<dbName>/bin/util

1. Run the script to change the password:

###### ./resetProvAdminPasswd.pl

1. Log on to the System Management Console.
2. From the configuration view, select **Network Elements, Provisioning Managers, <PROV\_instance>, NE Maintenance**.
3. In the Prov Maintenance window, under the Oper column, verify the Provisioning Manager status is Active.
4. Select the Provisioning Manager instance and click **Restart**.
5. Verify that the Provisioning Manager status returns to Active.
6. Use a supported Web browser to log on to the Provisioning Client for the Provisioning Manager that you restarted in [Step 7](#_bookmark260).

(The above script resets the password to a default of admin.)

1. From the Provisioning Client navigation pane, select **Administrator, Password**.
2. Type the new password for the Provisioning Manager admin account.
3. Type the new password again to confirm.
4. Type the old password (the default password is admin).
5. Click **Save**.

**--End--**

## Configuring cipher changes

The following are the recommended ciphers at the time of publication for System Manager (SM), Provisioning Manager (PROV), and Personal Agent (PA).

**For OAMP:**

|  |
| --- |
| TLS\_RSA\_WITH\_AES128\_CBC\_SHA |
| TLS\_DHE\_RSA\_ WITH\_AES\_128\_CBC\_SHA |
| TLS\_DHE\_DSS\_WITH\_ AES\_128\_CBC\_SHA |

**For external OAMP:**

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

**For HTTPS:**

TLS\_RSA\_ WITH\_AES\_128\_CBC\_SHA

**For Signaling:**

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

It is recommended that NULL and Weak cipher suites be disabled unless required within the network configuration. The applicable cipher suites are as follows.

**NULL cipher suites**

|  |
| --- |
| TLS\_RSA\_WITH\_NULL\_SHA |
| SSL\_RSA\_WITH\_NULL\_MD5 |
| SSL\_RSA\_WITH\_NULL\_SHA |

**Weak cipher suites**

|  |
| --- |
| SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA |
| SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 |
| SSL\_RSA\_WITH\_DES\_CBC\_SHA |
| SSL\_DHE\_RSA\_WITH\_DES\_CBC\_SHA |

**Weak cipher suites (cont'd)**

|  |
| --- |
| SSL\_DHE\_DSS\_WITH\_DES\_CBC\_SHA |
| SSL\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA |
| SSL\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA |

### Adjusting the cipher suites

Use the following procedure to adjust the cipher suites. **Step Action**

1. From your browser, go to http://<SM\_IP>:12120/ and click **Launch MCP System Management Console**.
2. Log in with your credentials.

The System Manager (SM) GUI opens.

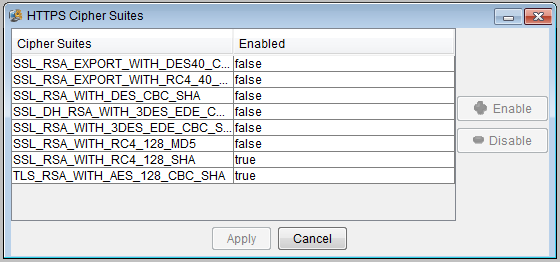
1. On the left pane, navigate to **Network Data and MTC > Cipher Suites**.
2. Expand **Cipher Suites**.

The following suites are displayed:

* + OAMP Channel Cipher Suites
  + External OAMP Cipher Suites
  + HTTPS Cipher Suites
  + Signaling Cipher Suites

1. Double-click the desired cipher suite.

A list of all ciphers for the protocol is displayed, as shown in the following example.



1. Select the desired cipher suite, and click **Enable** or **Disable** as required.
2. Click **Apply**.

**--End--**

EXPERiUS Application Server

Security

Release: 11.2

Publication: NN48111-612 Document Revision: 10.02

Document release date: 12 January 2016

Copyright © 2010-2016 GENBAND. All rights reserved. Use of this documentation and its contents is subject to the terms and conditions of the applicable end user or software license agreement, right to use notice, and all relevant copyright protections.

GENBAND, the GENBAND corporate logo and tagline, and certain of GENBAND's product and solution names are registered trademarks of GENBAND and its affiliates.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, GENBAND AND/OR ITS LICENSORS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY

KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

THE INFORMATION CONTAINED HEREIN IS THE PROPERTY OF GENBAND OR ITS LICENSORS AND MUST NOT BE DISCLOSED, OTHER THAN TO EMPLOYEES OF GENBAND OR CUSTOMERS WITH NEED-TO-KNOW, WITHOUT THE PRIOR WRITTEN CONSENT OF GENBAND OR ITS LICENSORS. THE INFORMATION MUST NOT BE DISCLOSED TO SUBCONTRACTORS OR REGULATORY AUTHORITIES. GENBAND MUST BE NOTIFIED OF ANY REQUEST OR ORDER FOR DISCLOSURE PRIOR TO SUCH DISCLOSURE.

For access to the Document Center, log in through the Customer Support website at [http://cust.genband.com](http://cust.genband.com/).

Software and documentation owned by or under license with Nortel Networks included in this Release or in any document provided with this Release is Copyright © 2010 Nortel Networks or its licensors. All rights reserved. Use of this software and/or documentation and its contents is subject to the terms and conditions of the applicable end user or software license agreement, right to use notice, and all relevant copyright protections.

[www.genband.com](http://www.genband.com/)

