



## AAA Device Configuration Listings

---

This appendix provides the following configuration listings:

- A.1.1 Example Local-Based Router AAA Configuration
- A.1.2 Example Server-Based TACACS+ NAS Configuration
- A.1.3 Example Server-Based RADIUS NAS Configuration
- A.4.1 CSU.cfg Listing
- A.4.2 CSConfig.ini Listing
- A.4.3 Oracle User Environment Variable
- A.4.4 listener.ora Listing

### A.1 Sample Cisco IOS Configuration Listings

The following listing represents the complete running configuration for the router and NAS used to illustrate AAA implementation in this solution guide. Listings are included for TACACS+ and RADIUS configurations.

## A.1.1 Example Local-Based Router AAA Configuration

The following example of a local-based router configuration includes both dial-in and EXEC shell access configurations.

```
maui-rtr-03#show running-config
Building configuration...

Current configuration:
!
! Last configuration change at 09:19:35 CST Thu Apr 13 2000 by brownr
! NVRAM config last updated at 09:14:55 CST Thu Apr 13 2000 by brownr
!
version 12.0
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname maui-rtr-03
!
no logging console
aaa new-model
aaa authentication login default local enable
aaa authentication login NO_AUTHEN none
aaa authorization exec default local
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default local
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
enable secret 5 xxxxxxxxxxxxxxxxxxxx
!
username admin privilege 15 password 7 xxxxxxxxxxxx
!
!
!
clock timezone cst -6
clock summer-time CST recurring
ip subnet-zero
ip domain-name maui-onions.com
ip name-server x.x.x.x
ip name-server x.x.x.x
!
!
!
!
!
interface Loopback0
 ip address 172.22.255.3 255.255.255.255
 no ip directed-broadcast
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 shutdown
 no atm ilmi-keepalive
!
interface Serial2/0
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
!
```

```
interface Serial2/1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial2/2
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial2/3
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Ethernet3/0
  ip address 172.22.241.3 255.255.255.0
  no ip directed-broadcast
  ip summary-address eigrp 69 172.22.80.0 255.255.240.0 5
!
interface Ethernet3/1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Ethernet3/2
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Ethernet3/3
  no ip address
  no ip directed-broadcast
  shutdown
!
interface FastEthernet4/0
  ip address 172.22.80.1 255.255.255.0
  no ip directed-broadcast
  ip summary-address eigrp 69 172.22.240.0 255.255.240.0 5
  half-duplex
!
router eigrp 69
  network 172.22.0.0
!
ip default-gateway 172.22.53.1
ip classless
ip http server
ip http authentication aaa
ip tacacs source-interface Loopback0
!
snmp-server engineID local 00000009020000D0BB7F5054
snmp-server community cisco xx
snmp-server community rules xx
snmp-server trap-source Loopback0
snmp-server contact
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps config
snmp-server enable traps envmon
tacacs-server host 172.22.53.201 key biteme
tacacs-server key ciscorules
!
line con 0
  authorization commands 15 NO_AUTHOR
```

```
authorization exec NO_AUTHOR
accounting commands 15 NO_ACCOUNT
login authentication NO_AUTHEN
transport input none
line aux 0
line vty 0 4
!
ntp clock-period 17179912
ntp source Loopback0
ntp update-calendar
ntp server 172.22.255.1
end
```

## A.1.2 Example Server-Based TACACS+ NAS Configuration

The following example of a server-based NAS configuration includes both dial-in and EXEC shell access configurations for TACACS+ implementations:

```
maui-nas-03#show running-config
Building configuration...

Current configuration:

maui-nas-03#sh run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname maui-nas-03
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default group tacacs+
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting network default start-stop group tacacs+
!
username admin privilege 15 password 7 xxxxxxxxxxxxxx
username diallocal access-class 110 password 7 xxxxxxxxxxxxxx
username diallocal autocommand ppp
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
spe 2/0 2/7
  firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
!
!
!
!
!
clock timezone CST -6
clock summer-time CST recurring
ip subnet-zero
no ip domain-lookup
ip domain-name maui-onions.com
ip name-server 172.22.53.210
!
isdn switch-type primary-ni
isdn voice-call-failure 0
partition flash 2 24 8
!
!
!
controller T1 0
```

```
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1
clock source line secondary 1
!
controller T1 2
clock source line secondary 2
!
controller T1 3
clock source line secondary 3
!
controller T1 4
clock source line secondary 4
!
controller T1 5
clock source line secondary 5
!
controller T1 6
clock source line secondary 6
!
controller T1 7
clock source line secondary 7
!
!
interface Loopback0
ip address 172.22.87.3 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback1
ip address 172.22.83.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Ethernet0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
clockrate 2015232
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
clockrate 2015232
```

```
!  
interface Serial2  
  no ip address  
  no ip directed-broadcast  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  no fair-queue  
  clockrate 2015232  
!  
interface Serial3  
  no ip address  
  no ip directed-broadcast  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  no fair-queue  
  clockrate 2015232  
!  
interface Serial0:23  
  description "PRI D channel"  
  ip unnumbered Dialer1  
  no ip directed-broadcast  
  encapsulation ppp  
  no ip route-cache  
  no logging event link-status  
  timeout absolute 240 0  
  dialer rotary-group 1  
  dialer-group 5  
  no snmp trap link-status  
  isdn switch-type primary-5ess  
  isdn incoming-voice modem  
  no fair-queue  
  compress stac  
  no cdp enable  
!  
interface FastEthernet0  
  ip address 172.22.80.3 255.255.255.0  
  no ip directed-broadcast  
  no ip route-cache  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
interface Group-Async1  
  ip unnumbered Loopback0  
  no ip directed-broadcast  
  encapsulation ppp  
  no ip route-cache  
  ip tcp header-compression passive  
  no ip mroute-cache  
  no logging event link-status  
  dialer in-band  
  dialer idle-timeout 900  
  async mode interactive  
  no snmp trap link-status  
  peer default ip address pool default  
  no fair-queue  
  no cdp enable  
  ppp max-bad-auth 3  
  ppp authentication pap chap  
  group-range 1 192  
!  
interface Dialer1
```

```

no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
no logging event link-statustimeout absolute 240 0
dialer in-band
dialer idle-timeout 300 either
dialer-group 5
no snmp trap link-status
peer default ip address pool default
no fair-queue
compress stac
no cdp enable
ppp max-bad-auth 3
ppp multilink
!
router eigrp 69
 network 172.22.0.0
!
ip local pool default 172.22.83.2 172.22.83.254
ip default-gateway 172.22.80.1
ip classless
ip tacacs source-interface Loopback0
ip http server
!
access-list 110 deny tcp any any eq telnet
access-list 110 permit tcp any any
tacacs-server host 172.22.53.204
tacacs-server key ciscorules
snmp-server engineID local 0000000902000050546B87BC
snmp-server community xxxxxxxx RO
snmp-server community xxxxxxxx RW
radius-server host 172.22.53.204 auth-port 1645 acct-port 1646 key ciscorules
banner login ^CC
Welcome to maui-nas-03
Maui-onions Lab
Learning Rack ISG
^C
!
line con 0
 authorization commands 15 NO_AUTHOR
 authorization exec NO_AUTHOR
 login authentication NO_AUTHEN
 transport input none
line 1 192
 session-timeout 15
 exec-timeout 48 0
 autoselect during-login
 autoselect ppp
 absolute-timeout 240
 script dialer cisco_default
 refuse-message ^CCCCCCC!!! All lines are busy, try again later ###^C
 modem InOut
 modem autoconfigure type mica
 transport preferred telnet
 transport input all
 transport output pad telnet rlogin udptn
line aux 0
line vty 0 4
!
end

```

## A.1.3 Example Server-Based RADIUS NAS Configuration

The following example of a server-based NAS configuration includes both dial-in and EXEC shell access configurations for RADIUS implementations:

```
maui-nas-03#show running-config
Building configuration...

Current configuration:

maui-nas-03#sh run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname maui-nas-03
!
aaa new-model
aaa authentication login default group radius local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default stop-only group radius
aaa accounting network default start-stop group radius
!
username admin privilege 15 password 7 xxxxxxxxxxxxxx
username diallocal access-class 110 password 7 xxxxxxxxxxxxxx
username diallocal autocommand ppp
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
spe 2/0 2/7
  firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
!
!
!
!
!
clock timezone CST -6
clock summer-time CST recurring
ip subnet-zero
no ip domain-lookup
ip domain-name maui-onions.com
ip name-server 172.22.53.210
!
isdn switch-type primary-ni
isdn voice-call-failure 0
partition flash 2 24 8
!
!
!
controller T1 0
  framing esf
  clock source line primary
```

```
    linecode b8zs
    pri-group timeslots 1-24
    !
  controller T1 1
    clock source line secondary 1
    !
  controller T1 2
    clock source line secondary 2
    !
  controller T1 3
    clock source line secondary 3
    !
  controller T1 4
    clock source line secondary 4
    !
  controller T1 5
    clock source line secondary 5
    !
  controller T1 6
    clock source line secondary 6
    !
  controller T1 7
    clock source line secondary 7
    !
    !
  interface Loopback0
    ip address 172.22.87.3 255.255.255.255
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    !
  interface Loopback1
    ip address 172.22.83.1 255.255.255.0
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    !
  interface Ethernet0
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    !
  interface Serial0
    no ip address
    no ip directed-broadcast
    encapsulation ppp
    no ip route-cache
    no ip mroute-cache
    shutdown
    no fair-queue
    clockrate 2015232
    !
  interface Serial1
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    no fair-queue
    clockrate 2015232
    !
  interface Serial2
```

```
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
clockrate 2015232
!
interface Serial3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
clockrate 2015232
!
interface Serial0:23
description "PRI D channel"
ip unnumbered Dialer1
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no logging event link-status
timeout absolute 240 0
dialer rotary-group 1
dialer-group 5
no snmp trap link-status
isdn switch-type primary-5ess
isdn incoming-voice modem
no fair-queue
compress stac
no cdp enable
!
interface FastEthernet0
ip address 172.22.80.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
!
interface Group-Async1
ip unnumbered Loopback0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
ip tcp header-compression passive
no ip mroute-cache
no logging event link-status
dialer in-band
dialer idle-timeout 900
async mode interactive
no snmp trap link-status
peer default ip address pool default
no fair-queue
no cdp enable
ppp max-bad-auth 3
ppp authentication pap chap
group-range 1 192
!
interface Dialer1
no ip address
no ip directed-broadcast
```

```

encapsulation ppp
no ip route-cache
no ip mroute-cache
no logging event link-statustimeout absolute 240 0
dialer in-band
dialer idle-timeout 300 either
dialer-group 5
no snmp trap link-status
peer default ip address pool default
no fair-queue
compress stac
no cdp enable
ppp max-bad-auth 3
ppp multilink
!
router eigrp 69
 network 172.22.0.0
!
ip local pool default 172.22.83.2 172.22.83.254
ip default-gateway 172.22.80.1
ip classless
ip tacacs source-interface Loopback0
ip http server
!
access-list 110 deny tcp any any eq telnet
access-list 110 permit tcp any any
tacacs-server host 172.22.53.204
tacacs-server key ciscorules
snmp-server engineID local 0000000902000050546B87BC
snmp-server community xxxxxxxx RO
snmp-server community xxxxxxxx RW
radius-server host 172.22.53.204 auth-port 1645 acct-port 1646 key ciscorules
banner login ^CC
Welcome to maui-nas-03
Maui-onions Lab
Learning Rack ISG
^C
!
line con 0
 authorization commands 15 NO_AUTHOR
 authorization exec NO_AUTHOR
 login authentication NO_AUTHEN
 transport input none
line 1 192
 session-timeout 15
 exec-timeout 48 0
 autoselect during-login
 autoselect ppp
 absolute-timeout 240
 script dialer cisco_default
 refuse-message ^CCCCCCC!!! All lines are busy, try again later ###^C
 modem InOut
 modem autoconfigure type mica
 transport preferred telnet
 transport input all
 transport output pad telnet rlogin udptn
line aux 0
line vty 0 4
!
end

```

## A.2 Router AAA Command Implementation Descriptions

Configurations addressed in this section focus on router administration configurations. Router administration configurations cause functions to run within the router shell. Examples include commands executed from a the router console, commands executed with a VTY connection, and a shell-initiated session established using a modem. Each is an example of an EXEC function. Table A-1 provides commands relevant for a router in a Cisco IOS AAA environment.

Table A-1 Cisco IOS Commands Required to Set AAA for a Router

Cisco IOS Command	Description/Application Comment
<b>tacacs-server key</b> <i>secret-key</i>	Specifies encryption key; must be the same in AAA server.
<b>aaa new-model</b>	Enables AAA. Forces an implicit login authentication default against all lines/console interfaces and an implicit <b>ppp authentication pap default</b> against all PPP interfaces.
<b>aaa authentication login default group tacacs+</b>	Causes router to forward all login requests to AAA server.
<b>aaa authorization exec default group tacacs+ if-authenticated</b>	Use default list for authorization to verify <b>service=shell</b> attribute is assigned to user and download appropriate shell attributes assigned in AAA server.
<b>aaa authorization commands 15 default group tacacs+ if-authenticated</b>	Use command authorization for privilege level 15 commands that must be assigned to router users for successful operation of these commands.
<b>aaa accounting exec default start-stop group tacacs+</b>	Logs EXEC shell information for user profile in <b>start-stop</b> TACACS+ format.
<b>aaa accounting commands 15 default stop-only group tacacs+</b>	Sends TACACS+ accounting stop record at the end of a privilege level 15 command.
<b>aaa accounting system default stop-only group tacacs+</b>	Performs accounting for all system level events not associated with users, such as reloads in <b>stop-start</b> TACACS+ format.
<b>ip tacacs source-interface</b> <i>FastEthernet0/0/0</i>	Specifies this interface IP address for management in the AAA server.
<b>ip http server</b>	Enables HTTP server access.
<b>ip http authentication aaa</b>	Forces AAA authentication and authorization at privilege level 15.
<b>tacacs-server host</b> <i>IP-address</i>	Specifies AAA server.

## A.3 NAS AAA Command Implementation Descriptions

Configurations addressed in this section focus on AAA with PPP. These configurations differ from router administration configurations. PPP is a *network* level function and is separate from router shell functions. You can configure PPP to be initiated automatically or you can initiate PPP with a terminal window after dialing in to a NAS. Table A-2 lists commands relevant for a NAS providing PPP access a Cisco IOS AAA environment.



Note

The following table lists Cisco IOS configuration commands required to support both TACACS+ and RADIUS AAA implementations.

Table A-2 Cisco IOS Commands Used to Set AAA with PPP for NAS (RADIUS and TACACS+)

IOS Command	Description/Application Comment
<b>aaa new-model</b>	Enables authentication, authorization, and accounting. Forces an implicit login authentication default against all lines/console interfaces and an implicit <b>ppp authentication pap default</b> against all ppp interfaces.
<b>aaa authentication login default group tacacs+</b>	Causes router to forward all login requests to a TACACS+ server.
<b>aaa authentication login default group radius</b>	Causes router to forward all login requests to a RADIUS server.
<b>aaa authentication ppp default if-needed group radius</b>	Use default list for PPP authentication; the <b>if-needed</b> keyword allows clients using “Terminal Window after Dial” option to successfully authenticate to RADIUS server and negotiate PPP, without using Windows dialup networking username and password combination.
<b>aaa authentication ppp default if-needed group tacacs+</b>	Use default list for PPP authentication; the <b>if-needed</b> keyword allows clients using “Terminal Window after Dial” option to successfully authenticate to TACACS+ server and negotiate PPP, without using Windows dialup networking username and password combination.
<b>aaa authorization exec default group radius if-authenticated</b>	Use default list to verify authorization.
<b>aaa authorization exec default group tacacs+ if-authenticated</b>	Use default list for authorization to verify <b>service=shell</b> attribute is assigned to user and download appropriate shell attributes assigned in AAA server.
<b>aaa authorization network default group tacacs+ if-authenticated</b>	Use default list for authorization to verify <b>service=-ppp</b> attribute is assigned to user or group and download appropriate PPP attributes assigned in AAA server. Command specifies that authorization is only permitted if user or group is properly authenticated through TACACS+.
<b>aaa authorization network default group radius if-authenticated</b>	Use default list for authorization to verify <b>Service-Type=Framed</b> attribute is assigned to user or group and download appropriate PPP attributes assigned in AAA server. Command specifies that authorization is only permitted if user or group is properly authenticated through RADIUS.
<b>aaa accounting exec default start-stop group tacacs+</b>	Logs EXEC shell information for user profile in <b>start-stop</b> TACACS+ format.
<b>aaa accounting network default start-stop group tacacs+</b>	Logs all network related services requests, such as PPP in <b>stop-start</b> TACACS+ format.
<b>aaa accounting exec default start-stop group radius</b>	Logs EXEC shell information for user profile in <b>start-stop</b> RADIUS format.
<b>aaa accounting network default start-stop group radius</b>	Logs all network related services requests, such as PPP in <b>stop-start</b> RADIUS format.

Table A-2 Cisco IOS Commands Used to Set AAA with PPP for NAS (RADIUS and TACACS+)

IOS Command	Description/Application Comment
<b>tacacs-server host</b> <i>IP-address</i> <b>key</b> <i>secret-key</i>	Specifies AAA server. Specifies encryption key; must be the same in AAA server.
<b>radius-server host</b> <i>IP-address</i> <b>auth-port 1645</b> <b>acct-port 1646</b> <b>key</b> <i>secret-keys</i>	Specifies RADIUS AAA server IP address by using default UDP Port 1645 for authentication and authorization and UDP Port 1646 for accounting.

## A.4 CiscoSecure for UNIX Configuration Listings

This section provides the following listings:

- A.4.1 CSU.cfg Listing
- A.4.2 CSConfig.ini Listing
- A.4.4 listener.ora Listing
- A.4.3 Oracle User Environment Variable

For a complete description of AAA server files, go to:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/cs\\_unx](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx)

## A.4.1 CSU.cfg Listing

```

# cd /opt/ciscosecure/config
# ls
CSConfig.ini  CSU.cfg      CSU.cfg.sav
# cat CSU.cfg
LIST config_license_key = {"a73dc113d300a5ba3459"};
STRING config_update_log_filename = "/opt/ciscosecure/logfiles/passwd_chg.log";
/* store accounting records here when database fails */
/* default = /var/log/CSAccountingLog */
STRING config_acct_filename = "/var/log/CSAccountingLog";

/* AAA Server Metrics */
/* default = 0 (disable) */
NUMBER config_metrics_enable = 0; /* 1 to enable, 0 to disable */
/* default = 8 seconds */
NUMBER config_metrics_log_interval = 8; /* in seconds */

/* Callerid as Username */
/* default = 1 (enable) */
NUMBER config_callerid_enable = 1; /* 1 to enable, 0 to disable */

/* Use default user profile when user/callerid can't be found */
/* default = 1 (enable) */
NUMBER config_defaultuser_enable = 1; /* 1 to enable, 0 to disable */

/* AAA Server MaxSessions Configuration */
/* default = 0 (disable) */
NUMBER config_maxsessions_enable = 0; /* 1 to enable, 0 to disable */
/* default = 24 hours */
NUMBER config_maxsessions_session_timeout = 1440; /* in minutes */
/* default = 60 minutes */
NUMBER config_maxsessions_purge_interval = 60; /* in minutes */

/* AAA Server Distributed MaxSessions Configuration */
/* default = 0 (disable) */
NUMBER config_distmaxsessions_enable = 0; /* 1 to enable, 0 to disable */
/* default = 0 (disabled) */
NUMBER config_dms_periodic_stats_interval = 0; /* 0 to disable, otherwise interval in seconds */

/* Cryptocard challenge lookahead */
/* default = 0, which is same as 1, do only 1 challenge, don't look ahead */
/* the maximum number of challenge look ahead is 20 */
NUMBER config_cryptocard_challenge_lookahead = 0;

/* Group Profile Cache Timeout; 0 == no timeout */
/* default = 5 seconds */
NUMBER config_cache_group_timeout = 5; /* in seconds */

/* Per-user accounting function */
/* default = 1 (enable) */
NUMBER config_acct_fn_enable = 1; /* 1 to enable, 0 to disable */

/* Extended Radius support */
NUMBER config_hex_string_support_enable = 0; /* 1 to enable, 0 to disable */

STRING config_server_ip_address = "172.23.25.41";
NUMBER config_token_cache_absolute_timeout = 86400;
NUMBER config_system_logging_level = 0x80;
NUMBER config_logging_configuration = 0xffffffff;
NUMBER config_warning_period = 20;
NUMBER config_expiry_period = 60;

```

```

NUMBER config_local_timezone = -8;          /* set this for your timezone */
NUMBER config_use_host_timezone = 0;        /* set value to 1 to always use system time
*/
NUMBER config_record_write_frequency = 5;   /* update frequency in seconds */
NUMBER config_max_failed_authentication = 10; /* nmbr of authen fails accepted *
/
/* before account is disabled. *
/

NAS config_nas_config = {
  {
    "", /* NAS name can go here */
    "ciscorules", /* NAS/CiscoSecure secret key */
    "", /* message_catalogue_filename */
    1, /* username retries */
    2, /* password retries */
    1 /* trusted NAS for SENDPASS */
  }
};

AUTHEN config_external_authen_symbols = {
  {
    "./libskey.so",
    "skey"
  }
  ,
  {
    "./libpap.so",
    "pap"
  }
  ,
  {
    "./libchap.so",
    "chap"
  }
  ,
  {
    "./libarap.so",
    "arap"
  }
};

AUTHOR config_external_author_symbols = {
  {
    "./libargs.so",
    "process_input_arguments",
    "process_input_arguments_ok",
    "process_input_arguments_fail",
    "process_output_arguments",
    "process_output_arguments_ok",
    "process_output_arguments_fail"
  }
};

/*
 * Sample of pre/post process configuration.
 *
AUTHOR config_external_author_symbols = {
  {
    "./libcustomerprovided.so",
    "customer_function"
  }
};
*

```

```
* end sample
*/

ACCT config_external_acct_symbols = {
    {
        "./libacctmember.so",
        "acct_member_fn"
    }
};

ADMIN config_external_admin_symbols = {
    "./libadmin.so"
};

DB config_external_database_symbols = {
    {
        "./libdb.so",
        "",
        ""
    }
};

PARSER config_external_parser_symbols = {
    "./libt+.so"
};

EVENT config_external_event_symbols = {
    {
        "./libdb.so",
        "",
        ""
    }
};

DMS config_external_dms_symbols = {
    "./libCiscoDMS.so"
};
#
#
```

## A.4.2 CSConfig.ini Listing

```

#
#cat CSConfig.ini
#####
#
# $Archive: $
#
# (C) Copyright 1996 Cisco Systems. All rights reserved.
#
# This is CiscoSecure DBServer main initialization file.
#
# $Log: $
#
# $NoKeyWords: $
#
#####
;----- Ruler Line ----->
;      1      2      3      4      5      6      7      8
;234567890123456789012345678901234567890123456789012345678901234567890
;
;-----
[System]
; Location where the system is installed
RootDir=/opt/ciscosecure

; Location of the default profile (default= $RootDir/config/DefaultProfile)
DefaultProfile=/opt/ciscosecure/config/DefaultProfile

;-----
[System Error]
SysErrorFileDir = /opt/ciscosecure/logfiles
; DBServer gets the default path for System error handler here
; if it was not specified at command line with option
; [-LOGPATH path] when starting the DBServer daemon.
; DBServer must have sufficient access privilege to create this
; path and the log file if it does not already exist.

; log levels are 1 thru 10 where Minor=1, Moderate=5, Severe=8, Catastrophic=10
; (note: Catastrophic errors will shutdown the daemon)
MinLogLevel = 8

;-----
[SessionMgr]
; Session Manager configurables, purge interval is in minutes
MaxSessions=1000
PurgeInterval=60

;-----
[AccountingMgr]

;If this parameter=enable then log acct packets into cs_accounting_log database
table
LogRawAccountingPacketToDB = enable

;If we are logging accounting records then this parameter decides whether to buffer the
records
; in memory and then save them to the database using a background process. Enabl
ing this will
; increase burst authentication performance.
;If enabled the DBServer will create enough buffers to match the value of 2 less
than
; the number of database connections available.

```

```

; NOTE: There is a risk of losing records that are in memory in the event of the
DBServer going
;       down ungracefully.
BufferAccountingPackets = enable

;This parameter decides the size of each accounting packet buffer. Legal values
are from 5 to 1000
AccountingBufferSize = 500

; if parameter=enable then dbserver will process user max session info and save
in memory,
; if disabled then ArchiveMaxSessionInfoToDB will also be disabled.
ProcessInMemoryMaxSessionInfo = enable

; If this parameter=enable then log user max session info into cs_user_accounting
database table
; Note that if the BufferAccountingPackets parameter is enabled AND
ProcessInMemoryMaxSessionInfo
; is enabled then max session info records will be buffered as well.
ArchiveMaxSessionInfoToDB = enable

; This is how often (in minutes) the system checks for accounting sessions to
; purge.
; NOTE: The purge interval is actually dependant upon a system background task
;       that is not guaranteed to run more frequently than 60 minutes. This
;       value is therefore not accurate to the minute and should not be set to
;       less than 60.
AcctPurgeInterval=60

; This is how long (in minutes) a session can be considered
; active before it is purged.
; NOTE: This value is dependent on the AcctPurgeInterval setting and is not
;       accurate to the minute. It is not intended to be set to less than 60.
AcctPurgeTimeOut=1440

;-----
[DBServer]
DBServerName = CSdbServer
Protocol=TCP
MaxPacketSize = 4096

; Each DBServer process should have it's own unique name.
; Do not put the hostname here in case more than one instance
; of the DBServer is running on the same machine

;The following is for internal use only by the DBServer
;Date format expected from the client application such as the GUI,
;to be used for parsing date/time string. The dbserver will reject
;inputs that contains other date/time format. This format will also
;be used to return date/time strings.
;Examples, "d MMM yyyy" => "12 Feb 1997", "EEE MMM d hh:mm:ss z yyyy" => "Tue Ap
r 1 09:26:55 PST 1997"
DateFormat = "d MMM yyyy"
DateTimeFormat = "EEE MMM d hh:mm:ss z yyyy"

;-----
[ValidClients]
100 = sleddog
; Add list of trusted clients above ^^^^ in the format:
;   ClientID = Client's Host Name
;   CGI stub's clientID=100, and it's host name
;   For example 100 = localhost or 100 = 192.92.182.2
;
;               101 = 192.92.190.5
;

```

```
;if ValidateClients=true, then we only allow the clients with ids listed
;above to connect to the dbserver
ValidateClients = false
;if FastAdminValidateClients = true, then we only allow the clients with ids
;listed below to connect to the FastAdmin
FastAdminValidateClients = false

;-----
[Protocol TCP]
HostName = sleddog
Port = 9900
; Name of host server

; Daemon port number
;Port=5001

;-----
[Workers Pool]
; Maximum numbers of connection workers in pool, beyond which
; newly added workers will be ignored (or deleted).
MaxInPool=50

;-----
[Database]
DataSource = ORACLE
DriverType = JDBC-Weblogic-Oracle
; Specify the rdbms installed and the driver type
; (ODBC or JDBC) that interfaces with the rdbms.
; Driver=ODBC or Driver=JDBC, then go to the [ODBC]
; or [JDBC] section to fill in the URL info.

# Oracle with ODBC
;DataSource = ORACLE
;DriverType = ODBC-Visigenic-Oracle

# Oracle with JDBC
;DataSource = ORACLE
;DriverType = JDBC-Weblogic-Oracle

# SQLAnywhere with ODBC
;DataSource = SQLAnywhere
;DriverType = ODBC-SQLAnywhere

# Sybase with ODBC
;DataSource = SYBASE
;DriverType = ODBC-Visigenic-Sybase

# Sybase with JDBC
;DataSource = SYBASE
;DriverType = JDBC-Weblogic-Sybase

# Test with some other DB that we did not qualify
;DataSource = OtherDB
;DriverType = ODBC-Visigenic

# names of data dictionary
ProfileAttr = cs_profile_attr_dict
ProfileCol = cs_profile_col_dict
UserAcct = cs_user_account_attr_dict

;-----
[SQLAnywhere]
;this is the bundle database
ConnectionLicense = 12
```

```

Username = DBA
Password = SQL

;-----
[OtherDB]
;number of open connections allowed to the data source(based on db license)
ConnectionLicense = 1
Username = csecure
Password = csecure

;-----
[ORACLE]
;number of open connections allowed to the data source(based on db license)
ConnectionLicense=4
Username = csecure
Password = csecure

;-----
[SYBASE]
;number of open connections allowed to the data source(based on db license)
ConnectionLicense = 8
Username = csecure
Password = csecure

;-----
[ODBC-SQLAnywhere]
;ODBC driver information
Manager = sun.jdbc.odbc.JdbcOdbcDriver
Driver = jdbc:odbc:SQLAnywhere;ENG=csecure;DBF=<database_file>;Start="dbeng50 -u
d"
;Property below is required for internal use only: connection usage property
PrepareStatement = 0

;-----
[ODBC-Visigenic-Oracle]
;ODBC driver information
Manager = sun.jdbc.odbc.JdbcOdbcDriver
Driver = jdbc:odbc:Oracle
;Property below is required for internal use only: connection usage property
PrepareStatement = 1

;-----
[ODBC-Visigenic-Sybase]
;ODBC driver information
Manager = sun.jdbc.odbc.JdbcOdbcDriver
Driver = jdbc:odbc:SybaseDBLib
;Property below is required for internal use only: connection usage property
PrepareStatement = 1

;-----
[JDBC-Weblogic-Oracle]
;JDBC driver information
Manager=cisco.ciscosecure.dbserver.jdbc.WeblogicOciDriverManager
Driver=jdbc:weblogic:oracle:ciscosj
;Property below is required for internal use only: connection usage property
PrepareStatement = 1

;-----
[JDBC-Weblogic-Sybase]
;JDBC driver information
Manager=cisco.ciscosecure.dbserver.jdbc.WeblogicDBLibDriverManager
Driver=jdbc:weblogic:sybase
;Property below is required for internal use only: connection usage property
PrepareStatement = 1

```

```
-----  
[ProfileCaching]  
EnableProfileCaching = OFF  
;Polling period in minutes for cs_trans_log table  
; Interval in seconds can be specified by fraction.  
; For example, '5/60' denotes 5 seconds and '1 1/2' denotes 90 seconds.  
; Setting to 0 disables polling.  
DBPollInterval = 30  
-----
```

## A.4.3 Oracle User Environment Variable

```
#su - oracle  
Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996  
$env  
HOME=/export/home/oracle  
HZ=100  
LD_LIBRARY_PATH=/opt/oracle/product/7.3.4/lib:/usr/openwin/lib:/usr/dt/lib:/usr/  
lib  
LOGNAME=oracle  
ORACLE_DOC=/doc  
ORACLE_HOME=/opt/oracle/product/7.3.4  
ORACLE_SID=ciscosj  
ORACLE_TERM=xsun5  
ORAENV_ASK=NO  
PATH=/usr/bin:/opt/oracle/product/7.3.4:/opt/oracle/product/7.3.4/bin:/usr/ccs/  
bin:  
SHELL=/bin/sh  
TERM=ansi  
TMPDIR=/var/tmp  
TNS_ADMIN=/opt/oracle/product/7.3.4/network/admin  
TZ=GMT-8
```

## A.4.4 listener.ora Listing

```

$cd $ORACLE_HOME/
$ls
bin      jdbc      nlsrtl3  orainst  precomp  sqlplus
book22   lib        ocommon  otrace   rdbms    svrmgr
dbs      network   oracore3 plsqli    slax
$cd network/admin
$ls
csmgen.tcl  listener.ora  tcl7.4      tnsnames.ora
csmman.man  sqlnet.fdf    tk4.0
$cat listener.ora
#
# Installation Generated Net V2 Configuration
# Version Date: Sep-16-97
# Filename: Listener.ora
#
LISTENER =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL= IPC) (KEY= ciscosj))
    (ADDRESS= (PROTOCOL= IPC) (KEY= PNPKEY))
    (ADDRESS= (PROTOCOL= TCP) (Host= sleddog) (Port= 1521))
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME= sleddog.)
      (ORACLE_HOME= /opt/oracle/product/7.3.4)
      (SID_NAME = ciscosj)
    )
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
TRACE_LEVEL_LISTENER = OFF
$ls
csmgen.tcl  listener.ora  tcl7.4      tnsnames.ora
csmman.man  sqlnet.fdf    tk4.0
$cat tnsnames.ora
#
# Installation Generated NetV2 Configuration
# Version Date: Sep-30-97
# Filename: Tnsnames.ora
#
ciscosj =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL= TCP) (Host= sleddog) (Port= 1521))
    (CONNECT_DATA = (SID = ciscosj))
  )

```

## A.5 CiscoSecure Log Files

```
$CSUBASE/logfiles/cs_install.log  
$CSUBASE/logfiles/cs_shutdown.log  
$CSUBASE/logfiles/cs_startup.log  
$CSUBASE/logfiles/csdblog_<date>  
$CSUBASE/logfiles/passwd_chg.log  
$CSUBASE/ns-home/CSUserver/logs/access  
$CSUBASE/ns-home/CSUserver/logs/errors  
$CSUBASE/ns-home/admserver/errors  
$CSUBASE/ns-home/admserver/access  
$CSUBASE/ns-home-httpd-csuserver/logs
```

