



CHAPTER 4

Configuring and Maintaining a Remote Agent

This chapter provides information about configuring and maintaining a Cisco Secure Access Control Server (ACS) Remote Agent, for Windows or Solaris.

This chapter contains:

-
- [Maintaining a Remote Agent](#)

Configuring a Remote Agent

You do all manual configuration of ACS Remote Agent by configuring the *CSAgent.ini* file.

[CSAgent.ini Location](#)

[CSAgent.ini Settings](#)

[Sample CSAgent.ini](#)

[Changing CSAgent.ini Settings](#)

CSAgent.ini Location

C:\Program Files\Cisco\CiscoSecure ACS Agent

CSAgent.ini

/opt/CSCOacsag

CSAgent.ini

For more information about the directory structure that results when you install a remote agent, see [File and Directory Structure](#).

CSAgent.ini Settings



The restrictions that the `PermittedClients` value imposes override restrictions that the CSLog Agent or `PermittedClients` values impose. ACS SEs with IP addresses not included in the `PermittedClients` value in the `PermittedClients` section are always denied remote agent services; even if you included the IP addresses in the `PermittedClients` values of the `PermittedClients` or `PermittedClients` sections.

In each IP address that you specify, you have three options for each octet in the address:

- **Number**—You can specify a number, for example, 10.3.157.98.

Numeric Range

Wildcard—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

As a further example, the `PermittedClients` value can use these options in each IP address in its list:

```
PermittedClients=10.3.157.10-50,10.3.157.52,10.3.158.*
```

Executable

CSAgent.exe

CSLogAgent

CSAgent.exe

records. The default value is 2006.

—The TCP port that `CSLogAgent` listens to for accounting records from ACS SEs. The default value is 2007.

—A comma-separated list of IP addresses from which `CSLogAgent` will accept requests. This setting is disabled by default, which has the effect of a `PermittedClients` value of `*`. If you enable this option, the remote agent provides logging services only to appliances whose IP addresses are included in the list of IP addresses. If you also enable the `PermittedClients` value in the `PermittedClients` section, the `PermittedClients` value provides a means to restrict the remote agent logging service to a subset of the IP addresses specified in the `PermittedClients` value.



You cannot use the `PermittedClients` value to permit an IP address that the `PermittedClients` value does not permit.

In each IP address you specify, you have three options for each octet in the address:

—You can specify a number, for example, 10.3.157.98.

—You can specify the low and high numbers of the range in the octet, if you separate them with a hyphen (-); for example, 10.3.157.10-50.

—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

CSUnixOutput

CSLogAgent records logs in comma-separated value (CSV) format or in the format that ACS Remote Agent for Solaris uses.



The CSUnixOutput option is applicable only to ACS Remote Agent for Solaris. The CSUnixOutput option does not exist in the _____ file of a Windows remote agent.

The only valid values for this option are:

0—Zero (0) specifies that the remote agent records logs in CSV format and that log filenames end with *.csv*

```
Date,Time,User-Name,Acct-Status-Type  
11/26/2003,10:48:36,jwiedman,Start
```

1

attribute recorded, an equal sign (=), and the attribute value. Two blank lines separate records. An abbreviated example of a single record in CSUnix format is:

```
Tue Nov 26 10:48:36 2003  
User-Name = "jwiedman"  
Acct-Status-Type = Start
```



```
.  
*.*.*.*
```



PermittedClients=10.3.157.10-50,10.3.157.52,10.3.158.*

Sample CSAgent.ini

```
[CSAgent]

; This is the main service's configuration section...
; To change the local port:
; Port=2004

; To set the config provider hostname/IP address:
; ConfigProviderHost=servername
; or
; ConfigProviderHost=127.0.0.1
ConfigProviderHost=192.168.1.102

; To set the config provider port:
ConfigProviderPort=2003

; To define the list of agents to activate:
;Agents=CSLogAgent,CSWinAgent
Agents=CSWinAgent

; To define a list of permitted clients
; PermittedClients=192.168.1.*,10.49.*.*

[CSLogAgent]

; This is the log agent's configuration section...
; Name of the agent's executable:
Executable=..\CSLogAgent\CSLogAgent.exe

; To change the local port:
Port=2006

; To change the accounting port:
AccountingPort=2007

; PermittedClients=192.168.1.*,10.49.*.*

; Use CSUnix output format
; possible values: 0 - csv, 1 - CSUnix format
; default is no (0)
; This option doesn't exist in a Windows remote agent CSAgent.ini file
CSUnixOutput=1

[CSWinAgent]

; This is the Windows agent's configuration section...
; This section doesn't exist in a Solaris remote agent CSAgent.ini file
```

```
; Name of the agent's executable:
Executable=..\CSWinAgent\CSWinAgent.exe

; To change the local port:
Port=2005

; PermittedClients=192.168.1.*,10.49.*.*
```

Changing CSAgent.ini Settings

Before You Begin

Step 1 By using an ASCII text editor, open the _____ file for the remote agent that you want to configure.



Tip

Step 2



Note

sudo vi CSAgent.ini

Step 3

Step 4



Note

Maintaining a Remote Agent

-
-
-
-
-

Stopping and Starting Remote Agent Services

Before You Begin

Step 1

Step 2

Step 3

```
net stop csagent
```

```
net start csagent
```



```
/etc/init.d/csagent stop
```



```
kill
```

```
ps -ef | grep "CS[AL]"
```

```
/etc/init.d/csagent start
```



```
/opt/CSCOacsag/CSAgent/CSAgent &
```

File and Directory Structure

-
-
-
-
-

Backup and Restore

DBReplicate

DbSync—Contains CSV files for RDBMS Synchronization logs.

- **Failed Attempts**
- Passed Authentications**
- RADIUS Accounting**
- ServiceMonitoring**
- TACACS+ Accounting**—Contains CSV files for TACACS+ Accounting logs.
- TACACS+ Administration**—Contains CSV files for TACACS+ Administration logs.
- VoIP Accounting**
- PasswordLogs**

Support

CSLogAgent

ACS SE includes a feature called Support, in the System Configuration section of the HTML Interface. When you select the Run Support Now option on the Support page of an appliance that you configured to use a remote agent for any service, the appliance instructs the remote agent to collect copies of its diagnostic logs. The Windows agent produces a cabinet file containing the log files. The Solaris agent produces a file containing the log files.

The remote agent places the resulting support file directly under the Remote Agent installation directory. The file name includes the date and time. When a new one is created previous support files are not overwritten.

To retrieve the support file, on the computer running the remote agent, access the Remote Agent installation directory. For more information about the directory structure under the installation directory, see [File and Directory Structure](#).

Running CSAgent in Debug Mode

Windows



CSAgent.exe

CSAgent.exe

Step 5

```
csagent.exe -z -p
```



```
csagent.exe -v
```

Step 6

Step 1



Tip

Step 2

```
/etc/init.d/csagent stop
```



Tip

```
ps -ef | grep "CS[AL]"
```

Step 4



Step 5



Sample CSAgent Debug Output

-
-

Sample Debug Output for a Windows Remote Agent

```
D:...\\CSAgent 33: csagent -p -z
Debug printing on..
Running CSAgent server from command line..
CSAgent server starting =====
Running as console application.
Will listen on port 2004
Configuration will be fetched from 192.168.12.208:2003
Agents: CSLogAgent,CSWinAgent
CSLogAgent File: ..\\CSLogAgent\\CSLogAgent.exe
CSLogAgent Port: 2006
```

```
CSWinAgent File: ..\CSWinAgent\CSWinAgent.exe
CSWinAgent Port: 2005
2 agents configured
Permitted CSAgent Clients: 192.168.12.1-127
Hit Return/Enter to stop...
```

```
Watchdog activated
Listener activated
CSLogAgent launched
CSWinAgent launched
```

```
Service stopping
Shutting down EndPoint library
Listener terminating
```

```
CSLogAgent server starting =====
Running as console application.
Configuration will be fetched from 192.168.12.208:2003
Permitted CSLogAgent Clients: *.*.*
Cant get max number of connections maxNumberOfConnections using default 32
Agent library initialisedAgentLib: Attempting to connect to config provider at
192.168.12.208:2003
AgentLib: Connection established, handle 0x7e4af8
AgentLib: GetLogConfig reply received
AgentLib: Disconnecting from config provider, handle 0x7e4af8
Config downloaded
Will listen on port 2007
Will not log to a datafile.
Stream thread started
Stream waiting for connection
Will use the Loglib library.
Listening thread started...
```

```
CSWinAgent server starting =====
Running as console application.
Will listen on port 2005
Permitted CSWinAgent Clients: *.*.*
NTLIB: Library behaviour mode 2
NTLIB: Initialising locally
NTLIB: The local computer name is ENG-IIS-WEST2
NTLIB: We are NOT a domain controller
NTLIB: We are a member of the ENGINEERING domain
Listener activated
```

```
cmi-xdm5:5> CSAgent -z -p
Running CSAgent server from command line..
Debug printing on..
CSAgent server starting =====
Running as console application.
Will listen on port 2004
Configuration will be fetched from 192.168.12.208:2003
Agents: CSLogAgent
CSLogAgent File: /opt/CSCOacsag/CSLogAgent/CSLogAgent
```

```
CSLogAgent Port: 2006
1 agents configured
Permitted CSAgent Clients: *.*.*
Listener activated
Hit Return/Enter to stop...

Watchdog activated
check_sys_limits set max file descriptors to 1024
Running CSLogAgent server from command line..
CSLogAgent server starting =====
Running as console application.
Configuration will be fetched from 192.168.12.208:2003
Permitted CSLogAgent Clients: *.*.*
Cant get max number of connections maxNumberOfConnections using default 32
CreateProcess cd /opt/CSCOacsag/CSLogAgent; /opt/CSCOacsag/CSLogAgent/CSLogAgent -z & pid
= 8686
CSLogAgent launched
Agent library initialised
AgentLib: Attempting to connect to config provider at 192.168.12.208:2003
AgentLib: Connection established, handle 0x916c8
AgentLib: GetLogConfig reply received
AgentLib: Disconnecting from config provider, handle 0x916c8
Config downloaded
Will listen on port 2007
Will not log to a datafile.
g_started_ok=1
Listening thread started...

Rollover on /opt/CSCOacsag/Logs/Failed Attempts\Failed Attempts active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/RADIUS Accounting\RADIUS Accounting active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/TACACS+ Accounting\TACACS+ Accounting active.csv reset to
manual.
Rollover on /opt/CSCOacsag/Logs/TACACS+ Administration\Tacacs+ Administration active.csv
reset to manual.
Will use the Loglib library.
Stream thread started
Stream waiting for connection

Service stopping
Shutting down EndPoint library
Watchdog done. send kill to 8714
```

