

Prison Communication Systems Pty Ltd (Austco) CellGuard

Device Driver Specification

13/03/2018



Table of Contents

1	Document Versions.....	4
2	Referenced Documents.....	4
3	Overview	5
4	Manufacturer	5
5	IPSecurityCenter Versions.....	6
6	Operating Systems	6
6.1	Client Side Functionality	6
6.2	Server Side Functionality	6
7	Models / Firmware Versions.....	6
8	Hardware Configuration	7
9	Driver Package	8
10	Driver Features.....	9
10.1	CellGuard Server	9
10.1.1	Device Connection and Online States.....	9
10.1.2	Properties.....	9
10.1.3	Methods.....	9
10.1.4	Events.....	10
10.2	BaseStation	10
10.2.1	Device Connection and Online States.....	10
	DC1.0 Device Online Status.....	10
	DC2.0 Authentication.....	10
10.2.2	Properties.....	10
	Base Station Name.....	10
10.2.3	Methods.....	10
10.2.3.1	MakeCall.....	10
10.2.3.2	DropCall.....	11
10.2.3.3	HoldCurrent.....	11
10.2.3.4	RecoverLastCall	12
10.2.3.5	PACallPoints	12
10.2.3.6	PATerminate	13
10.2.4	Events.....	13
10.2.4.1	CallStateChanged	13
10.2.4.2	TamperState.....	14

10.3	CallPoint	15
10.3.1	Device Connection and Online States.....	15
	DC1.0 Device Online Status.....	15
	DC2.0 Authentication.....	15
10.3.2	Properties.....	15
	Callpoint Name.....	15
	Parent Station	15
10.3.3	Methods.....	15
10.3.4	Events.....	15
	10.3.4.1 CallStateChanged	15
	10.3.4.2 CallPointRequest	16
	10.3.4.3 TamperState.....	17
11	Installation	18
11.1	Prerequisites	18
11.2	Driver Installation.....	18
	11.2.1 Device Configuration.....	18
	11.2.1.1 System Topology	18
	11.2.1.2 Driver Configuration.....	19
	11.2.2 Driver Compatibility	19
Appendix A	Notes and Observations.....	20
Appendix B	CSV file example.....	22

1 Document Versions

Version	Date	Name	Change
1.0	2018-05-04	AM	Document Created.
1.1	2018-12-06	GD	Minor updates and corrections.
1.2	2018-12-10	AM	Clarification on events raised on end of call
1.3	2018-12-11	AM	Additional clarification on call events.
1.4	2019-03-13	AM	Review and minor revisions

2 Referenced Documents

Document	Version	Description
Driver Project Requirements (DDK-PR)	1.0	The Prison Communication Systems Pty Ltd CellGuard driver must conform to all the requirements detailed in this document.
Driver Connection and Online States Requirements (DDK-DC)	1.0	The Prison Communication Systems Pty Ltd CellGuard driver must conform to all requirements in this document detailed in the section: Device Connection and Online States
Driver Specification – Austco CellGuard		Driver Specification

3 Overview

CellGuard is an intercommunications system that consist of a central monitoring Server, with an array of base stations each with an associated set of child callpoints.

Callpoints can request communications with a basestation, with any basestation in the system responding to the request and initiating a link to the callpoint.

Public address functionality is provided, but only between a basestation and its child callpoints, the system does not permit system wide callpoint address.

See Section 8 below

4 Manufacturer

Name Prison Communication Systems Pty Ltd



Website <https://cellguard.net.au/>

Description CellGuard is a intercommunication security system for custodial care solutions,

5 IPSECURITYCENTER Versions

The driver must be compatible with the following IPSECURITYCENTER versions:

IPSECURITYCENTER Version	Supported
5.3	<input checked="" type="checkbox"/>

6 Operating Systems

6.1 Client Side Functionality

Operating Systems	Supported
-------------------	-----------

N/A

6.2 Server Side Functionality

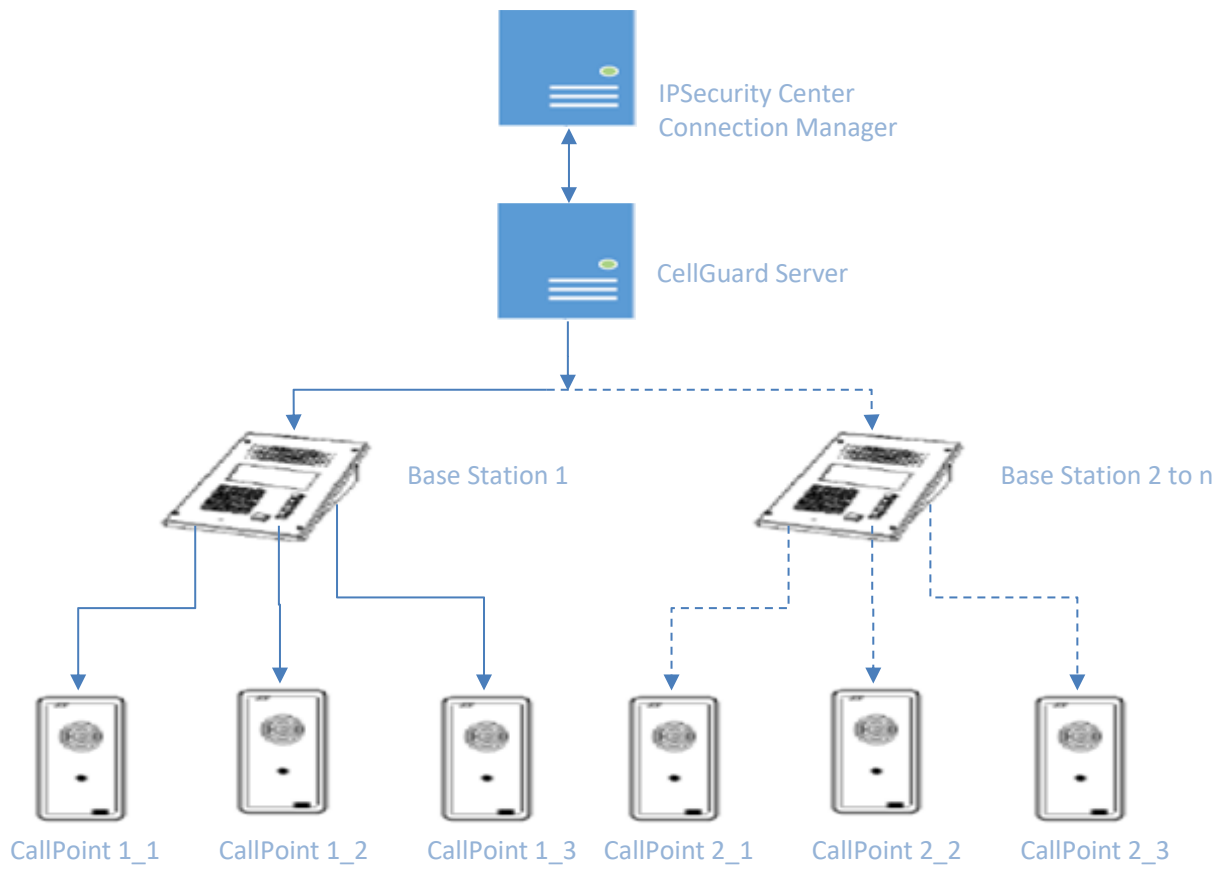
Operating Systems	Supported
Windows Server 2008 R2	<input checked="" type="checkbox"/>
Windows Server 2012	<input checked="" type="checkbox"/>

7 Models / Firmware Versions

Model	Versions	SDK
-------	----------	-----

N/A

8 Hardware Configuration



9 Driver Package

The driver package is named:

CNL.IPSecurityCenter.Driver.Austco.CellGuard.Version.[BUILD-VERSION].ipsedriver

10 Driver Features

10.1 CellGuard Server

10.1.1 Device Connection and Online States

The full requirements for these features can be found in the [Device Connection and Online States Requirements](#)

Feature	
Device Online Status	Ping
Authentication	None

10.1.2 Properties

General requirements for properties can be found in [Driver Project Requirements](#).

Name	Type	Description	Default Value & Ranges
TopographyFilePath	string	Path to the CellGuard system device topography	Default: Min: Max:
Server Name	string	Name of the root server	Default: Min: Max:
Service feedback Response time	int	Maximum time to wait for a command response from the CellGuard Server	Default: 30000 Min: Max:
Enable debug logging output	bool	Provide additional information into the loupe logs for issue diagnosis	Default: false

10.1.3 Methods

General requirements for methods can be found in [Driver Project Requirements](#).

The CellGuard Server does not implement any unique callable methods.

10.1.4 Events

10.1.4.1.1 Site Error

This event is raised when the server detects an error in the system

Name	Type	Description
Message	String	Indication of the detected issue within the system
Time event raised	string	Time at which the state change occurred
Time event cleared	string	Time at which the issue was reported as cleared, will be blank when issue is first detected and only set when issue is cleared.

10.2 BaseStation

10.2.1 Device Connection and Online States

The full requirements for these features can be found in the [Device Connection and Online States Requirements](#)

Feature	
DC1.0 Device Online Status	None
DC2.0 Authentication	None

10.2.2 Properties

General requirements for properties can be found in [Driver Project Requirements](#).

Name	Type	Description	Default Value & Ranges
Base Station Name	string	Base Station Name	N/A

10.2.3 Methods

General requirements for methods can be found in [Driver Project Requirements](#).

10.2.3.1 MakeCall

Creates a communications link between the selected basestation and a specified callpoint

Operator Action: true

Returns bool.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
callPoint	string	Name of the callpoint to connect to.	N/A
covertConnection	bool	Flag to indicate if the callpoint should announce the connection with an audio signal.	N/A

10.2.3.2 DropCall

Terminates a communications link between the selected basestation and the currently connected callpoint.

Operator Action: true

Returns bool.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
N/A			

10.2.3.3 HoldCurrent

Remembers the current communications link and initiates new a communications link between the selected basestation and a specified callpoint,.

Operator Action: true

Returns int – Number of calls in the held stack for this base station.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
callPoint	string	Name of the callpoint to connect to.	N/A
covertConnection	bool	Flag to indicate if the callpoint should announce the connection with an audio signal.	N/A

10.2.3.4 *RecoverLastCall*

Terminates the current communications link and reinitiates the last stored callpoint, the call connection is always announced by an audio signal

Operator Action: true

Returns int – Number of calls in the held stack for this base station.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
N/A			

10.2.3.5 *PACallPoints*

Creates a public announcement link between the selected basestation and all its child callpoints

Operator Action: true

Returns bool.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
N/A			

10.2.3.6 *PATerminate*

Terminates the public announcement link between the selected basestation its child callpoints

Operator Action: true

Returns bool.

Performance

The method must complete within 2 seconds.

Parameters

Name	Type	Description	Default Value & Ranges
N/A			

10.2.4 Events

10.2.4.1 *CallStateChanged*

Raised when the state of a connection between this basestation and a callpoint changes.

Note that on hang-up of a connection if the initial connection was raised in response to a request from a callpoint events will be raised for every basestation that was notified of the call request (see 10.3.4.2.)

Name	Type	Description
CallPoint	String	Name of callpoint involved in link

baseStation	string	Name of the basestation involved in link
State	CNL.IPSecurityCenter.Driver.Austco. CellGuard.Enums.CallState	Enumeration indicating the state of the link between the two points, can be one of the following: <ul style="list-style-type: none"> • Failed • Trying • Connecting • Connected • OnHook • Ringing
Description	string	Brief description associated with state change

10.2.4.2 *TamperState*

Event raised on the detection, or clearing of tampering to a BaseStation

Note CellGuard gives no text description of what caused the tamper event.

Name	Type	Description
CallPoint	string	Name of the callpoint That the tampering has been detected/cleared on.
State	CNL.IPSecurityCenter.Driver.Austco .CellGuard.Enums.TamperState	Enumeration indicating the state of the tampering and can be one of the following: <ul style="list-style-type: none"> • Active • Cleared
Time	string	Time at which the state changed

10.3 CallPoint

10.3.1 Device Connection and Online States

The full requirements for these features can be found in the [Device Connection and Online States Requirements](#)

Feature	
DC1.0 Device Online Status	None
DC2.0 Authentication	None

10.3.2 Properties

General requirements for properties can be found in [Driver Project Requirements](#).

Name	Type	Description	Default Value & Ranges
Callpoint Name	string	Callpoint name assigned by configuration file	Default: Min: Max:
Parent Station	String	Name of the Base station the callpoint is connected to.	Default: Min: Max:

10.3.3 Methods

General requirements for methods can be found in [Driver Project Requirements](#).

Callpoints implement no unique callable methods.

10.3.4 Events

General requirements for events can be found in [Driver Project Requirements](#).

10.3.4.1 CallStateChanged

Raised when the state of a connection between this basestation and a callpoint changes.

Note that on hang-up of a connection if the initial connection was raised in response to a request from a callpoint events will be raised for every basestation that was notified of the call request (see 10.3.4.2.)

Name	Type	Description
CallPoint	String	Name of callpoint involved in link

baseStation	string	Name of the basestation involved in link
State	CNL.IPSecurityCenter.Driver.Austco. CellGuard.Enums.CallState	Enumeration indicating the state of the link between the two points, can be one of the following: <ul style="list-style-type: none"> • Failed • Trying • Connecting • Connected • OnHook
Description	string	Brief description associated with state change

10.3.4.2 CallPointRequest

Raised when a CallPoint requests a connection to a basestation, or on termination of the connection when the request is cleared by the system

The initial event will be to the parent basestation, and if not responded to within the CellGuard configured interval (NOTE: this cannot be change via IPSC) then further events are raised to secondary basestations within the system.

Termination events will indicated which basestation accepted the call and which stations, if any, canceled the connection.

Name	Type	Description
CallPoint	String	Name of callpoint involved in link
baseStation	string	Name of the basestation involved in link
RequestState	CNL.IPSecurityCenter.Driver.Austco. CellGuard.Enums.CallRequestState	Enumeration indicating the state of the link between the two points, can be one of the following: <ul style="list-style-type: none"> • Requesting • Accepted • Canceled

10.3.4.3 *TamperState*

Event raised on the detection, or clearing of tampering to a callpoint

Note CellGuard gives no text description of what caused the tamper event.

Name	Type	Description
CallPoint	string	Name of the callpoint That the tampering has been detected/cleared on.
State	CNL.IPSecurityCenter.Driver.Austco .CellGuard.Enums.TamperState	Enumeration indicating the state of the tampering and can be one of the following: <ul style="list-style-type: none">• Active• Cleared
Time	string	Time at which the state changed

11 Installation

11.1 Prerequisites

There is no separate SDK to install for this integration, it is provided as an integral Dynamic Link Library (DLL) within the device driver package.

11.2 Driver Installation

- Start the IPSecurityCenter™ client and any supporting services
- Open the Device Driver Manager from the System Configuration
- Click the **Install** button
- Select the Prison Communication Systems Pty Ltd CellGuard Driver Package in the Open file dialog
- Wait for the driver to be uploaded

The driver packages should be listed in the Device Driver Manager.

11.2.1 Device Configuration

11.2.1.1 System Topology

The CellGuard system does not provide a method for determining the devices in the system and these must be specified via a Comma separated Variable (CSV) file – (See appendix Appendix B below) for an example configuration. Failure to provide this file will prevent the Server coming on line. Information for this configuration is provided by the customer and will be derived from the CellGuard ACM file for the system.

11.2.1.1.1 IPSC configuration File location

The file location and name can be specified, in the installation process, by the device installer and can be any location reachable by the IPSC applications Device Manager. If the the location is left blank the location will default to:

C:\ProgramData\CNL Software\IPSecurityCenter\Austco

With the filename:

CellGuardTopography.csv

If this file does not exist the system will be unable to function.

11.2.1.1.2 File format

The file uses the CSV format and consists of lines of four column values separated by the expected comma. Note that the system only allows for one root node, any attempt to supply more than one will cause the configuration to fail.

Column	Description	Observations
1	Parent node name	For the root node this should be left blank

2	Current node name	Any valid CellGuard device name (Always starts with a underscore) this is the node map as supplied in the CellGuard ACM configuration file.
3	Node Type	Can be any of the following three: <ul style="list-style-type: none"> • root • basestation • callpoint
4	Friendly name for node	Because the required names for connections are non-descriptive a friendly name can be supplied that is displayed in IPSC in place of the ACM derive node name and is used when creating a connection for a callpoint

Note: It is the configurators responsibility to make sure the friendly names are all unique, failure to observe this restriction will cause any attempts to access two devices with the same label to always access the first configured instance.

11.2.1.2 Driver Configuration

- Right click in a folder (e.g. Devices) in the System Configuration: **New → Device On → Server**
- Click **Next** on the introduction
- Select **Prison Communication Systems Pty Ltd** in the **Device Manufacturer** list
- Select **CellGuard Server** in the Available Devices list
- Click **Next** enter the device details:
 - The location of the CSV file defining the topology of the CellGuard network – if left blank the default location will be used (see 11.2.1.1.1 above)
 - The hostname or IP address, the port (use '0' to use the default port [22222])
 - There are no security settings associated with this device.
- Click **Next** and **Finish** to add the device.
- Enable the device to bring it online, this also creates the child devices from the topology file.

11.2.2 Driver Compatibility

The following devices are known to be incompatible with the Prison Communication Systems Pty Ltd CellGuard.

Model

N/A

Appendix A Notes and Observations

Unrecognised Devices

Because the CellGuard System cannot be interrogated for its configuration it is possible that devices may exist that are not in the known configuration, in this event those devices will not be accesable from IPSC. However if they initiate a communication or attempt to request a link to a base station an error event will be raised indictaing their presence.

CellGuard Server Device

The System only allows one root server node in the system, attempts to add multiple root nodes are rejected by the driver.

CallPoint initiated Calls

The Callpoints can request a base station initiate a communications link, but cannot initiate calls themselves, neither can one callpoint directly communicate with another callpoint.

Public Address (PA) functionality

The CellGuard system only allows for public address functionality between one base station and any of its attached child callpoints, it is not possible to initiate a system wide public address, nor from one basestation to the child callpoints of another basestation.

Initiating a public address will terminate any active calls

Active Callpoints

Only one callpoint in a callpoint group (a set of callpoints connected to a single basestation) can be in an active link at one time, If the link is from the primary basestation for that group attempts to connect from other basestations will be rejected with a "Busy here" status. However If the initial call is from another basestation a call from the primary station for a group will terminate the call from the seconardy station and inititate the link it has requested.

Callpoint End connection to control pannel

When making a call to the control station the call point raises an alarm event which appears as a CallPointRequest event with a RequestState of "Requesting". This alarm is sent to the primary control station and, if it is not responded to, alarms are also raised at other control stations in the system in an ACM configured priority order. When a call is answered various CallStateChanged events are raised.

These alarm events are only cancelled at the end of a call. At that point a CallPointRequest event with a RequestState of "Accepted" is raised for the control station that accepted the call and a CallPointRequest event with a RequestState of "Cancelled" is raised for any other control station that had the alarm directed to it.

Tamper Event

Tamper event notification have been implemented within the CellGuard system, but the functionality has not been tested since it is not possible to initiate a tamper sequence.

Error Events

Site error events have been implemented, but the functionality has not been tested. The event forwards the description provided by the cellguard system with raise/clear time.

The CellGuard documentation provides no indication of the range of events that can be raised this way, nor any raise/clear criterior.

Attempts to raise errors by the following has initiated no errors:

- disconnecting base stations
- Disconnecting callpoints
- Connecting to a callpoint with no callpoint attached
- Connecting to a callpoint with known fault.

Changing Device Labels within IPSC

The ability to change the device labels within the Configuration page of IPSC has been disabled since the change is not propagated down to the device driver and as a consequence reference to this changed label when attempting to initiate a call will fail with an unrecognised device name.

Device labels are configured as part of the configuration CSV file.

Appendix B CSV file example

The following file is an example file based on the development system based at the Camberley office (Note: the device names are defined within the cellguard system and must match those within its configuration file):

CellGuardTopology.csv

```
"",_201, root, CellGuard Server
root, _NODE-1, BaseStation, Primary Station
root, _NODE-2, BaseStation, Master Control
root, _NODE-3, BaseStation, Block 3
root, _NODE-4, BaseStation, Block 4
root, _NODE-5, BaseStation, Block 5
_NODE-1, _1_1, CallPoint, Cell 1
_NODE-1, _1_2, CallPoint, Cell 2
_NODE-1, _1_3, CallPoint, Cell 3
_NODE-1, _1_4, CallPoint, Cell 4
_NODE-1, _1_5, CallPoint, Cell 5
_NODE-1, _1_6, CallPoint, Cell 6
_NODE-1, _1_7, CallPoint, Cell 7
_NODE-1, _1_8, CallPoint, Cell 8
```