INTEGRITY Enterprise OS – Archon Edition, 1.0 Common Criteria User Guidance

Version: 1.2

Issued By:

Archon Secure LLC

Revision History:

Version	Date	Changes
Version 1.0	February 20, 2022	Initial Release
Version 1.1	April 5, 2022	Addressed validator ECRs
Version 1.2	April 27, 2022	Addressed validator comments

Contents

1. Introduction

This document ("[AGD]") is the Common Criteria Administrative guidance.

1.1 The INTEGRITY Enterprise OS Operating System

The INTEGRITY Enterprise OS – Archon Edition 1.0 allows users to securely access remote computer networks with only an internet connection. It does this by sending all network traffic between the end user device and remote systems over two third-party virtual private networks, which protect information from third-party access. Users can safely connect to their organization's secure remote systems and access sensitive information from anywhere with an approved internet connection.

With INTEGRITY Enterprise OS – Archon Edition 1.0, organizations can separate, isolate, and protect devices, critical networks, and data centers.

1.2 About This Manual

This guide is intended for system and network administrators and describes the installation, configuration, and administration procedures for the INTEGRITY Enterprise OS – Archon Edition 1.0.

2. Getting Started

2.1 Secure Acceptance, Installation, and Updates

Verify that the product you receive is the TOE.

Operating System (TOE)	Platform	CPU	HDD	RAM
INTEGRITY Enterprise OS Archon Edition 1.0	Archon ZV 5400	Intel Core i5-8365U	250 GB	8 GB

The Archon ZV 5400 is a customized Dell Latitude 5400 in a laptop form factor.

The TOE is INTEGRITY Enterprise OS – Archon Edition, which is verified by opening the Help interface with CTRL+WIN+F11, then navigating with CTRL+TAB to the "Version" tab. The Version tab shows the version of the installed Operating System, which must be: 1.0.

The INTEGRITY Enterprise OS – Archon Edition 1.0 will be pre-installed on the Dell Latitude 5400 laptop.

Throughout this document, the terms "client", "INTEGRITY Enterprise OS" and "TOE" may be used interchangeably. Unless the surrounding context indicates that the term references something more specific, the TOE is being discussed.

2.2 The Operational Environment

During initial installation, setup, and provisioning the client will need to access several components in the IT environment, including,

- Management Server: Allows the administrator to configure the client and set various parameters of operation
- Admin Server: Translates requests from the client to the management server
- Certificate Authority/Revocation Server: Provides certificate related functionality for the client

Both the management and admin servers will need Python version 3 installed for the admin and management tools to function properly. Deployment information for the Admin and Management Server can be found in Appendix A of this document.

2.3 Provisioning the Client

Provisioning mode is a special interface that allows system administrators to install new software and set a boot password for the client. When you boot a device that has not yet been provisioned or has only been partially provisioned, the factory image will automatically boot into provisioning mode.

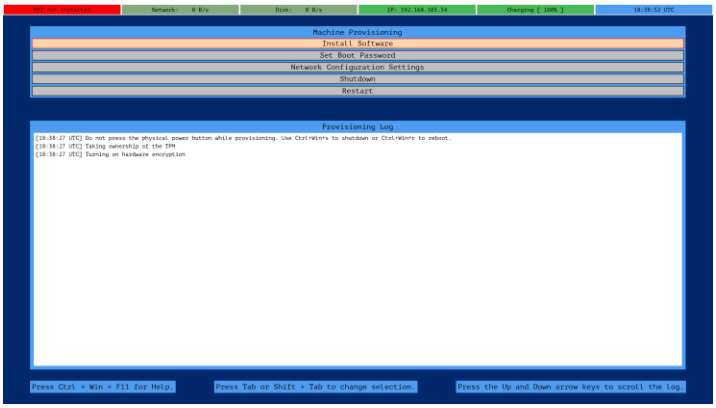

Figure 1 - Provisioning Mode Screen

The interface does not use a mouse but can be navigated by using the Tab key to change the focused element and the Enter key to select the focused element. Using provisioning mode to install new software requires that the device be connected via an Ethernet cable to the same network as the Admin and Management servers.

At any time, the administrator may access the help screen to get assistance with provisioning.

2.4 Provisioning File Types

There are three types of files which can be installed in provisioning mode.

- MFI ("Master File Index"): A MFI file describes the layout of partitions on the hard drive. A MFI must be installed before installing any other files. The MFI to install comes as part of the release.
- OTA ("Over-the-Air Update Bundle"): An OTA file bundles together a set of images and configuration files. A single OTA can be used to install many files at once. The release comes with two OTAs — one which installs the bootloader, and one which installs the Operating System.
- PCF ("Provisioning Command File"): A PCF file encodes a list of provisioning commands to follow in sequence. A single PCF can be used to install all the software needed for a device at once. The release comes with a PCF that installs the MFI and both OTAs.

2.5 Booting the Client in Provisioning Mode

To install the client on a device, the device must first be booted in provisioning mode. When you boot a device that has not yet been provisioned or has only been partially provisioned, the factory image will automatically boot into provisioning mode. If your device has already been fully provisioned, you can put it back in provisioning mode by either running a Factory Reset or a Clear Identity operation.

- Factory Reset— This operation removes all the software and credentials that have been installed on the device, returning it to the factory image. After running a factory reset, you will have to do a complete reinstall.
- Clear Identity— This operation removes all the credentials that have been installed on the device but leaves the software that has been installed intact. After clearing the identity, you will only have to reinstall certificates and configuration.

2.6 Provisioning Mode Status Bar

The provisioning mode status bar displays status information about the provisioning process. This can be useful for troubleshooting.

The status bar displays the following (from left to right):

- Installed: The first time the device boots after being factory reset, this field will be red and display the text MFI not installed. After the device has been partially provisioned, it will turn orange and display how many of the partition slots have items installed in them. When every slot has an item installed it will turn green.
- Network: Displays the current speed at which data is streaming over the network.
- Disk: Displays the current speed at which data is being read and written to the hard drive.
- IP Address: Displays the device's current IP address. If it is not connected to a network, it will turn red and say Link down.

- Battery: Displays whether the battery is charging and what percent of its charge is remaining.
- Time: Displays the system time.

2.7 Installing New Software in Provisioning Mode

The Install Software screen allows installation of new software on the device in any of the partition slots.

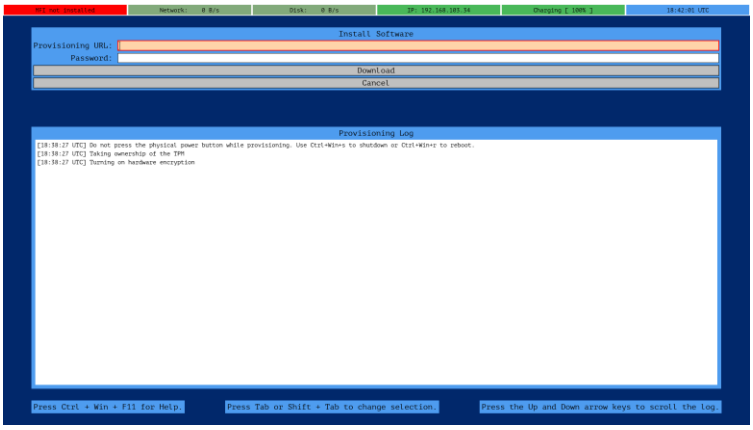

Figure 2 - The Install New Software Screen

To use this screen:

- Open the Install Software screen.
- Enter the URL of the provisioning file you want to install in the Provisioning URL field.
- Enter the password that can be used to decrypt it in the Password field. Leave this field blank if the provisioning file has no password.
- Tab to the Download button and press Enter.
- The Provisioning Log text box will display a log of what operations are performed. The Up and Down arrow keys can be used to scroll this log if it becomes too long to fit on a single screen.

2.8 Setting a Boot Password in Provisioning Mode

As an additional layer of protection, system administrators may optionally choose to set a boot password for the device. The boot password is the user authorization factor which unlocks the hard drive and permits decryption of the protected data. If left blank, the boot password will be the empty string. When the system boots, it first attempts to decrypt its hard drive using the default boot password (the empty string). If this fails, it prompts the user to enter their boot password so it can proceed through the boot process.

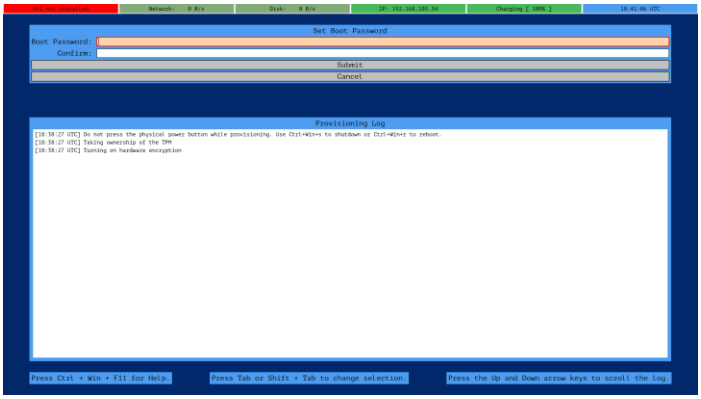

Figure 3 - Boot Password screen

To set a boot password:

- Open the Set Boot Password screen.
- Enter the password you want to set in the Boot Password field, and again in the Confirm field.
- Tab to the Submit button and press Enter.

The next time you boot the device you will be prompted for the boot password.

2.9 Configuring Network Settings in Provisioning Mode

By default, provisioning mode expects networks to automatically assign the device an IP address via DHCP. To support other use cases, the network configuration settings screen can be used to manually assign the device a static IP address.

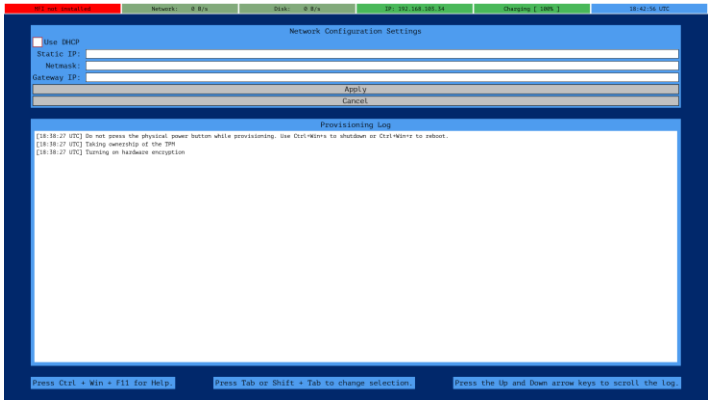

Figure 4 - Network Settings during Provisioning

To apply a static IP address:

- Open the Network Configuration Settings screen.
- Enter values in the Static IP, Netmask, and Gateway IP fields.
- Tab to the Apply button and press Enter.

To turn DHCP IP address assignment back on:

- Open the Network Configuration Settings screen.
- Check the Use DHCP box.
- Tab to the Apply button and press Enter.

2.10 Accessing Help in Provisioning Mode

To access the Help screen and system information in provisioning mode, press Ctrl+Win+F11. To return to the provisioning screen from the help screen, press Ctrl+Win+F12.

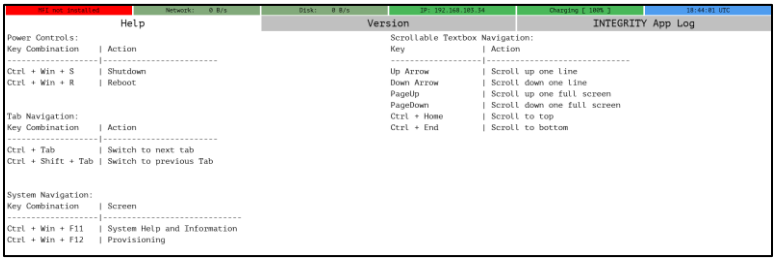

Figure 5 - Help during Provisioning

2.11 Completing Provisioning

After you have fully provisioned the device, you must shut down or restart to complete Provisioning. The following describes the steps to shut down or restart the client.

- Return to the Main menu
- Tab to either the Restart or Shutdown buttons and press Enter
- Alternatively, you may use the CTRL+WIN+R or CTRL+WIN+S keyboard shortcuts.
- The device will exit provisioning mode. The next time the device boots, it will detect that it is fully provisioned and boot in user mode.

3. Cryptographic Operations

This section describes the steps necessary to configure the client's cryptographic engine to operate in the manner described in [ST] and in conformance with the requirements of the PP_OS_v4.2.1.

3.1 Configuring the Cryptographic Engine

The client's cryptographic engine is pre-configured and cannot be configured by a user or administrator. The only cryptographic engine that was evaluated is the default INTEGRITY Cryptographic Library. No other cryptographic engines were used. It is not possible to configure the client to use any other cryptographic engine. All cryptographic options supported by the client are pre-configured. No additional configuration is available. By default, the client's cryptographic engine supports the following:

SFR	Cryptographic Algorithm	Operating Env.	Modes & Key Sizes	CAVP
FCS_CKM.1	*ECC KeyGen in accordance with FIPS 186-4 Appendix B.4*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	NIST Curves P-256, P-384, P-521	C1871
FCS_CKM.2	*Elliptic Curve key establishment in accordance with NIST SP 800-56A*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	NIST Curves P-384	C1871
FCS_COP.1(1)	*AES-XTS in accordance with NIST SP 800-38E*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	256-bit	C1871
	AES-GCM in accordance with NIST SP 800-38D	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	256-bit	C1871
FCS_COP.1(2)	*SHA-1, SHA-256, SHA-384, SHA-512 in accordance with FIPS Pub 180-4*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	160 bits for SHA-1, 256 bits for SHA-256; 384 bits for SHA-384; 512 bits for SHA-512	C1871
FCS_COP.1(3)	*ECDSA SigGen and SigVer in accordance with FIPS Pub 186-4 Section 5*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	NIST curve P-384	C1871
	RSA SigGen and SigVer in accordance with FIPS Pub 186-4	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	2048-bit	C1871
FCS_COP.1(4)	*SHA-1, SHA-256, SHA-384, SHA-512 in accordance with FIPS Pub 198-1 and FIPS Pub 180-4*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	For SHA-256, a 256-bit key size and message size. For SHA-384, a 384-bit key size and message size. For SHA-512, a 512-bit key size and message size.	C1871
FCS_RBG_EXT.1	*HMAC_DRBG in accordance with NIST SP 800-90A*	SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel	Random number generation for all cryptography	C1871

3.2 Transport Layer Security (TLS)

The client acts as a TLSv1.2 client for communication with the Administration Server, supporting the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The administrator configures the reference identifier for certificate validation by assigning the DN of the destination server(s), which is compared to the DN in the certificate received. This configuration, and choosing which local certificate to use, are performed in the configuration file update downloaded by the client from the Administration Server. The client uses the ECDSA public key from the INTEGRITY keypair for signature verification of update candidates. The client generates symmetric data-encrypting-

keys (DEKs) by invoking the DRBG. The client supports the secp384r1 group extension. This is by default no configuration is available.

3.3 Cryptographic Key Destruction and Zeroization

The client stores keys as shown:

Key Name	Storage Location	Destruction Method	Destruction Timing
Data Encrypting Keys (Wrapped)	Non-volatile memory in the MFI Array	New Value of the Key Or Zeroes (“0x00”)	When commanded by administrator.
Data Encrypting Keys (Plaintext)	Volatile memory	Removal of power to memory	When powered down and no longer needed
Border Encryption Value “BEV”	Volatile Memory	Removal of power to memory	When powered down and no longer needed
Public ECDSA Keys	Non-Volatile memory in the TPM	New Value of the key (when provided by updates) Or Zeroes (“0x00”, when performing Factory Reset)	When TPM zeroization is commanded by administrator.

Administrators may command the client to destroy keys at any time.

To perform a complete Factory Reset, the administrator executes ctrl-win-F11. Then control-tab to special operations. Then tab to factory reset.

To destroy keys in volatile memory, power off the client. This will remove power to the memory, which will cause keys to decay. To ensure that keys are sufficiently decayed to be beyond recovery via even physical recovery attacks, the administrator is advised to wait five (5) minutes after power off before the memory is considered “zeroized”. There are no other states or conditions which could cause key zeroization to fail, or to be performed in any way other than as described above.

To overwrite the old values of the X.509v3 certificate keys with new values, the new values are packed into a configuration update file. Other keys are overwritten with zeroes when the Factory Reset command is performed.

4. Updating the Client

Updates to the client are performed via Over-the-Air ("OTA") updates. OTA updates require the IT Environment to include an Admin and Management Server. Deployment information for the Admin and Management Server can be found in Appendix A of this document.

4.1 Over-The-Air Update System Overview

Updates are performed to install INTEGRITY-provided updates for new functionality, to deliver patches, to replace certificates before they expire, and/or to change configuration settings or apply new IT policies. The OTA Update process is as shown:

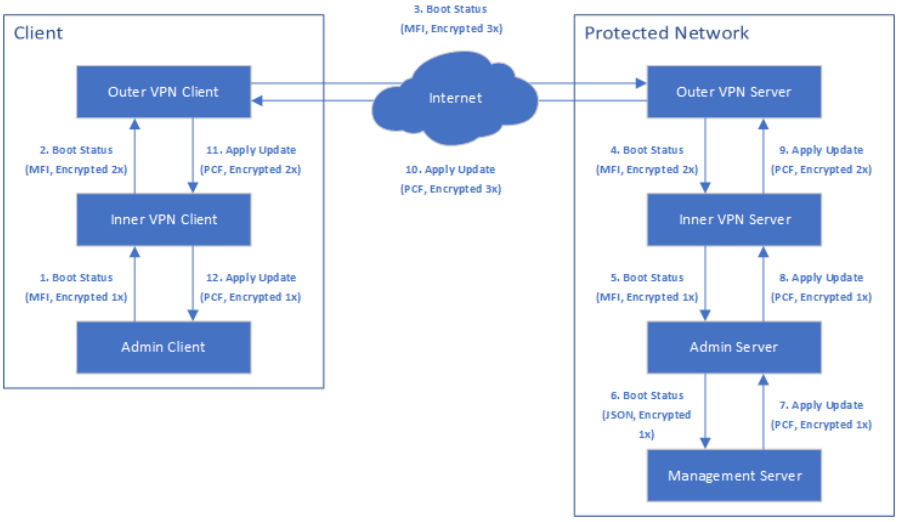

Figure 6 - OTA Update Process

- Every time the client boots up, it sends its boot status message as an HTTPS POST request. This message contains the device's sanitized Master File Index (MFI) — a binary file describing precisely what is installed on the machine.
- The Admin server authenticates the client device, decrypts the HTTPS POST request, and translates the binary MFI format into JSON format which it sends to the management server.
- The Management server reads the JSON message. It consults its database to determine what action the client should take, then creates a Provisioning Command File (PCF), which describes that action. It sends back the PCF to the admin server. Note that, unlike the PCFs used for initial provisioning, this update PCF is sent over a secure channel and is therefore not itself encrypted.
- The admin server forwards the PCF to the client.
- The admin client receives the PCF response and follows the instructions to update itself. The client will always perform validity checks on the update candidate to verify that the candidate has not been corrupted in transit and is digitally signed by the vendor. If the update candidate fails any of the validity checks, the update process fails, and the software is not updated.

Both the connection between the client and the admin server and the connection between the admin server and the management server are protected by TLS. The client reaches out to the admin server using the URL and port specified in its configuration. The admin server listens on a port provided on the command line and then reaches out to the management server using a URL and port provided on the command line.

4.2 Configuring Automatic Updates

The client can be configured to perform automatic software updates. When automatic updates are enabled, the client communicates with its administrative server to automatically find and install software updates. These updates install in the background while the client is in use. After updates completely install, the client will boot with the updated software after a restart or shut down. There is no indicator to show whether the system is in the process of being updated. Users can safely turn off the client at any point while updates are automatically installing in the background. The update will resume one the client is powered on.

If the client fails to connect to its administrative server after three connection attempts immediately following an update, it reverts to the software that was running before the update. This prevents updates from accidentally breaking network connectivity.

Automatic software updates are configured by the system administrator. Users can perform manual software updates via the “Check for Updates” button in the Help and Information Menu, which will check to see if there are updates. If so, the “Update” button will become available, and administrators may click the button to perform the update.

5. Remote Management Operations

This section describes remote management of the client. Remote management requires the IT Environment to include an Admin and Management Server. Deployment information for the Admin and Management Server can be found in Appendix A of this document.

5.1 Using the Management Utility

Archon Security provides a program known as the Management Utility which can be used on the Management Server to create files for provisioning or configuring the client.

5.2 Creating the Configuration Tree

The client has three layers of configuration:

- The INTEGRITY Enterprise OS software, which contains all the software that runs on the device and a suite of default settings
- The settings associated with the "site" the device belongs to. This may include root certificates, gateway IP addresses, etc.
- Device-Specific Settings. These include the device's unique certificates and keys.

When the Management utility is used to create a provisioning file, it takes two arguments. First, the directory containing the uncompressed INTEGRITY Enterprise OS software, and second the directory containing the configuration tree.

Each "Site" should be thought of as a logical grouping of devices, as all devices associated to a specific site will use those settings.

Each site has an associated folder. This folder contains a YAML configuration file for the site and a CLIENTs subfolder. The CLIENTS subfolder contains YAML configuration files for each client associated with the site. The certificate files associated with the sites and clients (root CA certs, intermediate CA certs, device end-entity certificates) may be placed anywhere in the file system, as the YAML configuration files reference them via relative paths.

5.3 Release Contents

A release bundle contains a number of configuration files and binaries.

The following configuration files are used to create a configuration tree:

- eras.defaults.yaml: The default configuration settings.
- eras.model-name.defaults.yaml: The model-specific default configuration settings. For every model supported by the release, there is a corresponding file.
- eras.site-template.yaml: The template for a site configuration file.
- eras.client-template.yaml: The template for a client configuration file.

The following binaries are included with the release:

- PSIDRevert.efi: An executable used to create a bootable USB stick that can revert the OPAL drive on a device.
- eras.mfi: The Master File Index describing the layout of the hard drive.
- eras.boot.ota: An installable bundle containing the parts of the software needed to boot the laptop that are shared by all models.

- eras.persona.ota: An installable bundle containing the parts of the software needed to run the device in user mode that are shared by all models.
- eras.model-name.boot.ota: An installable bundle containing the parts of the software needed to boot the laptop that are specific to the model. For every model supported by the release, there is a corresponding file.
- eras.model-name.persona.ota: An installable bundle containing the parts of the software needed to run the device in user mode that are specific to the model. For every model supported by the release, there is a corresponding file.
- eras.model-name.pcf: A Provisioning Command File that installs all of the software needed to run the model. For every model supported by the release, there is a corresponding file.

The files provided as part of the release are intended to be used as-is and should not be modified.

5.4 Default Configuration Settings File

The default configuration file (eras.defaults.yaml), documents the available configuration settings for the client, with default values for as many settings as possible. The model-specific default configuration files (eras.model-name.defaults.yaml) provide additional model-specific default settings which override the base default settings file but are overridden by the site and client configuration files.

For the full list of available configuration options see the default configuration file included in the latest release bundle.

5.5 Commanding the Management Server

The server listens on the command address in its config file for messages sent. These messages are HTTP POST requests with JSON bodies describing what should be done. They are not sent over HTTPS as they are expected to originate locally.

The server is commanded by sending it HTTP messages because this is an easy action to automate. However, for manual use, it is usually better to interact with a CLI. For this reason, the server also comes with a script for sending it commands.

The REPL can be opened with the following:

mgmnt_cli.py [--url <url>]

- --url <url>: Specifies the URL to send the management server commands on. The default is http://localhost:6666

From within the REPL invoke the following for a list of commands and options:

> help [subcommand]

subcommand

Optional argument that specifies which subcommand to print help for. If not passed, the list of subcommands is printed.

To leave the REPL invoke the following:

> exit

5.6 Creating a PCF for Remote Administration

When the management server receives a boot status from a client, it sends back a PCF containing a set of instructions for the client to execute. As this PCF is sent over a secure channel it is not itself encrypted. To create a PCF for remote administration, invoke the management utility's gen-update-pcf subcommand:

- gen-update-pcf, pcf

  Generate a PCF.

For example, suppose that the management server receives a boot status message from client1 and is informed that it is out of date. The last time provisioning files were exported, it created an update PCF for client1 which is available on https://*provisioning.example.org*/sites/site1/client1/update.pcf with the password foo. Before installing the update, it requests the client upload its audit logs to https://*logs.example.org*/upload

To create a PCF for the client, the server invokes the management utility as a subprocess as follows:

> python3 management_util.py gen-update-pcf -a https://logs.example.org/upload \ -u https://provisioning.example.org/sites/site1/client1/update.pcf -p foo

In the above command, instead of specifying an output file, the management server informs the management utility to output the binary PCF on stdout directly. The management server then captures the output of the subprocess. For example, in Python this looks like the following:

```
import subprocess
pcf = subprocess.check_output([
        'management_util.py', 'gen-update-pcf',
        '-a', 'https://logs.example.org/upload',
        '-u', 'https://provisioning.example.org/sites/site1/client1/update.pcf',
        '-p', 'foo'
])
```

After calling into the management utility, the management server then sends the output of the subprocess back to the client as the body of its HTTP response.

6. Client "User" Operations

6.1 Booting the Client

To boot the client:

- Press the power button.
- The client will turn on and display the INTEGRITY bootloader.
- When prompted for the boot password, input it, then press Enter.
- The client will prompt to boot the INTEGRITY Enterprise OS by pressing a key.
- Press a key to boot into the operating system.

Note: If you enter the boot password incorrectly too many times in a row, the client will display the error message "Too many attempts. Please reboot" and will not allow additional boot password attempts. To continue booting, hold down the client's power button until all its lights turn off, wait at least 10 seconds, and then press the client's power button to boot it again.

6.2 The User Interface

After successfully booting the client, a site administrator configured logo with a status bar at top is displayed.

This logo contains any advisory messages that are required per the deploying organization.

6.3 The Status Bar

The client always displays a status bar at the top of its screen to indicate connection statuses and which system is being viewed. The segment of the status bar that is currently displayed is indicated by a black outline. Segments for systems and logs that are not currently displayed have white outlines. This is a representative status bar, when Integrity OS is running the three containers mentioned previously

Figure 7 - Status Bar

The status bar is divided into the following sections, from left to right:

- Network connection status
- Outer VPN connection status
- Inner VPN connection status
- Remote Desktop connection status
- Battery level
- Current time

The first four segments of the bar are color-coded, to indicate the following statuses:

Color	Status
Grey	Initializing or shutting down
Blue	Not connected
Orange	Authentication
Yellow	Connecting
Green	Connected

The battery level section displays the client's battery level as a percentage and whether the client is running from battery power or charging. It is color coded:

Color	Status
Red	Under 25% battery capacity
Orange	25% to 75% battery capacity
Green	Over 75% battery or charging

The test configuration includes 2 VPNs, referred to as the Inner VPN and Outer VPN. This is the VPN configuration required by NSA's CSfC Mobile Access Capability Package (MACP). Acting as an End User Device (EUD) as defined in MACP is a primary use case for this TOE.

6.4 Shortcuts and System Commands

The following shortcuts are used to shut down, reboot, and to view different systems and items in the Status Bar.

Shortcut	Action
CTRL+WIN+1	Switch to network configuration utility
CTRL+WIN+4	Switch to Remote Desktop Client
CTRL+WIN+F1	Switch to network configuration log
CTRL+WIN+F2	Switch to Outer VPN Log
CTRL+WIN+F3	Switch to Inner VPN Log
CTRL+WIN+F4	Switch to Remote Desktop Client Log
CTRL+WIN+F11	Switch to System Help and Information Screen
CTRL+WIN+F12	Switch to Authentication screen
CTRL+WIN+S	Shutdown the client
CTRL+WIN+R	Reboot the client

6.5 The System Help and Information

The client comes with a built-in utility menu which is always available. The system help and information menu ("F11 Screen") provides information about using the system and its current configuration. To view the help screen and its tabs, press CTRL+WIN+F11 to open the HELP tab. Use CTRL+TAB and CTRL+SHIFT+TAB to navigate between tabs. Use the TAB key to navigate between UI elements (buttons, fields, etc) and use the ENTER key to select / confirm a UI element (press a button, fill out a field, etc)

6.6 The Help Tab

The HELP tab displays keyboard shortcuts for the system and instructions for navigating the HELP tabs.

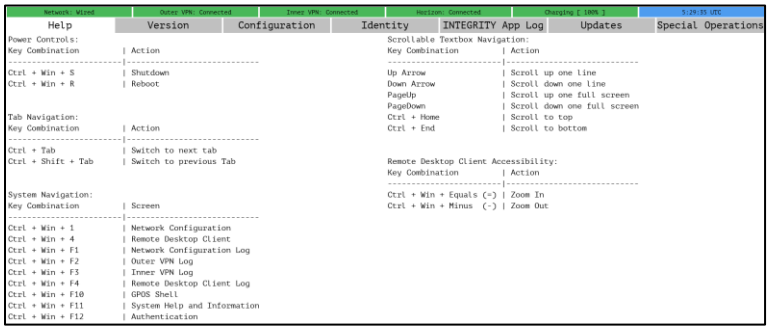

Figure 8 - The HELP Tab

6.7 The Version Tab

The VERSION tab displays the client version number, the model of the physical platform being used, and a table listing other installed software.

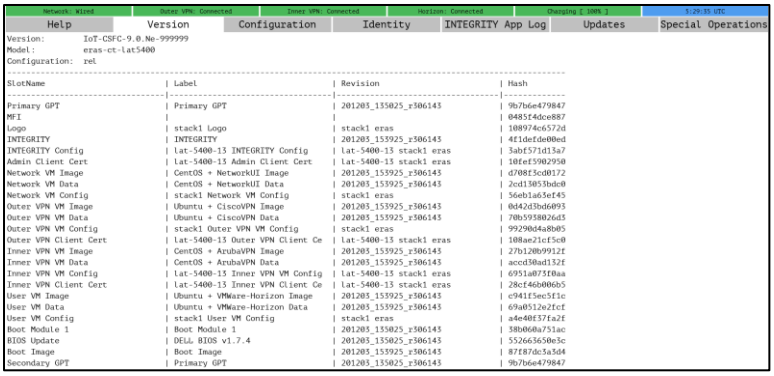

Figure 9 - The VERSION Tab

6.8 The Configuration Tab

The CONFIGURATION tab displays the configured max-incorrect-logins and idle-timeout values.

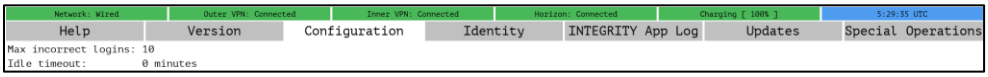

Figure 10 - The CONFIGURATION Tab

The “MAX INCORRECT LOGINS” value is used to determine when the client will lock an administrator account after too many failed login attempts. The Idle Timeout value determines how long the client will wait for user input before shutting down. This value is configurable remotely via OTA file update and is not configurable locally.

6.9 The Identity Tab

The IDENTITY tab displays information related to the currently configured user, certificates.

Figure 11 - The IDENTITY tab

6.10 The Special Operations Tab

The SPECIAL OPERATIONS tab provides options for reconfiguring the client. All operations require that the user enter their boot password.

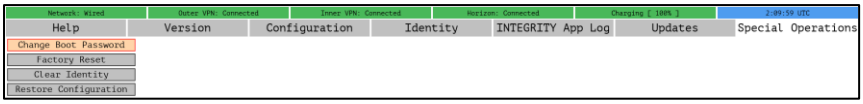

Figure 12 - The SPECIAL OPERATIONS tab

Change boot Password: The administrator my change the password used to decrypt the hard drive.

Factory Reset: Completely reset the client to default/unprovisioned settings. After using Factory Reset, new software can be installed, and new user configurations can be set.

6.11 User Passwords

Administrators configure the initial "boot password" (user authorization factor) by:

- CTRL+WIN+F11 to open the system help, status bar menu
- opening the "set boot password" screen
- Enter the password in the "boot password" field and again in the "confirm" field
- Select "Submit" and press enter.

To change or delete a password, follow the above steps but change the password in the "boot password" and "confirm" fields. The password may be composed of the following characters:

- All ASCII upper case characters
- All ASCII lower case characters
- All ASCII numbers, and

<space>	!	"	#	$	%	&	'	(	)
*	+	,	-	.	/	:	;	<	=
>	?	@	[	\	]	^	_	`	{
|	}	~							

Figure 13 - Supported Special Characters

NOTE: After provisioning the client, the boot password cannot be changed via remote configuration/PCF file update. In the evaluated configuration, the password can only be updated at the local client keyboard.

6.12 Sensitive Data Protection

The client may contain the following "sensitive data":

- User application private keys
- User login information
- The administration/update/audit client private key.

All "sensitive data" is automatically encrypted with AES-XTS. No user intervention is required to protect them.

6.13 Network Configuration and Choosing a Network

After successfully booting, the client attempts to connect to networks. If the client can automatically connect to a network, it will proceed. If the client cannot automatically connect to a network, it will display the NETWORK SETTINGS tab, as described in this section. The client attempts to establish connections in the following order of preference:

- Ethernet
- Cellular data

These connections may be limited by hardware or administrator configuration restricting certain communication types. The NETWORK SETTINGS tab of the Network Configuration utility is used to select network connections to the internet and configure connections. The Network Configuration utility can be accessed at any time with the keyboard shortcut Ctrl+Win+1.

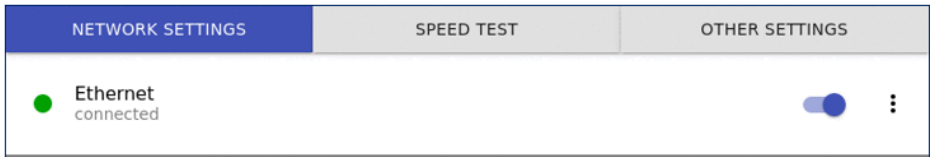

Figure 14 - Network Settings screen

The network configuration utility saves network configuration preferences. A green dot next to a connection type indicates that the client is connected to a network of that type. Cellular Data connections can be enabled or disabled by clicking the "toggle switches" next to their names. The switches will be colored blue when the connection is enabled, and gray when disabled.

6.14 Configuring Ethernet Connections

To configure an ethernet connection, plug a working ethernet cable into the client's ethernet port. The client will automatically use ethernet whenever it is available.

6.15 Configuring Cellular Data Connections

To configure a cellular data connection, open the Network Settings tab in the network configuration utility and toggle the "LTE" switch to the ON position to enable cellular data connections. To use an LTE connection, the client must not be connected to any other networks.

Figure 15 - TOE with Cellular Data Connection Enabled

If no SIM card is installed in the client, you must install one:

- Remove the SIM card tray by inserting a paper clip into the small round hole in the tray until the tray releases.
- Pull the SIM card tray out of the TOE.
- Insert a SIM card into the tray.
- Push the SIM card tray back into the TOE until the tray locks in place.

For information about SIM cards and SIM card activation, contact the SIM card's wireless carrier. To use a configured cellular data connection, the client must not be connected to any other network.

6.16 Configuring Network Details Manually

Some networks require manually entering configuration settings. Network administrators for these networks typically give users required configuration settings, which should be used without altering. To perform this type of setup, connect to the network to be configured and open the Network Settings tab in the network configuration utility, then open the overflow menu (three stacked dots) next to the connection type to be configured:

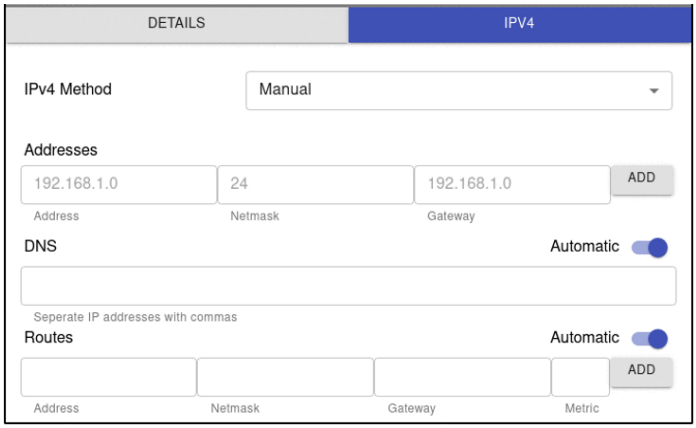

Figure 16 - Manual etworking configuration

Click the IPv4 tab and select MANUAL from the Method drop down menu.

- To configure static IP addresses: enter the requested information in the fields and click “add.”
- To configure DNS servers: either enable “automatic” or enter the IP addresses of DNS servers.
- To configure IP routes: either enable “automatic” or enter the requested information in the fields and click “add.”
- Click “Apply” to apply the new configuration.

To view information about a working connection, open the overflow menu next to the connection of interest.

6.17 Powering the Client on and OFF

The client may be shut down using the CTRL+WIN+S keys to shut down. The client may be rebooted using the CTRL+WIN+R keys. Alternatively, the local administrator may shut the client down by pressing the power button.

The administrator may configure a timeout period. This value is set by remote OTA update and is not locally configurable. After the timeout value expires without any user interaction, the client will power off.

7. System Logs and Audit Trail

The client stores information about events in binary format. These unprocessed logs are not human readable and must be processed using the script process_audit_log.py.

This chapter provides information about the processed audit logs and contains the following sections:

- Boot Cycle Header
- Audit Events

7.1 Boot Cycle Header

Each boot cycle has a header with the following information:

================ Reboot [<first event number>:<last event number>] ================

TSC Frequency = <tsc frequency>

Boot UTC = <DOW Month Day HH:MM:SS Year>

- TSC Frequency is the frequency of the timestamp counter.
- Boot UTC is the value of the UTC_0YYM and UTC_DHMS events in UTC. This time is derived from the system clock.

7.2 Audit Events

Audit events can take more than two minutes to become available in the unprocessed audit log. However, audit events are added to the unprocessed audit log on shutdown and the unprocessed log will be up to date upon reboot.

Processed audit events have the form:

Timestamp | VAS | User | Event | Event Name | Event Data

- Timestamp is the time (in seconds) since power was applied to the system, if the TSC frequency was logged. If the TSC frequency was not logged, this is the timestamp counter value.
- VAS is the process that logged the event. Some events are logged by a virtual AddressSpace on behalf of another virtual AddressSpace. When this occurs, the User will be changed. The process is specified as “AuditProxy” when the OS performs a service on behalf of a virtual AddressSpace (e.g. adding a user account), as opposed to an action being performed by the OS (e.g. start shutdown).
- User is the Username or User ID that logged the event. Most of the time this will be the System user, if the event happens automatically without user actions. Sometimes it will be the name of the virtual AddressSpace that the event is being logged on behalf of. The User ID will display if the virtual AddressSpace does not log the name of the user before the event was added.
- Event is the number used to signify the Event Name.
- Event Name is a short description of the event.
- Event Data is a number or text describing what happened.

The remainder of this chapter provides details about the different security-relevant audit events that are logged. Other logs that only provide diagnostic information may also be found in the logs.

Note: Some of the extra whitespace in the events in the following subsections has been removed.

7.3 Audit Startup

Some events may show up before this event after being processed, but this is the first event in the unprocessed log.

<timestamp> | Audit | System | 0x0002 | Reboot | 0

7.4 Audit Shutdown

These events might not be found at the end of a boot cycle due to power being cut to the system too early.

<timestamp> | Audit | System | 0x000d | AuditShutdown |0
<timestamp> | Audit | System | 0x0003 | WriteLogToStorage | 0

7.5 Privileged/Special Rights Events for GPOS

The following are privileged/special rights events:

<timestamp> | GPOS | <User> (<UserID>) | 0x8000 | Login | system: login <User> [Success]
<timestamp> | GPOS | System | 0x8000 | Login | system: login <User> [Failed]
<timestamp> | GPOS | <User> (<UserID>) | 0x8004 | Passwd | <User>: passwd [Success]
<timestamp> | GPOS | <User> (<UserID>) | 0x8004 | Passwd | <User>: passwd [Failed]
<timestamp> | GPOS | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd <User2> [Success]
<timestamp> | GPOS | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd <User2> [Failed]
<timestamp> | GPOS | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd [Unauthorized]
<timestamp> | GPOS | <User> (<UserID>) | 0x8003 | Userdel | <User>: userdel [Faile d]
<timestamp> | GPOS | <User> (<UserID>) | 0x8003 | Userdel | <User>: userdel <User2> [Success]
<timestamp> | GPOS | System | 0x8001 | Logout | <User>: logout [Success]
<timestamp> | Admin | System | 0x8004 | System Update | Installing update
<timestamp> | Admin | System | 0x8004 | System Update | Successfully installed update
<timestamp> | Admin | System | 0x8004 | System Update | Failed to install update
<timestamp> | Admin | System | 0x8004 | System Update | Failed to check for updates: Failed to connect to admin server
<timestamp> | Admin | System | 0x8004 | System Update | Failed to check for updates: Dry run of update install failed
<timestamp> | Admin | System | 0x8000 | Error | <Reason for error>
<timestamp> | Admin | System | 0x8001 | Info | [<OTA slot name>]: Installing (<OTA label>)
<timestamp> | Admin | System | 0x8002 | Change Boot Password | Boot password changed
<timestamp> | Admin | System | 0x8002 | Change Boot Password | Failed: User entered incorrect boot password
<timestamp> | Admin | System | 0x8003 | Upload Audit Log | Uploaded the audit log
<timestamp> | Admin | System | 0x8003 | Upload Audit Log | Failed to upload the audit log

The following are privilege or role escalation events for GPOS:

<timestamp> | GPOS | <User> (<UserId>) | 0x8000 | Login | system: login <User> [Success]
<timestamp> | GPOS | System | 0x8000 | Login | system: login <User> [Failed]

7.6 Privileged/Special Rights Events Audit Proxy

The following are logged by the AuditProxy on behalf of the GPOS:

<timestamp> | AuditProxy | <User> (<UserID>) | 0x8000 | Login | system: login <User> [Success]
<timestamp> | AuditProxy | GPOS | 0x8000 | Login | system: login <User> [Failed]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8004 | Passwd | <User>: passwd [Success]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8004 | Passwd | <User>: passwd [Fai led]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd <U ser2> [Success]

<timestamp> | AuditProxy | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd <U ser2> [Failed]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8002 | Useradd | <User>: useradd [Unauthorized]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8003 | Userdel | <User>: userdel [Failed]
<timestamp> | AuditProxy | <User> (<UserID>) | 0x8003 | Userdel | <User>: userdel <U ser2> [Success]
<timestamp> | AuditProxy | System | 0x8001 | Logout | <User>: logout [Success]

The following are logged by AuditProxy on behalf of the OTA virtual AddressSpace:

<timestamp> | AuditProxy | OTA | 0x8004 | System Update | Installing update
<timestamp> | AuditProxy | OTA | 0x8004 | System Update | Successfully installed update
<timestamp> | AuditProxy | OTA | 0x8004 | System Update | Failed to install update
<timestamp> | AuditProxy | OTA | System Update | Failed to check for updates: Failed to connect to admin server
<timestamp> | AuditProxy | OTA | 0x8004 | System Update | Failed to check for update s: Dry run of update install failed
<timestamp> | AuditProxy | OTA | 0x8000 | Error | <Reason for error>
<timestamp> | AuditProxy | OTA | 0x8001 | Info | [<OTA slot name>]: Installing (<OTA label>)
<timestamp> | AuditProxy | OTA | 0x8003 | Upload Audit Log | Uploaded the audit log
<timestamp> | AuditProxy | OTA | 0x8003 | Upload Audit Log | Failed to upload the audit log

The following are logged directly by the virtual AddressSpace in the second column of the log:

<timestamp> | Admin | System | 0x8002 | Change Boot Password | Boot password changed
<timestamp> | Admin | System | 0x8002 | Change Boot Password | Failed: User entered incorrect boot password
The following are logged by AuditProxy on behalf of virtual AddressSpaces that do TLS:

<timestamp> | AuditProxy | OTA_TLS | 0x0006 | Trusted Channel | Attempt to establish trusted channel to admin server at <URL>
<timestamp> | AuditProxy | OTA_TLS | 0x0006 | Trusted Channel | Failed to establish trusted channel to admin server at <URL>

The following are privilege or role escalation events for ERAS-9:

<timestamp> | AuditProxy | <User> (<UserId>) | 0x8000 | Login | system: login <User> [Success]
<timestamp> | AuditProxy | GPOS | 0x8000 | Login | system: login <User> [Failed]

7.7 System Reboot, Restart, and Shutdown

The following events define the start of the system's shutdown sequence. The device will turn off in 30 seconds or less after these are logged, shutdown cannot fail or be stopped by the user by the time these events are logged.

<timestamp> | Power | System | 0x8000 | Start Shutdown | System Reboot
<timestamp> | Power | System | 0x8000 | Start Shutdown | System Shutdown

7.8 Audit Records Associated with the Tested Configuration

The following audit events are generated by test components such as the VMs providing VPN implementations. Depending on the VMs installed, these audit records may or may not be found in the logs:

<timestamp> | <Varies> | System | <Varies> | Trusted Channel | Attempt to establish trusted channel to admin server at <URL>
<timestamp> | <Varies> | System | <Varies> | Trusted Channel | Failed to establish trusted channel to admin server at <URL>
<timestamp> | <Varies> | System | 0x8003 | VMShutdownReq | 0

The Process/VAS in these reflects the VMs in use for testing. For example, the following values may be present in logs:

- VMM_User1
- VMM_VPN_I
- VMM_VPN_O
- Guest_Net

8. Troubleshooting

8.1 Cryptographic Self-Testing Fails

If the client's self-tests fail, the client will audit the failure and then halt. It must be rebooted to recover. If the client continues to fail self-testing, the administrator should contact their local IT support, which in turn may contact INTEGRITY technical assistance.

8.2 Shuts down by itself

The client includes an idle timeout which can be configured to shut down the client after it receives no user input for a set length of time. To view the configured idle timeout, open Configuration tab of the Help bar. The client may also have run out of battery. The battery level section of the status bar displays the battery charge level. Users should monitor the battery level and charge it when low to avoid unexpected shutdowns.

8.3 Ethernet connection fails

The Ethernet cable in use may not be working. Open the Network Configuration utility with the Ctrl+Win+1 shortcut. If the NETWORK SETTINGS tab of the Network Configuration utility shows Ethernet's status as device unavailable, the Ethernet cable is not connected to a working network. Try using a different Ethernet cable and make sure that the cable is plugged into the correct networking equipment. Also, because some Ethernet slots can be tricky, verify that the cable is firmly inserted into the slot until it snaps into place.

8.4 Cellular Data Connection Fails

The SIM card may not be activated. Check with your administrator or cellular carrier to ensure that the SIM card is activated. The client may also be out of range of your carrier's cell towers or have minimal signal. To check the signal strength of your cellular data connection, open the Network Configuration utility with the Ctrl+Win+1 shortcut, then open the overflow menu next to LTE on the NETWORK SETTINGS tab. The signal strength is listed as a percentage. If the signal strength is low, the client will not be able to maintain a good connection.

8.5 Unable to Connect to Internet through Local Network

The client's connection to the local network may not be configured correctly. If an administrator provided network configuration settings for the local network, try entering them again. If the client's connection to the local network is configured correctly but the client still cannot connect to the internet, the local network may not be connected to the internet. Try using a different internet connection.

Appendix A: Admin Server and Management Server

Deploying the Administrative Server

The admin server is a small executable that authenticates connections with the client and then translates their binary boot status messages into a JSON format which it forwards to the management server. The admin server is also responsible for forwarding back the management server's response to the client.

To run the admin server, the following parameters must be provided on the command line:

--cert path
The PEM formatted certificate for the admin server to use.
--private_key path
The PEM formatted private key for the admin server to use.
--root_ca path
The PEM formatted certificate for the root certificate authority.
--mgmnt_server_addr address
The IP address or URL for the management server.
--mgmnt_server_port portNum
The port to connect to the management server on.
--connect_port portNum

The port to listen for client device messages on.

The admin server also takes the following optional parameters:

--log path
The file to log output to. The default is stdout.
--verbosity level
How much information to log. The level ranges between 0 (no logging) and 3 (maximal logging). The default value is 0.
--mgmnt_endpoint path
The HTTPS endpoint that the admin server forwards client requests to. The default value is /bootstatus/.
--help
Print usage information and exit.

Creating a Management Server Configuration File

To create a management server configuration file, use igs_management setup as follows:

```
igs_management setup <config-file>
--audit-url <audit-url> --bootstatus-addr <bootstatus-addr>
--cert <cert> --cmd-addr <cmd-addr> --key <key> --log-dir <log-dir>
--management-util <management-util> --manifest <manifest>
--provisioning-url <provisioning-url> [--revoked-clients <revoked-clients>]
--root-cert <root-cert> --site <site> [--send-factory-reset] [--run]
```

This creates a management server configuration file containing all of the options passed on the command line.

The following arguments are required:

- <config-file>

The path to the config file to create

- --audit-url <audit-url>
  The URL the client should upload audit logs to
- --bootstatus-addr <bootstatus-addr>
  The address to listen on for boot status connections
- --cert <cert>
  The path to the certificate to use for the server
- --cmd-addr <cmd-addr>
  The address to listen on for administration commands
- --key <key>
  The path to the private key to use for the server
- --log-dir <log-dir>
  The directory which will be used to store server logs
- --management-util <management-util>
  The path to the management utility
- --manifest <manifest>
  The path to the manifest file to run the server for
- --provisioning-url <provisioning-url>
  The URL which serves provisioning files
- --root-cert <root-cert>
  The path to the trusted root certificate for the server
- --site <site>
  The name of the site to run the management server for

The following arguments are optional:

- --revoked-clients <revoked-clients>
  The path to a file containing a newline separated list of revoked clients
- --send-factory-reset
  Pass this flag if the server should send factory reset PCFs to bad clients
- -v, --verbose
  Log management server output to the console
- --run
  Run the server after creating the config file

Running the Management Server

To run the management server, use igs_management run as follows:

igs_management run <config-file>

The following argument is required:

- <config-file>
  The path to the config file to load

The following argument is optional:

- -v, --verbose
  Log management server output to the console

--- End of Document ---