Software House, a brand of Tyco Security Products

iSTAR Ultra Door Controller

Hardware Model Numbers: USTAR008, USTAR016, and USTAR-GCM-2U
Firmware Version: 6.1
Label Part Number: STAR-FIPS-LBLS

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 0.14

Prepared for:

SOFTWARE HOUSE
A Tyco International Company

Software House, a brand of Tyco Security Products
6 Technology Park Drive
Westford, MA 01886
United States of America

Phone: +1 978 577 4000
http://www.swhouse.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the following product line from Software House, a brand of Tyco Security Products:

- iSTAR Ultra Door Controller
    - Hardware Model Numbers: USTAR008, USTAR016, and USTAR-GCM-2U
    - Firmware Version: 6.1

This Security Policy describes how the iSTAR Ultra Door Controllers meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The iSTAR Ultra Door Controllers are also referred to in this document as the iSTAR Ultra, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Software House website (http://www.swhouse.com) contains information on the full line of products from Software House.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Software House. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Software House and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Software House.

2 iSTAR Ultra Door Controllers

2.1 Overview

The iSTAR Ultra Door Controllers are hardware devices which are connected to at least one card reader and a door. After a card is swiped through a connected card reader, the information contained on the card about the person to whom the card is assigned is transmitted to the door controller. The door controller then consults its database and determines whether to allow access to the person by opening the door. The door controller will then send a message to open the door if access is allowed. If access is not allowed, then the door will not open and the user is denied entry.

These powerful IP[1] edge devices provide a strong feature set to secure any door. These features include peer-to-peer communication, intrusion zones and keypad commands, extended card numbers, advanced door monitoring, and anti-passback. Multiple iSTAR Ultra Door Controllers can be networked into user-defined, logical groups called clusters. Each controller in the cluster is called a cluster member, and each cluster has one controller that serves as the Master Controller.

> ***NOTE****: FIPS mode is set at the cluster level; thus, every controller in the cluster will reflect the same FIPS status. For this validation, however, it is critical to note that a cluster can consist of a single controller. In a single-controller cluster, the lone controller acts as the Master Controller. Thus, any discussion in this document referencing "clusters" (except where multi-controller configurations are expressly stated) refers to a single-controller cluster, which represents the module.*

The iSTAR Ultra comes in two form factors: an 8-reader or 16-reader wall-mount device (Figure 1) and a 32-reader rack-mount device (Figure 2).

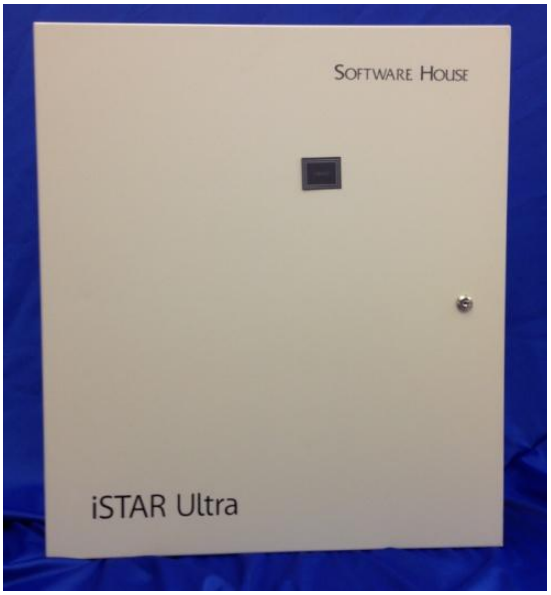


Figure 1 – 8-Reader/16-Reader Wall-Mount iSTAR Ultra

[1] IP – Internet Protocol

Figure 2 – 32-Reader Rack-Mount iSTAR Ultra

The iSTAR Ultra enclosures, and are protected with a built-in tamper switch to ensure the controller is not accessed by unauthorized personnel. Security risks are significantly reduced with encrypted communications and denial-of-service protection against network intrusion, making the iSTAR Ultra a highly-secure network device.

The iSTAR Ultra has expansion capability for up to four input/output modules and consists of three models:

- USTAR008 – 8-reader model (wall-mount) with 1 onboard ACM[2]
- USTAR016 – 16-reader model (wall-mount) with 2 onboard ACMs
- USTAR-GCM-2U – 32-reader 2U model (rack-mount) (Note that this model is delivered with up to 4 ACMs, each with its own physically-separate enclosure. These units are not part of the validated module).

2.1.1 iSTAR Ultra Management

The iSTAR Ultra is managed using the following tools:

- C●CURE – C●CURE is a Windows-based administration application for managing iSTAR devices. It is installed on an external host server and connects to the iSTAR controllers via an Ethernet network. A single C●CURE host server can be used to manage one or more clusters.

- iSTAR Configuration Utility (ICU) – ICU provides configuration, diagnostic, and troubleshooting options. The ICU is included as part of the C●CURE installation, and is used to designate the Master Controller, define Master IP[3] addresses, and define the IP address of the host server. Since other configuration information is defined and downloaded from the C●CURE host server, the information that is entered in the ICU must match the information that is entered in C●CURE to ensure correct configuration.

The Master Controller handles the communication of all event and cardholder data between the cluster and a C●CURE host server. Each cluster member communicates to the other cluster members through the Master to link events and share cardholder status and location to mitigate the occurrence of such activities as “tailgating” (following another cardholder into a secured area without presenting a separate badge) and “passback” (passing back a card to another person to use) in the area secured by this cluster of controllers. The iSTAR Ultra features strong 256-bit AES[4] network encryption for both controller-to-host communications and controller-to-controller communications.

The iSTAR Ultra Door Controllers are validated at the FIPS 140-2 section levels shown in Table 1.

[2] ACM – Access Control Module
[3] IP – Internet Protocol
[4] AES – Advanced Encryption Standard

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	2

2.2 Module Specification

The iSTAR Ultra is a multi-chip standalone hardware module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the iSTAR Ultra is defined by the hard metal chassis, which surrounds all the hardware and firmware components.

The module is composed of the following hardware components:

- General Control Module (GCM) – The iSTAR Ultra employs a board called the GCM that provides the primary logic and functionality of the controller. The board contains a 1 GHz ARM Cortex-A9 dual-core CPU, with 2GB DDR3[5] DRAM and a 16GB SD[6] card. It runs Ubuntu Linux 12.04.2, Kernel 3.0.35; it includes the module's various data ports and interfaces; and it controls the input and output to and from all the attached card readers.

- LCD[7] Display and LEDs[8] – The LCD Display is a display that is used during setup and configuration of the module to monitor the status of the device and the self-tests. The LCD Display panel is located on the front panel of the rack-mount iSTAR Ultra enclosure, and on the inside of the wall-mount iSTAR Ultra enclosure. The LCD display provides clear startup and troubleshooting information. The LED displays power, LAN[9] activity, serial port activity, and output status.

- Tamper Switch – The Tamper Switch detects attempts at unauthorized entry into the controller enclosures, and provides alerts to the management station when such attempts are detected.

- Power over Ethernet (PoE) module – Mounted to the GCM, the PoE module allows the door controller to power 2-to-4 network-attached access control.

- Access Control Module – The ACM is an auxiliary board that communicates with the GCM and provides additional reader connectors, supervised inputs, relays, and output connectors.

[5] DRAM – Dynamic Random Access Memory
[6] SD – Secure Digital
[7] LCD – Liquid Crystal Display
[8] LED – Light-Emitting Diode
[9] LAN – Local Area Network

Approved security functions and function components (and their associated algorithm/CVL[10] implementation certificate numbers) offered by the module are listed in Table 2 below.

Table 2 – Approved Security Functions and Function Components

Approved Security Function	Certificate Number
AES[11] 256-bit in CBC[12] mode	#2856
SHA[13]-1, SHA-256, SHA-384, SHA-512	#2400
HMAC[14] with SHA-1, SHA-256, SHA-384, SHA-512	#1797
SP[15] 800-90A DRBG[16] (HMAC-based)	#506
ECDSA[17] Key Generation (B-571 Curve)	#506
ECDSA Signature Generation and Verification (B-571 Curve)	#506
CVL – ECC CDH[18] SP 800-56A (B-571 Curve)	#292
CVL – TLS v1.0/1.1/1.2 KDF[19]	#293

Additionally, the iSTAR Ultra implements the following non-Approved algorithms:

- Hardware noise sources – for seeding the FIPS-Approved DRBG
- EC Diffie-Hellman – used for key agreement
- MD5 – used as part of the TLS handshake

2.2.1 Exclusions

On the wall-mount Ultra devices, the ACM is contained within the device enclosure. On the rack-mount Ultra device, ACMs are delivered in the form of separate, independent units that connect to the GCM via USB[20] cable connection. Thus, for the purposes of this validation, the ACMs on the rack-mount Ultra have been excluded from FIPS requirements.

On the wall-mount Ultra enclosures, the removal of punch-out hole fillers is required for module wiring. These punch-out holes provide visual access to the module's motherboard. However, only non-security-relevant components (such as power-related components) can be seen through the open holes. These components do not store or process keys and CSPs, and are therefore excluded.

2.3 Module Ports and Interfaces

Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

- Data Input Interface

[10] CVL – Component Validation Listing
[11] AES – Advanced Encryption Standard
[12] CBC – Cipher Block Chaining
[13] SHA – Secure Hash Algorithm
[14] HMAC – Keyed-Hashed Message Authentication Code
[15] SP – Special Publication
[16] DRBG – Deterministic Random Bit Generator
[17] ECDSA – Elliptic Curve Digital Signature Algorithm
[18] ECC CDH – Elliptic Curve Cryptography Cofactor Diffie-Hellman
[19] KDF – Key Derivation Function
[20] USB – Universal Serial Bus

- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

The iSTAR Ultra provides the ports and interfaces shown in Table 3 below.

Table 3 – iSTAR Ultra Ports and Interfaces

Port/Interface	Model		
	8-Reader	16-Reader	32-Reader
Wiegand Reader connectors	8	16	0
Supervised input ports	24	48	0
Special Purpose inputs (“Tamper Detect”, “AC Fail”, “Low Battery”)	Yes	Yes	Yes
Relay output ports	16	32	0
RS-485 Serial ports (for RMs, I/8-CSIs, and R/8s)	10	18	2
USB ports	5	5	4x USB / 1x Micro
Fire Alarm Input (FAI) connectors	Yes	Yes	No
Local LCD Display	Yes	Yes	Yes
LEDs (for power, LAN activity, serial port activity, and output status)	Yes	Yes	Yes
External Power Interface	Yes	Yes	Yes
10/100/1000 Ethernet port	2	2	2
Reset button	Yes	Yes	Yes
Encryption switch	Yes	Yes	Yes
Auxiliary outputs (power)	8	16	0

For models with a PoE module, power is provided via Ethernet connection; otherwise, power is provided over a connection to an external power supply. The RS-485 Serial ports are used to communicate with RM card readers or I/8 or R/8 reader module boards. The USB ports can be used in provisioning, for connecting additional card readers, or for GCM-to-ACM connections on the rack-mount model. The Ethernet port is used for establishing TLS communications with other iSTAR Ultra devices and with the C●CURE host server. The Direct Wiegand reader ports are used for connecting card readers directly to the module. The Supervised input ports and Relay output ports are for connecting other peripherals such as door sensors and audible alarms.

All of these physical interfaces map to logical interfaces (as defined by FIPS 140-2) as described in Table 4 below.

Table 4 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Module Interface
Data Input	Wiegand Reader connectors, Supervised input ports, RS-485 Serial ports, Ethernet port, USB ports
Data Output	Relay output ports, RS-485 Serial ports, Ethernet port

FIPS 140-2 Logical Interface	Module Interface
Control Input	Special purpose inputs, FAI connectors, Ethernet ports, Reset button, Encryption switch
Status Output	Ethernet ports, LEDs, RS-485 Serial ports
Power Input	External Power interface, Battery power interface, Ethernet port (for models with PoE module)

The module is designed to accept access credentials in multiple formats from a wide variety of external input devices. As stated above, card readers can be connected to the module via the data input interfaces. Software House offers several types of readers that are designed and vendor-tested for use with the module, including:

- RM Card Readers
- Multi-Format Proximity Readers
- Multi-Technology Readers

2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

2.4.1 Authorized Roles

There are two roles in the module that operators may assume: a Crypto Officer (CO) role and a User role.

- Crypto Officer – The Crypto Officer role is responsible for the initialization and management of the cryptographic functions provided by the module. This role is generally assumed by an operator accessing the module's management applications: the iSTAR Configuration Utility (ICU) and the C●CURE host server.

- User – The User role is assumed by a networked controller (i.e. a cluster member or Master Controller) in a single- or multi-controller environment. The User role is responsible for establishing the TLS session with the module and for the secure transmission of access control data to the module.

The module also supports a Maintenance role. Operators assuming this role are allowed physical access to the module in order to perform battery replacement tasks as required (see section 3.1.5 below for more information).

2.4.2 Services

The services that require operators to assume the Crypto Office or User role are listed in Table 5 and Table 6, respectively. Additional services that do not require the assumption of an authorized role are listed in Table 7. Please note that the Critical Security Parameters (CSPs) listed in the table use the following indicators to show the type of access required:

- **R (Read)**: The CSP is read
- **W (Write)**: The CSP is established, generated, modified, or zeroized
- **X (Execute)**: The CSP is used within an Approved or Allowed security function or authentication mechanism

For a complete listing of all services (both security-related and non-security-related), please review the appropriate iSTAR Administration Guide.

Table 5 – Mapping of Crypto Officer's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Configure the module	Configure the module using the required IP address and connection data	IP data via management application	None	None
Configure the module for Approved mode of operation	Configure the module for FIPS-Approved mode of operation	FIPS selection from the configuration screen	None	None
Create database of access card rights	Create database of access card rights	User names and applicable authorization data	None	None
Reboot the module	Command the module to reboot and restart	Reboot command	Module reboots	None
Generate an ECC key pair	Generate a new ECC key pair	Message from the C●CURE host server to generate a new ECC key pair	New ECC key pair is generated	HMAC_DRBG 'V' Value – RX HMAC_DRBG 'Key' Value – RX ECC Public Key – W ECC Private Key – W
Generate an ECC certificate	Generate a new ECC certificate	Message from the C●CURE host server to generate new ECC key pair	New ECC certificate is generated and signed	ECC Public Key – R ECDSA Private Key – W
Load new firmware	Load a new firmware image onto the module	Selection of the appropriate menu item on the C●CURE host server	New firmware image is loaded	Firmware Upgrade Key - RX
Show status	Display module status information	Selection of the appropriate menu item on the C●CURE host server	Status window is displayed on the C●CURE host server	None
Perform self-tests	Initiate and run all power-up self-tests	Reboot command	Module reboots and initiates power up self-tests	TLS Session Key – W PRNG seed – R

Table 6 – Mapping of User's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Initiate a secure TLS session	Initiate a secure TLS session with a cluster member.	Digital certificate	Secure connection established	TLS Session Key – RX ECC Public Key – R ECC Private Key – R
Check access rights	Check access card rights database	Access rights information request	Access approval or denial	None
Terminate a secure TLS session	Terminate a secure TLS session with a cluster member.	None	Secure connection terminated	ECC Public Key – R ECC Private Key – R

Table 7 – Mapping of Additional Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Initiate access request process	Request access to controlled area	Access rights information (via card swipe on card reader)	Opened door for approved access request	None
Zeroize	Zeroize keys and CSPs	Reboot or power-cycle	Module reboots; keys are cleared	ECC Private Key – W ECDSA Public Key – W ECDSA Private Key – W Entropy Input – W HMAC_DRBG ‘V’ Value – W HMAC_DRBG ‘Key’ Value – W

For further details regarding module services, please review the appropriate iSTAR Administration Guide.

2.4.3 Authentication Mechanisms

The module supports role-based authentication. Module operators must authenticate to the module before being allowed access to services which require the assumption of an authorized role. The module employs the authentication methods described in Table 8 to authenticate Crypto Officers and Users.

Table 8 – Authentication Mechanisms Employed by the Module

Role	Type of Authentication	Authentication Strength
Crypto Officer, User	Certificate	During TLS session negotiation, the module authenticates the CO or User using a 571-bit ECC public key. Using conservative estimates, the probability for a random attempt to succeed is = 1:2^{571} = 1:(7.73 x 10^{171}) which is less than a 1:1,000,000 probability as required by FIPS 140-2. The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data (1000 × 10^6 × 60 seconds, or 6 × 10^{10}) can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is = 1: (2^{571} possible keys / ((6 × 10^{10} bits per minute) / 571 bits per key)) = 1: (2^{571} possible keys / 105,078,809 keys per minute) = 1: (7.36 × 10^{163}) which is less than a 1:100,000 probability as required by FIPS 140-2.

As a part of its primary function, the module receives access credential data from individuals swiping a card through an attached card reader. These credentials do not authenticate cardholders to the module; rather, the credentials are simply data that is processed by the module and used to determine the cardholders’ access rights to protected areas. Thus, for the purposes of this validation, those credentials are not considered authentication data, and are not discussed in the narrative above.

2.5 Physical Security

The iSTAR Ultra is a multi-chip standalone cryptographic module. All firmware and hardware components of the module are entirely contained within a steel enclosure, which defines the module's cryptographic boundary. Each enclosure is opaque within the visible spectrum. The wall-mount enclosure includes a door with a locking mechanism, while the rack-mount enclosure includes a removable top cover. The enclosures are protected with serialized tamper-evident labels in order to provide evidence of tampering. The Crypto Officer is responsible for applying the labels as well as for periodically inspecting the tamper-evident labels for signs of tampering. See Section 3.1.1.1 for instructions on how to affix the tamper-evident labels.

The iSTAR Ultra Door Controllers have been tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.6 Operational Environment

The requirements associated with this section are not applicable, as the iSTAR Ultra does not provide a general-purpose operating system (OS) to module operator. The module employs a System-On-Module (SOM) that includes a 1GHz Freescale i.MX6 Dual ARM Cortex-A9 processor running Ubuntu Linux 12.04.2, Kernel 3.0.35. The operating system is stored on the module's flash and executes the code on the processor chip.

The module provides a method to update the firmware in the module with a new version, which involves downloading a digitally-signed firmware image from the C●CURE host server to the module.

2.7 Cryptographic Key Management

The module supports the critical security parameters (CSPs) listed in Table 9 below.

Table 9 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation[21]/ Input	Output	Storage	Zeroization	Use
ECC Public Key	571-bit	Internally generated by FIPS-Approved DRBG	Output in certificate form during TLS session negotiation	Plaintext in non-volatile memory	When a new ECC key pair is generated	Establishing a TLS session
		Input in certificate form during TLS session negotiation	Never output	Plaintext in volatile memory	Deleted after session is over	
ECC Private Key	571-bit	Internally generated by FIPS-Approved DRBG	Never output	Plaintext in volatile memory	When a new ECC key pair is generated; by removing power or reboot	Establishing a TLS session

[21] The module complies with IG 7.8 Scenario 1 for symmetric key generation as well as the seed supplied to the algorithm for generating asymmetric keys.

Key	Key Type	Generation[21]/ Input	Output	Storage	Zeroization	Use
ECDSA Public key	B-571 curve	Internally generated	Output in plaintext	Plaintext in volatile memory	When a new ECDSA key pair is generated; by removing power or reboot	Signature verification
ECDSA Private key	B-571 curve	Internally generated	Never output	Plaintext in volatile memory	When a new ECDSA key pair is generated; by removing power or reboot	Signature generation
TLS Session Integrity Key	HMAC SHA-1 key	Internally generated	Never output	Plaintext in RAM for duration of the session	Deleted after session is over	Data integrity for TLS sessions
TLS Session Key	256-bit AES CBC key	Established from a shared Master Secret during TLS session negotiation	Never output	Plaintext in RAM for duration of the session	Deleted after session is over	Encrypting data exchanges during TLS sessions
Entropy Input	256-bit value	Internally generated	Never output	Plaintext in volatile memory	By removing power or reboot	Entropy material for DRBG
HMAC_DRBG 'V' Value	Internal DRBG state value	Internally generated	Never output	Plaintext in volatile memory	By removing power or reboot	Generating random numbers
HMAC_DRBG 'Key' Value	Internal DRBG state value	Internally generated	Never output	Plaintext in volatile memory	By removing power or reboot	Generating random numbers
Firmware Upgrade Key	ECDSA public key (B-571)	Externally generated and hard-coded into the module's firmware	Never output	Hard-coded into the module	Never	Firmware load test

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

The iSTAR Ultra Door Controllers perform the following self-tests at power-up:

- Firmware integrity check (using a 32-bit Cyclic Redundancy Check)
- Cryptographic Library File integrity check (using HMAC SHA-1)
- Cryptographic algorithm tests
  - AES Known Answer Test (KAT) for encrypt
  - AES KAT for decrypt
  - HMAC SHA-1 KAT
  - HMAC SHA-256 KAT
  - HMAC SHA-384 KAT

- HMAC SHA-512 KAT
- HMAC DRBG KAT
- ECC CDH KAT (as outlined in Section 5.6.2.5 of NIST SP 800-56A)
- ECDSA Pairwise Consistency Test (PCT)

Note that no independent SHA KATs are implemented. Rather, the full functionality of the SHA variants is tested by the KATs for HMAC SHA-1/256/384/512.

If one of the self-test fails, then the module will transition to a critical error state. An error message is logged in the System Log for the Crypto-Officer to review. This error state can only be cleared by rebooting or power-cycling the module.

2.8.2 Conditional Self-Tests

The iSTAR Ultra performs the following conditional self-tests:

- Continuous RNG test for the Approved DRBG
- Continuous RNG test for non-deterministic RNG
- ECDSA PCT
- EC DH Public Key Assurance Test (as outlined in Section 5.6.2.5 of NIST SP 800-56A)
- Firmware Load Test (using ECDSA signature verification with NIST-recommended curve B-571)

If the Firmware Load Test fails, the module will abort the load process and continue executing with the current firmware. If one of other the self-test fails, then the module will transition to a critical error state. An error message is logged in the System Log for the Crypto-Officer to review. This error state can only be cleared by rebooting or power-cycling the module.

2.8.3 Critical Functions Tests

The module implements four critical functions tests that support the Approved DRBG (as specified in NIST SP 800-90A):

- DRBG Instantiate
- DRBG Generate
- DRBG Reseed
- DRBG Uninstantiate

If any one of these self-test fails, then the module will transition to a critical error state. This error state can only be cleared by rebooting or power-cycling the module.

Additionally, the module performs the following tests on the entropy it generates:

- Monobits Test
- Runs Test

If the entropy tests are passed, then the generated entropy will be used to seed the DRBG. If they are failed, then the entropy value will not be used. Any associated key generation process will abort, and the operator will be notified of the key generation failure via the status output interface.

2.9 Mitigation of Other Attacks

The module also provides mitigation for the following attack(s):

- Tampering – In addition to the tamper-evident labels that secure the module, each enclosure also includes a tamper switch attached to each door/removable cover. The switch is wired to the controller’s Main Processing Board via the special purpose “tamper detect” input.

The tamper input activates when the controller enclosure is opened or removed from its mounting surface. Upon activation, notice of a controller tamper violation is reported to the C●CURE host server. Switch action can be configured to take additional actions. Please refer to the C●*CURE 9000 Hardware Configuration Guide* for more information.

- Denial-of-Service (DoS) – The module's firmware includes protection against DoS attacks. The module employs a proprietary algorithm that prevents it from processing access control requests during a DoS attack.

3 Secure Operation

The iSTAR Ultra Door Controllers meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Crypto Officer Guidance

The Crypto Officer must ensure that the module is properly mounted, and that the power and Ethernet cables are properly connected. All installation activities not performed by the Crypto Officer (including the removal of punch-out hole fillers from the wall-mount models and the securing of punch-out holes after connections are made) must be performed by a certified professional under the direct supervision of the Crypto Officer.

Before the iSTAR Ultra Door Controllers are installed, the following must be performed:

- Check equipment (hardware, software, power supply, and wiring). Verify that the contents of the shipped boxes match the packing lists. Contact Software House if any items are missing or damaged.
- Check power, wiring, equipment clearances, and code compliance at the site.
- Ensure proper tools for mounting and wiring the iSTAR Ultra Door Controllers are available.

The wall-mount models of the module do not include wall-mounting hardware for installation. Mounting hardware depends upon the site and must be approved by a Structural Engineer or other certified professional. Software House recommends anchoring systems to a structure capable of sustaining a 75 lb. (34.1 kg) load. The wall-mount models of the module will need to be mounted and the power and Ethernet connections made before the tamper-evident labels are applied.

All installation activities not performed directly by the Crypto Officer (including the removal of punch-out hole fillers from the wall-mount models) must be performed under the Crypto Officer's direct supervision. Additionally, the Crypto Officer shall ensure that only those fillers covering punch-out holes that are necessary to fully cable the module shall be removed; all other fillers shall be left in place and intact.

3.1.1 Initialization

The Crypto Officer is responsible for initialization and security-relevant configuration and management activities for the module through the management interfaces. Initialization and configuration instructions for the module can also be found in the appropriate Installation and Configuration Guide.

The Crypto Officer must follow these steps to ensure that the module is operating in its Approved mode:

1. Set the Encryption Switch for FIPS-Approved encryption
2. Secure the enclosure door/cover
3. Enable Approved mode of operation
4. Verify Approved mode of operation

All of these steps are required by this policy, and the module is considered to be in its Approved mode of operation only after these steps are successfully completed. Any operation of the module without performing these steps is outside the scope of this policy.

3.1.1.1 Setting the Encryption Switch for FIPS-Approved Encryption

The iSTAR Ultra GCM board includes an Encryption Switch (S1-1) that enables the use of 256-bit AES encryption. This switch setting must match the software configuration of the module (and the cluster). For Approved mode of operation, this switch must be set to the ON position.

3.1.1.2 Securing the Enclosure Door/Cover

The Crypto Officer must first ensure that the module's physical security mechanisms are in place before operation. This includes the locking of the wall-mount enclosure door and the application of tamper-evident labels. All physical security mechanisms shall be installed for the module to operate in its FIPS-Approved mode of operation.

To mitigate visual access of internal components, the module enclosures provide the necessary level of opacity without any additional baffles or operator-applied mechanisms. For the wall-mount enclosures, once the module is are fully installed, the cabling will provide additional opacity. Note that during installation of the wall-mount enclosure, only those fillers covering punch-out holes that are necessary to fully cable the module shall be removed.

The module ships with fourteen (14) serialized tamper-evident labels. The steps below provide instructions for applying the tamper-evident labels to the module's enclosure. When applying labels, the Crypto Officer shall do the following:

- Ensure the system is unplugged and the enclosure door is locked (or cover is closed).
- Clean the label placement locations with 99% isopropyl alcohol solution and dry with a clean cloth.
- Allow a minimum of 24 hours for the labels to cure.

Wall-mount enclosure – The module's wall-mount enclosure is a hard metal enclosure that includes a door with a locking mechanism and a tamper-response switch. The Crypto Officer shall apply two (2) tamper-evident labels to the module door such that each label is affixed to both the door and the enclosure along the top and bottom of the door (see Figure 3). The Crypto Officer must ensure that the tamper-evident labels are affixed to the bare metal, and do not adhere to any other labels, stickers, or seals on the enclosure.

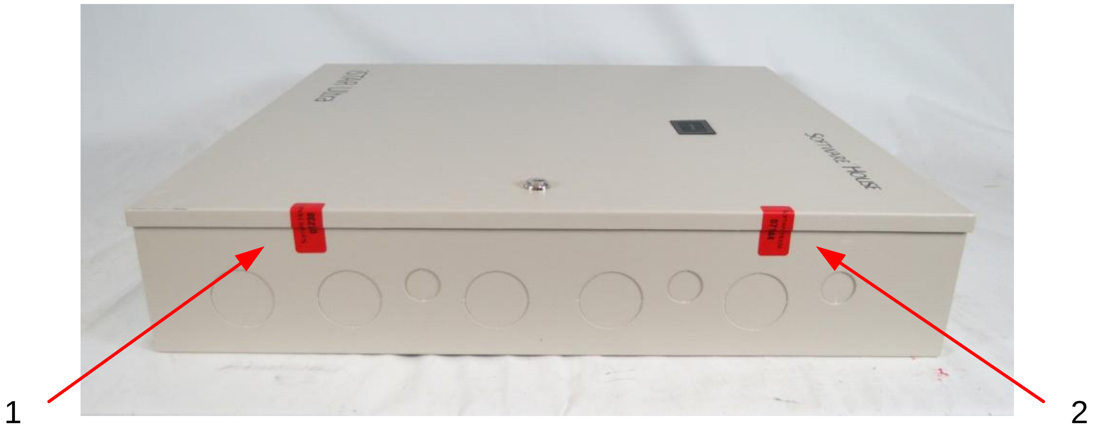


Figure 3 – Tamper-Evident Label Placement (Wall-Mount Enclosure)

Rack-mount enclosure – The module's rack-mount enclosure is a hard metal enclosure with a tamper-response switch. The rack-mount unit also has a removable back panel. The Crypto Officer shall apply two (2) tamper-evident labels to the module's removable back panel such that each label is affixed to both the enclosure chassis and its back panel (see Figure 4 below). Ensure that the tamper-evident labels are affixed to the bare metal, and do not adhere to any other labels, stickers, or seals on the enclosure.

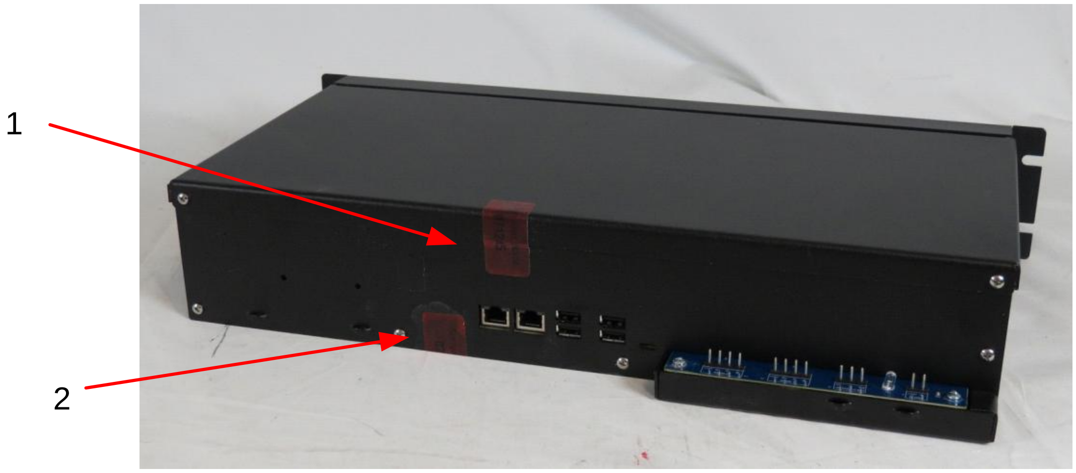


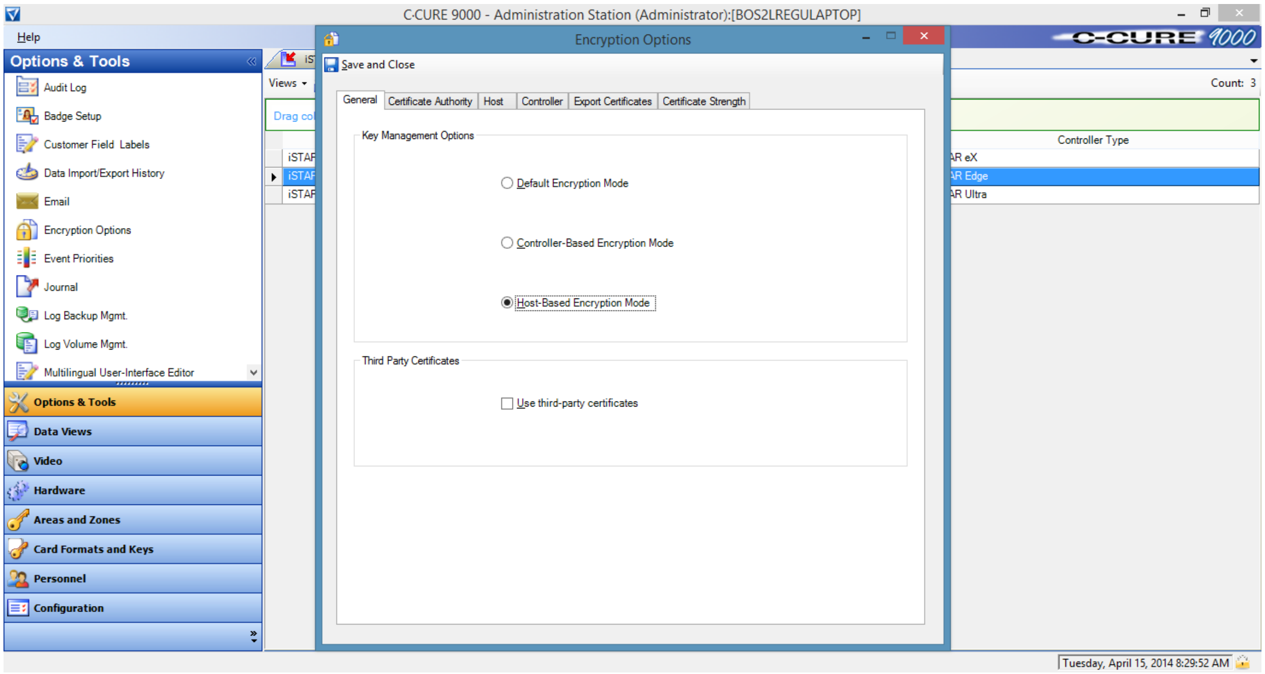
Figure 4 – Tamper-Evident Label Placement (Rack-Mount Enclosure)

Log the serial numbers of the applied labels. Once properly sealed, any attempts to tamper with the module will leave visible evidence in the form of label residue or physical damage to the enclosure. After the physical security mechanisms are placed as instructed above, the module can be powered up, and the Crypto Officer may proceed with initial configuration.

3.1.1.3 Enabling Approved Mode of Operation

To enable the Approved mode, the CO must accomplish three tasks: enable the custom key management mode, set the certificate strength, and enable the Approved mode of operation. The required setup procedures can be performed from either the C●CURE or the ICU management tool.

1. Enable the custom key management mode.
    a. On the C*CURE server, navigate to the "iSTAR Controller" tab. This will display a list of all managed controllers.
    b. Select the desired controller, and then click "Hardware". This will display the iSTAR Cluster Hardware Tree.
    c. Select the desired controller from the list.
    d. Click "Options & Tools", and then select "Encryption Options" from the Options & Tools list. This will display the **Encryption Options** window.
    e. Under the "General" tab, select either **Controller-Based Encryption Mode** or **Host-Based Encryption Mode** as the key management option (see Figure 5 below).
2. Set the encryption method's certificate strength to a FIPS-Approved method.
    a. Under the "Certificate Strength" tab, select **ECC** as the encryption method (see Figure 6 below). This will regenerate all certificates in the cluster using the selected method.
    b. Click "Save and Close" on the **Encryption Options** screen. This will close the screen and again display the list of controllers in the cluster.
3. Enable the Approved mode of operation for the controller (this is done at the cluster level).
    a. Select and enable the desired cluster (see Figure 7 below).
    b. Under the "Encryption" tab, select **FIPS 140-2 Validate mode**. All on-line controllers in the selected cluster will reboot in the Approved mode and reconnect back to the host server.



Key Management Options

○ Default Encryption Mode

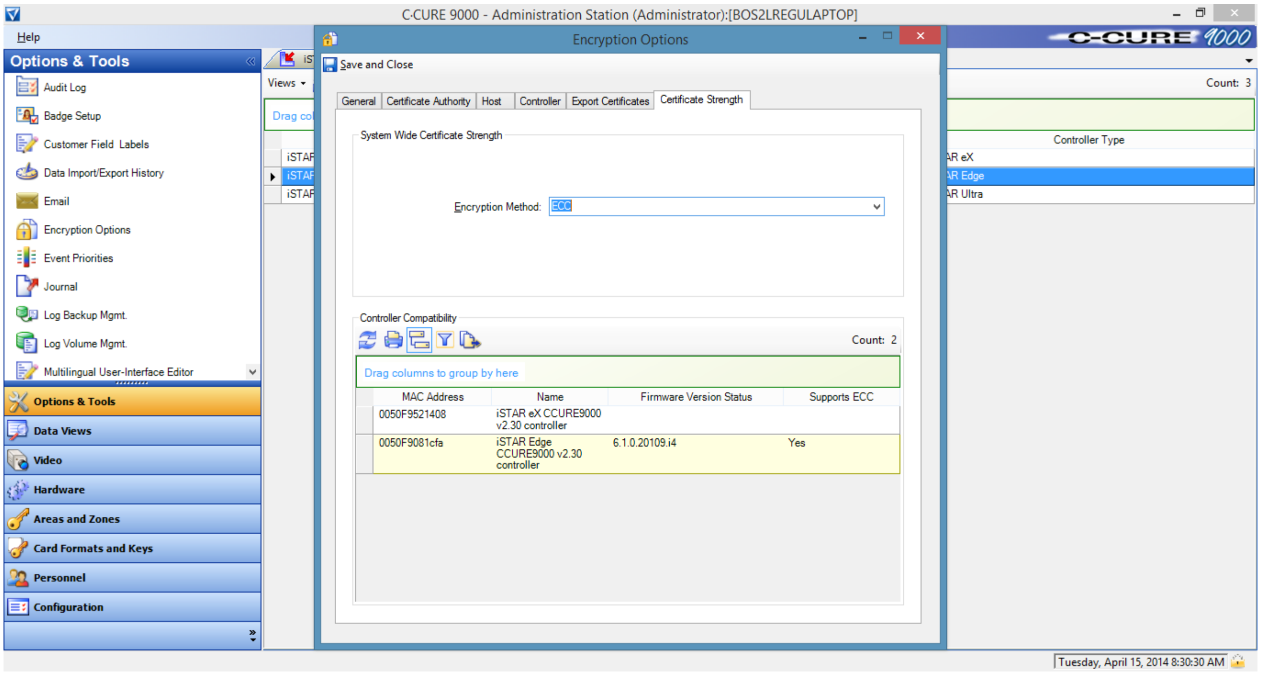
○ Controller-Based Encryption Mode

● Host-Based Encryption Mode

Third Party Certificates

□ Use third-party certificates

Figure 5 – "Encryption Options => General" Tab



System Wide Certificate Strength

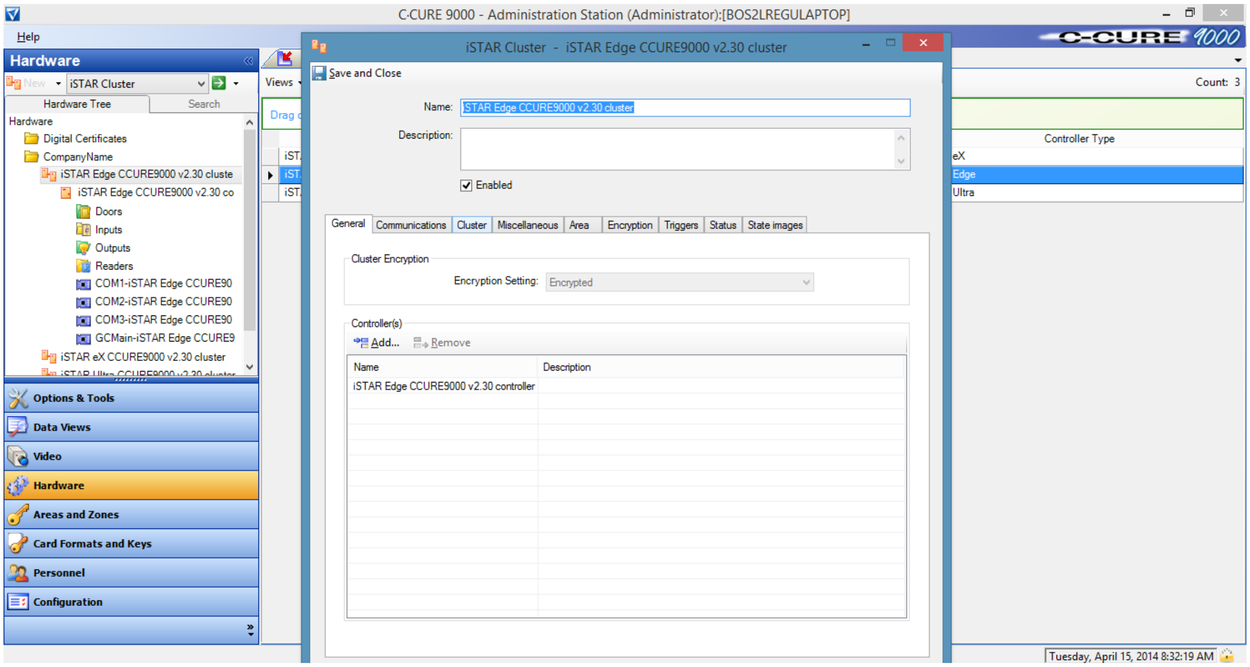
Encryption Method: ECC

Controller Compatibility

Count: 2

MAC Address	Name	Firmware Version Status	Supports ECC
0050F9521408	iSTAR eX CCURE9000 v2.30 controller		
0050F9081cfa	iSTAR Edge CCURE9000 v2.30 controller	6.1.0.20109.i4	Yes

Figure 6 – "Encryption Options => Certificate Strength" Tab



Name: iSTAR Edge CCURE9000 v2.30 cluster

Description:

☑ Enabled

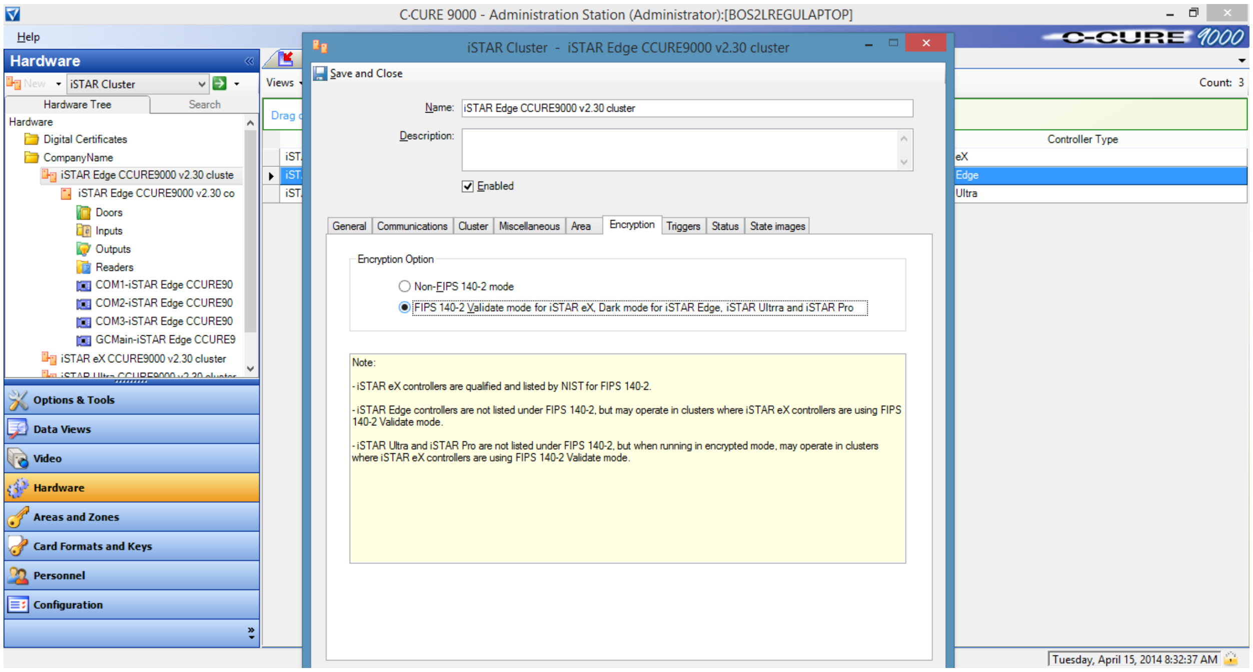
Cluster Encryption

Encryption Setting: Encrypted

Controller(s)

Name	Description
iSTAR Edge CCURE9000 v2.30 controller	

Figure 7 – "iSTAR Cluster" Screen



Name: iSTAR Edge CCURE9000 v2.30 cluster

Description:

☑ Enabled

Encryption Option

○ Non-FIPS 140-2 mode

● FIPS 140-2 Validate mode for iSTAR eX, Dark mode for iSTAR Edge, iSTAR Ultrra and iSTAR Pro

Note:

- iSTAR eX controllers are qualified and listed by NIST for FIPS 140-2.

- iSTAR Edge controllers are not listed under FIPS 140-2, but may operate in clusters where iSTAR eX controllers are using FIPS 140-2 Validate mode.

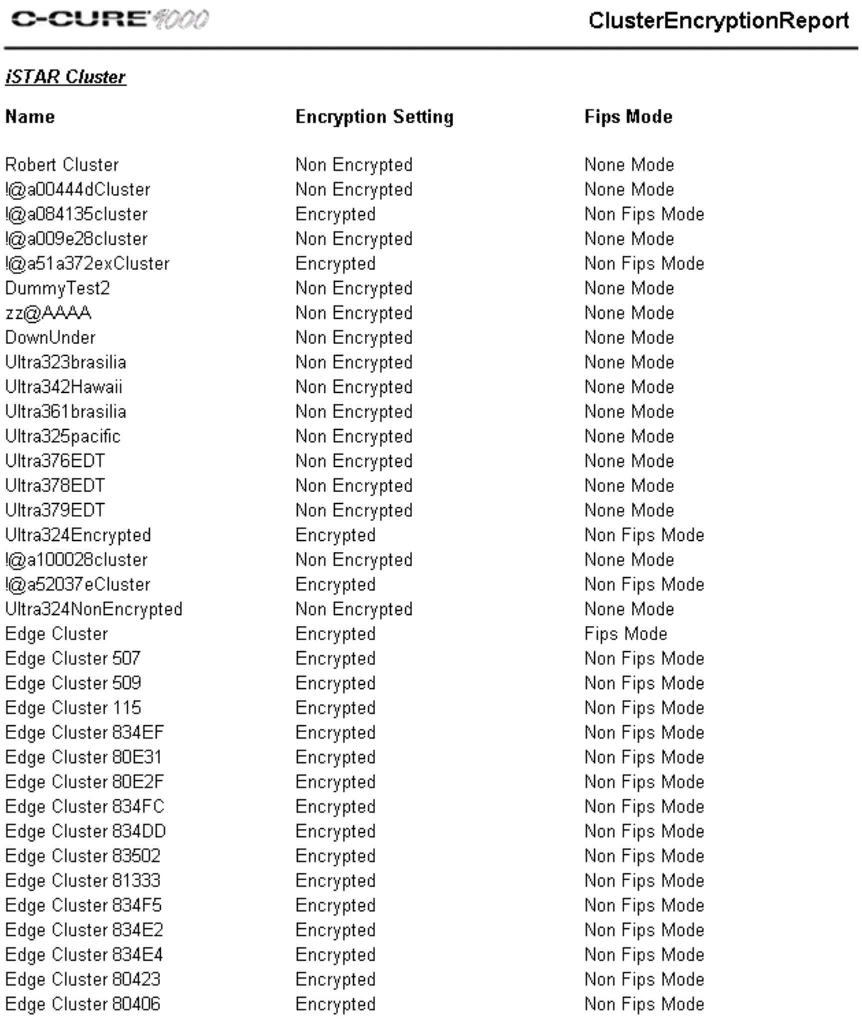
- iSTAR Ultra and iSTAR Pro are not listed under FIPS 140-2, but when running in encrypted mode, may operate in clusters where iSTAR eX controllers are using FIPS 140-2 Validate mode.

Figure 8 – "iSTAR Cluster => Encryption" Tab

Refer to the appropriate Installation and Configuration Guide for details on creating the required certificates.

3.1.1.4 Verifying Approved Mode of Operation

To determine if the module is operating in its Approved mode, navigate to **Report** => **Hardware** => **iSTAR Cluster** in the C●CURE host server, and a Cluster Encryption Report will be generated (see Figure 9 below).



C-CURE 9000 ClusterEncryptionReport

iSTAR Cluster

Name	Encryption Setting	Fips Mode
Robert Cluster	Non Encrypted	None Mode
!@a00444dCluster	Non Encrypted	None Mode
!@a084135cluster	Encrypted	Non Fips Mode
!@a009e28cluster	Non Encrypted	None Mode
!@a51a372exCluster	Encrypted	Non Fips Mode
DummyTest2	Non Encrypted	None Mode
zz@AAAA	Non Encrypted	None Mode
DownUnder	Non Encrypted	None Mode
Ultra323brasilia	Non Encrypted	None Mode
Ultra342Hawaii	Non Encrypted	None Mode
Ultra361brasilia	Non Encrypted	None Mode
Ultra325pacific	Non Encrypted	None Mode
Ultra376EDT	Non Encrypted	None Mode
Ultra378EDT	Non Encrypted	None Mode
Ultra379EDT	Non Encrypted	None Mode
Ultra324Encrypted	Encrypted	Non Fips Mode
!@a100028cluster	Non Encrypted	None Mode
!@a52037eCluster	Encrypted	Non Fips Mode
Ultra324NonEncrypted	Non Encrypted	None Mode
Edge Cluster	Encrypted	Fips Mode
Edge Cluster 507	Encrypted	Non Fips Mode
Edge Cluster 509	Encrypted	Non Fips Mode
Edge Cluster 115	Encrypted	Non Fips Mode
Edge Cluster 834EF	Encrypted	Non Fips Mode
Edge Cluster 80E31	Encrypted	Non Fips Mode
Edge Cluster 80E2F	Encrypted	Non Fips Mode
Edge Cluster 834FC	Encrypted	Non Fips Mode
Edge Cluster 834DD	Encrypted	Non Fips Mode
Edge Cluster 83502	Encrypted	Non Fips Mode
Edge Cluster 81333	Encrypted	Non Fips Mode
Edge Cluster 834F5	Encrypted	Non Fips Mode
Edge Cluster 834E2	Encrypted	Non Fips Mode
Edge Cluster 834E4	Encrypted	Non Fips Mode
Edge Cluster 80423	Encrypted	Non Fips Mode
Edge Cluster 80406	Encrypted	Non Fips Mode

Figure 9 – FIPS Mode Report

There is a **Fips Mode** column in the generated report which will indicate in what mode the cluster is running (note that every controller in the cluster will be in that mode). The following mode indicators are used:

- **"Fips Mode"** – each controller in the cluster is using Approved encryption. The Encryption Switch (S1-Position 1) is in the ON position.
- **"Non-Fips Mode"** – each controller in the cluster is using non-Approved encryption. The Encryption Switch (S1-Position 1) is in the ON position.
- **"None Mode"** – each controller in the cluster is not using any encryption. The Encryption Switch (S1-Position 1) is in the OFF position.

The CO must ensure that the Encryption Switch is set to the appropriate position as described above, and that the module's cluster is set to **Fips Mode**.

3.1.2 Management

Management of the iSTAR Ultra Door Controllers is handled through the C●CURE host server and the ICU. The ICU is a diagnostic tool for setting parameters on the iSTAR Ultra, including the device IP address and host IP address. The ICU, however, is disabled when the module is running in its Approved mode of operation, so all management must be accomplished via the C●CURE host server while in the Approved mode.

The C●CURE host server is the access control system. The C●CURE host server is used to set up the rules governing access and actions. Those rules are then downloaded as a database file to the iSTAR Ultra so it can make its own decisions.

The CO shall ensure that the module is installed, initialized, and configured to operate in its tested and Approved manner. Once properly setup, the Crypto Officer shall ensure that the module remains in its tested and Approved configuration. Operation of the module using any other configuration is outside of the scope of this Security Policy. If any irregular activity is noticed or the module is consistently reporting errors, then Software House Customer Service should be contacted.

3.1.3 Physical Inspection

The Crypto Officer shall check the module on a monthly basis for evidence of tampering (including unusual dents, scrapes, removal of additional punch-out hole fillers, or damage to the tamper-evident labels or enclosure) and to verify that the tamper-evident labels still have the proper serial numbers.

Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO shall also be responsible for the following tasks:

- Securing and having control at all times of any unused labels
- Direct control and observation of any changes to the module where the tamper-evident labels are removed or installed to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO shall perform the periodic inspections at intervals specified per end-user policy. If evidence of tampering is found during periodic inspection, the Crypto Officer shall zeroize the keys and re-initialize the module before bringing it back into operation.

To request additional labels, the Crypto Officer must contact the local authorized Software House integrator. The Crypto Officer must be sure to include contact information and the shipping address, as well as the appliance serial number, shipping address, and label part number (STAR-FIPS-LBLS).

3.1.4 Zeroization

To zeroize keys, the module operator must reboot or power-cycle the module. Keys are also automatically be zeroized in the event of power loss or battery failure.

Additionally, the TLS Session Key is a temporary key and is automatically zeroized after the TLS session is terminated. The module's ECC Public and Private Keys are overwritten when a new key pair is generated.

3.1.5 Battery Replacement

Backup power is provided to the wall-mount models of the module via four on-board non-rechargeable alkaline AA batteries. To replace the batteries:

- Zeroize all keys by power down the module.
- Remove tamper-evident labels, being sure to clean any residue left as a result of removal.
- Open the enclosure door.

- Remove the old batteries and replace with fresh batteries.
- Re-accomplish all initialization steps as described in section 3.1.1.

3.2 User Guidance

The User is a cluster member that shares access data with other instances of the module over a secure connection. This role has no ability to affect the configuration or security parameters of the module.

3.3 Non-Approved Mode of Operation

When installed, initialized, and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

4 Acronyms

Table 10 provides definitions for the acronyms used in this document.

Table 10 – Acronyms

Acronyn	Description
AC	Alternating Current
ACM	Access Control Module
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSEC	Communications Security Establishment
CSP	Critical Security Parameter
CVL	Component Validation Listing
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FAI	Fire Alarm Interface
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GCM	General Control Module
HMAC	Keyed-Hash Message Authentication Code
I/O	Input / Output
ICU	iSTAR Configuration Utility
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LCD	Liquid Crystal Display

Acronyn	Description
LED	Light-Emitting Diode
MB	Megabyte
NC	Normally Closed
NIST	National Institute of Standards and Technology
NO	Normally Open
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PCT	Pairwise Consistency Test
PoE	Power Over Ethernet
RAM	Random Access Memory
RM	Reader Module
RNG	Random Number Generator
SD	Secure Digital
SHA	Secure Hash Algorithm
SP	Special Publication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus