C•CURE 9000 and iSTAR
Cybersecurity Overview
White Paper
C•CURE 9000 v2.5
iSTAR v6.4
Proactively Monitoring and Managing Cybersecurity Risks

Not all security manufacturers' cyber security programs are equal because not all engineering teams are equal. Our autonomous Cyber Protection Team, an independent branch of Tyco Security Products development group, has deep process control knowledge and specialized expertise in cyber concerns with physical security systems. With the authority and responsibility of managing the Cyber Protection Program, the team uses best practices to monitor compliance:

Secure Product Development Practices
With secure coding and testing backgrounds, our highly trained engineers minimize the possibility of inadvertently introducing vulnerabilities during product development.

Inclusive Protection of Components and Systems
Our holistic approach includes the ability to secure systems with a range of capabilities to complement diverse security needs. For example, a C∙CURE 9000 and iSTAR access control system can be configured to support some of the most stringent controls necessary for secure network communication.

Configuration Guidelines for Compliance
We provide comprehensive guidelines on how to configure C∙CURE 9000, VideoEdge and victor systems to assist customers in complying with their identified regulatory requirements.

Testing Procedures
The Cyber Protection Team employs rigorous, continuous testing, both internally and with an independent test house, to minimize the risk of introducing new vulnerabilities to software updates and new configurations of our cyber program-compliant products.

Rapid Response to Vulnerabilities
When a vulnerability is announced, the team quickly assesses the situation, distributes an advisory bulletin, and follows up with fully qualified patches.

Education and Advocacy
In addition to maintaining critical training and development certifications, our Cyber Protection Team travels the world, speaking and advocating for the rigorous protection of all security systems.
Executive Summary

Software House C•CURE 9000 and iSTAR controllers are some of the most versatile and secure products produced by Tyco Security Products. They have been widely adopted by government and critical infrastructure sites as well as financial, medical, and educational facilities and have undergone multiple certifications and security audits.

When in FIPS-approved (or “dark”) mode, the iSTAR controllers disable all access except direct communications from C•CURE 9000. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has achieved FIPS 140-2 and FIPS 197 validation.

Both C•CURE 9000 and the iSTAR controllers are developed under a Secure Development Life Cycle that includes secure coding techniques, strict source code control, regular vulnerability and penetration testing, and vulnerability management. When vulnerabilities are discovered after deployment, the cross-functional Cyber-Response team can provide a response within 24 hours.

C•CURE 9000 and the iSTAR controllers offer a secure platform that can be customized to meet the security policies of almost any installation and are backed by a dedicated support team to address vulnerabilities and other security issues as they arise. This document serves to answer many frequently asked cybersecurity questions and to identify key security features available in C•CURE 9000 and the iSTAR controllers. If additional questions or issues arise, please contact your Software House representative or myself.

William L Brown Jr. / Sr. Engineering Manager / Regulatory and Product Security / willbrown@tycoint.com
Contents

C•CURE 9000 .......................................................................................................................... 5
   Enterprise Architecture ........................................................................................................ 5
   Microsoft® Windows® Operating System ........................................................................... 6
   Windows Updates .................................................................................................................. 6
   Anti-Virus / Anti-Malware Recommendations .................................................................. 7
   Failover ................................................................................................................................. 7
   Database Backup .................................................................................................................. 8
   Authentication ...................................................................................................................... 9
   Separation of Responsibilities ......................................................................................... 9

iSTAR.................................................................................................................................... 11
   Operating System ............................................................................................................... 11
   Windows CE ....................................................................................................................... 12
   Ubuntu Linux ..................................................................................................................... 12
   iSTAR Logical Access Control ......................................................................................... 14
   Tamper Detection ............................................................................................................... 15
   Firmware Updates ............................................................................................................ 15
   Database Theft Protection (CPNI Mode) ........................................................................... 15
   Personnel and Configuration Updates ............................................................................. 16
   Denial of Service Protection .............................................................................................. 16
   SNMP (Simple Network Management Protocol) ................................................................ 17

System Communication Protection - Encryption .................................................................... 18

Patch and Update Schedule ................................................................................................. 19
   Security Assessment – Tyco Software ............................................................................... 20
   Reporting a Vulnerability .................................................................................................. 20
   Security Assessment – Third Party Software ................................................................... 21
   Life Safety and Security Exemptions ................................................................................. 21

Security Approvals and Certifications .................................................................................. 22
   FISMA ................................................................................................................................. 22
   NERC CIP v5 ...................................................................................................................... 22
   FICAM FIPS-201 ............................................................................................................... 23
   FIPS 140-2 .......................................................................................................................... 23
   FIPS 197 ............................................................................................................................ 24

C•CURE 9000 Services ........................................................................................................... 25

C•CURE 9000 Permissions ...................................................................................................... 28
   SQL .................................................................................................................................... 28
   Tyco Directory .................................................................................................................... 28

APPENDIX – Resources and References ................................................................................ 30
   Tyco Documents .............................................................................................................. 30
   Laws and Regulations ...................................................................................................... 30
   FIPS Publications ............................................................................................................ 30
   NIST Publications .......................................................................................................... 30
C•CURE 9000

C•CURE 9000 is a flexible, object-oriented security and event management system that features a variety of customizable interfaces for maintaining the system and for monitoring the sites that the user wants to secure. C•CURE 9000 provides extensive information management capability using Microsoft SQL Server and Microsoft .NET Framework V4.5. With its distributed client-server architecture, C•CURE 9000 is capable of supporting a large array of clients, controllers, and input devices, including various card readers and cameras.

Enterprise Architecture

C•CURE 9000 Enterprise Architecture is a licensable option that allows the user to configure multiple C•CURE 9000 servers to communicate with a Master Application Server (MAS). The MAS provides a platform for global management of personnel, video, and access security objects on two or more Satellite Application Servers (SAS).

This architecture provides the capability for central monitoring and reporting for the entire enterprise. Global data such as personnel records, clearances, and operators is located on the MAS and is synchronized to each SAS. The MAS does not have direct connection to controllers or video servers but can be used to remotely monitor and manage devices connected to a SAS within the enterprise. A C•CURE 9000 installation connected to the MAS can view events, activities, and the status on every SAS in the
enterprise, while local installations can connect to a SAS will have visibility only to devices connected to that server.

Microsoft® Windows® Operating System

The licensed capabilities of C•CURE 9000 correspond to the specific version of the Windows operating system on which the software is installed. As the host environment, Windows provides the underlying foundation for configuring a secure C•CURE 9000 system. Tools such as Microsoft Security Configuration Manager, Security Compliance Manager and Windows domain policies can be used to optimize the system's security. Additionally, the roles and responsibilities assigned to each C•CURE 9000 user are dependent on the specific Windows operator. This allows the user credentials and access to the system to be controlled through Windows Active Directory®.

Windows Updates

To date, the Software House Technical Support and Quality Assurance teams have not reported any conflicts or issues with C•CURE 9000 and Microsoft Windows Service Packs and security updates.

Software House is a Microsoft Certified Gold Partner. Qualification of all C•CURE 9000 releases, including service packs and critical updates, is performed using the latest Microsoft Windows Service Packs and security updates. Software House Technical Support can identify when new updates and patches are approved.

We recommend that Microsoft Windows updates be applied and kept current. However, we also recommend that the system is configured to require a manual restart of the server to prevent automatic shut down during use.
Anti-Virus / Anti-Malware Recommendations

We recommend that third-party Anti-Virus / Anti-Malware software apply the following exclusions for the C•CURE 9000 application server.

- The complete Tyco directory (i.e. C:\Program Files (x86)\Tyco)
- The Microsoft SQL Server directory (i.e. C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA)

These directory exclusions will help prevent a conflict while C•CURE 9000 is attempting to read or write a file.

No directory exclusions are necessary for C•CURE 9000 Client workstations.

Because C•CURE 9000 systems are critical to operation, it is also important to disable any ability to force a restart of the C•CURE 9000 server or client workstations.

Failover

Stratus Technologies’ everRun® fault tolerant redundancy solutions deliver a fault tolerant solution that requires limited or zero downtime. The solution supports symmetric multiprocessing and multi-core environments offering affordable, continuous security solutions for businesses during component system failures. Stratus Technologies’ everRun Enterprise and Express, and SplitSite provide a high availability, fault tolerant solution for C•CURE 9000 systems. Stratus’ everRun platforms offer additional reliability to C•CURE access control systems. While some redundancy platforms run on a recovery-based model in the event of failures, everRun platforms utilize a new preventive-based model which offers the ability to continue to compute through failures. everRun Snapshots provide information rollback of the C•CURE database at a single point in time to assist with the recovery of data loss or system corruption.

everRun Enterprise and Express combine the physical resources of two standard Windows servers into a single, unified operating environment. This provides complete redundancy of all underlying data and hardware. By keeping the operating environment
in the single, unified system, applications will be kept up and running in the event of a system or component failure. everRun Enterprise provides a full, level-3 fault tolerant system with no restarts for continuous operation. everRun Express provides a component, level-2 fault tolerant system with failover restart in seconds to minutes for minimal downtime.

Database Backup

C•CURE 9000 uses three databases that can be backed up at any time using the System Backup feature.

- The Core database is a core component of the management platform upon which C•CURE 9000 is built. It is the central repository for configuration details describing objects created, monitored, and maintained in C•CURE 9000.
- The Audit Log provides a history of changes to configurations managed by C•CURE 9000.
- The Activity Journal maintains a record of activity monitored by the system. Records in the Activity Journal provide a historical view of activity that has occurred within the system, statistical information on resource usage, and personnel and asset location information.

In the event of a system failure or corruption of the Core, Audit Log or Activity Journal database, one or more of these databases can be restored from a backup of the respective database.

The C•CURE 9000 Server Configuration Application Guide describes the details for performing system backup and restore. User access to the System Backup feature is controlled through the user configuration.
Authentication

User authentication into C•CURE 9000 was designed for seamless deployment in an Active Directory domain environment utilizing Windows Single Sign-On (SSO).

C•CURE 9000 uses the Windows login credentials to manage permissions but does not store or have any visibility of the credentials. Password rules and policies such as predefined number of login attempts, character length, use of alphanumeric characters, and user-defined lockouts are managed by the local Microsoft Windows operating system or the domain controller.

Separation of Responsibilities

Separation of roles is easy to manage through two thick client applications: Administration Station and Monitoring Station. The Administration Station is used by security managers to customize the C•CURE 9000 functions, objects, and views of the Monitoring Station. Other roles use the Monitoring Station application to track events and monitor devices status. Depending on the configuration and operator privileges, the Monitoring Station may allow manual actions such as locking/unlocking doors and arming/disarming alarms.

C•CURE 9000 has highly configurable operator privilege functionality. Using the Privilege Editor feature, administrators can specify the objects, programs, reports, personnel, events, and actions that operators can view and use. The feature also allows for exceptions and bulk configuration.
iSTAR

The iSTAR controllers are the hardware controllers that interface with access control card readers, locks, and other physical security hardware. They may be configured into clusters with a single master controller communicating to the iSTAR host and store a local version of the access control database so they may continue to operate during a network failure.

Operating System

The iSTAR operating systems have been customized so only essential services and functionality remain. A custom image of this Just Enough Operating System (JEOS) is provided for each firmware release. Patches and updates are provided as part of the firmware update.

- iSTAR Pro: Windows CE v3.0
- iSTAR Edge and iSTAR eX: Windows CE v5.0
- iSTAR Ultra: Linux Ubuntu LTS
Windows CE

Microsoft Windows CE is a minimized version of Windows 95 designed specifically for embedded devices. The iSTAR Pro, iSTAR eX, and iSTAR Edge controllers use a customized version containing only the services and functionality needed to communicate to C•CURE 9000 and the iSTARs in the cluster and to perform its access control functions.

The firmware for these controllers includes the image of the operating system, so every firmware update resets the operating system. Additionally, the customization of the operating system prevents any remote access like telnet, SSH, or FTP and there is no ability to execute any type of script.

Because of the customization of the Windows CE operating system, it is not possible to run third-party anti-virus software on the iSTAR controllers. However, it is also not possible to install or execute any third party or malicious software on the controllers. Further, a reset of the controller, or a firmware updates, will force the controller back to its default configuration.

_Known Limitation:_ the iSTAR Edge contains logical UDP ports that are always open: 137, 138, and 1025. These ports are a legacy of the Windows CE operating system, and even with direct assistance from Microsoft; our developers have been unable to close them. However, all traffic on these ports is ignored the iSTAR firmware.

As these ports are not required for the operation of the iSTAR Edge, network firewalls may be configured to block all traffic on them.

Ubuntu Linux

The iSTAR Ultra uses a specially built version of the Linux Ubuntu 12.04 LTS operating system. We have removed all but the essential services and functionality necessary to communicate between the iSTAR Ultra and the C•CURE 9000 server. We then construct a custom image that is integrated into every firmware release, so every firmware update resets the operating system image. Additionally, the customization of
the operating system prevents any remote access like telnet, SSH, or FTP and there is no ability to remotely execute any type of script. The Ubuntu automatic package upgrade feature is turned off, and we selectively patch security and feature packages in a fully controlled fashion.

Because of the customization of Linux operating system that is used, it is not possible to run third-party anti-virus software on the iSTAR Ultra.

The iSTAR Ultra’s embedded web server was developed internally and may be disabled.

Software House does have the ability to modify all the code on the iSTAR Ultra including the Ubuntu operating system applications and libraries as well as the Linux kernel and drivers. All modifications undergo quality assurance testing as well as architecture and legal review to ensure continued performance and compliance with open source licenses and supplier agreements.
iSTAR Logical Access Control

There are three methods of communication to an iSTAR controller.

**ICU** – ICU is a program used to locate and configure the name, MAC address, IP address, host address, and static/DHCP setup of the iSTAR controllers. When an iSTAR controller is put in FIPS or “dark” mode, communication with ICU is disabled. iSTAR controllers configured with a cluster password (through C•CURE 9000) require that password to be reentered before ICU can configure the controller. All iSTAR controllers can be set for ICU block through hardware settings that prevent ICU commands from being sent to the controller.

*Known Limitation:* There is currently no method to log failed login attempts through ICU or with the cluster password.

**Diagnostic Web Page** – The diagnostic web page is used when troubleshooting the iSTAR controller. The web server is password-protected which is configured through a system variable in C•CURE 9000. The server may also be disabled either through C•CURE 9000 system variables or by placing the iSTAR into FIPS or “dark” mode.

*Known Limitation:* There is currently no method to log failed login attempts to the diagnostic webpage.

**C•CURE 9000** – C•CURE 9000 is the normal method of communication to iSTAR controllers. Authentication and authorization for C•CURE 9000 is managed through the Microsoft Windows credentials and may be configured with Microsoft Active Directory. iSTAR controllers can only connect to one C•CURE 9000 host and will prompt an alert if connected to multiple hosts.
Tamper Detection

All iSTAR controllers include tamper detection that will prompt an alarm if the enclosure has been opened. The iSTAR Ultra includes an optional installation of a back tamper that can detect if the controller is removed from the wall.

Firmware Updates

Firmware updates are performed from the Monitoring Station by user with the correct permissions, or from a separate utility called ICU. The firmware is downloaded to the controller, which will continue to operate during the download process. When the controller receives the proper checksum, which validates the firmware, the controller will need to reboot. After a successful reboot when communication to the server is restored, the C•CURE 9000 server will download the latest database to the controller.

Firmware updates to the iSTAR controllers are available on the Software House Support website: www.swhouse.com/Support

The site also contains the release notes that detail the changes made to the firmware, including security updates.

Database Theft Protection (CPNI Mode)

Activating the CPNI mode on the iSTAR Ultra will prevent the database from being stored in persistent memory. In this mode, if power is removed from the controller, the database is erased.
Personnel and Configuration Updates

When a controller is first placed online, the C•CURE 9000 server will perform a fast personnel download and will send the configuration to the controller. The fast personnel download uses a single file with the personnel data and access privileges for all doors associated with that controller. The configuration data includes the iSTAR configuration and events. Any additional incremental system changes with respect to cardholder or hardware configurations are downloaded in real-time. Major personnel changes implemented at the server will cause the system to perform a fast personnel download to the controllers that are affected.

Denial of Service Protection

The iSTAR controllers provide Denial of Service Protection. When unusual network traffic targeting iSTAR is detected, the controller temporarily disables the network ports. After a period of time, the ports will reopen, but if the unusual traffic is still present, it will repeat the process, going offline for a longer period of time. During this time, the iSTAR continues to perform it access control functions.

When an iSTAR goes into hiding due to detecting a denial of service attempt, C•CURE 9000 will alert the monitoring station with a “Network Storm Detected” alert.
SNMP (Simple Network Management Protocol)

iSTAR controllers are provided with SNMP enabled by default. For the iSTAR Ultra, the SNMP statistics are required to support the Denial of Service protection and cannot be disabled. However, for security purposes, the libraries are read-only and only contain the name of the controller.

All other iSTARs can have SNMP configured (or disabled) through the ICU configuration.
The Crossfire service manages communication between the C•CURE 9000 server and the iSTAR controllers, database, and client devices. By default, the Crossfire service uses AES-256 encryption that has been FIPS 197 validated.

In standard mode, the iSTAR ex, iSTAR Edge and iSTAR Ultra use FIPS 197 validated AES 265 encryption to securely communicate with the host and other cluster members. In FIPS mode, these controllers uses TLS to authenticate to the C•CURE 9000 host server. The system can use third party Certificate Authority (CA) certificates, or one of the following two options can be used to generate a certificate:

- **Controller-based Encryption Mode** – C•CURE 9000 creates the host server and CA certificates at the C•CURE 9000 host computer and then directs the controller to generate new public and private keys.
- **Host-based Encryption Mode** – C•CURE 9000 creates the host, controller, and CA certificates on the host computer and then sends the controller’s public and private keys and CA certificate to the controller.

The default asymmetric encryption is RSA 1024, but it may be changed to ECC 571 at the cluster level. The symmetric key will remain AES 256.

**Known Limitation:** By default, the iSTAR Pro communication is unencrypted. There is an optional setting to use RC4 128-bit symmetric encryption. The iSTAR Pro is not FIPS 140-2 validated and does not have a FIPS or “dark” mode.
Patch and Update Schedule

The policy documented herein sets forth the current internal operating guidelines and process for Tyco Security Products, which may change at any time at the sole discretion of Tyco Security Products. Tyco Security Products employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy as determined by Tyco Security Products at its discretion. Regardless, Tyco Security Products endeavors to address issues that arise with our products according to the severity that they warrant.

When a critical security vulnerability is discovered, Tyco Security Products will use commercially reasonable efforts to:

- Issue a Critical Service Pack for the current version of the affected product as soon as is reasonably practicable
- Subsequently issue a Critical Service Pack for previous versions based on the back port policy listed below

When non-critical vulnerabilities are discovered, Tyco Security Products will use commercially reasonable efforts to:

- Apply fixes for high severity vulnerabilities in the next immediate release
- Apply fixes for low-medium vulnerabilities in the next major release
C•CURE 9000 and iSTAR
Cybersecurity Overview

<table>
<thead>
<tr>
<th>Product</th>
<th>Release Schedule (Approximate)</th>
<th>Back Port Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>C•CURE 9000</td>
<td>Major Release: 8 months</td>
<td>Two major releases prior to current</td>
</tr>
<tr>
<td></td>
<td>Service Pack: 3 months</td>
<td>For example: if the current version is 2.5, security updates will be provided for version 2.5, 2.4, and 2.3</td>
</tr>
<tr>
<td>iSTAR</td>
<td>Major Release: 8 months</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Patch Release: 3 months</td>
<td></td>
</tr>
</tbody>
</table>

Security Assessment – Tyco Software

Vulnerabilities discovered in Tyco proprietary software are assessed on the CVSS v2 score.

<table>
<thead>
<tr>
<th>CVSS v2 Score</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 9</td>
<td>Critical</td>
</tr>
<tr>
<td>≥ 7</td>
<td>High</td>
</tr>
<tr>
<td>&lt; 7</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Reporting a Vulnerability

If you believe you have discovered a vulnerability in C•CURE 9000 or iSTAR, contact the Software House Technical Support team. They are kept up to date with all resolved vulnerabilities and have direct access to the Cyber Protection and development teams to help assess and resolve any issues.
Security Assessment – Third Party Software

Tyco Security Products shall use commercially reasonable efforts to monitor third party and open source software included with the products listed above for disclosed vulnerabilities from the product vendors and open source communities. Vulnerabilities that are discovered and disclosed will be assessed first on their assigned CVSS v2 score from the product vendor or the National Vulnerability Database and then on the ability to be exploited within the affected product.

<table>
<thead>
<tr>
<th>CVSS v3 Score</th>
<th>Exploitability</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 9</td>
<td>Exploitable</td>
<td>Critical</td>
</tr>
<tr>
<td>≥ 9</td>
<td>Not Exploitable</td>
<td>High</td>
</tr>
<tr>
<td>≥ 7</td>
<td>Exploitable</td>
<td>High</td>
</tr>
<tr>
<td>≥ 7</td>
<td>Not Exploitable</td>
<td>Medium</td>
</tr>
<tr>
<td>&lt; 7</td>
<td>Exploitable</td>
<td>Medium</td>
</tr>
<tr>
<td>&lt; 7</td>
<td>Not Exploitable</td>
<td>Low</td>
</tr>
</tbody>
</table>

If a patch is not available to correct the vulnerability, Tyco Security Products use commercially reasonable efforts to mitigate the vulnerability within its capabilities.

Life Safety and Security Exemptions

In cases where the Life Safety or Security functionality of a product may be compromised due to a security vulnerability, the vulnerability will be treated as critical and patched accordingly.
Security Approvals and Certifications

C•CURE 9000 and iSTAR have been installed in many installations that require accreditation. Below is a list of how the Cyber Protection Program and Software House can assist in meeting the strictest requirements.

FISMA

The C•CURE 9000 and iSTAR system can be configured to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access
- Account login/logout management
- Role-based separation of capabilities, permissions, and privileges
- System event and configuration change auditing, alerting, and management
- Restriction of ports, protocols, and services to only those required
- Encrypted communications

For more information, see the C•CURE 9000 FISMA-Ready Compliance Guide.

NERC CIP v5

The C•CURE 9000 and iSTAR NERC-CIP V5 READY Compliance Guide provides an overview of the Tyco Security Products’ NERC-CIP Ready Program and describes how the C•CURE 9000 and iSTAR System may be configured to meet the requirements of the NERC-CIP v5 requirements. When used in conjunction with the C•CURE 9000 installation and configuration guides, this information should assist in the installation of a compliant system and provide the necessary information for an audit.
FICAM FIPS-201

The C•CURE 9000 and iSTAR system has been tested and certified as an end-to-end physical access control system (PACS) with high assurance readers and validation software and approved as a fully compliant FICAM Solution by the U.S. General Services Administration (GSA).

C•CURE 9000 provides a solution for HSPD-12 / FIPS-201 and 800-116 compliance for smart card credentials, along with support for PIV-I, PIV-C, TWIC and the DOD CAC credential using authentication software with its Server-based Certificate Verification Protocol (SCVP) client.

FIPS 140-2

The iSTAR Edge and Ultra controllers have been certified by the NIST CMVP as meeting the requirements of FIPS 140-2 Level 2.

As part of their FIPS 140-2 validation, the iSTAR Ultra and iSTAR Edge provide physical protection of the internal encryption module through the metal enclosure, physical tamper, and the use of tamper-evident labels.

In FIPS mode, the iSTAR controller will also disable all ports except those required for communication between the C•CURE 9000 host and other iSTAR controllers in FIPS mode. It will only accept communication from the C•CURE 9000 host and the controllers in its cluster and will disable communication to the ICU tool.

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

- iSTAR Edge: FIPS 140-2 certificate #2309
- iSTAR Ultra: FIPS 140-2 certificate #2315
FIPS 197

C•CURE 9000 and the iSTAR Controllers have been certified by the NIST CMVP as meeting the requirements of FIPS 197 AES encryption algorithm standard.


Safety Act

Tyco International PLC received Safety Act designation for Software House C•CURE 9000 and iSTAR controllers. According to the U.S. Department of Homeland Security, the Safety Act provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies - whether they are products or services. The goal of the SAFETY Act is to encourage the development and deployment of effective anti-terrorism products and services by providing liability protections. A rigorous review of the products, our development processes, documentation, training, tech support, and more is required in order to receive the designation.
C•CURE 9000 Services

Programs that are required for C•CURE 900 operation (including third party software), which are imported during prerequisites installation

### MAS
- For a machine with SQL as a remote instance, if SQL database is internal to the unit, please refer to the SQL portion in the SAS list
- For a server that has .NET Framework as a feature, not an installed program
  - ADSDK Redistributable
  - Adobe Flash Player
  - CCURE9000 Client
  - Microsoft .NET Framework 4 Multi-Targeting Pack
  - Microsoft Primary Interoperability Assemblies 2005
  - Microsoft Report Viewer 2012 Runtime
  - Microsoft Silverlight
  - Microsoft Sync Framework 2.1
  - Microsoft Sync Framework 2.1 Core Components
  - Microsoft Sync Framework 2.1 Database Providers
  - Microsoft Sync Framework 2.1 Providers Services
  - Microsoft Visual C++
    - Microsoft Visual C++ Redistributable
    - Microsoft Visual Studio
    - Visual Studio Prerequisites
- Tyco Update Repository
- victor Application Server

### SAS
- For a machine with SQL internal to the unit
- For a server that has .NET Framework as a feature, not an installed program
  - ADSDK Redistributable
  - Adobe Flash Player
CCURE9000 Client
Microsoft .NET Framework 4 Multi-Targeting Pack
Microsoft Primary Interoperability Assemblies 2005
Microsoft Report Viewer 2012 Runtime
Microsoft Silverlight
Microsoft SQL Server
  •  Microsoft SQL Server Management Objects
  •  Microsoft SQL Server Setup
  •  Microsoft SQL Server Setup Support Files
  •  Microsoft SQL Server Native Client
  •  Microsoft SQL Server Transact SQL Compiler Services
  •  Microsoft SQL Server Transact SQL ScriptDom
  •  Microsoft SQL Server Compact 4.0 SP1
  •  Microsoft SQL Server System CLR Types
  •  Microsoft VSS Writer for SQL Server
  •  SQL Server Browser for SQL Server
  •  Microsoft System CLR Types for SQL Server
Microsoft Sync Framework 2.1
  •  Microsoft Sync Framework 2.1 Core Components
  •  Microsoft Sync Framework 2.1 Database Providers
  •  Microsoft Sync Framework 2.1 Providers Services
Microsoft Visual C++
  •  Microsoft Visual C++ Redistributable
  •  Microsoft Visual Studio
  •  Visual Studio Prerequisites
Tyco Update Repository
victor Application Server
### Client

For a machine that requires .NET Framework installed as a program:

- ADSDK Redistributable
- Adobe Flash Player
- CCURE9000 Client
- CCURE9000 Web Client (if desired for web operation)
- Microsoft .NET Framework 4 Multi-Targeting Pack
- Microsoft Primary Interoperability Assemblies 2005
- Microsoft Silverlight
- Microsoft Sync Framework 2.1
  - Microsoft Sync Framework 2.1 Core Components
  - Microsoft Sync Framework 2.1 Database Providers
  - Microsoft Sync Framework 2.1 Providers Services
- Microsoft Visual C++
  - Microsoft Visual C++ Redistributable
  - Microsoft Visual Studio
  - Visual Studio Prerequisites
C•CURE 9000 Permissions

For the C•CURE 9000 server to operate properly, the following minimum privileges are required.

**SQL**

The account used to install the C•CURE 9000 software must have full rights to the four Software House databases: (ACVSCore, SWHSystem, SWHSystemAudit, SWHSystemJournal).

The account used to run the C•CURE 9000 CrossFire Framework Service needs to have these SQL rights:

- **SWHSystemAudit**
  - db_owner
- **SWHSystemJournal**:
  - db_owner - The service will rename the current ACVSJournal and create a new ACVSJournal (this may be disabled if the installation wishes to perform its own archiving)
- **ACVSCore and SWHSystem**
  - db_datareader – To read all the database tables used by C•CURE 9000
  - db_datawriter – To update, create, and delete all the database tables used by C•CURE 9000
  - db_backupoperator – To perform scheduled database backups
  - db_ddladmin – Creation and deletion of UDF fields requires modifications to the db schema
  - db_owner – For the following reasons:
    - To achieve the best performance for journal/audit sync from SAS to MAS
    - Track tables for journal/audit by deleting and recreating tables
    - Alarm acknowledgement and log message functions may not function because the db_owner role is required to create and drop objects from dbo.xfEventLog located in SWHSystemJournal

**Tyco Directory**

The Tyco directory can be modified, but it is dependent upon intended use and integrations required.
The Tyco directory is installed correctly with access to all users (and is required for proper installation), but should be downgraded after.

The subfolders and applications within the Tyco directory need to be filtered based on intended use.

The client folders are required access by all (operators/users that will use it, administrators and runtime users). The Update folders are only needed if deployed, and would only be used by administrators and runtime users. Crossfire folder only is used by administrators and runtime users.

Read, write and execute is required for these folders.
APPENDIX – Resources and References

Tyco Documents

- VideoEdge NVR Security User Guide
- VideoEdge NVR Installation and User Guide
- VideoEdge, victor, and C•CURE Port Map
- FISMA-Ready: VideoEdge System
- FISMA-Ready: victor System
- FISMA-Ready: C•CURE 9000 System
- CCURE 9000 and iSTAR NERC Compliance Guide

Laws and Regulations

- Federal Information Security Management Act of 2002
- Federal Information System Modernization Act of 2014

FIPS Publications

- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS PUB 197, Advanced Encryption Standard
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems

NIST Publications

- NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST 800-30, Risk Management Guide for Information Technology Systems
- NIST 800-34, Contingency Planning Guide for Information Technology Systems
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
- NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
- NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
- NIST 800-64, Security Considerations in the Information System Development Life Cycle
- Framework for Improving Critical Infrastructure Cybersecurity